



CALL RECORDING

Portal Administrator Quick Reference Guide

LOGIX
FIBER NETWORKS

Powered By:



Contents

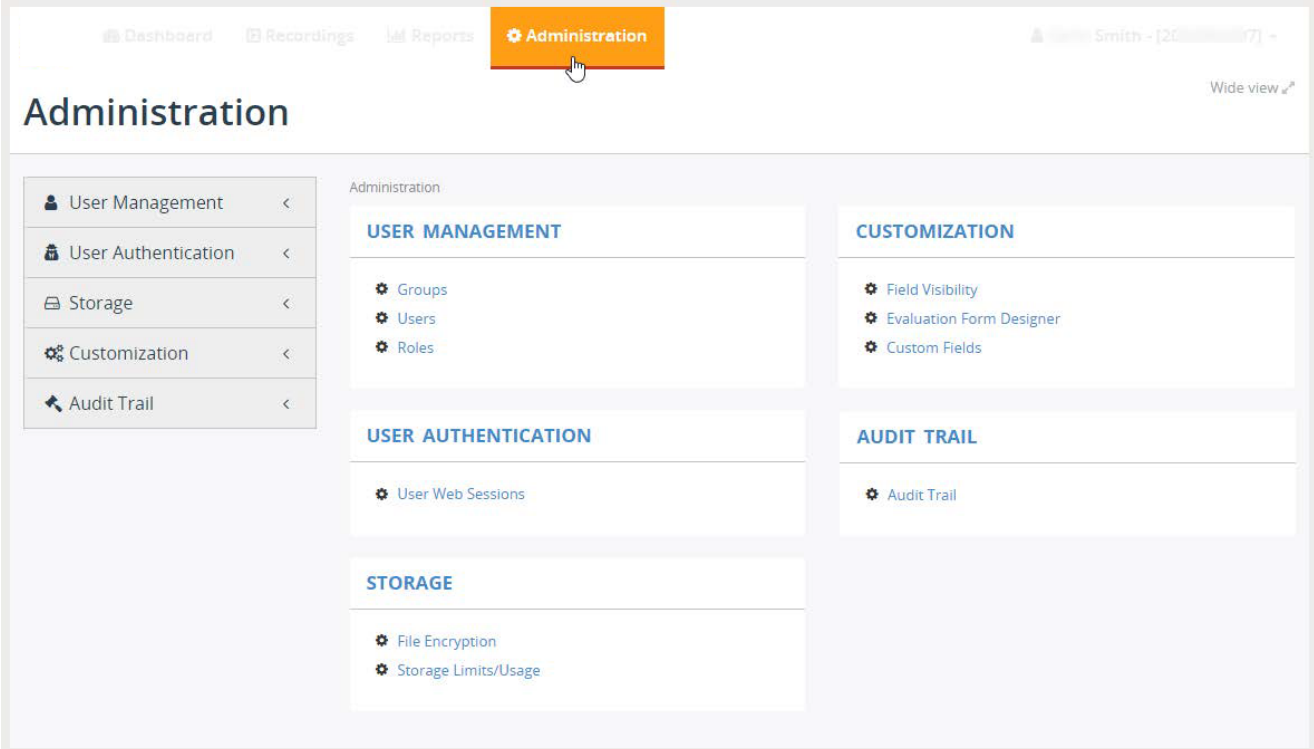
| | |
|---|----------|
| ADMINISTRATION | 4 |
| ACCESS AND PERMISSIONS | 5 |
| USER MANAGEMENT | 5 |
| <i>Roles</i> | 5 |
| List of Roles | 6 |
| Access Level / Scope | 6 |
| Permissions | 7 |
| <i>Groups</i> | 7 |
| View Group Members | 7 |
| Add a Group | 8 |
| Edit Group Settings | 9 |
| Add Users to a Group | 9 |
| <i>Users</i> | 9 |
| View List of Users | 9 |
| View User Settings | 10 |
| View User Security Settings | 11 |
| Revoke User Device Access | 11 |
| Terminate a User Web Session | 11 |
| Reset Password | 12 |
| Edit a User | 13 |
| Associating Calls with Users | 14 |
| Manage Calls That Are Not Yet Assigned to Users | 15 |
| Impersonate a User | 16 |
| STORAGE | 17 |
| <i>Storage Targets</i> | 17 |
| Search Storage Targets | 18 |
| View Storage Target Setup | 18 |
| Test a Target Connection | 18 |
| Add a Storage Target | 19 |
| Edit a Storage Target | 20 |
| Delete a Storage Target | 20 |
| <i>File Encryption</i> | 21 |
| Encryption Key Configuration | 23 |
| 1. Create New Encryption Key | 23 |
| 2. Import Encryption key | 23 |
| 3. Export Encryption Key | 24 |
| 4. Grant Access to Encryption Key | 26 |
| 5. Enable File Encryption | 27 |
| 6. Export of the Encrypted Files | 28 |
| <i>Storage Limits/Usage</i> | 28 |
| USER AUTHENTICATION | 29 |
| CUSTOMIZATION | 29 |
| <i>Field Visibility</i> | 30 |
| <i>Custom Fields</i> | 30 |
| To Add a Custom Field | 31 |
| To Edit a Custom Field | 31 |
| To Delete a Custom Field | 31 |
| <i>Evaluation Form Designer</i> | 32 |
| Add Form | 32 |

| | |
|--|----|
| AUDIT TRAIL | 33 |
| SPEECH ANALYTICS..... | 35 |
| <i>Set up Google Cloud Speech API</i> | 36 |
| A. Create a Google Cloud Platform account | 36 |
| B. Create New Project..... | 38 |
| C. Enable Google Cloud Speech API for your project | 39 |
| D. Create a Service Account Key..... | 41 |
| E. Create Google Cloud Storage Bucket..... | 43 |
| Call Recording Configuration..... | 43 |
| SCREEN RECORDING..... | 50 |
| <i>Architecture</i> | 50 |
| <i>Authorization Phase</i> | 50 |
| <i>Recording Phase</i> | 51 |
| <i>Configure Licensing</i> | 51 |
| Assign Licenses to Users..... | 51 |
| Configure Storage..... | 52 |
| <i>Configure Screen Recording Settings</i> | 53 |
| Generate Secure Token | 54 |
| Install Client Application..... | 55 |
| Verify Installation..... | 55 |
| Authorize New Workstations | 56 |
| <i>Configure Users for Screen Recording</i> | 57 |
| Step 1. Configure Screen Recording Login..... | 57 |
| Step 2. Assign Screen recording license | 57 |
| Verify Screen Recording..... | 57 |
| <i>Troubleshooting Screen Recording</i> | 59 |
| Client Side..... | 59 |
| Enable Logging for Service Application | 59 |
| Enable Logging for Desktop Capturing Process..... | 60 |
| Server Side..... | 60 |
| HARDWARE STORAGE CONFIGURATION REQUIREMENTS..... | 62 |
| <i>Recommended Hardware Configurations</i> | 62 |
| For Recording 50-500 Users..... | 62 |
| For Recording 500-1,000 Users | 62 |
| For Recording 1,000-2,000 Users | 63 |
| More Than 2,000 Users | 63 |
| High Availability and Redundancy | 63 |
| Decoupled Architecture | 64 |
| Hardware Specification Recommendations | 65 |
| <i>Recording Server Hardware Requirements</i> | 65 |
| <i>Disk Space Requirements</i> | 67 |
| <i>Screen Recording Storage Requirements</i> | 68 |
| <i>Firewall Configuration</i> | 68 |
| BACKUP AND RESTORE..... | 69 |
| <i>Backup Call Recordings</i> | 69 |
| <i>Restore Call Recordings</i> | 70 |
| MORE RESOURCES..... | 71 |

ADMINISTRATION

For organizations who have purchased licenses for Call Recording (powered by MiaRec), Authorized Administrators may be setup to work in the Call Recording portal at the 'Tenant' level. This means that the Administrator has been granted permission to manage the groups, user assignments, and tools the organization has purchased for Call Recording only for their organization with enough access to perform tasks that pertain only to their enterprise (AKA: the Tenant).

To view Administration tools, click on the Administration tab at the top of the portal view.



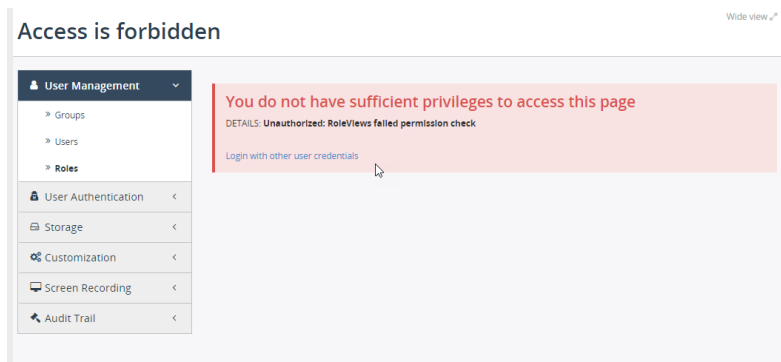
The screenshot displays the Administration section of the Call Recording Portal. At the top, a navigation bar includes tabs for Dashboard, Recordings, Reports, and Administration (which is highlighted in orange). The user profile 'Smith - [20...7]' is visible in the top right corner. The main content area is titled 'Administration' and features a sidebar on the left with a list of menu items: User Management, User Authentication, Storage, Customization, and Audit Trail. The main content area is organized into several sections, each with a gear icon for settings:

- Administration**
 - USER MANAGEMENT**
 - Groups
 - Users
 - Roles
 - USER AUTHENTICATION**
 - User Web Sessions
 - STORAGE**
 - File Encryption
 - Storage Limits/Usage
 - CUSTOMIZATION**
 - Field Visibility
 - Evaluation Form Designer
 - Custom Fields
 - AUDIT TRAIL**
 - Audit Trail

Each area shown within the Administration section offers information and helpful tools for Admins.

Access and Permissions

Please note, there are many areas in Administration where information may be displayed to the Administrator where it is helpful to see, but specific actions can remain locked and related tasks cannot be performed without additional access permissions. If an Administrator (or Supervisor) attempts to access areas or perform tasks that they have not been granted access to, the system will provide a notification to the user:

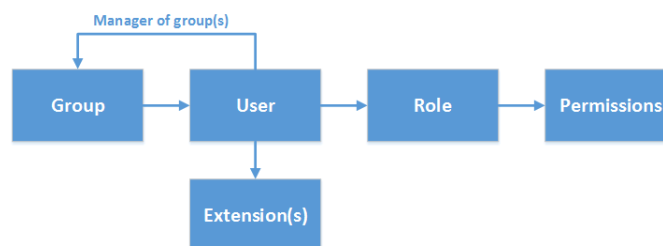


The way permissions are used for Roles, Groups, and Users at the organizational (AKA: Tenant) level is described in the sections below.

User Management

Roles

Call Recording software provides role-based access control features with granular permissions. Each user account is associated with one role, and each role is pre-configured with a set of permissions.



Each licensed user in the Call Recording system needs to have an assigned **Role**. The role fundamentally defines which system resources are accessible to the user and what operations or tasks they are permitted to perform using the service resources they are licensed to use.

Roles may only be added or deleted by the Root Administrator and cannot be edited or added by a Tenant level Administrator. Permissions include such privileges like "Configure System", "Configure Users", "Playback calls", "Delete calls", "set Screen Recording Settings", etc.

By default, the following roles are pre-defined in the Call Recording system. An authorized Root Administrator may create new roles or modify existing ones:

Root Administrator – (Service Provider) This role has unlimited access to the system to assist Tenant level Administrators with implementation and maintenance at the highest levels – this level is for service provider access.

Administrator – (Tenant Admin) Users assigned to this role have a useful set of permissions as configured by the Root Administrator to manage groups, users, and tools at the tenant or enterprise level. This type of Administrator is generally authorized to manage other user accounts for call recording access and usage within their organization.

Supervisor – Supervisors are generally granted access to review and work with call recordings and possibly reports or other add-on tools that are associated with the users in his/her managed group(s). Supervisors are not granted permissions to create or delete other user accounts. A supervisor may be granted limited access to edit Agent/User accounts (to assist with password issues, etc.)

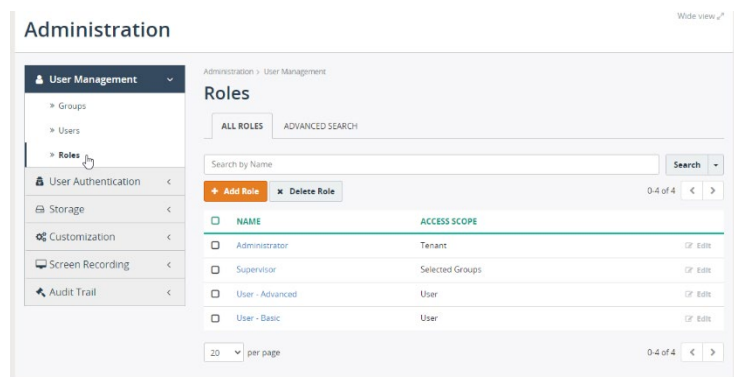
Users/Agents – This role is (and should be) limited in access. Most Users/Agents will not be granted permission to access the Call Recording portal or have access see or modify to their own call recordings. This role should be utilized for call center agents or employees who will just have calls recorded but will not manipulate those call recording files in any way. If there is a need for someone to review their call recordings (or the recordings of others), that user should be assigned to the Supervisor role and provided with access credentials to log into the portal. If permission is granted to a User/Agent to access the Call Recording portal and their recordings, the minimum level of access to specific tools should be enabled and caution should be used to ensure the organization clearly defines the amount of access each individual should have to delete, mark as confidential, or modify the information related to their call recordings.

List of Roles

Navigate to **Administration > User Management > Roles** to see a list of available roles in use within your enterprise.

During installation Call Recording automatically loads the default roles defined by your organization and LOGIX. These are generally license-based and provide a specific set of features and tools for each user type by default. An Administrator may view the roles and their settings. Only LOGIX may change Roles or their settings.

Note: In general it is best to edit feature or tool access permissions individually for each user rather than attempting to modify Roles.



Access Level / Scope

Access scope setting specifies which resources are accessible by a user assigned to a specific Role. An authorized Root Admin (LOGIX) has access to define Roles and modify Access Level and Scope.

Tenant Admins may view the current access level / scope for each role by going to:

Administration > Roles > click on the desired Role name to review the currently defined settings.

Permissions

Permissions settings specify what operations are permitted on the accessible resources. These operations include view, edit, delete, playback etc. and permission at the Role level are defined at the Root Admin level by LOGIX

Tenant Admins may view the current permissions for each role by going to:

Administration > Roles > click on the desired Role name to review the currently defined settings.

Note: The organization's Call Recording Admin should contact LOGIX for more information or assistance with Roles.

Groups

Each Call Recording license holder (user/supervisor/admin) will belong to at least one group by default, and can be re-assigned to different to a group by an Administrator. Most Call Recording license holders are just members of a group being recorded and *do not require or need access to the Call Recording portal* to perform tasks. But some Call Recording license holders may be assigned a Supervisor role, and they may also be allowed to manage call recordings for one or more groups. Each license holder will be assigned to one group - but may also be a member of multiple managed groups. An Admin may set Supervisors or Admins to manage one or multiple groups.

Navigate to **Administration > User Management > Groups** to see a list of available groups. During installation Call Recording automatically pre-creates a few sample groups. An authorized Administrator may create new groups or edit existing ones.

The screenshot displays the 'Administration' portal with a sidebar menu on the left containing 'User Management', 'User Authentication', 'Storage', 'Customization', 'Screen Recording', and 'Audit Trail'. The 'User Management' section is expanded to show 'Groups', 'Users', and 'Roles'. The main content area is titled 'Groups' and includes a search bar, 'Add Group' and 'Delete Group' buttons, and a table listing groups. The table has columns for 'NAME' and 'TOTAL USERS'. One group is listed with ID '3100004554-01' and 5 users. A pagination control shows '20 per page' and '0-1 of 1'.

| NAME | TOTAL USERS |
|---------------|-------------|
| 3100004554-01 | 5 |

View Group Members

Click on the Group name in the list to view the group's profile page. This view displays a list of all users, who are currently assigned members of this group.

Administration > User Management > Groups

Group «31000...-01» [Edit Group](#) [Delete Group](#)

Group Name: 31000...01
Timezone: default

Users

Search by Text [Search](#)

[Bulk Edit](#) 0-8 of 8 < >

| <input type="checkbox"/> | NAME | ROLE | RECORDING | EXTENSION |
|--------------------------|------------------|---------------|-----------|-----------------------------------|
| <input type="checkbox"/> | Bill - [20] [06] | Administrator | Always | 21 @myntm.us Edit |
| <input type="checkbox"/> | Ca - [20] [07] | Administrator | Always | 21 @myntm.us Edit |
| <input type="checkbox"/> | fal - [20] [08] | Administrator | Never | Edit |
| <input type="checkbox"/> | Jer - [20] [09] | Administrator | Always | 21 @myntm.us Edit |
| <input type="checkbox"/> | Ni - [20] [10] | Administrator | Always | 21 @myntm.us Edit |
| <input type="checkbox"/> | Pa - [20] [11] | Administrator | Always | 21 @myntm.us Edit |
| <input type="checkbox"/> | RC - [20] [12] | Supervisor | Always | 21 @myntm.us Edit |
| <input type="checkbox"/> | Ty - [20] [13] | Supervisor | Always | 21 @myntm.us Edit |

20 per page 0-8 of 8 < >

AUDIT TRAIL

Show

Add a Group

While viewing Groups, click on the **Add Group** button.

Enter a unique name and (optional)select a Timezone, then click Save.

This group will be available for selection when Adding or Editing Users.

Administration > User Management > Groups

Add Group

Name *

Timezone

Leave empty for default

[Save](#)

Edit Group Settings

While viewing the profile, click on Edit group button. Configuration of group includes the following options:

- **Group Name**
- **Timezone**, which will be used by default for each user in this group. The timezone setting may be overridden on user's profile page.
- Click [Save](#) when finished.

Edit Group «Administrators»

Group Name *

Timezone

[Save](#)

Add Users to a Group

See [Add/Edit User](#)

Users

View List of Users

Navigate menu **Administration > Users Management > Users** to see a list of users. You can use the Search tool to find users by name, group, role, or extension.

User Management

- Groups
- Users
- Roles

Administration > User Management

Users

ALL USERS ADVANCED SEARCH

Select a Group Search by Name, Extension, Group, Role [Search](#)

Bulk Edit 0-13 of 13 < >

| <input type="checkbox"/> | NAME | GROUP | ROLE | RECORDING | EXTENSION | |
|--------------------------|-------------|---------------|---------------|-----------|------------------|----------------------|
| <input type="checkbox"/> | Bill Tre... | 3100004554-01 | Administrator | Always | 20...08@mymtm.us | Edit |
| <input type="checkbox"/> | Carin S... | 3100004554-01 | Administrator | Always | 20...07@mymtm.us | Edit |
| <input type="checkbox"/> | ... | 3100004554-01 | Administrator | Never | | Edit |
| <input type="checkbox"/> | Jessica | 3100004554-01 | Administrator | Always | 20...37@mymtm.us | Edit |
| <input type="checkbox"/> | Nicole I | 3100004554-01 | Administrator | Always | 20...39@mymtm.us | Edit |
| <input type="checkbox"/> | Pamela | 3100004554-01 | Administrator | Always | 20...99@mymtm.us | Edit |
| <input type="checkbox"/> | RC Adm | 3100004554-02 | Administrator | Always | 20...28@mymtm.us | Edit |
| <input type="checkbox"/> | RC Bas | 3100004554-01 | Supervisor | Always | 20...18@mymtm.us | Edit |
| <input type="checkbox"/> | RC Sup | 3100004554-02 | Supervisor | Always | 20...12@mymtm.us | Edit |
| <input type="checkbox"/> | Tyler D | 3100004554-01 | Supervisor | Always | 20...33@mymtm.us | Edit |
| <input type="checkbox"/> | User O | 3100004554-02 | User - Basic | Always | 20...46@mymtm.us | Edit |
| <input type="checkbox"/> | User T | 3100004554-02 | User - Basic | Always | 20...39@mymtm.us | Edit |
| <input type="checkbox"/> | User T | 3100004554-02 | User - Basic | Always | 20...41@mymtm.us | Edit |

20 per page 0-13 of 13 < >

View User Settings

While viewing the Users list, click on a user's name to open a view of the current settings.

Administration > User Management > Users

User «RC Basic Supervisor - [20...8]»

[Edit User](#) [Reset Password](#)

User Info Security

Name: RC Basic Supervisor - [20...18]
 Status: **Active**
 Role: **Supervisor**
 Group: 310...01
 Managed groups: 310...01
 Email:
 Timezone: **America/Chicago**
 Language: **Default**
 Created Time: **Aug 25, 2021, 3:14 PM**

RECORDING SETTINGS

Record: **always**
 Record direction: **any direction**
 Extensions: 20...@mymtm.us
 Confidential: **no**
 Screen Recording Login:

WEB ACCESS SETTINGS

Login: 20...@mymtm.us
 Allow web access: **yes**
 Authenticate with: **Password**
 Must change password: **no**
 Valid till: **Dec 30, 2099**
 2-step verification: **Disabled** 2-step verification is not configured on this system
 Last login time: **Aug 26, 2021, 11:30 AM**

AUDIT TRAIL

Show

Edit User Settings

Click on the **Edit User** button (top right) to review and manage the specific settings that are available be modified at the Tenant Level.

