Administration

This guide is for administrators of their own on-prem YuChat installation: managing accounts, organizations, Workspaces, Channels, and access permissions. Menu items depend on your role, the version, and the features enabled for the installation.

Access · Sections · Scenarios · Unavailable actions ·

Sign in

Open the address provided by your YuChat administrator and sign in through Keycloak. The panel opens the Workspace list after login. The top bar offers language and theme selection; use the menu to sign out.

If login fails, use the retry link. A no-access message means the panel could not determine an eligible administrator role: contact the installation administrator. Your organization may also restrict access to the panel address and authentication through Keycloak.

Roles and access scope

Panel role	Scope
System Admin	Your entire installation; accounts and system administrators; organizations and their Workspaces

Panel role	Scope
Org Admin	Assigned organizations, their Workspaces, administrators, and synchronization
WS Admin	Workspaces where the account has active **Administrator** (`ADMIN`) or **Owner** (`OWNER`) membership; their members, Channels, permissions, and statistics

The owner of an ordinary Workspace can sign in as WS Admin. The panel derives this role automatically from active membership; a separate system administrator assignment is unnecessary. Creating a Workspace gives its creator `OWNER` membership, but does not grant Org Admin or System Admin access. Signing in with the same account does not expand that scope.

Org Admin may also see Workspaces outside assigned organizations where they are an owner or administrator. Workspace deletion and cloning, synchronization management, and organization permission locks require access to the relevant organization; WS Admin alone is insufficient. Each operation also checks access to the selected object.

Find the right section

- Accounts: profiles, memberships, and account-wide deactivation.
- Workspaces: members, permissions, deletion, and cloning.
- Workspace members and Channels: roles and access within a Workspace.
- Organizations and system administrators.
- Permissions: organization rules and local Workspace values.
- User synchronization: Keycloak rules, filters, and Channel mappings.
- Statistics: activity, workload, and metric export.

- Bots and templates, when enabled.

Search, filters, and CSV

Use search fields, column header filters, and sorting in the tables. Text searches in the main lists usually apply after three characters; shorter input may leave the results unchanged. Bot name search starts at two characters.

Total in Accounts, Workspaces, Workspace members, Channels, and Organizations reflects the current selection. **Export CSV** in these five sections downloads the filtered and sorted selection, including rows on other pages. Select a Workspace before exporting members. The limit is 50,000 rows; the panel reports truncation when reached. Narrow the filters and export again. Files use UTF-8 and `;` as the delimiter.

Sizing workload has a separate export of daily metrics for the selected period. List exports do not export user conversations or files.

Accounts

Access: System Admin.

The screen shows email, name, type, status, and account creation date. Search by email or name and filter by type and status. Statuses are pending (`PENDING`), active (`ACTIVE`), and suspended (`SUSPENDED`). Integration bots include a creator tooltip.

Check a profile and Workspace memberships

1. Find the account and select **Actions → Profile**.
2. Check the email and status. The profile shows the avatar and available position, department, phone, location, status, biography, and custom fields. Empty details are omitted.
3. Select a Workspace in the membership list to open its members. Expelled and suspended memberships are marked separately.
4. For membership history, open **Actions → Workspaces**: inspect role, status, join and exclusion dates, and exclusion reason; filter by role or status.

Disable an entire account

1. Verify the person using their email and profile.
2. Select **Delete**, read the confirmation, and confirm.

The result is account-wide deactivation in YuChat. This is not a procedure for physically deleting all account data. Delete is hidden for `SUSPENDED` accounts. To remove access to only one Workspace, use membership suspension.

Workspaces

Access: System Admin, Org Admin, and WS Admin within their scope.

The list shows name, identifier, subdomain, type, status, organization, creation/update/deletion dates, and member, guest, pending-user, and chat counts. Search by name, ID,

subdomain, or organization; types are `REGULAR`, `DEMO`, and `UBER`.

Active only hides deleted Workspaces. Clear it to find a record with a deletion date. Row actions:

- **View members** opens the member list with this Workspace selected.
- **Manage permissions** opens the permission matrix.
- **Clone Workspace** requires the enabled feature and organization access.
- **Delete Workspace** requires System Admin or Org Admin of that Workspace's organization. Deleted rows hide both deletion and cloning.

Delete a Workspace: why Delete is disabled

1. Verify the target Workspace's name, subdomain, and organization.
2. Select **Actions → Delete Workspace**.
3. Enter the **exact display name**, including capitalization and spaces. The name inside the empty field is a placeholder that must be entered explicitly.
4. Once it matches, click the enabled **Delete** button.

Until the name matches, Delete is disabled even for System Admin. Authorization for deletion is checked separately: Workspace `OWNER` or `ADMIN` membership is insufficient. If an active Workspace has no deletion action, check administrator access to its organization.