For example: In the Edit User view the selected license holder may be assigned to be a member of one or more **Groups**, and if a license holder assigned the Supervisor Role was selected, they may also be granted access to one or more **Managed Groups** (those groups containing a set of the users whose call recordings the Supervisor should be able to see and manage within the Call Recording Portal).

Additional editable settings shown in the *Edit User* view may include Recording Settings, Web Access Settings, etc.

View User Security Settings

While in the User setting dialog, click on the Security tab to review the latest access information.

The Admin can view information about devices used to access Call Recording and recent web sessions. Tools may be provided to allow the Admin to Revoke device access or Terminate the current web session.

Administration > User Management > Users

User «RC Basic Supervisor - [208]»

[Edit User](#) [Reset Password](#)

User Info **Security**

USER DEVICES

[✕ Revoke](#)

| <input type="checkbox"/> | FIRST ACCESS | LAST ACCESS | LOCATION | CLIENT | SYSTEM | |
|--------------------------|------------------------|---------------|----------------|---------|---------|----------------------|
| <input type="checkbox"/> | Sep 10, 2021, 10:37 AM | 2 minutes ago | 148.75.112.216 | Firefox | Windows | View |
| <input type="checkbox"/> | Sep 10, 2021, 8:28 AM | 2 hours ago | 148.75.112.216 | Firefox | Windows | View |
| <input type="checkbox"/> | Sep 10, 2021, 8:23 AM | 2 hours ago | 184.91.120.143 | Chrome | Windows | View |
| <input type="checkbox"/> | Aug 26, 2021, 9:46 AM | 14 days ago | 76.97.114.163 | Chrome | Windows | View |
| <input type="checkbox"/> | Aug 26, 2021, 9:15 AM | 15 days ago | 76.97.114.163 | Chrome | Windows | View |
| <input type="checkbox"/> | Aug 26, 2021, 9:14 AM | 15 days ago | 76.97.114.163 | Chrome | Windows | View |

USER WEB SESSIONS

[✕ Terminate](#)

| <input type="checkbox"/> | SESSION START TIME | LOCATION | CLIENT | SYSTEM | |
|--------------------------|--|----------------|---------|---------|----------------------|
| <input type="checkbox"/> | Sep 10, 2021, 10:37 AM (2 minutes ago) | 148.75.112.216 | Firefox | Windows | View |

Revoke User Device Access

1. Click to place a check in the box adjacent to a listed user device to select it.
2. Click the Revoke button (above the User Device list) to disallow access by the selected device(s).

Terminate a User Web Session

1. Click to place a check in the box adjacent to a listed User Web Session to select it.
2. Click the [Terminate](#) button (above the User Web Session list) to end the session.

Reset Password



Important Note:

Use the following steps **ONLY** if SSO is not in use and direct login steps are used.

Where Single Sign On (SSO) protocols are in use for the organization, Admins should manage Password Credentials in the Cloud Services Portal. When Call Recording is accessed via the link in either the Dashboard Applications widget or the Call Recording section of the Cloud Services Portal, Reset Password in the Call Recording portal should not be used and may be disabled to ensure the SSO protocol is sustained.

Reset Password

While reviewing the User settings dialog, an Admin may have access to Reset a user's password.

1. Click on the **Reset Password** button (top right) to open the *Reset Password...* dialog.

2. Select or define the following:
 - ❖ **Reset Password Type** – Pick the way the password will be updated:
 - Select **Create a new password for user** and enter the New Password ensuring it meets all security requirements, OR...
 - Select **Send user a reset password link by email** (recommended) to allow the user to securely create their new password.
 - ❖ **Must Change Password** (optional) – Click to enable the **Must Change password on next login** option to require the user to update the password the next time they sign in.
3. Click the **Reset Password** button to save and submit the new information.

Edit a User

If the Administrator has access to perform this task while viewing the list, click on the **Edit** link adjacent to a user (far right), OR While viewing the User's settings, click on the **Edit User** button (top right). When finished making changes click **Save**.

User Profile Settings

The first section includes the following fields and settings:

- ❖ **User Name** – Required. Enter a unique name.
- ❖ **Active** – Click to place a check next to Yes, user is active. Return here if there is a need to remove the check and make the user inactive, or to check to see if that permission needs to be re-enabled.
- ❖ **Role** – The role for the user is defined when the license is ordered and may be Supervisor, Admin, or User/Agent (not working in this portal).
- ❖ **Group** – Select the correct group(s) to which this user belongs. This could be set based on locations, departments, or any other useful grouping protocol. Each user may be assigned to one or to multiple groups.
- ❖ **Managed Groups** – If the user's role has access level Supervisor or Administrator, then you can select the group(s) that this user will manage (may see/access the audio/video recordings, make notes, and perform reporting tasks for the users assigned to the groups selected here). You may select one or more groups from the list for the Supervisor to see in the Call Recording portal.
- ❖ **Email** – Enter an email address for this user. This email will be used to send updates (if these features are in use).
- ❖ **Timezone** – By default the timezone is derived from the host server's timezone setting, however it may be defined here. Please note, the user may also update this information in their profile.

Edit User «David Amado»

User Name *

Active? * Yes, user is active

Role *

Group *

Managed Groups

Email

Timezone

RECORDING SETTINGS

Record * Yes On-demand only Never Default

Record Direction Inbound Outbound

Extension * x

[Add Extension](#)

WEB ACCESS SETTINGS

Allow Web Access? * Yes

Authenticate With * MiaRec Password LDAP Directory Service

Managed Groups

Email

Timezone

User Recording Settings

- ❖ **Record** – Define whether and when recordings will occur – **Yes (always), On-demand only, Never, or Default (defined by the organization and set at the root level).**
- ❖ **Record Direction** – Define whether recordings will trigger on inbound only, outbound only or both.
- ❖ **Extension** - *Call Recording uses the extensions configuration to automatically associate call recordings with users.* If it is

RECORDING SETTINGS

Record * Yes On-demand only Never Default

Record Direction Inbound Outbound

Extension * x

x

[Add Extension](#)

necessary to record the calls of a user or Supervisor, then all of the extensions that are assigned to this user must be specified. One user may have more than one extension. Tools are provided to include more extensions, as needed.

User Web Access Settings

If the user needs access to Call Recording web portal, then administrator may create a login for him/her.

Note: For security it is recommended that only Supervisors and Administrators receive credentials to access to the portal.

WEB ACCESS SETTINGS

Allow Web Access? Yes

Authenticate With MiaRec Password LDAP Directory Service

Web Access Login

LDAP Login

Should include domain name, like "domain\user"

Password
 Confirm Password

Must Change Password Must change password on next login

Valid Till

Associating Calls with Users

Call Recording automatically associates calls to users based on the extension(s) defined in the User's profile.

| USER | DATE | TIME | DURATION | FROM | TO |
|------------------|--------------|---------|----------|----------------------------|--------------------------------|
| 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 |
| Carrol Robards | Feb 17, 2015 | 6:29 PM | 2:49 | 1636250930 | 21311001010 (Carrol Robards) |
| Lynn Lafever | Feb 17, 2015 | 5:27 PM | 0:14 | 4781430872 | 21311002004 (Lynn Lafever) |

Administrator should configure extension on user's profile page. In below screenshot user "Roland Corry" is configured with extension "21311005005". When Call Recording recognizes a call with extension "21311005005", then the call is automatically associated with user "Roland Corry".

Such call association allows quick filtering of calls by user name. Also, this information is used when granting access to recordings. For example, Supervisor will be able to view only call recordings, which are associated with users in his/her group.

Edit User «Roland Corry»

User Name

Active? Yes, user is active

Role

Group

Managed Groups

Email

Timezone

RECORDING SETTINGS

Record Yes On-demand only Never Default

Record Direction Inbound Outbound

Extension

[Add Extension](#)

Manage Calls That Are Not Yet Assigned to Users

If Call Recording doesn't recognize an extension for a newly recorded call, **then a default recording rule applies for the call**. By default, Call Recording is configured to record such unknown calls that come into the system and display them to authorized Administrators, but this behavior may be changed by LOGIX.

Administrators may see that a call with an unknown extension is recorded in the Recordings list. The column "User" will be empty (as shown in below screenshot).

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

Also, these calls are displayed in the "Not assigned to users" view (visible only to Administrators).

ALL CALLS ACTIVE CALLS MY CALLS BY USER **NOT ASSIGNED TO USERS** BY CATEGORY

Select a Date Range Search a Text

Delete Categories

| <input type="checkbox"/> | USER | DATE | TIME | DURATION | FROM | TO |
|--------------------------|------|-------------|----------|----------|---------|---------|
| <input type="checkbox"/> | | Today | 12:41 PM | 0:17 | 1002 | 3210685 |
| <input type="checkbox"/> | | Today | 12:41 PM | 0:17 | 1002 | 3210685 |
| <input type="checkbox"/> | | Oct 1, 2014 | 1:15 PM | 0:24 | 3210000 | 1023 |
| <input type="checkbox"/> | | Oct 1, 2014 | 1:15 PM | 0:24 | 3210000 | 1023 |

An authorized Administrator can manually assign the call to one of existing users.

1. Click on a call to display call details.
2. Click on **Assign to user**.
A new page displays the following options to review:

Extension – Select the number/extension or the phone name to associate and display for calls in the lists.

Assign to User – Select The user to associate this call with.

Apply this rule to all similar calls - When checked, then other calls with the same extension will be automatically assigned to this user. Note, Call Recording will search only calls which are not assigned yet to any of the users.

3. Click **Save** and the recorded calls will be searched and automatically assigned to the selected user. Additionally, the selected extension will be automatically added to user profile.

ALL CALLS ACTIVE CALLS MY CALLS BY USER **NOT ASSIGNED TO USERS** BY CATEGORY

Select a Date Range Search a Text Search

Delete Categories 0-3 of 3 < >

| <input type="checkbox"/> | USER | DATE | TIME | DURATION | FROM | TO | CATEGORIES |
|--------------------------|------|--------------|----------|----------|-------------------|-------------------------|------------|
| <input type="checkbox"/> | | Today | 12:41 PM | 0:17 | 1002 | 3210685 | |
| <input type="checkbox"/> | | Oct 1, 2014 | 1:15 PM | 0:24 | 3210000 | 1023 | |
| <input type="checkbox"/> | | May 13, 2009 | 10:13 AM | 0:12 | 3095 (2128123095) | 3086 (Lora Leavenworth) | |

From: 3095 2128123095 assign to user

To: 3086 Lora Leavenworth assign to user

Date/Time: May 13, 2009 10:13:28

Duration: 0:12

Save audio file

Assign call to user

Extension * 3086

Lora Leavenworth

Assign to User * Lora Leavenworth

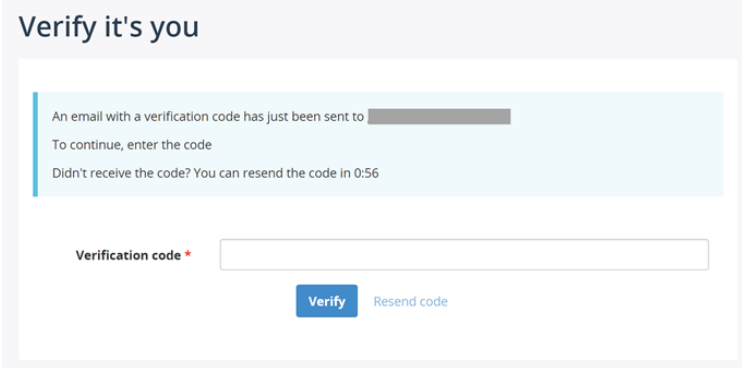
Apply this rule to all similar calls

Save

Impersonate a User

Call Recording offers authorized Admins a tool for viewing the portal the way another licensed user does. This is called **Impersonation**. This tool may be useful for seeing how a dashboard looks to a user with less access or to ensure a Supervisor can see all users they should manage. Please note that while in Impersonate mode, an Admin can only perform the level of tasks the user is permitted. Administration tasks should only be performed when NOT in Impersonate mode.

1. Navigate to **Administration > User Management > Users**
2. Click on the name of a licensed user in the list.
3. Click on the **Impersonate** button (top right) to begin reviewing Call Recording as though logged in as the person selected for impersonation. Please note, some organizations using SAML 2.0 access may require the Admin to *verify it's you* (if enabled on the tenant) to add another level of security when attempting to make changes while impersonating another user. Enter the verification code (sent via SMS or Email as defined by the organization) when prompted and click **Verify** to continue. A *Resend code* option is available, if needed.



Verify it's you

An email with a verification code has just been sent to [redacted]

To continue, enter the code

Didn't receive the code? You can resend the code in 0:56

Verification code *

Verify Resend code

4. When you are finished reviewing the user's view of Call Recording and wish to return to view the portal using your own Administrator account credentials, click on the drop-down arrow next to the user's name being impersonated and select the **Exit user impersonation** option.

Storage

Click on Storage to view information about Storage Targets, File encryption and the Storage Limits/Usage.

The screenshot shows the 'Administration' portal with the 'Storage' section selected in the sidebar. The main content area is titled 'Storage' and contains two panels: 'FILE ENCRYPTION' and 'STORAGE LIMITS/USAGE'. The 'FILE ENCRYPTION' panel has a 'View details' button. The 'STORAGE LIMITS/USAGE' panel has a 'View details' button.

Storage Targets

Click on **Storage Targets** (if available) to view or manage recording storage locations.

The screenshot shows the 'Administration' portal with the 'Storage Targets' section selected in the sidebar. The main content area is titled 'Storage Targets' and contains a table with columns: TENANT, NAME, TYPE, and ROOT PATH. The table has two rows. The first row is selected. There are 'Add' and 'Delete' buttons above the table. There are also search and pagination controls.

| TENANT | NAME | TYPE | ROOT PATH |
|--------|------------------------------------|-----------|------------------------------------|
| System | https://s3-us-east-1.amazonaws.com | Amazon S3 | https://s3-us-east-1.amazonaws.com |
| System | 192.168.1.100:22 | SFTP | 192.168.1.100:22 |

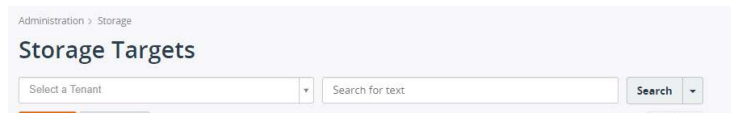
Call Recording provides helpful tools for Admins to manage recording storage. Tasks that can be made available to Administrators once a storage option is defined/purchased include the ability to view, test, add, edit, and delete storage targets.

Storage can be hosted (\$) or non-hosted and the following storage target types are supported:

- Option 1 Non-Hosted - Audio and/or Video recordings are available in storage for 90 days. Customer can download recordings for archive at any time as desired for up to 90 days (from the date of recording).
- Option 2 Provider Hosted (\$) - Purchase of license(s) required. Audio and/or Video of recordings are stored by LOGIX for the amount of time purchased. Customer may download for archive at any time while the recordings are available in storage.
- Option 3 BYO Storage (\$) - A fee for setup / implementation is required. Audio and/or Video recordings are stored to the customer's storage site.

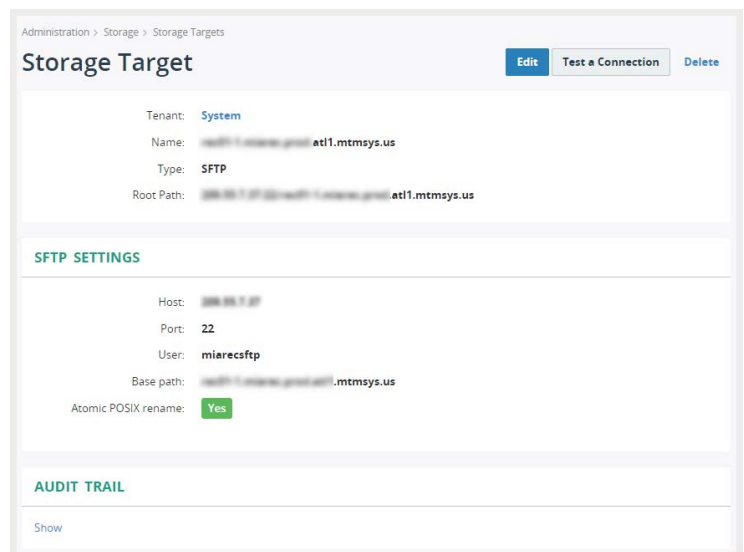
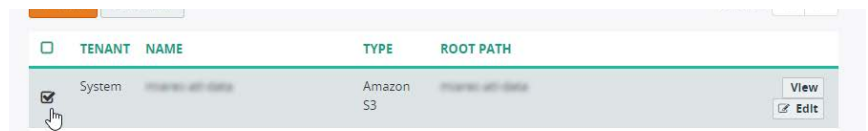
Search Storage Target List

While viewing Storage Target list, the section above the list offers useful search tools. The Admin can use the Search by Tenant selection tool or enter text and then click the adjacent **Search** button to filter the list and locate the correct item(s).



View Storage Target Setup

While viewing the Storage Target list, an authorized Admin may click to place a check in the adjacent check box to select it and then click the listing's **View** button (far right) to open a dialog that displays the item's current setup.

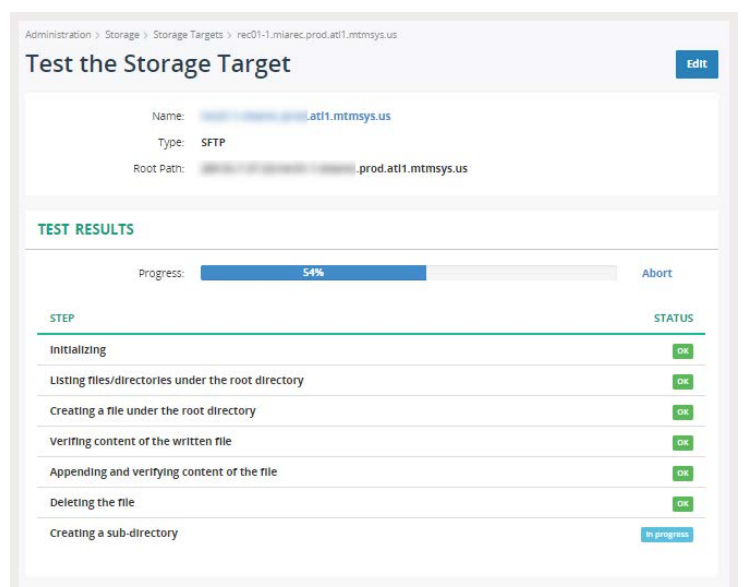


Test a Target Connection


Call Recording offers authorized Admins a tool to Test the connection to a Storage Target while viewing the Storage Target setup. Note: A similar test tool is also available when Editing or Adding a Storage Target.

Click on the **Test a Connection** button in the dialog (or *Test and Save* in an Edit/Add dialog).

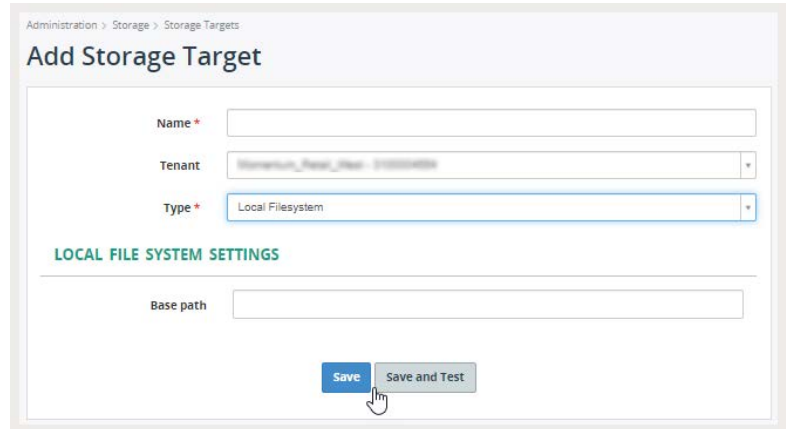
A new dialog displays which provides a dynamic view of the test process steps and color coded final results for review.



Add a Storage Target

1. While viewing the Storage Target list
2. Click on the  Add button to begin creating a new Storage target.
3. Enter a unique Name for the target.
4. Select the correct storage **Type** per your license agreement.
5. The dialog will dynamically display additional fields based on the selection made here to assist with setup.

Here are some examples of the dynamic views displayed to assist in the setup of storage target types:



Administration > Storage > Storage Targets

Add Storage Target

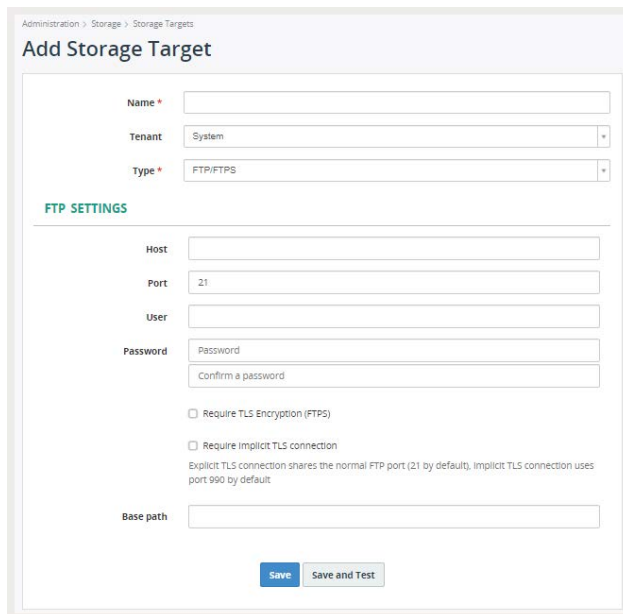
Name *

Tenant

Type *

LOCAL FILE SYSTEM SETTINGS

Base path



Administration > Storage > Storage Targets

Add Storage Target

Name *

Tenant

Type *

FTP SETTINGS

Host

Port

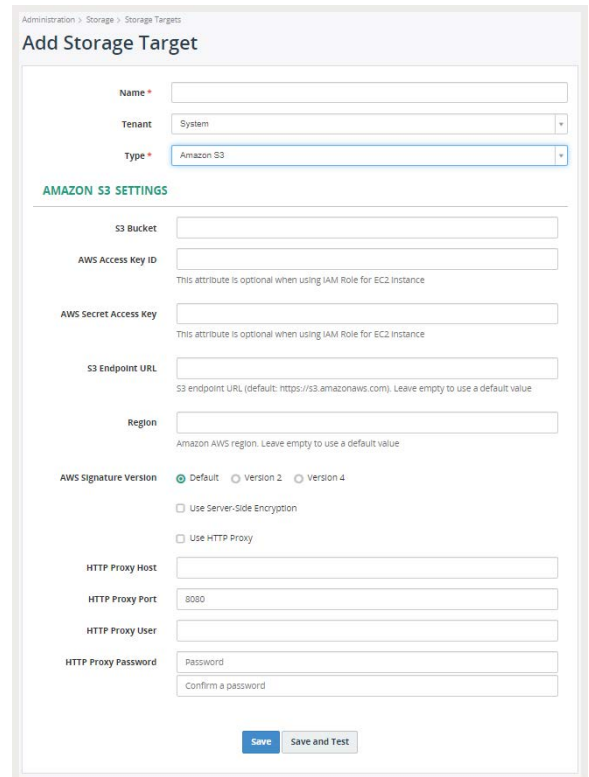
User

Password

Require TLS Encryption (FTPS)

Require implicit TLS connection
 Explicit TLS connection shares the normal FTP port (21 by default), implicit TLS connection uses port 990 by default.

Base path



Administration > Storage > Storage Targets

Add Storage Target

Name *

Tenant

Type *

AMAZON S3 SETTINGS

S3 Bucket

AWS Access Key ID
This attribute is optional when using IAM Role for EC2 Instance

AWS Secret Access Key
This attribute is optional when using IAM Role for EC2 Instance

S3 Endpoint URL
S3 endpoint URL (default: https://s3.amazonaws.com). Leave empty to use a default value

Region
Amazon AWS region. Leave empty to use a default value

AWS Signature Version Default Version 2 Version 4

Use Server-Side Encryption

Use HTTP Proxy

HTTP Proxy Host

HTTP Proxy Port

HTTP Proxy User

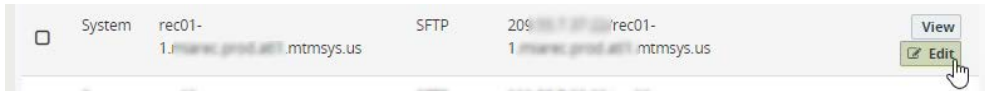
HTTP Proxy Password

7. Complete the required fields for the storage type selected, and include any additional information in the optional fields.
8. Recommended: Click **Save and Test** when finished to ensure the connection is good for the new target, or click the **Save** button.

Note: To cancel without creating a new storage target, simply exit the dialog without clicking a Save option, or click the back button on the browser to return to the previous view.

Edit a Storage Target

1. While viewing the Storage Target list
2. Click on the adjacent Edit button (far right) to begin modifying a Storage target.



3. Edit the information or type for the target, as needed. The dialog will dynamically display any necessary fields based on the new selections made.
4. Recommended: Click **Save and Test** when finished to ensure the connection is good for the new target - Or click the **Save** button.

Or click the **Save** button.

Note: To cancel without making changes to the storage target, simply exit the dialog without clicking a Save option, or click the back button on the browser to return to the previous view.

Administration > Storage > Storage Targets

Edit Storage Target

Name *

Type *

SFTP SETTINGS

Host

Port

User

Password

Either Password or SSH Key is required

SSH key

Either Password or SSH Key is required

Base path

Atomic POSIX rename Use 'posix-rename' extension
 Use the 'posix-rename' extension introduced in OpenSSH 4.8 and some other SFTP servers (recommended)

Delete a Storage Target

Use Caution. This action is performed immediately.

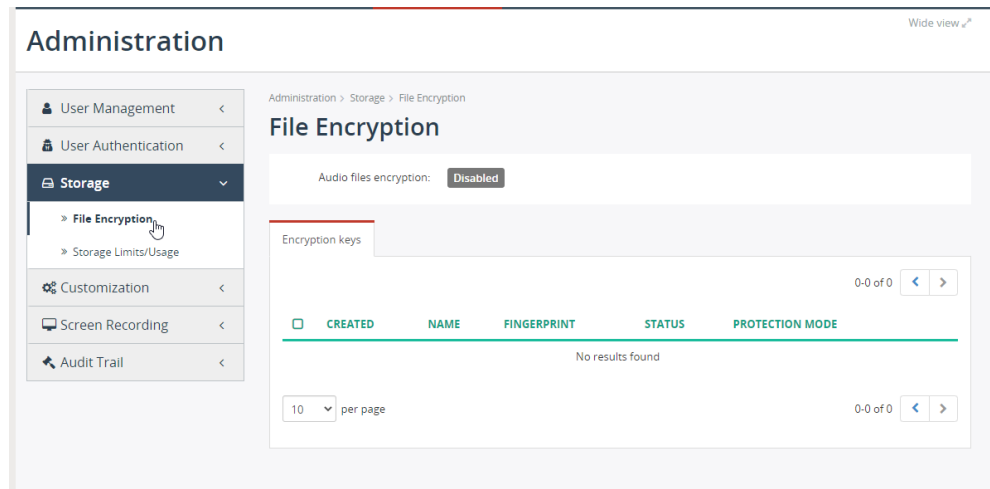
1. While viewing the Storage Target list
2. Click to place a check mark next to the desired item in the Storage Target list.
3. Click the **Delete** button displayed above the list.
The storage target is immediately deleted, however an UNDO option displays to allow the Admin to reverse the action and return the storage target to the list.



Click the **UNDO** link above the list to keep the storage target and cancel the delete action.

File Encryption

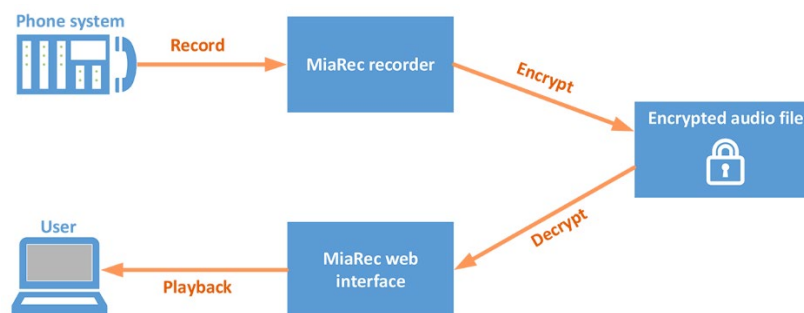
Click on **File Encryption** to review information about the configuration and encryption keys.



Call Recording provides rock-solid audio encryption functionality, 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.

Some key features of Call Recording audio file encryption:

- Asymmetric encryption, where a public key is used for encrypting and a private key is used for decrypting
- Administrator has control over who can play back (decrypt) the recordings
- In a multi-tenant mode, each tenant has its own unique encryption key
- Encryption is applied to backup data, as well



Audio File Encryption vs Role-Based Access Control

Call Recording role-based access control system provides protection of data from unauthorized access to the Call Recording web-portal. Everyone accessing the system must be an authenticated user with associated set of permissions. Audio file encryption provides an additional layer of security over the role-based access control system in Call Recording. If encryption is enabled, then audio files are stored on a hard disk in encrypted format. This insures that even if unauthorized user gains physical access to the storage system, he/she has no ability to play back recordings because he/she doesn't have the private encryption key.

Download of Encrypted Recordings

When a user downloads individual call recordings through Call Recording portal, the file is **decrypted** during that process. The file is saved on the user's computer in unencrypted form and they can play the .wav file at will.

*However, when a user uses the **bulk download** feature to download multiple call recordings, then the downloaded files are retrieved in encrypted form in a ZIP archive. The user cannot play back such call recordings unless he/she imports them into the Call Recording system together with private encryption key.*

Encryption for Backups

Use of file encryption is beneficial for backup data, as well. All recordings in backup archive can be encrypted.

Encryption Algorithms

Call Recording encrypts every call recording with asymmetric encryption. For every recording, Call Recording generates a random AES encryption key. This symmetric encryption key is then encrypted using asymmetric encryption (one key for encryption - often referred to as the "public" key - and a different key for decryption - often referred to as the "private" key).

Call Recording uses Advanced Encryption Standard (AES) for symmetric encryption (256-bit key) and the Rivest-Shamir-Adleman (RSA) public key algorithm for asymmetric encryption (2,048-bit keys).

The details and theory behind the asymmetric encryption method is beyond the scope of this article. However, a good primer is available at https://en.wikipedia.org/wiki/Public-key_cryptography. In short, a public key is used for encrypting data and private key is used for decrypting it. The public key doesn't need to be stored securely. Anyone can access the public key, but no one can use the public key to decrypt the data that the public key encrypted. The only way users can decrypt data is with the private key.

User Access to Encryption Keys

LOGIX must grant particular Administrators access to encryption key(s) before they can play back (decrypt) audio files. Note, the administrator may grant access only to those encryption keys which are granted to him/her. If administrator (even if he/she has role "Root administrator") has no access to the encryption key, then he/she cannot grant access to other users for the same key.

Call Recording software never stores encryption keys in the database in plain text for security reasons. Even if an unauthorized party gains access to database files, he/she could not retrieve the private keys because they are stored in encrypted format. There is no way to gain user's private key without knowing the user's password.

Encryption Key Configuration

These tasks require the Administrator to have permissions to access. Contact LOGIX for assistance.

1. Create New Encryption Key

If authorized: Navigate to Administration > Storage > File Encryption to create new encryption key.

Administration > System Configuration

Encryption

Audio files encryption: **Enabled** [Edit configuration](#)

Caution! Above setting applies to system account only. [Edit tenant's configuration](#)

Encryption keys

Select a Tenant Search by Key Fingerprint [Search](#)

[+ Add Encrypt Key](#) [x Delete Encrypt Key](#) 0-3 of 3 < >

| <input type="checkbox"/> | CREATED | FINGERPRINT | TENANT | STATUS | |
|--------------------------|------------------------|----------------------------------|--------|-------------------|---|
| <input type="checkbox"/> | Today, 2:45 PM | e259168e28b236f6f9d0f8c7a0b7cb24 | Flexus | Active | View Edit |
| <input type="checkbox"/> | Nov 20, 2015, 10:34 AM | d4c32bda54662d63fb2a4351d818784 | System | Active | View Edit |
| <input type="checkbox"/> | Nov 19, 2015, 3:29 PM | adfadd4ca8843766153b182c224ff9ab | System | Not active | View Edit |

20 per page 0-3 of 3 < >

Administration > System Configuration > Encryption

Add Encrypt Key

Tenant:

Active? Yes, use this key for oncoming calls

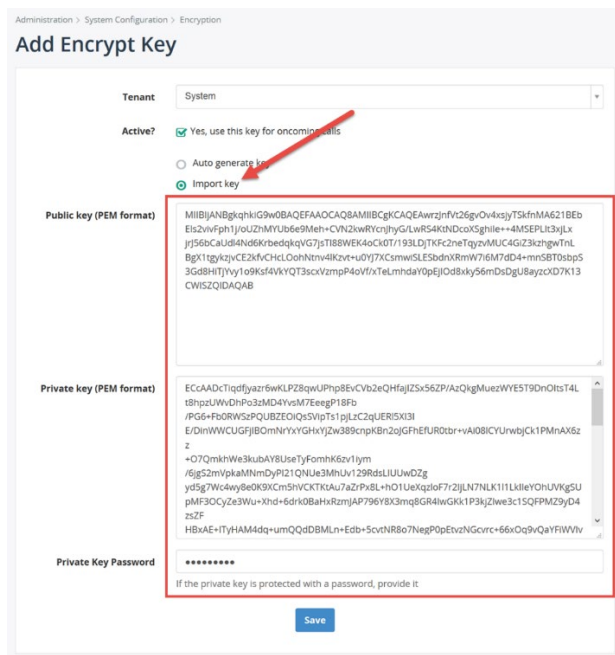
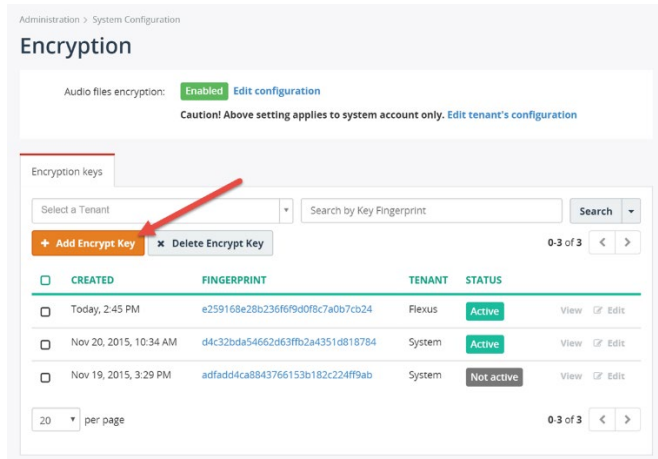
Auto generate key
 Import key

Key length * 1024-bit
 2048-bit
 4096-bit

[Save](#)

2. Import Encryption key

Encryption key can be imported from the existing key rather than generated from scratch. Navigate to **Administration > Storage > File Encryption** to import the existing encryption key.



3. Export Encryption Key

Navigate to **Administration > Storage > File Encryption** to export the existing encryption key. It is highly recommended to export all existing keys and store them in secure place for backup purposes. You may need such backup copies when all authorized people forgot their passwords or database is destroyed and you need to recover the audio files from archive.

Administration > System Configuration

Encryption

Audio files encryption: **Enabled** [Edit configuration](#)
Caution! Above setting applies to system account only. [Edit tenant's configuration](#)

Encryption keys

Select a Tenant: Search by Key Fingerprint: [Search](#)

[+ Add Encrypt Key](#) [x Delete Encrypt Key](#) 0-3 of 3 < >

| CREATED | FINGERPRINT | TENANT | STATUS | |
|---|----------------------------------|--------|-------------------|---|
| <input type="checkbox"/> Today, 2:45 PM | e259168e28b236f69d0fbc7a0b7cb24 | Flexus | Active | View Edit |
| <input type="checkbox"/> Nov 20, 2015, 10:34 AM | d4c32bda54662d63ffb2a4351d818784 | System | Active | View Edit |
| <input type="checkbox"/> Nov 19, 2015, 3:29 PM | adfadd4ca8843766153b182c224f9ab | System | Not active | View Edit |

20 per page 0-3 of 3 < >

Administration > System Configuration > Encryption

Encrypt Key

[Export Key](#) [Edit Key](#) [Delete Key](#)

Fingerprint: d4c32bda54662d63ffb2a4351d818784
Created: Nov 20, 2015, 10:34 AM
Tenant: System
Status: **Active**
Key length: 2048 bits
Public Key: MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArz3nFvt26gv0v4es3y7SKfnA621BEBE3s2v1vphjJ/ouZHYU6e99eh+CVN2ku6Ycn3hy6/LuR54KtNcoXghIe++4HSEPLIt3xJLxj356bcaud48d6kr-bedqkqW7s1T8BUEK4ocK97/193103JfFczmeTqzvmUC46L23kzhgurlNL8pX11gpkzjyCC2kFvclCooNtOm=1IZcvr+u8f73JCsmc5LE5ldoDRm8f718H7J04=ms5B78khp536d8H1T3Yoy1a9Ks+f4VkyQ13scxVzmp4oVf/xTeLhdaY0pE310d8kxy56nd5DgI8ayzcXD7K13CW1S2QIDAQAB

Authorized Users [Unauthorized Users](#)

Search by Text: [Search](#)

[Revoke access](#) 0-2 of 2 < >

| NAME | WEB LOGIN | ENCRYPT ACCESS STATUS | |
|--|---------------|-----------------------|----------------------|
| <input type="checkbox"/> admin | admin | Authorized | Edit |
| <input type="checkbox"/> David Cummins | david.cummins | Authorized | Edit |

20 per page 0-2 of 2 < >

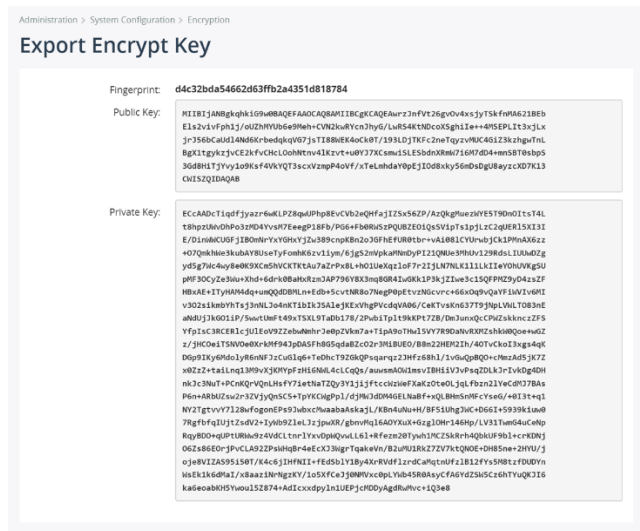
Administration > System Configuration > Encryption

Export Encrypt Key

Password (recommended):
strong

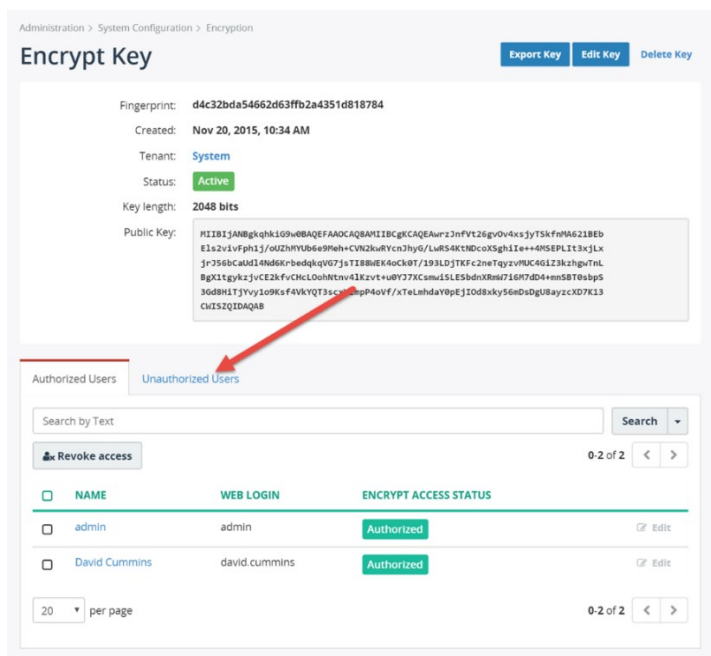
If specified, the private encryption key will be protected with a password

[Export](#)



4. Grant Access to Encryption Key

Navigate to **File Encryption**, select the appropriate key and authorize users to access the data encrypted with the same key. Administrators need to grant particular users the access to encryption key(s) before they can play back (decrypt) audio files. Note, the administrator may grant access only to those encryption keys which are granted to him/her. If administrator (even if he/she has role "Root administrator") has no access to the encryption key, then he/she cannot grant access to other users for the same key. Call Recording software never stores encryption keys in the database in plain text for security reasons. Even if an unauthorized party gains access to database files, he/she could not retrieve the private keys because they are stored in encrypted format. There is no way to gain user's private key without knowing the user's password.