This procedure supports `REGULAR` and `DEMO`. Before deleting an `UBER` Workspace, delete all remaining `REGULAR` and `DEMO` Workspaces in the same organization. Deleted records are hidden by **Active only**.

Copy a Workspace into another organization

Access: System Admin or Org Admin with access to both source and target organizations; cloning must be enabled.

1. Select **Clone Workspace** from the Workspace menu.
2. Choose the **Target organization** and check the **New Workspace name**. The source organization is excluded from the target choices.
3. Click **Start clone** and wait for **Ready**. Status refreshes automatically while the dialog stays open.
4. Read the error description on failure; save the new Workspace ID on success.

Cloning creates a separate Workspace with a new ID. This menu cannot directly reassign an existing Workspace to another organization; the original Workspace is not moved.

Workspace members

Access: administrator of the relevant Workspace, its organization, or the system.

Select a **Workspace**, then search by name or email. The list shows account type, role, status, registration/exclusion dates, and exclusion reason. Filter by type, role, or status.

The default role filter is **All except Guest Caller**. Choose **All** or **Guest Caller** to inspect conference guests. `GUEST_CALLER` is assigned by the system and cannot be selected manually.

Assign an owner, administrator, or member

1. Check the selected Workspace and the member's email.
2. Select **Change role**.
3. Choose **Guest**, **Member**, **Administrator**, or **Owner**, then click **Save**.

Role changes are hidden for `SUSPENDED` members. The server also checks the initiator's permissions: WS Admin may need permissions to grant/revoke administrator or owner roles. On denial, check permissions or contact Org Admin/System Admin. **View details** opens the account profile, which requires System Admin.

Suspend one Workspace membership

Find the member, verify the Workspace, and select **Suspend membership**. This executes immediately after selection, without a separate confirmation. The action is hidden for already suspended members.

This removes access to the selected Workspace rather than disabling the entire account. Check the status and exclusion date for the result. The server also validates permission to remove the member.

Channels

Access: System Admin, Org Admin, or WS Admin within their scope.

The section shows Channel name, type, Workspace, and creation, archive, and deletion dates. Search by name or Workspace; types are `PUBLIC`, `PRIVATE`, `GENERAL`, and `BREAKOUT`. **Active only** hides archived and deleted Channels.

Change a Channel role or remove a Channel member

1. Find the Channel and open **Members**.
2. Search by name or email. The dialog shows role and join/leave dates.
3. To change a role, choose `MEMBER`, `ADMIN`, or `OWNER` in the **Role** cell and save it.
4. To remove a member, select **Exclude** and confirm. This action is available for members without a leave date.

Channel exclusion does not disable the account or remove Workspace membership. Creating, archiving, and deleting Channels are not actions offered by this panel section.

Organizations

Access: System Admin or Org Admin of assigned organizations.

The screen shows organization ID, name, and creation date. Search by name. Open an existing row to edit **Organization name** and **Locale**, then save. The panel does not create

organizations.

Row actions include **Workspaces**, **Admins**, **Add admin**, **Manage permissions**, and **Delete organization**.

Grant or revoke Org Admin access

1. Open **Add admin** for the target organization.
2. Find and select an existing account. The selector offers accounts with membership in at least one of that organization's Workspaces; if the account is missing, check that membership first.
3. Confirm the grant.
4. To inspect or revoke assignments, open **Admins**, choose the relevant account's revoke action, and confirm.

System Admin can perform these actions for all organizations; Org Admin can do so for their own. Revoking this role does not deactivate the account; other administrator roles may remain.

Delete an organization

Access: System Admin only, even if Org Admin can see the menu item.

First open the organization's **Workspaces** and check the list. Then select **Delete organization** and read the confirmation. The operation also deletes linked Workspaces: ordinary Workspaces first, then the organizational `UBER` Workspace, then the organization itself. Confirm only for the organization you checked.

System administrators

Access: System Admin. The list shows account ID, email, and name.

Hand over system administration

1. Click **Add administrator**.
2. Find an existing account by email, name, or ID and select it.
3. Verify its details and confirm **Grant rights**.
4. To revoke access, select **Revoke rights** for the relevant account and confirm.

The last System Admin cannot be revoked. Assign another administrator before handing over control. This role grants instance-wide access; use organization or Workspace roles for narrower responsibilities.

Organization and Workspace permissions

Manage permissions in an organization or Workspace menu opens the action/role matrix. It controls invitations, role assignment, Channel/thread creation, files, conference recording, bots, shared links, and other available actions.

The `OWNER`, `ADMIN`, `MEMBER`, and `GUEST` columns are Workspace member roles. Their values do not assign panel administrator roles.