Administration > System Configuration > Encryption

Encrypt Key

Export Key Edit Key Delete Key

Fingerprint: d4c32bda54662d63ffb2a4351d818784
 Created: Nov 20, 2015, 10:34 AM
 Tenant: System
 Status: Active
 Key length: 2048 bits
 Public Key: M1IB1JANgkqhki69h0BBAQEFAAOCQAQIIBICgKCAQEAvuz3nFY128gv0v4xx3yTSMf0MA6218EB
 E1a2v1Vfph1j/0UZNYU6e9Ph+hCVN2ku8Ycn2hy6/LuR54KXNDcoX5ghIe++4MSEPLI3xjLx
 J7356bcu0J4N68KrbodqkqV73tI8B8K6cK07/193LDTKFczne7qyzvMOC46123kzhgufnL
 8g121gkxjJcC2kFCkCL0o0hntv1kzcvf40P73JCmwaJSLF5h0b08h0718H7J044m587F0h3p5
 3Gd8HL1Yvy1oRkx4FvLYQT3ccvZmp4uVf/xTeLhhdAybpE1IOdRky56nd0g08ayzcX07k13
 CUISZQIDAQAB

Authorized Users Unauth. Users

Search by Text Search

Grant access 2 items selected 0-4 of 4

| NAME | WEB LOGIN | ENCRYPT ACCESS STATUS |
|---|---------------|-------------------------|
| Administrator | Administrator | LDAP auth not supported |
| <input checked="" type="checkbox"/> John Smith | john.smith | Unauthorized |
| <input checked="" type="checkbox"/> Marry Smith | marry.smith | Unauthorized |
| <input type="checkbox"/> REST API user | apiuser | Unauthorized |

20 per page 0-4 of 4

5. Enable File Encryption

If authorized - Navigate to **Administration > Storage > File encryption** and click "Edit configuration**" to enable encryption for all data.

Administration > System Configuration

Encryption

Audio files encryption: Enabled Edit configuration

Caution! Above setting applies to system account only. Edit tenant's configuration

Encryption keys

Select a Tenant Search by Key Fingerprint Search

+ Add Encrypt Key x Delete Encrypt Key 0-3 of 3

| CREATED | FINGERPRINT | TENANT | STATUS |
|------------------------|----------------------------------|--------|------------|
| Today, 2:45 PM | e259168e28b236fef9d0f8c7a0b7cb24 | Flexus | Active |
| Nov 20, 2015, 10:34 AM | d4c32bda54662d63ffb2a4351d818784 | System | Active |
| Nov 19, 2015, 3:29 PM | adfadd4ca8843766153b182c224ff9ab | System | Not active |

20 per page 0-3 of 3

Administration > System Configuration > Encryption

Edit Encryption Settings

Audio files encryption * Enable encryption

Save

6. Export of the Encrypted Files

An important aspect of any file encryption facility's design is that file data is never available in unencrypted form except to users that access the file via the encryption facility. This restriction particularly affects backup process when data is exported to external storage. Call Recording addresses this problem by keeping files in encrypted form during backup process. The backup utility don't have to be able to decrypt file data before backup. It is safe to export encrypted files to backup archive. The backup archive may be imported back to the same system or to new system during recovery process. When importing data to new system, it is necessary to [import old encryption key](#) as well.

Storage Limits/Usage

Click on **Storage Limits/Usage** to review information about the current settings for audio and (where in use) screen recordings. Management is performed at the root level. Contact LOGIX for assistance.

The screenshot displays the 'Administration' section of the Call Recording Portal Administrator. The navigation menu on the left includes 'User Management', 'User Authentication', 'Storage', 'Customization', 'Screen Recording', and 'Audit Trail'. The 'Storage' menu is expanded, showing 'File Encryption' and 'Storage Limits/Usage', with the latter being selected. The main content area shows the 'Storage Limits/Usage' configuration page. The breadcrumb trail is 'Administration > Storage > Storage Limits/Usage'. The page title is 'Storage usage'. The 'Storage Limits' status is 'Enabled'. Below this, there are two sections: 'AUDIO RECORDINGS' and 'SCREEN RECORDINGS'. Both sections show 'Storage usage: No recordings' and 'Storage limits: - / - / 30 days'. A yellow notification banner at the bottom of each section states 'Usage info is updated less than a minute ago'.

User Authentication

This area in Administration allows authorized Admins to review the current User Web Sessions and terminate a session as needed.

The screenshot shows the 'User Web Sessions' page within the 'Administration' section. The breadcrumb trail is 'Administration > User Authentication'. The page title is 'User Web Sessions'. There is a search bar labeled 'Search by User, Login, Ip-address' with a 'Search' button. Below the search bar is a 'Terminate' button and a pagination indicator '0-1 of 1'. A table lists the sessions with columns for 'USER', 'LOGIN', 'IP-ADDRESS', and 'SESSION START TIME'. One session is listed for 'Smith - [2...7]' with a login of '2f...' and IP address '184.91.120.143', starting on 'Jul 30, 2021, 1:56 PM (6 minutes ago)'. A 'View' link is next to the session. At the bottom, there is a '20 per page' dropdown and another '0-1 of 1' pagination indicator.

Customization

Click on **Customization** in the Administration section to view information about Field Visibility, Custom Fields, and (if in use) the Evaluate add-on Evaluation Form Designer.

The screenshot shows the 'Customization' page within the 'Administration' section. The breadcrumb trail is 'Administration'. The page title is 'Customization'. There are three main sections: 'FIELD VISIBILITY' with the description 'Configuration of field visibility on different pages like call recordings list, user list etc.' and a 'View details' button; 'CUSTOM FIELDS' with the description 'Configuration of custom fields' and a 'View details' button; and 'EVALUATION FORM DESIGNER' with the description 'Designer of agent evaluation forms' and a 'View details' button. The left sidebar shows the 'Customization' menu item selected.

Field Visibility

Click On the View Details button (or the *Field Visibility* left menu option) to open the list of fields shown in each view within Call Recording. The tools here allow an authorized Admin to define which fields are visible in the layout and what columns display in each view.

The screenshot shows the 'Field visibility' configuration page. On the left, the 'Customization' menu is open, and 'Field Visibility' is highlighted. The main area displays a table of views with their respective visible columns and an 'Edit' button for each. The 'Edit' button for the 'Recordings - All Calls' view is circled in red.

| LAYOUT | VISIBLE COLUMNS | Action |
|-----------------------------------|--|--------|
| Recordings - All Calls | User Date Time Duration From To Tags | Edit |
| Recordings - My Calls | Date Time Duration From To Tags | Edit |
| Recordings - Active Calls | User Date Time Duration From To Timeline | Edit |
| Recordings - By User | Date Time Duration From To Tags | Edit |
| Recordings - By Client | Client Date Time Duration From To | Edit |
| Recordings - By Tag | User Date Time Duration From To Tags | Edit |
| Recordings - Not assigned to user | Date Time Duration From To | Edit |
| Recordings - Advanced Search | Date Time Duration From To | Edit |
| Recordings - Interaction | Time Duration From -> To | Edit |
| Recordings - By Keywords Category | User Date Time Duration From To Topics Topic.Total Score | Edit |

1. Click **Edit** next to a Layout in the list to review all possible fields/columns for the selected view.
2. Click **Hide** on an item to remove and click **Show** on an item to make the item visible in the view.
3. Click **Save** when finished to update the selected view. Repeat as necessary for other views.

Custom Fields

Authorized Administrators may create special fields that can be used to add more information or identify calls for reporting or in searches.

Go to **Administration > Customization > Custom Fields**.

Click on the View Details button under Custom Fields to open the Custom Fields dialog. This area allows the Admin to Search and Edit any Custom fields already created, Add Custom Fields, and Delete Custom Fields.

The screenshot shows the 'CUSTOM FIELDS' configuration page. It displays the title 'CUSTOM FIELDS' and the subtitle 'Configuration of custom fields'. A 'View details' button is visible, with a mouse cursor pointing to it.

The screenshot shows the 'Custom Fields' dialog. It features a search bar with the text 'Search by Name' and a 'Search' button. Below the search bar are '+ Add' and 'x Delete' buttons. The main area shows a table with columns 'NAME' and 'TYPE', and the text 'No results found'.

To Add a Custom Field

While viewing Custom Fields

1. Click + **Add**.
2. Enter or select the following:

- ❖ **Name** – Required.
- ❖ **Description** - Optional
- ❖ **Field Type** – Choose from the following:
 - **Text:** Provide a text field for data entry.
 - **Date:** Allows entry or selection of a date.
 - **Option:** Opens fields to type one or more options that can be selected when this field is in view. Click on Add Option to create multiple options.

Administration > Customization > Custom Fields

Add Custom Field

Name *

Description

Field type Text
 Date
 Option

Field length *

Editable Authorized users can edit values of this field

Allow search Advanced search
 Free text search (for Text only)

Save

- ❖ **Field length** – Enter the number of characters and spaces allowed for the field.
- ❖ **Editable** – Click to enable if you wish to have Authorized users edit the field.
- ❖ **Allow Search:** Options here that can be enabled include adding the field as a filter in Advanced Searches and allowing the use of free text searches of the field entries.

3. Click **Save** when finished.

To Edit a Custom Field

When a Custom Field has been created it may be edited by authorized Admins.

Click the **Edit** link next to the desired field, make changes to the text or settings, and click **Save**.

To Delete a Custom Field

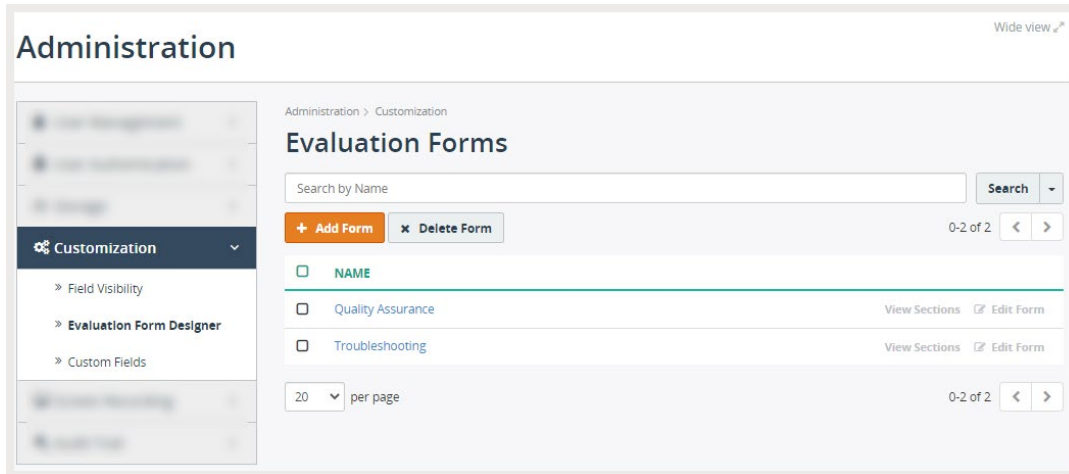
Click to place a check in the box next to a Custom Field in the list to select it and click **Delete**.

Note: This action is immediate, however the system offers the option to Undo.

Evaluate Form Designer

Authorized Administrators (or supervisors) may have access to add and manage the Evaluate forms used when evaluating agents' call recordings for performance evaluations and call quality assurance.

Note: Evaluate is an add-on license that must be assigned to each agent/user who will be evaluated.



Add Form

Click on **Add Form** button to create a new evaluation form. And then use the Edit tools to create sections with questions and answers, set the way it will display when used, define scores for each question (totaling 100% for all) and **Save**.

More tools may be available (authorization required) and can include:

View Sections – Click this button adjacent to the desired listing to review or edit each form section.

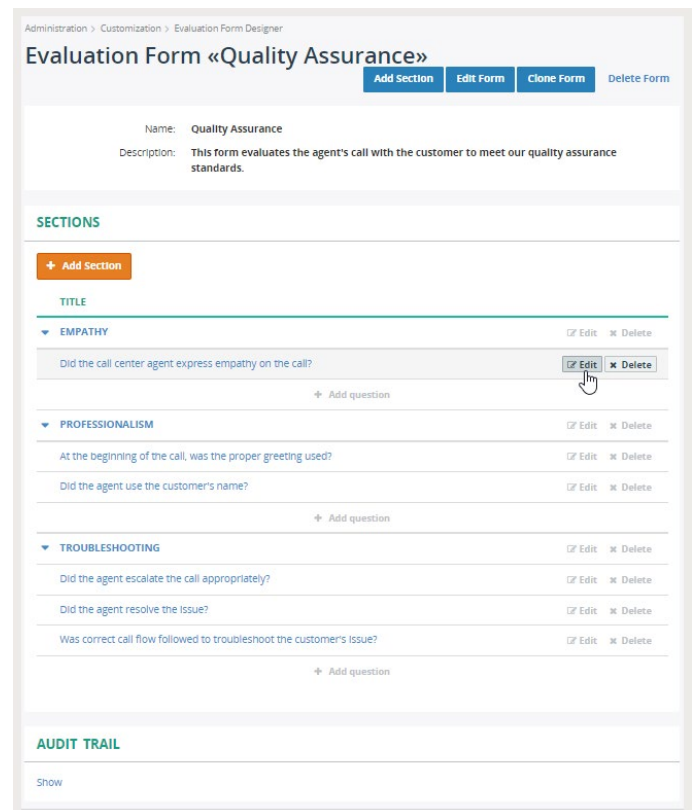
Add Section – Allows the Admin to create additional sections and the questions used in the evaluation.

Edit Form – Click this button to open the Edit dialog and modify the form as needed. Click Save when finished.

Clone Form – Click this button to use the current form as a template for creating another. Modify to give it a unique name, redefine or add sections, adjust scoring as desired, and click Save when finished.

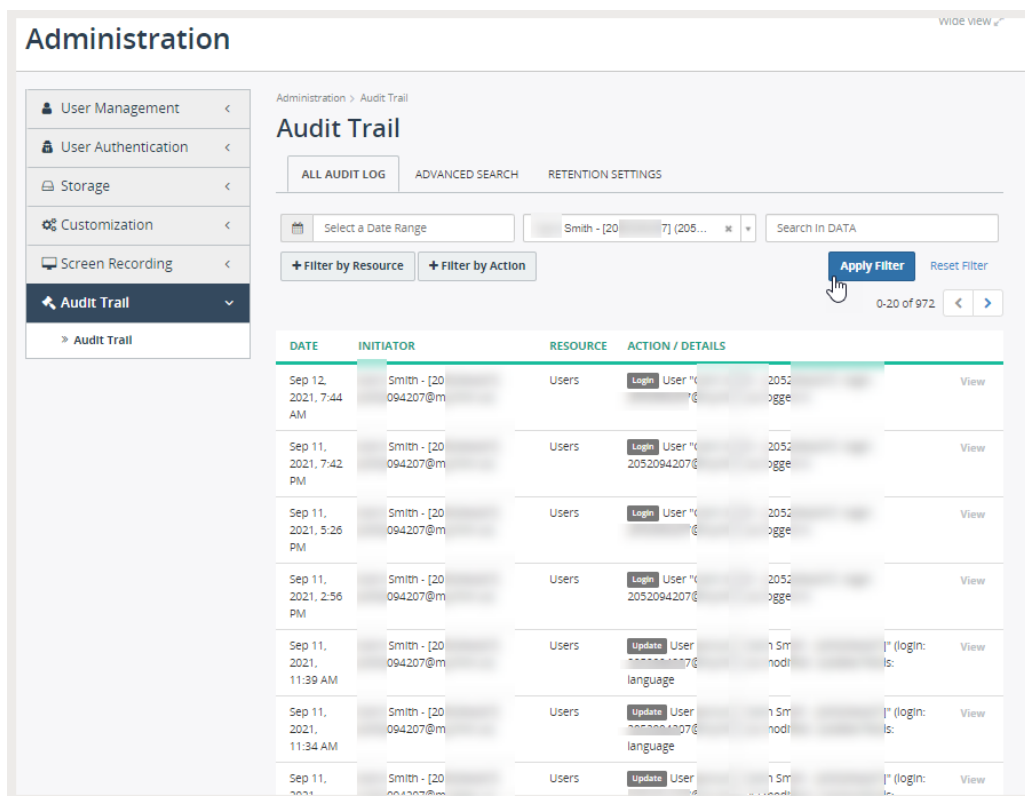
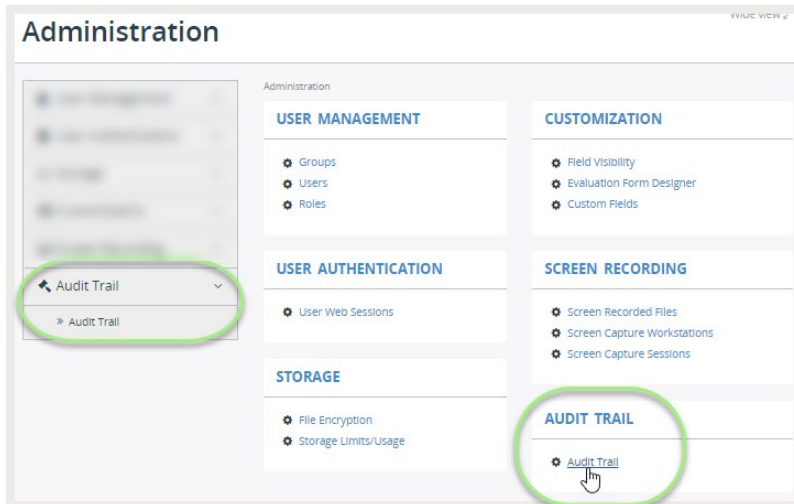
Delete Form – Click within the check box next to an item in the list to select it and click Delete Form. This action is immediate; however the system offers an Undo option.

Audit Trail – Click to see the latest information about edits to or creation of Evaluation forms.



Audit Trail

Authorized Admins may click on the link under the Audit Trail menu option to review or manage portal activity.



Tabs across the top of the Audit Trail dialog offer access to the full Audit log of activity, Advanced Search tools, and (where authorized to view) the Retention Settings (Service Provider access).

The list may be filtered or searched, and each listing may be reviewed in more detail using the adjacent [View](#) link (far-right on an individual line in the table).

Opening a single listing displays the access information, along with the User's ID and basic profile data, the activity, and the areas or tools that were accessed. Links to other views, such as the User's Profile are provided here as well.

The Related Records section offers a link to review similar access patterns, as well.

Administration

Wide view ²

- [Administration](#)
- [Audit Trail](#)
- [Audit Trail](#)

Administration > Audit Trail > Audit Trail

Action «Login»

Time: **Sep 11, 2021, 7:42:01 PM**

Initiator: **Smith - [2052094207]**

Client ip-address: **10.10.10.10**

Application: **web**

Resource: **Users**

Action: **Login**

Related To: **User [redacted] (view)**

Details: **User [redacted] logged in**

| FIELD | VALUE |
|---------|--------------------------------|
| login | [redacted] |
| message | |
| name | h - [redacted] |
| user_id | 7c5e [redacted]-005 [redacted] |

RELATED RECORDS

| DATE | INITIATOR | RESOURCE | ACTION / DETAILS |
|------------------------|-----------------------------------|-------------------|--|
| Sep 12, 2021, 7:44 AM | [redacted] - [2052094207]@mytm.us | Users | Login User [redacted] (login: [redacted]) View |
| Sep 11, 2021, 5:26 PM | [redacted] - [2052094207]@mytm.us | Users | Login User "C [redacted]" (login: [redacted]) View |
| Sep 11, 2021, 2:56 PM | [redacted] - [2052094207]@mytm.us | Users | Login User "C [redacted]" (login: [redacted]) View |
| Sep 11, 2021, 11:39 AM | [redacted] - [2052094207]@mytm.us | Users | Update User [redacted] (logged in: [redacted]) fields: language Updated View |
| Sep 11, 2021, 11:33 AM | [redacted] - [2052094207]@mytm.us | Users | Login User "C [redacted]" (login: [redacted]) View |
| Sep 11, 2021, 7:12 AM | [redacted] - [2052094207]@mytm.us | Users | Login User "C [redacted]" (login: [redacted]) View |
| Sep 10, 2021, 1:58 PM | [redacted] - [2052094207]@mytm.us | User auth devices | Create User " [redacted]" logged in View |
| Sep 10, 2021, 1:58 PM | [redacted] - [2052094207]@mytm.us | Users | Login User "C [redacted]" (login: [redacted]) View |
| Sep 10, 2021, 9:27 AM | [redacted] - [2052094207]@mytm.us | User auth devices | Create User " [redacted]" logged in View |
| Sep 10, 2021, 8:29 AM | [redacted] - [2052094207]@mytm.us | User auth devices | Create User " [redacted]" logged in View |
| Sep 10, 2021, 8:23 AM | [redacted] - [2052094207]@mytm.us | User auth devices | Create User " [redacted]" logged in View |
| Sep 10, 2021, 7:31 AM | [redacted] - [2052094207]@mytm.us | Users | Update User [redacted] (logged in: [redacted]) field: [redacted] Updated View |
| Sep 10, 2021, 7:31 AM | [redacted] - [2052094207]@mytm.us | User auth devices | Create User " [redacted]" logged in View |
| Sep 10, 2021, 7:31 AM | [redacted] - [2052094207]@mytm.us | Users | Login User "C [redacted]" (login: [redacted]) View |
| Sep 9, 2021, 1:25 PM | [redacted] - [2052094207]@mytm.us | User auth devices | Create User " [redacted]" logged in View |
| Sep 9, 2021, 1:25 PM | [redacted] - [2052094207]@mytm.us | Users | Login User "C [redacted]" (login: [redacted]) View |

20 per page 0-20 of 66

Speech Analytics

How it works - Speech Analytics

Where licensed, enabled and implemented:

Call Recording automatically uploads audio files to the Google Cloud Speech service for transcription. Once transcription is completed, the results are shown in the call details view.

The screenshot below shows the transcription in a textual representation of the conversation below the audio representation.

When you play back the recording, the transcript is automatically highlighted at that position (see the yellow background in the following screenshot). Click on any word in the transcription and the audio player will fast forwarded to that location.

MEDIA PLAYER Switch to basic player | Wide view ↗

0 | 10 | 20 | 30 | 40 | 50 | 60 | 1:10 | 1:20 | 1:30 | 1:40 | 1:50 | 2:00 | 2:10 | 2:20 | 2:30 | 2:40 | 2:50 | 3:00 | 3:10 | 3:20 | 3:30 | 3:40 | 3:50 | 4:00 | 4:10

|| Pause ⬇ Save audio file

TRANSCRIPT

Side 1 [0:00]: Lesley

Side 2 [0:00]: Looks good .

Side 1 [0:01]: thank you for holding . I do apologize for the wait . We have this new tool that I'm trying to do a search and to find more information about the lamp itself , and I'm not quite sure how to use it yet , so I'm kind of experimenting with it here that I can find the information that we're looking for but supposedly it has the information we're looking for so bear .

Side 2 [0:25]: Well , okay cool now . I'm fine **I'm calling at lunch . You're fine**

Side 1 [0:29]: Bear with me here , and hopefully we'll be able to find out the information .

Side 2 [0:34]: Okay , terrific .

Side 1 [0:35]: Maybe I need to do a test okay . There's a lamp for came up .
Alright .

You can use "Advanced Search" page to locate recording with a particular keyword or transcription text.

CALLS MY CALLS BY USER NOT ASSIGNED TO USER BY CATEGORY **ADVANCED SEARCH**

Transcript Includes This call may be monitored

+ Add criteria

Run Search Save Search

No auto-refresh Categories Download Delete More

0-3 of 3

| <input type="checkbox"/> | DATE | TIME | DURATION | FROM | TO |
|--------------------------|--------------|----------|----------|------------|--------------|
| <input type="checkbox"/> | Apr 20, 2017 | 12:58 PM | 0:21 | 1210HIDDEN | +14086081250 |
| <input type="checkbox"/> | Apr 11, 2017 | 4:20 PM | 0:21 | 5281HIDDEN | +14086081250 |

Set up Google Cloud Speech API

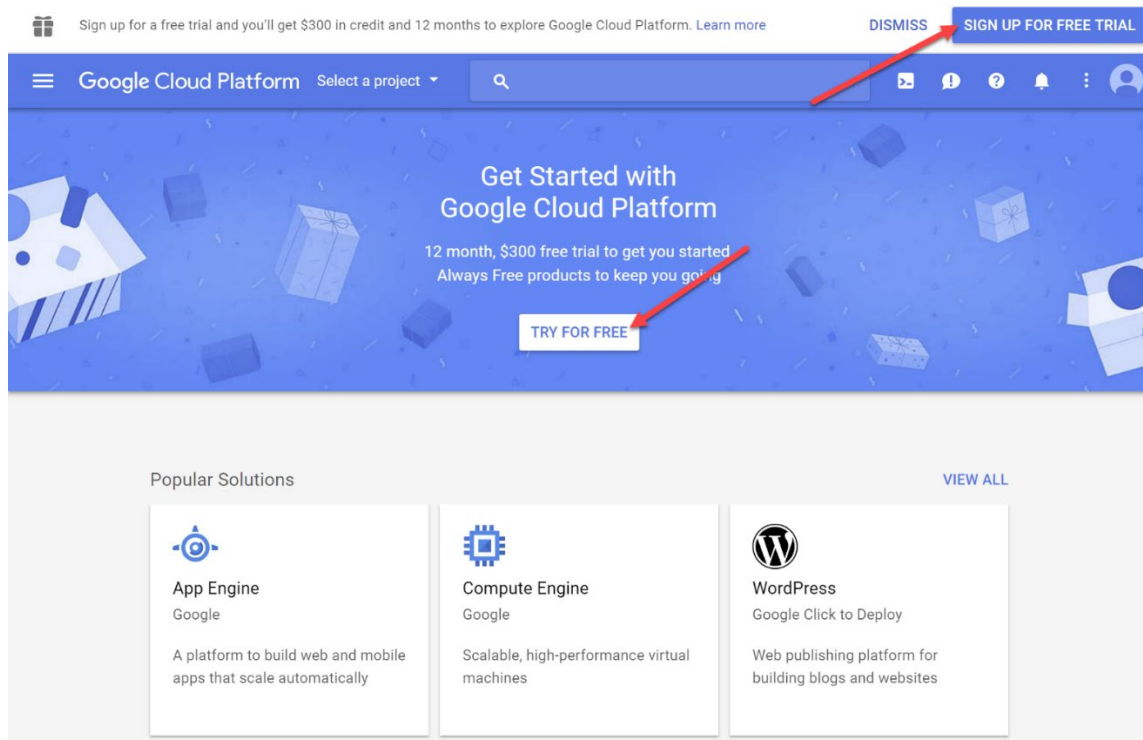
This section provides step-by-step instruction for configuring the **Google Cloud Speech API**, a speech to text conversion powered by machine learning.

Call Recording uses the [Google Cloud Speech API](#) to transcribe voice recordings to text. A transcribed text is used further for speech analytics in Call Recording application.

The Google Speech API recognizes over 110 languages and variants. Call Recording application automatically upload audio to Google Cloud for transcription and retrieves the results back into the application.

A. Create a Google Cloud Platform account

1. [Sign in](#) to your Google account. If you don't already have one, [sign up for a new account](#).
2. Open **GCP Console** at console.cloud.google.com
3. If you were not using Google Cloud Platform before, then click **Sign up for a free trial** button in the top of page or **Try for free** in the middle of screen.





Try Cloud Platform for free Google

Country

United States

Acceptances

Please email me updates regarding feature announcements, performance suggestions, feedback surveys and special offers.

Yes No

I have read and agree to the [Google Cloud Platform Free Trial Terms of Service](#).
Required to continue

Yes No

Agree and continue

- Access to all Cloud Platform Products**
Get everything you need to build and run your apps, websites and services, including Firebase and the Google Maps API.
- \$300 credit for free**
Sign up and get \$300 to spend on Google Cloud Platform over the next 12 months.
- No autocharge after free trial ends**
We ask you for your credit card to make sure you are not a robot. You won't be charged unless you manually upgrade to a paid account.

4. Provide **Customer info** (address, primary contact and payment method / credit card or bank account).



Try Cloud Platform for free Google

Customer info

Account type
Business

Name and address

Primary contact

- Access to all Cloud Platform Products**
Get everything you need to build and run your apps, websites and services, including Firebase and the Google Maps API.
- \$300 credit for free**
Sign up and get \$300 to spend on Google Cloud Platform over the next 12 months.
- No autocharge after free trial ends**
We ask you for your credit card to make sure you are not a robot. You won't be charged unless you manually upgrade to a paid account.

How you pay

Automatic payments

You pay for this service only after you accrue costs, via an automatic charge when you reach your billing threshold or 30 days after your last automatic payment, whichever comes first.

Payment method ⓘ

Add credit or debit card

Card number MM YY CVC

#

Cardholder name

Credit or debit card address is same as above

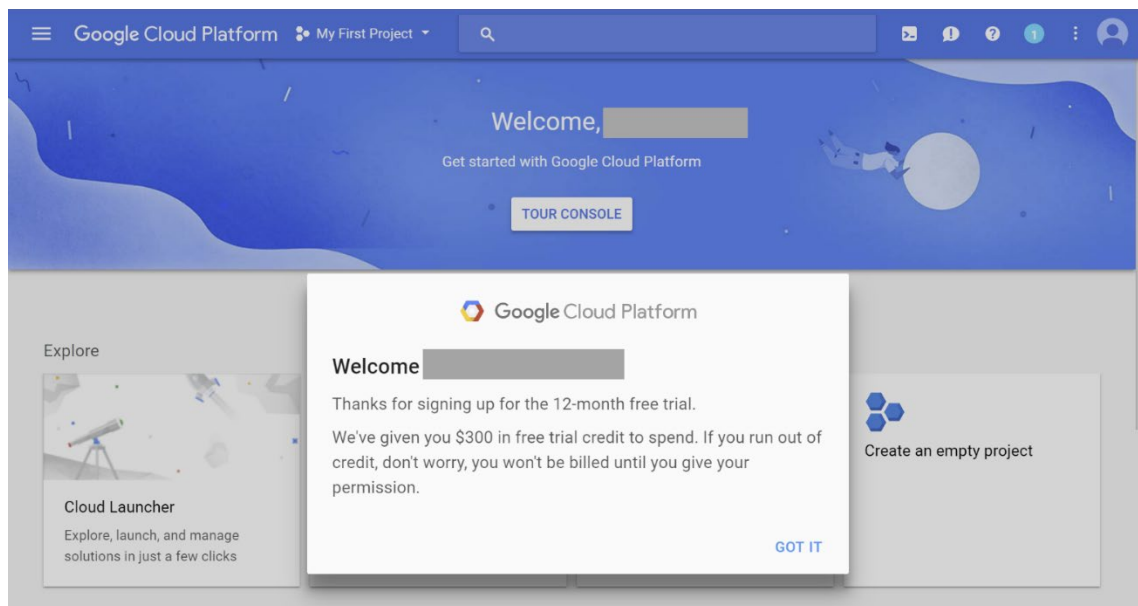
[Start my free trial](#)

Access to all Cloud Platform Products
Get everything you need to build and run your apps, websites and services, including Firebase and the Google Maps API.

\$300 credit for free
Sign up and get \$300 to spend on Google Cloud Platform over the next 12 months.

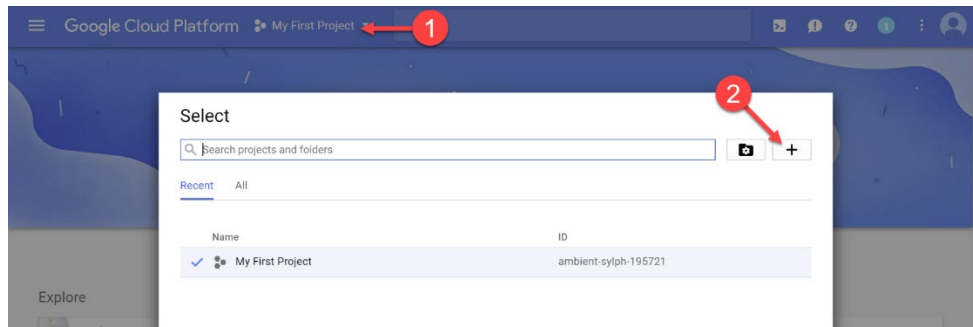
No autocharge after free trial ends
We ask you for your credit card to make sure you are not a robot. You won't be charged unless you manually upgrade to a paid account.

- The **Welcome screen** is displayed when account is activated.



B. Create New Project

- Create new project by clicking on **My First Project** in the top menu and then clicking + button.



2. Choose the name for the project. In our example, we choose Call Recording-speech-analytics. Note the **Project ID** for your project. Google requires the project ID to be a globally unique identifier.

New Project

i You have 11 projects remaining in your quota. [Learn more.](#)

Project name ?

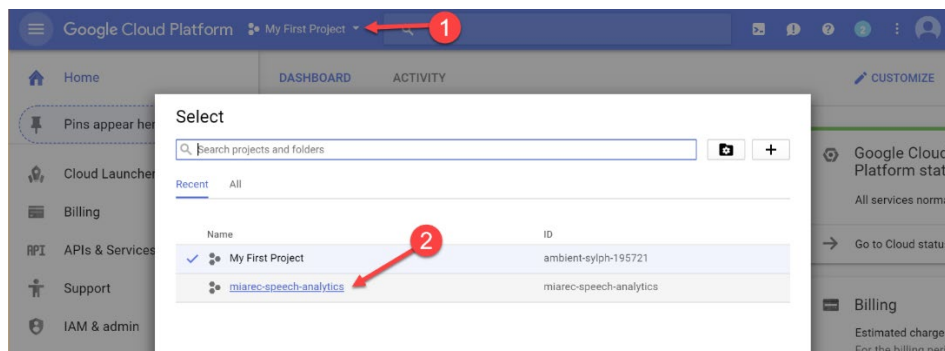
miarec-speech-analytics

Your project ID will be miarec-speech-analytics ? [Edit](#)

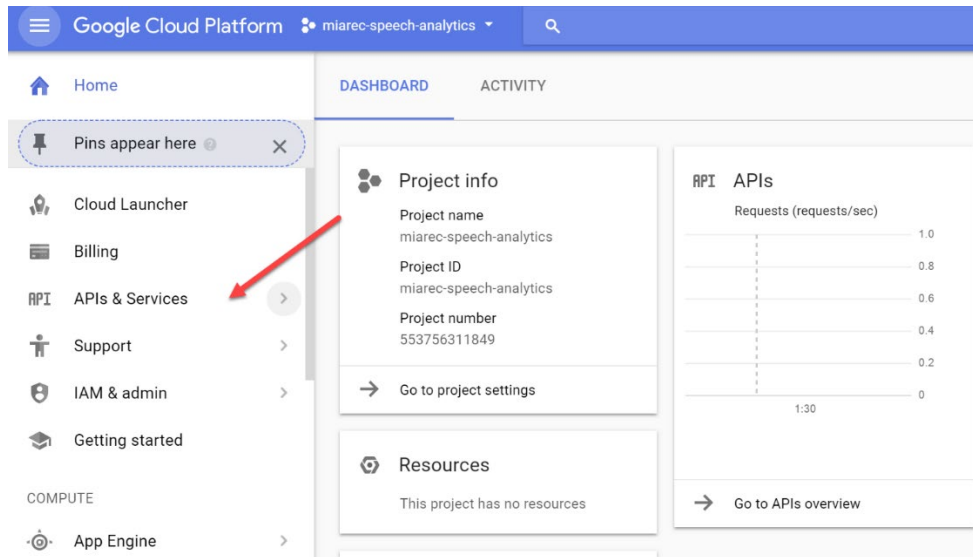
Create **Cancel**

C. Enable Google Cloud Speech API for your project

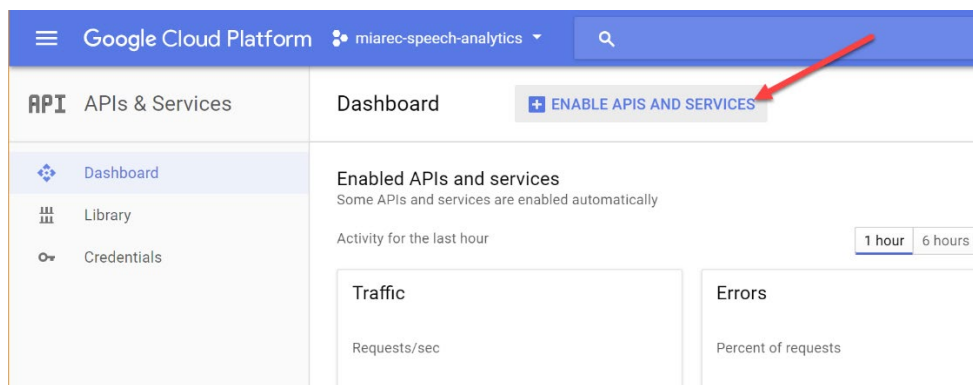
1. Select the newly created project from the list.



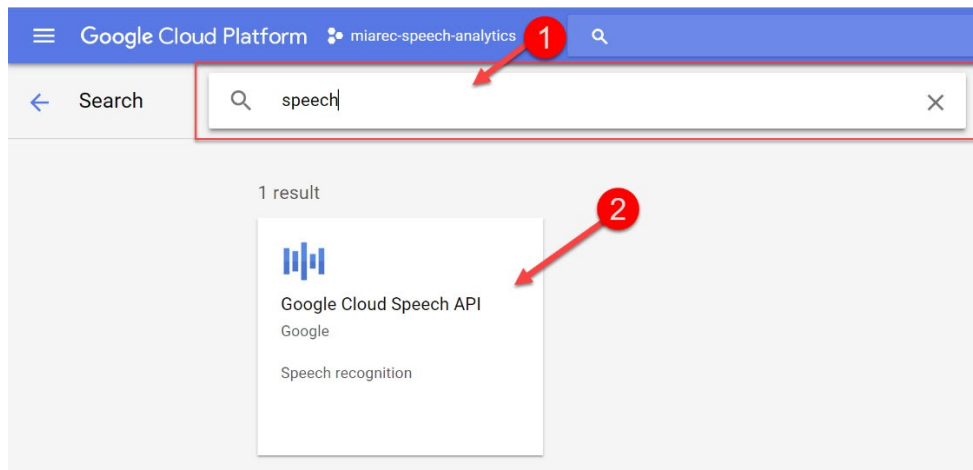
2. Navigate to **APIs & Services**.



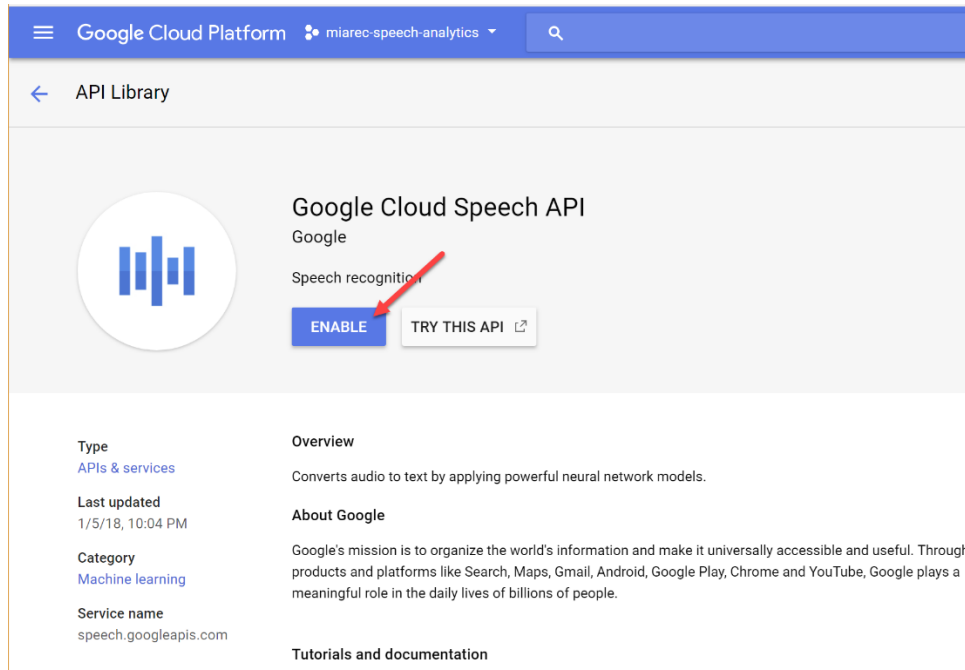
3. Click **Enable APIs and Services**



4. Type **speech** in the **Search box** to and click on **Google Cloud Speech API**

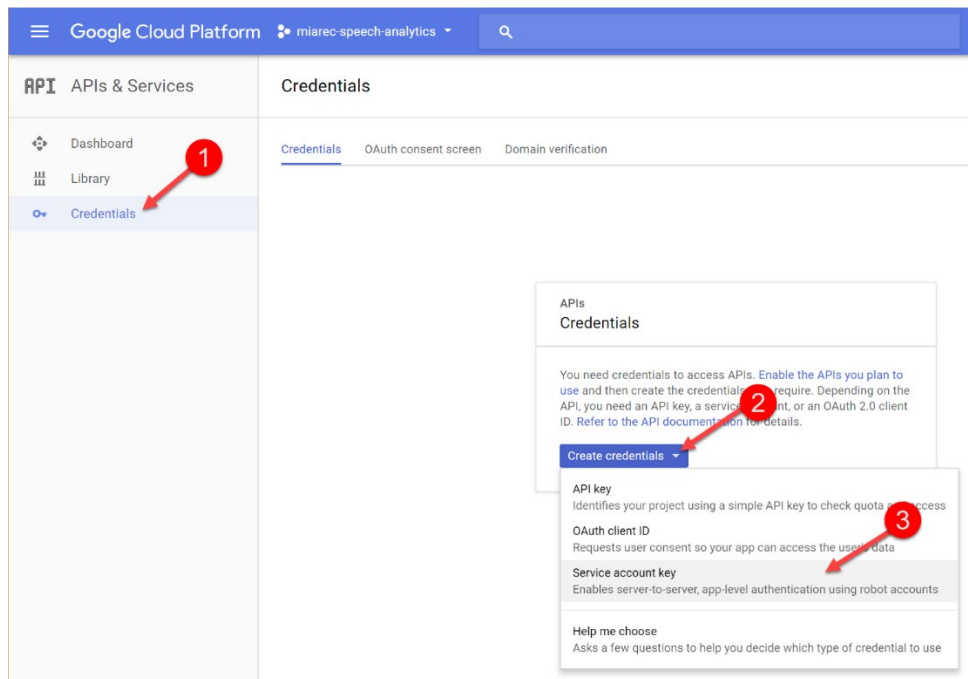


5. Click **Enable** button for **Google Cloud Speech API**



D. Create a Service Account Key

1. Navigate to **Credentials** in the left pane and click **Create credentials** button. Choose **Service account key** from the drop-down menu.