Why cells are disabled

At organization level, the **checkbox** determines whether a role can perform an action. The **lock** determines whether individual Workspaces may change that value. A closed lock blocks local changes; an open lock allows them.

Locks are closed by default. Without an explicit organization setting, the corresponding Workspace cell is unavailable. The entire matrix in a new Workspace may therefore be disabled even for its creator or System Admin. System administrator rights do not bypass organization locks. `REGULAR` supports permission configuration; Workspace type affects defaults rather than the ability to unlock a cell.

Instance-locked permissions are hidden from both matrices and cannot be changed here.

Allow local configuration and change a value

1. Check which organization owns the Workspace.
2. As System Admin or Org Admin of that organization, open **Organizations → Actions → Manage permissions**.
3. Find the action and target role. Set the base value with the checkbox and open the cell's lock.
4. Click **Save**. Changing the checkbox alone does not allow local overrides.
5. Reopen the Workspace matrix, change the available cell, and save. Its WS Admin can also perform this step.

An open lock permits local configuration by administrators of **all Workspaces in that organization**. Configure other action/role pairs separately. Until a local override is saved, the Workspace inherits the organization value. Changed cells are highlighted; **Save** requires changes and no save already in progress.

For example, to prevent ordinary members from creating public Channels in just one Workspace, unlock **Create public Channels** for **Member** in the organization, then clear that cell's checkbox in the target Workspace and save.

Enforce a rule and reset overrides

- Close the organization's lock and save to enforce its value. Local overrides for that action/role pair are removed from its Workspaces; reopening the lock does not restore them.
- **Reset to default** on a Workspace row removes its local values for that action and restores inheritance.
- Resetting an organization row removes its settings and the related Workspace overrides. Defaults apply again, with locks closed.

Resetting previously saved values applies immediately and reloads the whole matrix. **Save edits in other rows first** to avoid losing unsaved changes. If a row has no saved overrides yet, resetting it only discards that row's edits.

User synchronization

Access: System Admin or Org Admin of the target Workspace's organization. WS Admin does not manage synchronization configurations.

This section defines rules for bringing Keycloak/LDAP users into Workspaces and Channels. The list shows Workspace, LDAP OU, the update-existing flag, and dates. Row actions are **Edit**, **Copy**, and **Delete**; use **Add configuration** for a new rule.

Create, copy, or edit a configuration

1. Click **Add configuration** and complete the four tabs below.
2. Save the form. This stores the rule; it is not confirmation that all users have already synchronized.
3. For a similar rule, select **Copy**. Settings are copied, but choose the Workspace and LDAP OU again. Recheck Channel mappings for the new Workspace; the new record does not replace the original.
4. Workspace and LDAP OU cannot be edited in an existing configuration. Create or copy a rule to change them.
5. To delete, choose **Delete** and confirm the configuration using its displayed OU.

Main settings

Provide the required **Workspace** and **LDAP OU**, such as `ou=users,dc=example,dc=com`. Optional controls:

- **Update existing users** updates attributes of already created users.

- **Remove members not in organizational unit** removes Workspace members who leave the selected OU.

Workspace removal and removal by a Channel rule are separate settings. Check the OU and selection conditions before enabling removal.

Attribute mapping

Map profile fields to Keycloak attributes. Empty fields retain defaults: department — `department`, position — `position`, phone — `phone`, full name — `displayName`; Entry DN uses `entryDn`.

User filters

For each filter, set the attribute name, comparison, and value. Supported comparisons are **Equals**, **Not equals**, **Contains**, **Does not contain**, **Empty**, **Not empty**, and **Regular expression**. **Empty / Not empty** hides the value field. Add or remove conditions as needed; they restrict which users are synchronized into the Workspace.

Chat mapping

1. Select the Workspace under **Main settings** first.
2. Open **Chat mapping → Add mapping**, select the Channel, and optionally add a description.
3. Enter comma-separated Keycloak groups and/or attribute conditions. At least one condition is required. Attribute comparisons are the same; **Empty / Not empty** needs no value.
4. Enable **Remove non-matching members** if needed: this removes users from this Channel, not the entire Workspace.

5. Click **Create** or **Save** in the mapping dialog, then **Save** in the main configuration form. Saving the nested dialog alone does not save the entire configuration.

Group and attribute conditions use **AND**; multiple attributes also use **AND**. An attribute-only rule is supported. For example, `department EQ Sales` selects matching users for the sales Channel; adding `position NOT_EMPTY` also requires a populated position. Edit or remove rules in the mapping list.

Statistics

Access: all three administrator roles within their scope. System Admin can select the instance, an organization, or a Workspace; Org Admin works with assigned organizations/Workspaces; WS Admin selects only an available Workspace.