2. Choose the **Service account name** and set **Role** to **Project > Owner** and click **Create** button.

← Create service account key

Service account

New service account

Service account name [?] miarec

Role [?] Owner

Service account ID
miarec @miarec-speech-analytics.iam.gserviceaccount.com

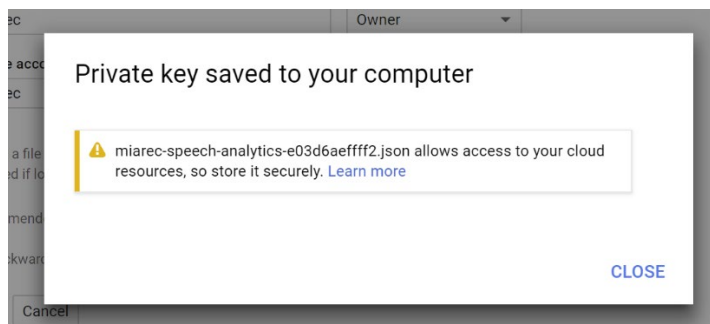
Key type
Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

JSON
Recommended

P12
For backward compatibility with code using the P12 format

Create Cancel

1. Save the **JSON** file to secure place. You will need to import this file into Call Recording application.



JSON file looks like (the private key is stored in the private_key attribute):{

```
"type": "service_account",
"project_id": "Call Recording-speech-analytics",
"private_key_id": "123456789f276ed94a5bd2a11ee645678945679",
"private_key": "-----BEGIN PRIVATE KEY-----\nMIIEvAIBA... "client_email": "Call
Recording@Call Recording-speech-
analytics.iam.gserviceaccount.com",
"client_id": "12345678945678945613",
"auth_uri": "https://accounts.google.com/o/oauth2/auth", "token_uri":
"https://accounts.google.com/o/oauth2/token", "auth_provider_x509_cert_url":
"https://www.googleapis.com/oauth2/v1/certs",
```

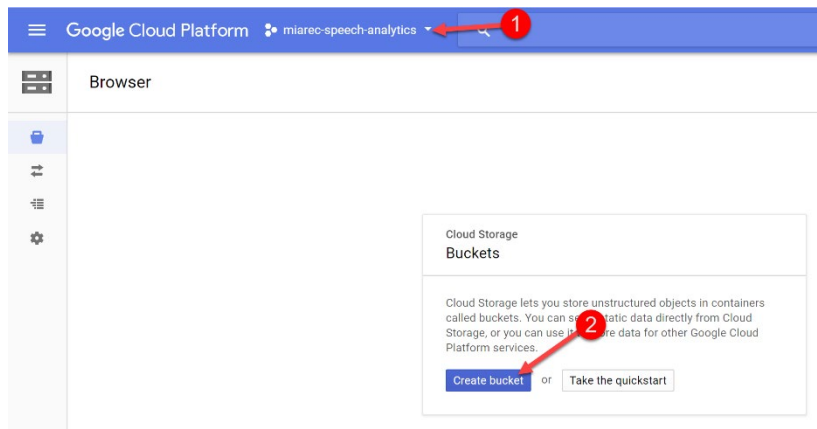
```
"client_x509_cert_url":  
"https://www.googleapis.com/robot/v1/metadata/x509/Call Recording%40Call Recording-speech-  
analytics.iam.gserviceaccount.com"  
}
```

E. Create Google Cloud Storage Bucket

This guide provides step-by-step instructions for configuring Google Cloud Storage bucket. Call Recording needs to upload the audio file to Google Cloud Storage bucket before it is submitted to the Speech API service for transcription.

1. Create Bucket

1. Navigate to Google Cloud Storage console at <https://console.cloud.google.com/storage>
2. Make sure the previously created project is selected. Then click **Create bucket**.



3. Choose a globally unique name for the bucket, set **Default storage class** to **Regional** and choose a region closer to your datacenter (in our example, we choose **us-west1**).

← Create a bucket

Name [?]
Must be unique across Cloud Storage. **Privacy:** Do not include sensitive information in your bucket name. Others can discover your bucket name if it matches a name they're trying to use.

Default storage class [?]

Multi-Regional
Use to stream videos and host hot web content.
Best for data accessed frequently around the world.

Regional
Use to store data and run data analytics.
Best for data accessed frequently in one part of the world.

Nearline
Use to store rarely accessed documents.
Best for data accessed less than once per month.

Coldline
Use to store very rarely accessed documents.
Best for data accessed less than once per year.

Regional location
Redundant within a single region.

Specify labels

2. Create Lifecycle Rule

The Cloud Storage bucket is used only for a temporary storage of audio files. Call Recording application uploads the files to this bucket and instructs the Speech API to take the file from there for transcription. Once the transcription is completed, the file can be deleted from the bucket.

In this step, we will configure automatic deletion of audio files after 24 hours.

1. In the browser page, click on **None** in the **Lifecycle** column for the previously created bucket

| Name | Default storage class [?] | Location | Lifecycle [?] | Labels [?] |
|--|------------------------------------|----------|------------------------|---------------------|
| <input type="checkbox"/> miarec-speech | Regional | US-WEST1 | None | |

2. In the new window, click **Add rule**

[←](#) View object lifecycle rules

miarec-speech

Lifecycle rules apply to all objects in a bucket. If an object meets the conditions for multiple rules, only one action will be taken, with the following priorities:

- Deletion will always take place over a change in storage class
- A change in storage class will always go to Coldline if a change to Nearline has also been set

[Add rule](#) [Delete all](#)

Rules

You haven't added any lifecycle rules to this bucket.

3. Select **Object condition** to **Age 1 days** and **Action** to **Delete**. Click **Continue** buttons and then **Save**

[←](#) Add object lifecycle rule

miarec-speech

After you add or edit a rule, it may take up to 24 hours to take effect.

1 Select object conditions [^](#)

The action will be triggered when all selected conditions are met.

Age
All objects this age or older.
 days

- Creation date
- Storage class
- Newer versions
- Live state

[Continue](#)

2 Select action [^](#)

- Set to Nearline
- Set to Coldline
- Delete

Call Recording Configuration

1. Configure Audio File Format

First, you need to change the audio file format settings to increase transcription accuracy. Navigate to **Administration > Storage > File format** and apply the following changes:

- Set **WAV** file format
- Set **Stereo** format
- Disable **Automatic Gain Control (AGC) filter**
- Disable **Packet Loss Concealment (PLC) filter**

Administration > Storage > File Format

Edit File Format Settings

File format * WAV MP3

Audio format * Mono Stereo

AGC * Enable Automatic Gain Control (AGC) Filter
AGC automatically normalizes volume levels between two audio channels

AGC maximum gain level *
Limit the maximum possible amplification level. It is necessary to prevent situations, when a slight noise is amplified to high volume level. Default is 3.0

PLC * Enable Packet Loss Concealment (PLC) filter
PLC filters improves audio quality when there is a slight packet loss (less than 5%). Without PLC filter there would be noticeable crops inside recorded audio

MP3 bitrate * 8 kbps 16 kbps 24 kbps 32 kbps 64 kbps
Bitrate in kilobits per second (kbps) per each audio channel and per each 8000Hz of sample rate. For example, if audio file is stereo (2 channels) and sample rate is 16000 Hz (twice bigger than normal 8000 Hz), then the final file bitrate will be x4 bigger than this setting. Default is 16

MP3 quality *
Quality and speed of MP3 compression algorithm. Default is 5

2. Configure Speech Recognition Job

The speech recognition job automatically uploads audio recordings to the cloud service for transcription and then retrieves back the transcription results. Multiple jobs can be created with unique settings, for example, one job processes recordings in English and the second in Spanish.

1. Navigate to **Administration > Speech Analytics > Speech-to-Text Jobs**, click "New Job".

Administration

Wide view

Administration > Speech Analytics

Speech-to-Text (Google)

[+ New Job](#) [x Delete](#) 0-0 of 0

| <input type="checkbox"/> | JOB NAME | STATUS | SCHEDULE | LATEST RUN |
|--------------------------|----------|--------|----------|------------|
| History is empty | | | | |

20 per page 0-0 of 0

- Choose a descriptive name for this job. Upload the Google Cloud Service Key JSON file, created in previous steps. Set the **Mode** to **Incremental**.

Add Job «Speech-to-Text (Google)»

Name *

Log file Write detailed log to file

Keep job history days

Access scope *

- Unrestricted - All tenants, including System
- Tenants only - All tenants, excluding System
- One tenant

Test only This is a test-drive. Write log file, but keep data untouched

Mode *

- Full
- Incremental

Service account key file miarec-spec...en_ben.json

Within the Google Cloud Platform Console, navigate to the "API Manager -> Credentials" and create service account key of JSON type. Check <https://cloud.google.com/speech/docs/common/auth> for detailed instructions

- Set **Language**.

Optionally, provide the **Phrase hints**. You may use these phrase hints in a few ways:

- Improve the accuracy for specific words and phrases that may tend to be overrepresented in your audio data. For example, if specific commands are typically spoken by the user, you can provide these as phrase hints. Such additional phrases may be particularly useful if the supplied audio contains noise or the contained speech is not very clear.
- Add additional words to the vocabulary of the recognition task. The Cloud Speech API includes a very large vocabulary. However, if proper names or domain-specific words are out-of-vocabulary, you can add them to the phrases provided to your requests's speechContext.

Phrases may be provided both as small groups of words or as single words. When provided as multi-word phrases, hints boost the probability of recognizing those words in sequence but also, to a lesser extent, boost the probability of recognizing portions of the phrase, including individual words.

In general, be sparing when providing speech context hints. Better recognition accuracy can be achieved by limiting phrases to only those expected to be spoken. For example, if there are multiple dialog states or device operating modes, provide only the hints that correspond to the current state, rather than always supplying hints for all possible states.

Language English (United States) ▼

Phrase Hints x

[Add phrase](#)

These phrases can boost the probability that such words or phrases will be recognized. In general, be sparing when providing speech context hints. Better recognition accuracy can be achieved by limiting phrases to only those expected to be spoken.

4. Specify **Filtering criteria** for recordings. For example, you can limit transcription to specific group, duration, date, etc.

FILTERING CRITERIA (OPTIONAL)

Group ▼ Is ▼ Sales Department x ▼

Duration ▼ Between ▼ 1:00 - 30:00 x

[+ Add criteria](#)

5. Configure a **Schedule** for transcription job. The job can be run either manually or by schedule (every hour/day/week or more often). In the example below, the transcription job will run every 2 minutes.

SCHEDULE

Run this job *

Manually
 Every Hour
 Every Day
 Every Week
 Custom (crontab)

Minute (0-59)

Hour (0-23)

Day (1-31)

Month (1-12)

Weekday (0-6)

3. View results

If you run the job manually, then you can see the progress of uploading process:

LATEST RESULTS

Stage: **Uploading..**

Progress: **50%**

Elapsed Time: **0:02**

Total recordings to upload: **2**

Uploaded successfully: **1**

Remaining: **1**

Skipped: **0**

[View statistics per day](#)

It takes some time for the cloud service to complete transcription and return results. Usually, the results are available in a couple of minutes after upload.

You can check the status of the recently uploaded files via menu **Administration > Speech Analytics > Speech Analytics Processed Records**.

After the status changes to "**COMPLETE**", you can view the call details and transcription by clicking "**View call**" right on this page. Or you can open the call details from "**Recordings**" page as usual.

Administration > Speech Analytics

Speech Analytics Processed Records

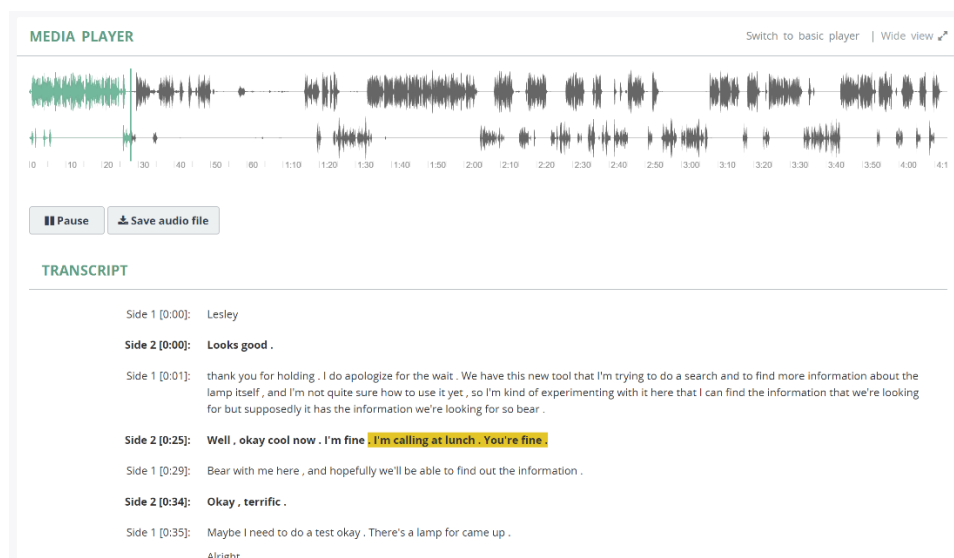
Select a Date Range Search a Text **Search** ▾

Delete 0-20 of 234 < >

| <input type="checkbox"/> | PROCESS TIME | STATUS | FROM: | TO: | |
|--------------------------|----------------|----------|---------------------------|--------------------------|---------------------------|
| <input type="checkbox"/> | Today, 4:45 PM | COMPLETE | +191 <input type="text"/> | 808 <input type="text"/> | View Call |
| <input type="checkbox"/> | Today, 4:45 PM | COMPLETE | +131 <input type="text"/> | 806 <input type="text"/> | View Call |
| <input type="checkbox"/> | Today, 4:45 PM | COMPLETE | 843 <input type="text"/> | 808 <input type="text"/> | View Call |
| <input type="checkbox"/> | Today, 4:44 PM | COMPLETE | +161 <input type="text"/> | 806 <input type="text"/> | View Call |
| <input type="checkbox"/> | Today, 4:44 PM | COMPLETE | +131 <input type="text"/> | 808 <input type="text"/> | View Call |

The screenshot below shows the example of transcription.

When you playback the recording, the transcript is automatically highlighted at that position (see the yellow background in the following screenshot). Click on the interesting word in transcription and the audio player will be fast forwarded to that location



Screen Recording

Architecture

Call Recording solution relies on Screen Recording Client running on agent desktops to perform screen captures during a call.

The controller application is responsible for authentication of clients and initiating capture process when agent handles new call.

The following diagram illustrates a high-level architecture of Call Recording screen recording solution. The next chapters cover the architecture in more details.

Components:

- The **Screen Recording Client** runs on the Agent's workstations as a Windows Service.
- The **Screen Recording Controller** authenticates all clients and controls a recording process, i.e. starts/stops screen capturing when agents receive/make calls.
- When the call ends, the **Client** uploads the video file to the server for storage and playback.

Authorization Phase

When the Client application is deployed on new computer, it has to be authorized first by system administrator (menu **Screen recording > Screen recording workstations**).

The following diagram illustrate the authorization phase.

Recording Phase

Once the Screen Capture Client is authorized and associated with the corresponding agent profile, it automatically starts screen recording when agent receives/makes calls.

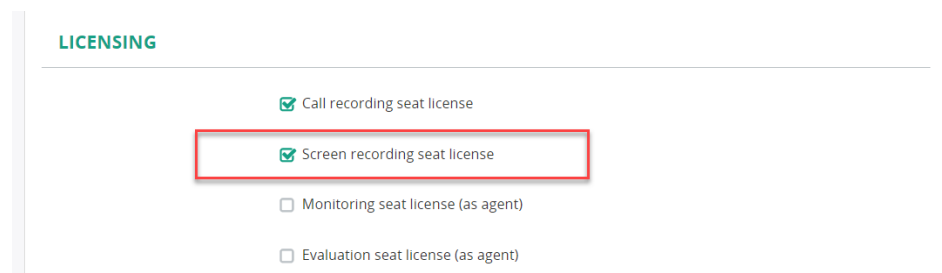
The following steps illustrate a recording process in detail:

1. The Call Recording **Call Recorder** detects new call from the **Phone System**.
2. The **Call Recorder** notifies the **Screen Recording Controller** about the particular agent has new call
3. The **Screen Recording Controller** locates the active session for that agent and sends **Start capturing** command to the **Capture Client**
4. Both **Call Recorder** and **Screen Recording Controller** save metadata in **Database**, so users can playback audio and video recordings using the **Web Portal**.
5. The **Call Recorder** detects call end event.
6. The **Call Recorder** saves the recorded audio file to the **File Storage**.
7. The **Call Recorder** notifies the **Screen Recording Controller** about call end.
8. The **Screen Recording Controller** sends **Start capturing** command to the **Capture Client**. If wrapup recording is enabled, then screen capturing process continues for a pre-defined amount of time, usually for a couple of minutes. Otherwise, a screen capturing is completed immediately.
9. The **Capture Client** uploads the recorded video file to the **Web portal**.
10. The **Web Portal** service stores the file to the **File Storage**

Configure Licensing

Assign Licenses to Users

Navigate to **Administration > User Management > Users**. On user profiles, check the **Screen recording seat license** for each of eligible users.



Configure Storage

Generally handled by the Root Administrator.

Navigate to menu **Administration > Storage > Storage Targets**. Click

Add to create a storage target for screen recording files (*.mp4). Files can be stored:

- Locally on the same server as the Call Recording web application
- Remotely on FTP, SFTP server
- Remotely in Amazon S3 bucket

The following screenshot demonstrates configuration of local storage in directory /var/Call Recording/screen_recordings.

Administration > Storage > Storage Targets

Add Storage Target

Storage Target Name *

Tenant

Storage Target Type

LOCAL FILE SYSTEM SETTINGS

Base path

On Linux system, configure folder permissions

For local storage target, configure permissions for the directory. This directory should be writable by Apache web server process. On Centos 6/7, execute the command:

```
chown -R apache:apache /var/Call Recording/screen_recordings
```

On Ubuntu:

```
chown -R www-data:www-data /var/Call Recording/screen_recordings
```

On Windows, there is no need to configure permissions for folder.

Configure Screen Recording Settings

Navigate to menu **Administration > Screen Recordings > Screen Recording Settings**. Click as needed:

- **Storage Target*** - Enter the URL defined for screen recordings in *Storage Targets*
- **Video file name format*** - Enter the parameterized file name format.
- **"Look-back" on-demand recording** - Set to **Yes** to enable and record the full call from the start when On Demand recording is triggered; set to **NO** to only record the call from the time On Demand recording is triggered.
- **Pause recording timeout** - Define the number of seconds allowed before automatically resuming recording if paused. Set to 0 to disable this timeout. Leave empty to use a BroadSoft system default setting for pause timeouts.
- **Capture rate (fps)** - Define how often to capture the screen (frames per second)
- **Wrap-up time** - Define a number of seconds to continue screen recording after voice interaction (call) completes.
- **Max recording duration** - Set a number of seconds to allow screen recording to take place. (limits maximum size of video file).
- **Max file duration** - Set a number of seconds to allow for each file duration (applies to each related recording for a session)
- **Multi-monitor support** - Select **Record Primary monitor only** or **Record all monitors**.
- **Max width/height** - Define the size parameters of the captured image(s). Call Recording automatically resizes the image. This setting is per-monitor, that is, multi-monitor configuration, the picture is downsized only when either of the monitors has larger resolution size.

Administration > Screen Recording > Screen Recording Settings

Edit Screen Recording Settings

STORAGE SETTINGS

Storage Host URL

URL of the storage server for screen recordings (it should be accessible from outside by the clients). The clients automatically upload the recorded video files to that server. In a single-server setup, it should be the same as the web portal. In a multi-server setup, it is possible to a dedicated server the file upload traffic. Format examples: http://miarec.example.com, https://10.0.0.5:8443

Storage Target *

Video file name format *

Parameterized file name format

RECORDING SETTINGS

"Look-back" on-demand recording default no yes

When enabled, audio will be recorded from the beginning of a call. Otherwise, audio will be recorded from a moment when the on-demand recording is triggered

Pause recording timeout seconds

Recording will be automatically resumed after the specified timeout. Set to 0 to disable a timeout. Set to empty value to use a system default setting

Capture rate (fps) *

Wrap-up time (seconds) seconds

The screen recording continues for the specified amount of time after the voice interaction completes

Max recording duration (seconds) seconds

The recording is automatically terminated after the the specified amount of time passes. This value should be at least as large as the longest call.

Max file duration (seconds) seconds

The recording session may consists of multiple smaller files. This option specifies the maximum duration of individual file.