Check activity and compare people with bots

1. Select the organization and Workspace if those fields are available.
2. Choose **7**, **30**, **90**, or **365 days**; the default is 7.
3. Select **All**, **Humans only**, or **Bots only**.
4. Inspect account counts and charts for messaging activity, messages per day, Calls, Call participants, Workspaces with Calls, audio/video notes, screen recordings, and registrations by provider and device platform.

Empty charts are omitted: a missing chart can mean no data in the selected period. Check filters and access scope.

Assess workload and export metrics

As System Admin, select **All organizations** to see **Sizing workload**. It includes active chats, Calls and duration, participant counts, concurrency peaks, hourly participant minutes, file growth/storage, and transcription.

Select the period and use this block's separate **Export CSV** for daily metrics. The human/bot filter applies to ordinary statistics; sizing covers the entire instance.

Bots

Access: the section must be enabled and available for the organization. WS Admin can inspect bots within their scope; management and statistics require at least Org Admin. A visible menu item does not bypass bot-type or operation-specific authorization.

The integration-bot list shows name, email, scope, status, Workspace, organization, owner, and creation date. Name search starts at two characters; filters and a total count are available. **Info** shows details and associated Workspaces. Actions that change the bot are hidden for inactive accounts.

Add an existing bot or create one

1. Click **Add bot**, then select an organization and Workspace.
2. Add an available existing bot, or create a new one with a name and scope.
3. When creating one, save the displayed token in the integration's secure storage: it is shown once.

Scope limits distribution: `WS` — its original Workspace; `ORG` — Workspaces in the same organization; `PUB` — multiple organizations. Public-bot operations additionally require public-bot management authorization or System Admin.

Replace a token, stop access, or remove a bot

- **Refresh token**: confirm, save the new one-time token, and update the integration. The old token stops working immediately.
- **Revoke token**: stops token access until regeneration.
- **Remove from Workspace**: removes the bot only from the selected Workspace.
- **Disable**: disables the bot account; confirmation warns that tokens are revoked and sessions closed.

In **Statistics**, choose the organization and an interval from 1 hour to 7 days, then load data. Inspect request counts, bot counts, each bot's methods, and the most-used methods. The screen warns that data is available since the last backend restart. The panel does not offer scope changes for an existing bot.

Templates

Access: System Admin. The **Email** and **Call transcripts** tabs appear when their respective features are enabled.

Upload or replace a template

1. Select the tab and find a template by name/locale. Download the existing file if you need a reference.
2. When adding, specify name, format, and locale, then select the file. For **Replace**, check the existing name, format, and locale and select a new file: these parameters cannot be edited in the replacement dialog.
3. Click **Upload & Activate**. Matching name, locale, and format replaces the existing template.
4. Arrange a rolling restart of backend replicas with the infrastructure administrator: changes take effect after it, as the screen states.

Transcripts use JRXML templates and PNG assets. Download, add, or replace them; PNG assets can also be deleted with confirmation. Check that templates no longer reference an asset before deletion. An activation action does not mean the restart has already happened.

Choose a scenario

Each scenario is documented next to its screen so procedures are not repeated.

- Employee offboarding: disable the whole account or remove access to one Workspace.
- Find memberships, profile information, or an exclusion reason: profiles and Workspaces.
- Find Call guests, promote a guest to member, assign an owner or administrator: Workspace members.

- Assign a Channel administrator or exclude someone from one Channel: Channel members.
- Delete a test Workspace, find a deleted one, or copy it into another organization: Workspaces.
- Grant/revoke Org Admin or delete an organization: organizations.
- Hand over system administration: system administrators.
- Block public Channel creation in one Workspace, enforce an organization rule, or restore inheritance: permissions.
- Add Sales users to a Channel by group/attribute, remove members after an OU change, or copy a rule: synchronization.
- Assess monthly activity, compare people with bots, or export workload: statistics.
- Add a bot, replace its token, or stop integration access: bots.
- Replace an email/transcript template or PNG: templates.

When an action is unavailable

- **A section is missing**: ask the installation administrator to check your role and feature availability. For example, WS Admin does not manage organizations or synchronization.
- **No results**: check organization/Workspace selection, search length, and status/type/role filters; clear **Active only** when looking for deleted records.
- **The entire matrix is disabled**: check organization locks. Granting System Admin alone does not unlock cells.
- **Delete is disabled**: enter the exact Workspace name.

- **Save is disabled**: change an editable field, complete required values, and wait for any current save to finish.
- **Permissions just changed**: refresh the page; if the new role is absent, sign out and back in.

Related guides: YuChat role model, Keycloak integration, System audit.