Multi-monitor support Record primary monitor only Record all monitors

Max image width pixels

Maximum width of the captured screen image. If the actual monitor width is bigger, then the screen image is automatically resized

Max image height pixels

Maximum height of the captured screen image. If the actual monitor height is bigger, then the screen image is automatically resized

- **Video file bitrate** - type the kbps needed for screen

recordings. **Network Settings**

- **Controller TCP port** - Set the listening port for client controller communication or 0 to disable
- **Controller TLS port** - set the TLS listening port for encrypted client controller or set to 0 to disable.
- **SSL private key file** - Set the location private key file for inbound TLC connections from clients.
- **SSL certificate file** - Set the location of PEM encoded certificate file for inbound TLC connections from clients.
- **SSL CA certificates** - Set the CA certificate used to verify the client certificate on client authentication. (all in one file | concatenated)

Video file bitrate kbps
The lower bitrate, the smaller file size and the worse quality. The higher bitrate, the bigger file size and the better quality

NETWORK SETTINGS

Controller TCP port
Listening TCP port for Client -> Controller communication (use 0 to disable TCP)

Controller TLS port
Listening TLS port for encrypted Client -> Controller communication (use 0 to disable TLS)

SSL private key file
Location of PEM-encoded private key file for inbound TLS connections from clients. The private key will be automatically generated if does not exist yet.

SSL certificate file
Location of PEM-encoded certificate file for inbound TLS connections from clients. The certificate will be automatically generated if does not exist yet.

SSL CA certificates (optional)
This optional directive sets CA certificates used to verify the client certificate on Client Authentication. It should point to all-in-one file containing concatenated PEM-encoded CA

Important! If Call Recording is deployed on Linux, then make sure the Apache process has write permissions to the storage target directory.

On Centos, run as an example:
chown -R apache:apache /var/Call Recording/screen-recordings

On Ubuntu, run:
chown -R www-data:www-data /var/Call Recording/screen-recordings

Assuming that directory /var/Call Recording/screen-recordings is used for storing of uploaded video files.

Generate Secure Token

Single Tenant:

Navigate to **Administration > Screen Recording > Screen Recording Settings** to view the current **Screen recording token** (see below screenshot).

This token should be used during installation of the Screen Recording Client application.

Administration > Screen Recording

Screen Recording Settings [Edit Configuration](#)

SCREEN RECORDING TOKEN

Screen recording token:

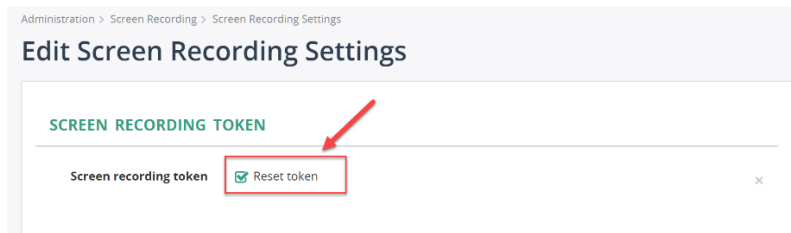
STORAGE

Storage upload URL: http://192.168.1.106:6543/screen_recordings_upload

Storage Target: [SFTP 192.168.1.70 \(2\)](SFTP 192.168.1.70 (2))

Audio file name format: `%{start-time#%Y%m%d}%{start-time#%Y%m%d%H%M%S}-%{recording-id}.mp4`

To generate new token, click **Edit Configuration** button and check **Reset token** option.



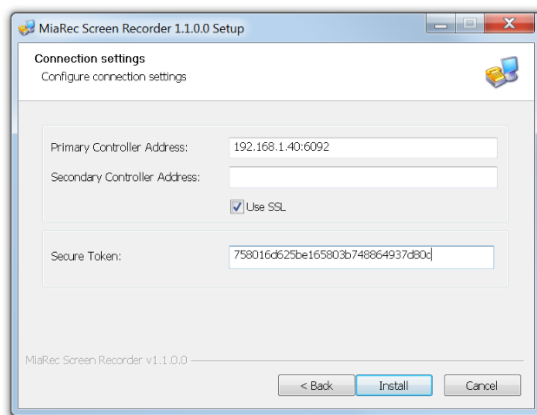
Install Client Application

[Download Call Recording Screen Capturing application](#) and install on agent desktops.

Supported operating systems: Windows 7, 8, 10, Server 2008/2012/2016 with the latest windows updates installed.

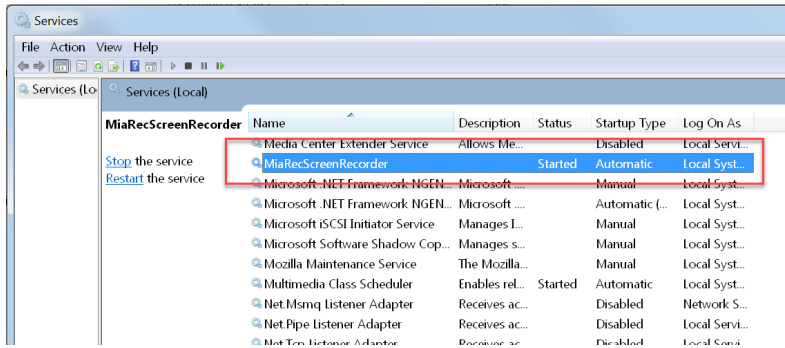
During installation, provide the address of the Call Recording Screen Controller server and "Secure Token". You can retrieve the secure token on the tenant profile page (see above).

Enter the IP-address or DNS name of Call Recording server in the **Primary Controller Address** field. By default, port **6092** is used for SSL connection and **6091** for non-SSL connection (see **Administration > Screen Recording > Screen Recording Settings** for exact port values).

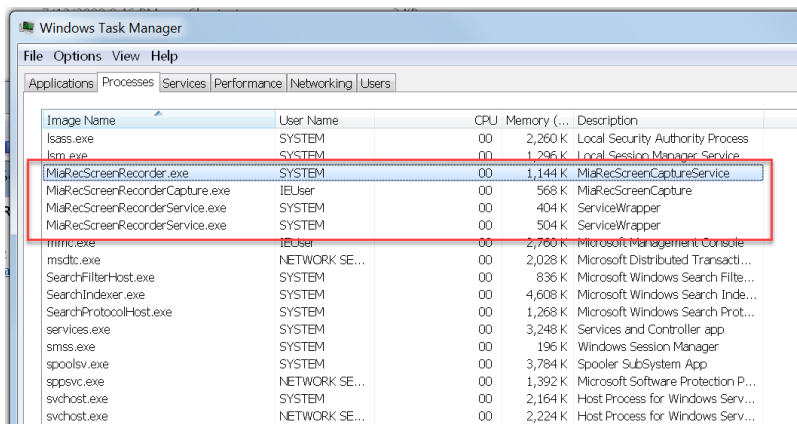


Verify Installation

Call Recording Screen Recording Client silently works in background. It is visible in **Control Panel > Services**.



Also, you can see the application in the list of running processes.

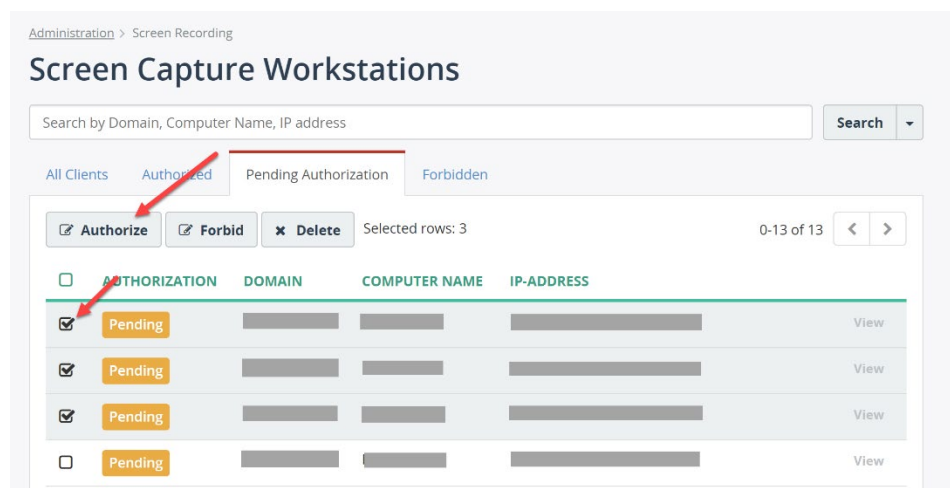


Authorize New Workstations

The capturing client application automatically establishes a network connection with the Call Recording screen recording controller. New workstation requires authorization before it can record screen. Every workstation is uniquely identified using the automatically generated secure workstation token. The administrator can authorize new workstations using Call Recording Web UI. Navigate to menu **Administration > Screen Recording > Screen Capture Workstations**.

New workstations are shown in the **Pending authorization** tab.

Select the corresponding workstation(s) and authorize them.



Configure Users for Screen Recording

Navigate to **Administration > User Management > Users** and click **Edit** for the corresponding user profile.

Step 1. Configure Screen Recording Login

Under **Recording settings**, configure the Windows login name in the **Screen recording login** attribute. This value should match to username, the user is using to login to Windows machine. Optionally, you can specify a domain name if your organization has multiple domains.

RECORDING SETTINGS

Record Always On-demand Never Default

Record direction Inbound Outbound

Extension ×
[Add Extension](#)

Confidential calls Automatically mark all calls of this user as confidential

Screen Recording Login
Supported formats: NETBIOS\login, DOMAIN\login, login

Step 2. Assign Screen recording license

Under **Licensing**, assign the Screen recording seat license to user.

LICENSING

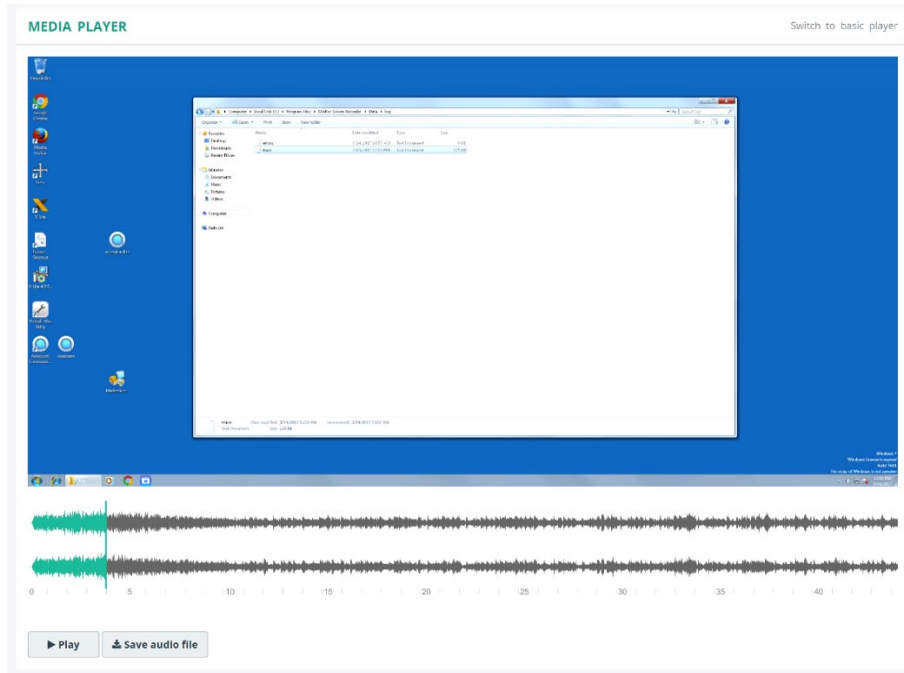
Call recording seat license

Screen recording seat license

If user logs into to the [authorized workstation](#) using the configured login name, a screen capture will be activated automatically.

Verify Screen Recording

Make a test call to verify screen recording. Once a call is completed, the video file should be automatically uploaded to the central storage server. You will be able to playback both audio and screen recordings simultaneously.



Upload process may take some time depending on network speed between client and server. The message **Screen recording file is not uploaded yet** is shown when upload is not completed yet:

Call 281558487 -> 300 [Mark as confidential](#) [Delete Call](#)

MEDIA PLAYER Switch to basic player

Screen recording file is not uploaded yet

| INFO | FROM | TO |
|-------------------------------------|--|--|
| Tenant: Flexus | User: | User: Justin Amado |
| Date: Today | Phone Number: 281558487 | Group: Users |
| Connect Time: 12:01:46 PM | Phone Name: | Phone Number: 300 |
| Disconnect Time: 12:02:33 PM | Phone Id: 281558487 | Phone Name: |
| Duration: 0:47 | Ip-address: 192.168.1.106 (3000) | Phone Id: 300 |
| Watermark: View | Live monitor phone 281558487 | Ip-address: 192.168.1.40 (5070) |
| | | Live monitor phone 300 |

Troubleshooting Screen Recording

Client Side

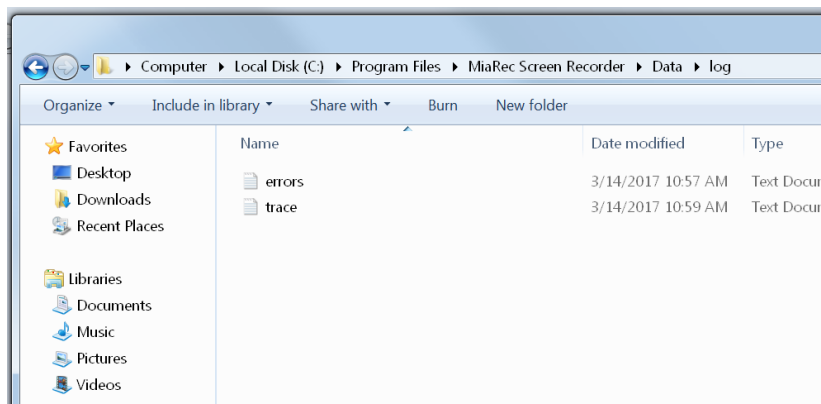
Enable Logging for Service Application

By default, client application doesn't write logs. Navigate to **INSTALL-FOLDER\Bin** and edit file **Call RecordingScreenRecorder.ini**. Change **Enable** to **1** in the section **[Trace]**:

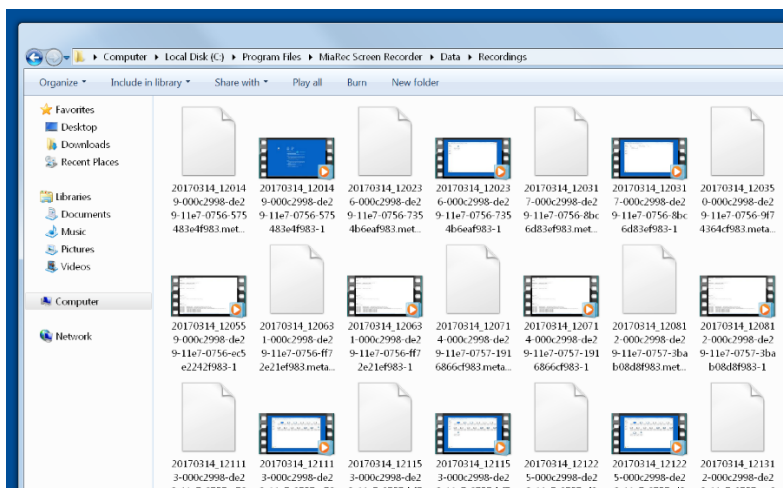
```
[Trace]
Enable=1
File=<INSTALL-FOLDER>\Data\log\trace.log
```

Restart service **Call Recording Screen Recorder**.

Once enabled, the logs are written into **INSTALL-FOLDER\Data\log\trace.log** file. Optionally, you can change a location of log file by editing **File** parameter in the INI file.



The video files are stored temporary in directory **INSTALL-FOLDER\Data\Recordings**. The client application automatically uploads the recorded files to the central storage server after call completion. Once uploaded, the files are removed from local storage. You can verify if any of files are recorded by the client but not uploaded yet.



Enable Logging for Desktop Capturing Process

To enable logging for the capturing process, first create new directory on computer where non-privileged users can write files. It should be outside of **C:\Program Files**. For example, create directory C:\Call RecordingLogs

Then, navigate to **INSTALL-FOLDER\Bin** and edit file Call RecordingScreenRecorder.ini

Under section **[Recording]** edit the parameter **CaptureProcessArgs**. Change it to:

```
CaptureProcessArgs = -ttttt -o C:\Call RecordingLogs\ScreenRecDesktop.log
```

Note, the directory **C:\Call RecordingLogs** should exist and it should be writable by non-privileged users.

Server Side

If the screen recording doesn't appear on the server for too long, then you need to check logs on both the server and client.

First, check, System Log on the server (menu **Administration > Maintenance > System Log**).

One of the common issues is insufficient permissions to the upload directory. The following screenshot shows one of such cases.

```

response = handler(request)
File "/var/www/miarec/pyenv/lib/python3.4/site-packages/pyramid-1.5.6-py3.4.egg/pyramid/router.py", line 163, in handle_
response = view_callable(context, request)
File "/var/www/miarec/pyenv/lib/python3.4/site-packages/pyramid-1.5.6-py3.4.egg/pyramid/config/views.py", line 596, in
return view(context, request)
File "/var/www/miarec/pyenv/lib/python3.4/site-packages/pyramid-1.5.6-py3.4.egg/pyramid/config/views.py", line 329, in a
return view(context, request)
File "/var/www/miarec/pyenv/lib/python3.4/site-packages/pyramid-1.5.6-py3.4.egg/pyramid/config/views.py", line 305, in p
return view(context, request)
File "/var/www/miarec/pyenv/lib/python3.4/site-packages/pyramid-1.5.6-py3.4.egg/pyramid/config/views.py", line 385, in v
result = view(context, request)
File "/var/www/miarec/pyenv/lib/python3.4/site-packages/pyramid-1.5.6-py3.4.egg/pyramid/config/views.py", line 491, in _
response = getattr(inst, attr)()
File "/var/www/miarec/app/miarecweb/views/admin/screen_recording_upload_views.py", line 604, in view_upload_file_content
os.makedirs(new_directory, exist_ok=True)
File "/usr/local/lib/python3.4/os.py", line 227, in makedirs
makedirs(head, mode, exist_ok)
File "/usr/local/lib/python3.4/os.py", line 237, in makedirs
mkdir(name, mode)
PermissionError: [Errno 13] Permission denied: '/var/miarec/screen_recordings'

```

In this case, you just need to grant the **write** permission on that folder to the Apache web server user account:

```
mkdir -p /var/Call Recording/screen_recordings
chown apache:apache /var/Call Recording/screen_recordings
```

Additionally, you can enable trace on server side. Navigate to menu **Administration > Screen Recording > Screen Recording Settings** and enable detailed trace logging.

TRACE LOG SETTINGS

| | |
|------------------------------|---|
| Enable * | <input checked="" type="checkbox"/> Enable writing of trace log information into file |
| Trace log file name * | <input type="text" value="/var/log/miarec_screen/trace/trace.log"/> <small>Full path to file trace log file</small> |
| Trace level * | <input type="text" value="5"/> <small>Depth of trace information (from 1 to 5). Default is 5</small> |
| Rotate * | <input type="text" value="Daily (once per day)"/> <small>When rotating the log file will be renamed into new one with name "*yyyyMMdd-hhmmss.EXT" (EXT is file extension)</small> |
| Rotate day * | <input type="text" value="1"/> <small>For weekly rotation, one of [Mon, Tue, Wed, Thu, Fri, Sat, Sun, 1, 2, 3, 4, 5, 6, 0]. For monthly rotation a day from 1 to 31. For monthly rotation a day from 1 to 31</small> |
| Rotate time * | <input type="text" value="23:55"/> <small>For hourly rotation format is MM (minutes). For daily, weekly and monthly rotation format is HH:MM (hour and minutes)</small> |

Hardware | Storage | Configuration Requirements

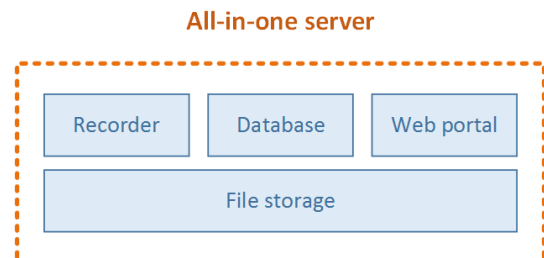
Call Recording solution has flexible architecture supporting various deployment scenarios depending on number of users and requirements to high availability and redundancy.

- All-in-one server. All components (recorder, database, web portal, storage) are deployed to a single server.
- **Decoupled architecture (multiple servers).** Each component is deployed to a dedicated server for redundancy and load balancing purposes.
- "All-in-one" configuration is recommended for up to 2,000 users.
- The distributed configuration is recommended for more than 2,000 users ([more details here](#))

All-In-One Server

This article provides hardware recommendations for "all-in-one" setup, where all software components (recorder, database, web portal and storage) are deployed in a single server.

"All-in-one" configuration is recommended for deployments up to 2,000 users. For larger deployments we recommend the use of [decoupled architecture](#) (multiple servers).



Recommended Hardware Configurations

For Recording 50-500 Users

Physical or virtual server with the following minimum hardware specification:

- CPU** Intel CPU quad-core or better. Frequency at least 2.0GHz.
- Memory** 16 GB or more
- Storage**
- Two high speed disks (at least 10,000 rpms HDD or preferably SSD) in RAID 1 configuration for storing operating system, program files and database data. Disk space requirements - at least 300GB.
 - High capacity disk array (local or NAS/SAN) in RAID 5/6 configuration for storing audio mp3 files and, optionally, log files. Disk space requirements - 0.24 MB/minute of recording For example, in average a business user makes 10 calls per day with a duration 5 minutes. This will end up to 1,000 minutes per user per month (assuming 20 working days). One month of storage for 500 users will require 120 GB of disk space.
- OS** Windows Server 2012, 2016 (64-bit) or Linux RedHat/Centos 7.x

For Recording 500-1,000 Users

Physical or virtual server with the following minimum hardware specification:

- CPU** Intel CPU six-core or better. Frequency at least 2.3GHz.
- Memory** 32 GB or more
- Storage**
- Two high speed disks (at least 10,000 rpms HDD or preferably SSD) in RAID 1 configuration for storing operating system, program files and database data. Disk space requirements - at least 600GB.

- High capacity disk array (local or NAS/SAN) in RAID 5/6 configuration for storing audio mp3 files and, optionally, log files. Disk space requirements - 0.24 MB/minute of recording. For example, in average a business user makes 10 calls per day with a duration 5 minutes. This will end up to 1,000 minutes per user per month (assuming 20 working days). One month of storage for 1,000 users will require 240 GB of disk space.

OS Windows Server 2012, 2016 (64-bit) or Linux RedHat/Centos 7.x

For Recording 1,000-2,000 Users Physical or virtual server with the following minimum hardware specification:

CPU Intel CPU hex-core or better. Frequency at least 2.3GHz. **Memory** 64 GB or more

- Storage**
- Two high speed disks (at least 10,000 rpms HDD or preferably SSD) in RAID 1 configuration for storing operating system, program files and database data. Disk space requirements - at least 1,000 GB.
 - High capacity disk array (local or NAS/SAN) in RAID 5/6 configuration for storing audio mp3 files and, optionally, log files. Disk space requirements - 0.24 MB/minute of recording. For example, in average a business user makes 10 calls per day with a duration 5 minutes. This will end up to 1,000 minutes per user per month (assuming 20 working days). One month of storage for 2,000 users will require 480 GB of disk space.

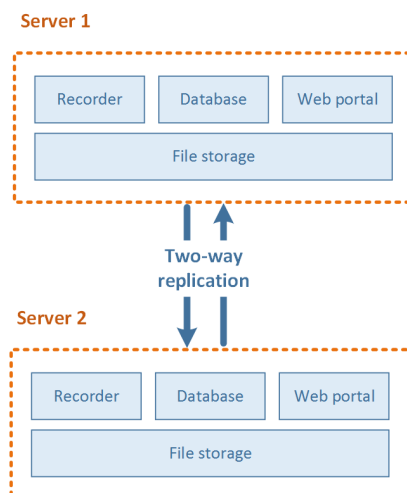
OS Linux RedHat/Centos 7.x

More Than 2,000 Users

For larger deployments we recommend the use of [decoupled architecture](#) (multiple servers).

High Availability and Redundancy

Call Recording supports High Availability setup using advanced multi-master asynchronous replication between multiple "all-in-one" servers.



Decoupled Architecture

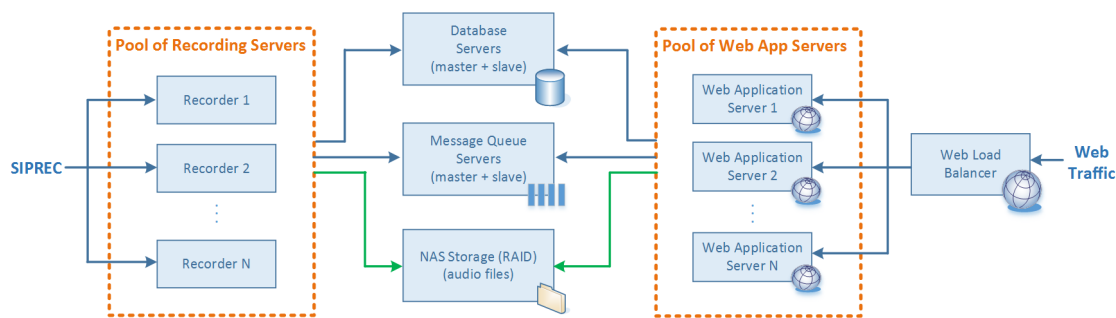
Within Call Recording's decoupled architecture, each software component (recorder engine, database, web portal, storage) is deployed on a dedicated server. As an option, the components may be duplicated to achieve full redundancy and/or scalability.

Decoupled architecture is recommended for recording 2000 or more users.

The following diagram shows the extreme case when at least two copies of each component are deployed on their own dedicated server (master/slave or multi-master) to achieve full redundancy.

Besides such extreme cases, Call Recording supports other configurations with a partial share of hardware resources with some other components. For example, for a small-scale deployment in a hosted environment we recommend you isolate a recording server as the minimum requirement. The rest of the components may share hardware resources on the second server. This two-server setup provides a good balance between security (isolation of a critical recording server) and cost (sharing of hardware resources by other components).

Nowadays a virtualization is a preferred deployment method for new software. In a virtual environment it is significantly cheap to spin up additional VMs and isolate components from each other to achieve reliability, security, and scalability.



Such architecture allows you to achieve the following goals:

- **Redundancy:** All components are duplicated to eliminate single-point-of-failure issues. Some of these components support master/master, others support master/slave configuration with a floating ip-address mechanism.
- **Performance:** The software components do not intend for the same server resources (CPU, Memory, I/O, etc.)
- **Scalability:** Multiple recording and web servers can be deployed for load balancing purposes. Additional server could be easily added to the solution to cover customer growth. Call Recording software architecture provides an almost linear scalability of individual components. For example, if the bottle-neck is a web portal, then you just need to spin up an additional VM with web application.
- **Reliability:** The components are isolated from each other. In a hosted environment, it is important to isolate recording servers from web servers in order to prevent potential disruption of service due to occasional spikes in web traffic. With such architecture, the issues with some of components are not propagated to other components. In the worst case, you may have slowdown of the web portal, but the recording process will not suffer from such issues, and you will not lose any recordings due to CPU/disk/network overload.
- **Security:** In a hosted environment, it is important to keep recording and database servers in a private network isolated from end-user facing web servers. A potential breach of the web server will not spread to other servers.

Hardware Specification Recommendations

Different components have different requirements to hardware. For example, Call Recording recording server benefits the most from multiple CPU cores and does not benefit at all from additional memory (for example, recording of 500 concurrent sessions consumes less than 1GB of memory, but requires 16-core CPU). The database server benefits the most from SSD disks with a high speed random access. The web portal doesn't benefit from SSD disks, but it benefits from additional memory.

Below you will find recommendations on the hardware specification of each individual component.

Recording Server Hardware Requirements

We recommend one recording server (or virtual machine) for each 500 concurrently recorded session (equivalent to approximately 5,000 users in a Hosted PBX environment). Call Recording recording engine has exceptional performance and can record 1,000 and more concurrent session on a single server; we recommend you keep an average load of 500 concurrent sessions per server in order to have enough room for potential spikes in load.

When using audio file encryption, the recommendations are one server per 250-300 concurrently recorded session.

Small Server Configuration

(About 1,000 users per recorder server)

CPU 4 cores or more. Frequency of at least 2.26GHz.

Memory 16 GB or more

- Storage**
- 2 hard disks using RAID 1 for storing OS, binary files, and log files. Minimum free disk space is 300GB (for log files).
 - 2 high speed hard disks (10K or 15K RPM) using RAID 1 for temporary storage of audio files for in-progress calls. Minimum free disk space is 300GB. (*)

Large Server Configuration

(About 10,000 users per recorder server)

CPU 12 cores or more. Frequency of at least 2.26GHz.

Memory 32 GB or more

- Storage**
- 2 hard disks using RAID 1 for storing OS, binary files, and log files. Minimum free disk space is 300GB (for log files).
 - 2 high speed hard disks (10K or 15K RPM) using RAID 1 for temporary storage of audio files for in-progress calls. Minimum free disk space is 300GB. (*)

(*) - For performance reasons it is recommended that you store audio files for in-progress calls locally on the server. The audio file will be moved to the network attached storage at the end of each call.

In addition to performance reasons, this solution provides another layer of protection to prevent network failures. In case there are network connection issues due to the NAS, the recorder process may continue to record calls, and store audio files locally till the connection to the NAS server is recovered.

Database Server Requirements

One or two database servers (PostgreSQL) in master/slave configuration using floating ip failover mechanism.

| | |
|----------------|--|
| CPU | 2 cores or more. Frequency of at least 2.26GHz. |
| Memory | 32 GB or more |
| Storage | Solid state drives (SSDs) using RAID 1 or RAID 10 with free space 3GB for each 1M records stored in database |

Web Application Server Requirements

One or more web application servers are required for load balancing and redundancy purposes.

Each of the servers host web portals as well as worker processes for task manager. The task manager is used to execute various maintenance tasks like export, backup, replication, retention, etc. The workers on multiple web application servers form the pool of workers, i.e. the tasks are automatically distributed over multiple application servers for redundancy and load balancing purposes.

The recommended number of web servers depends on anticipated pages/s web requests load.

For a hosted PBX environment, a rough estimate is one web server per 5,000 users.

| | |
|----------------|---|
| CPU | 4 cores or more. Frequency of at least 2.26GHz. |
| Memory | 16 GB or more |
| Storage | 2 hard disks using RAID 1 for storing OS, binary files and log files. Minimum free disk space is 150GB (for log files). |

Web Load Balancer Requirements

The web load balancer (HAProxy) is required when two or more web servers are deployed.

The load balancer server itself may be duplicated to eliminate a single point of failure situation. Switchover between load balancing servers is implemented using floating ip mechanism.

| | |
|----------------|---|
| CPU | 2 cores. Frequency of at least 3.00GHz. |
| Memory | 4 GB |
| Storage | Storage is not critical because HAProxy is mostly CPU consuming process (single thread). 64GB of disk storage for OS, application binary files and logs should be enough. |

Message Broker Server Requirements

One or two servers in master/slave configuration for message queue system. The message queue system is used for internal communication between various components of Call Recording solution.

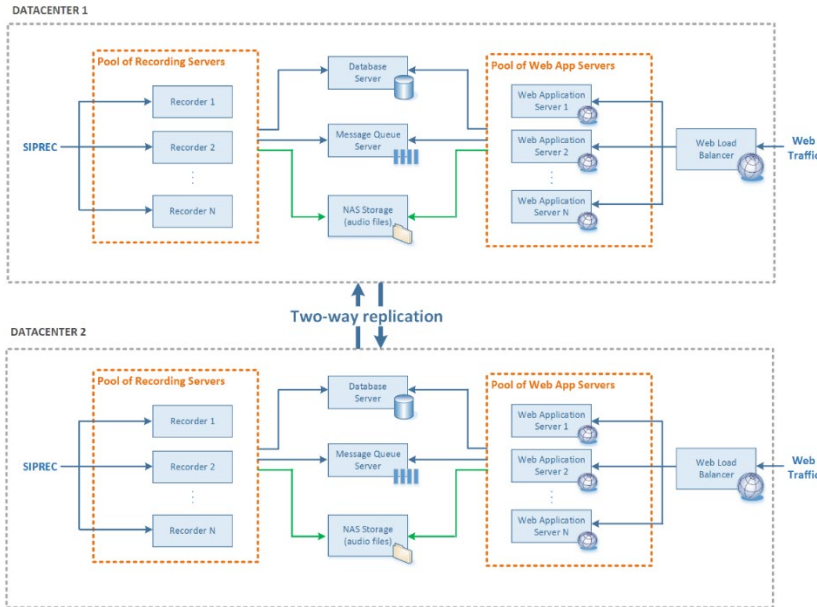
| | |
|----------------|---|
| CPU | 2 cores or more. Frequency of at least 2.26GHz. |
| Memory | 16 GB or more |
| Storage | <ul style="list-style-type: none"> 2 hard disks using RAID 1 for storing OS and binary files (64GB) 2 high speed hard disks (10K or 15K RPM) using RAID 1 for persistent storage of messages with free space at least 64GB. |

Network Attached Storage (NAS) for Audio Files

Call Recording stores audio files in compressed MP3 format. Default compression settings are 0.24MB/minute of recording.

Decoupled with GEO-Redundancy

Call Recording supports advanced multi-master asynchronous application-level replication between datacenters. It is quite unique on the market because other vendors mostly support either master/slave or master/master synchronous or SAN-based replication (expensive and not suitable for GEO-redundancy).



Disk Space Requirements

Call Recording supports following formats for audio files:

| Format | Size per minute | Hours per TB |
|-------------------------------|-----------------|------------------|
| MP3 (stereo 32kbps) - default | 0.24 MB/minute | 72,818 hours/TB |
| MP3 (mono 16kbps) | 0.12 MB/minute | 146,636 hours/TB |
| WAV (stereo) | 1.92 MB/minute | 9,102 hours/TB |
| WAV (mono) | 0.96 MB/minute | 18,204 hours/TB |

Format of audio file and MP3 bitrate settings are configurable.

Example of disk space requirements calculations

Assumptions:

- In average, a business user makes 10 calls per day with a duration 5 minutes. This results into 1,000 minutes per user per month (assuming 20 working days).
- File format is MP3 stereo 32kbps, i.e. 0.24MB/minute

Approximate disk space requirements (see assumptions):

| Total users | 30 days storage | 1 year storage | 3 year storage | 7 year storage |
|-------------|-----------------|----------------|----------------|----------------|
| 50 | 12 GB | 144 GB | 432 GB | 1,000 GB |
| 100 | 24 GB | 288 GB | 864 GB | 2,000 GB |
| 200 | 48 GB | 576 GB | 1,728 GB | 4,000 GB |

| Total users | 30 days storage | 1 year storage | 3 year storage | 7 year storage |
|--------------------|------------------------|-----------------------|-----------------------|-----------------------|
| 500 | 120 GB | 1,440 GB | 4,320 GB | 10,000 GB |
| 1,000 | 240 GB | 2,880 GB | 8,640 GB | 20,000 GB |
| 2,000 | 480 GB | 5,760 GB | 17,280 GB | 40,000 GB |

ScreenRecordingStorageRequirements

Screen recording compression is configurable under **Administration > Screen Recording > Screen Recording Settings**.

A default bitrate is 256kbps, which is the best balance between video quality and file size.

| Bitrate | Size per minute | Hours per TB |
|----------------|------------------------|---------------------|
| 256kbps | 1.92 MB/minute | 9,102 hours/TB |

Firewall Configuration

Ensure the firewall ports are open, which are used for accessing Call Recording from other computers on the network/Internet.

Open Ports for Call Recording

Call Recording uses following ports, which should be opened on firewall:

| Port | Description |
|---------------------|---|
| | Call Recording Web-portal (HTTP protocol) |
| 80 (TCP) | It is possible to change this port to other value during installation (for example, to 8080). |
| 443 (TCP) | Call Recording Web-portal (HTTPS protocol) |
| 6554 (TCP) | Live monitoring (RTSP signaling). |
| 7000 - 7999 (UDP) | If live monitoring is not used, then this port can be closed on firewall. |
| 5070 (TCP) | Live monitoring (RTP audio). |
| 20000 - 21999 (UDP) | If live monitoring is not used, then these ports can be closed on firewall. |
| 5080 (TCP, UDP) | Cisco SIP trunk recording signaling (SIP protocol) - for Cisco UCM only |
| 22000 - 23999 (UDP) | Cisco SIP trunk recording media (RTP protocol) - for Cisco UCM only |
| 32000 - 33999 (UDP) | SIPREC recording signaling (SIP protocol) - for SIPREC recording only |
| 6091 (TCP) | SIPREC recording media (RTP protocol) - for SIPREC recording only |
| 6092 (TCP) | Avaya DMCC recording media (RTP protocol) - for Avaya DMCC recording interface only |
| | Screen recording controller, unencrypted (optional) |
| | Screen recording controller, encrypted (TLS) |

BACKUP AND RESTORE

Backup Call Recordings

Authorized Administrators may have access to navigate to **Administration > Storage > Export Recordings** to review or manage backup jobs.

A backup job may be started manually or scheduled as needed (for example, nightly, weekly, every other week, etc.).

Add Job «Backup calls»

Name *

Output Folder *

Filename Format *

Backup mode * Full backup
 Incremental backup

Metadata only * Backup call metadata only, but do not backup audio files

Remove after backup * Remove records after successful backup

FILTERING CRITERIA (OPTIONAL)

[+ Add Criteria](#)

SCHEDULE

Run Job * Manually
 Every Hour
 Every Day
 Every Week
 Custom (crontab)

Example when exporting to an FTP server:

Administration > Storage > Export Recordings

Edit Job «Backup calls»

Name *

Destination * Local drive (on server)
 FTP
 FTPS

FTP Host

FTP Port

FTP Login

FTP Password

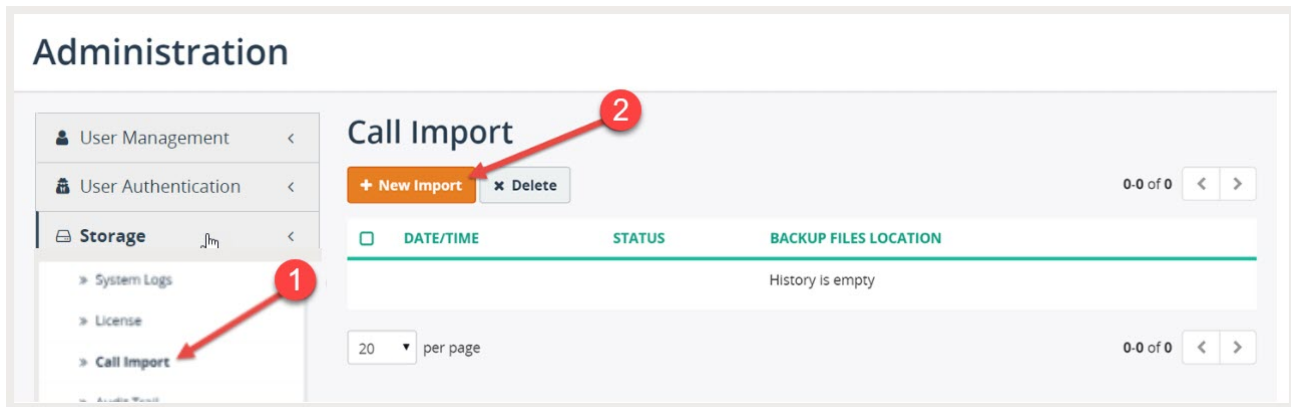
FTP Folder
 Folder on FTP server, for example /folder/

Filename Format *

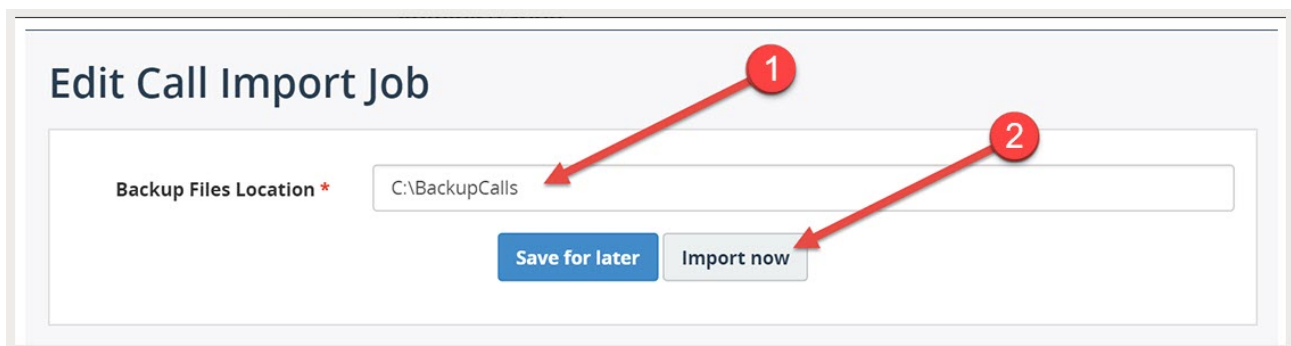
Backup mode * Full backup
 Incremental backup

Restore Call Recordings

Authorized Administrators may navigate to **Administration > Storage > Import Recordings** to access restore tools. Contact LOGIX for assistance with these tools if your credentials do not allow access.



In "Edit Call Import Job" form specify the location of backup files and click on "Import now" button.



Additional steps in case the backup files are located on network share:

It is important to note, that backup files will be accessed by a program application running on MiaRec server rather than from the computer on which you open MiaRec web portal. This means that even if you can access backup files from your own computer, the same files may be inaccessible from MiaRec server.

If backup files are stored on a network share, then on Windows servers you should use correct UNC path like `\server\dir`, on Linux servers you should mount the network share to a local file system, for example, `/mount/backup`.

When using UNC path on Windows, take into account that such path will be accessed by a process running as a Windows service application. By default service applications are running under credentials of LOCAL_SYSTEM user account. This is internal user account, which has no access to network. To solve this issue, you would need to change parameters of "MiaRec Celery" service and run it under credentials of some user account, which can access the backup network share.