Trust Room Manager Guide

Who is the Trust Room manager?

Essentially the Trust Room manager is not a user but a group. A Trust Room manager is therefore a member of that group. This group is generated automatically at Trust Room creation and is the owner of all Trust Room's resources. This means, its members are the only ones authorized to view and change the Trust Room settings and to create new rooms, users and groups.
The role of the Trust Room manager is thus configuring the Trust Room to the desired form: define the defaults / the rules of the Trust Room (like notification settings, data leakage preventions rules, condition of use), create users and groups and assign them access to newly created rooms.
For big communities, the powers of the Trust Room managers group can be delegated: we may have Trust Rooms with someone responsible for the users and groups administration, someone other for setting up the different rooms and another one for configuring the Trust Room settings.
We always recommend assigning such permissions not to single users but to a group: this will simplify the handling for example in case of staff turnover.
In any case it is always a good idea to have more than one Trust Room manager: in case you don't have "physically" another person, you may create a "virtual backup account", which credentials are kept in a safe place for emergency cases.

Trust Room emergency code

What can you do when you forget your credentials? You can contact your Trust Room manager asking him to send you a new password. And in case he is not available or even worse, in case YOU are the ONLY Trust Room manager? You may think to contact the AGORA hotline asking them to reset your password. Unfortunately (or better, at the end "fortunately" for you) this is not possible. Since all the data inside your Trust Room is encrypted using a key available only to Trust Room members, externals (like the system administrators) cannot view or edit any data inside the Trust Room and therefore also not the passwords.
To help you in such situation comes the "Trust Room emergency code". This code (a pretty long random sequence of letters and numbers) has to be generated by the Trust Room manager and kept the relative PDF sheet in a safe place.
When you (or another user) can't access the Trust Room and no one is able to help, you can go to the address https://collaboration.agora-secureware.ch/#/cec and enter your name, your Trust Room and, instead of your password, the Trust Room emergency code.
At this point, you would not gain directly access to the Trust Room (which could be a security breach). Instead you will simply receive (through the standard communication ways: SMS or email) a new password that you can use to enter the Trust Room.
In case of use of the Trust Room emergency code, the Trust Room managers are going to be alerted.
A Trust Room emergency code can be reused multiple times.
To generate a new Trust Room emergency code, click in the top bar on the Administration icon and select "Settings", then select "Generate emergency code" from the "… Actions" button.
Seen its importance we recommend doing it immediately as soon you enter your new Trust Room.

Trust Room Manager Guide

Manage the Trust Room settings

To manage the settings of your Trust Room, click in the top bar on the Administration icon and select "Settings".

Basic settings

If you click on "Edit" you can change following settings:

- **Default language** — The default language to be set by the creation of new users.
- **Allowed notifications** — The notifications channels (email/SMS) to be allowed inside your Trust Room.
- **One-time guests** — Whether you want to allow the creation of one-time guests
- **Allow guest creation** — Whether you want to give the possibility to your members to create guest access on single resources, where they are owner. You can also assign this permission to single users.
- **Allow homonyms in users' names** — Whether to allow the creation of users with the same last name / first name combination.
- **Disable inactive users** — Whether to disable inactive users after a certain amount of days after their last login.
- **Default authentication method** — The default authentication method for new users.
- **Session timeout** — The max. time between each request to the system before the session get invalided.
- **Password settings** — You can define here the password settings like:
  - Min. length
  - Min. Quality
  - Force periodical password change
  - Prevent re-use of previously used passwords
  - Max. wrong login attempts before blocking the account
- **Lost credentials key** — If you want an automatic support in case of lost credentials, please paste here the current Trust Room emergency code.
- **Geofencing support** — You can activate this flag if you would like to limit the access to your Trust Room for some user to specific places. Possible options are:
  - Geo IP: you will be able to define for each user from which country they can login
  - IP filter: you will be able to define for each user from which IP range (for example your company public IP) they can login
- **Enable Google maps** — Enabling this feature allows you to see on a map the address of your Trust Room users as well as the location of your events/meetings.
- **Mask mobile numbers** — Enable this flag if you don't want that the users can see each other mobile numbers.

- **List items per page** — With this option you can define how many items are going to be displayed on one page.
- **Trash bin** — With this flag enabled, if you delete a resource (room, file, event, …) this one is first moved to the trash bin so that you have eventually the possibility to restore it.
- **Automatically empty trash bin** — You can define to empty the trash bin automatically after a certain number of days are passed from the resource's deletion date.

Notifications settings

To set the default notifications settings for your users, select "Set notifications" from the "... Actions" button in the "Trust Room settings" page. Here you can define how users have to be notified in case of normal and high priority notifications (the priority is chosen by the owner of the relative resource) as well as for chat notifications. The available media (email or SMS) depend on the selection you have done in the basic settings of your Trust Room.
These settings can be overwritten for each user.

Customize logo

If you would like to replace the AGORA logo on the top of the page with your own logo, you can simply upload it using the "Change logo" button on the "Trust Room settings" page.
The available place for the logo is wide 220 px and high 80 px. Biggest images are scaled.

Data leakage prevention

You can define your Trust Room's data leakage prevention (DLP) rules for the files uploaded by your members resp. by your guests. You can specify:

- Max. size
- Allowed file formats
- Prohibited file formats
- Prohibited keywords inside the files

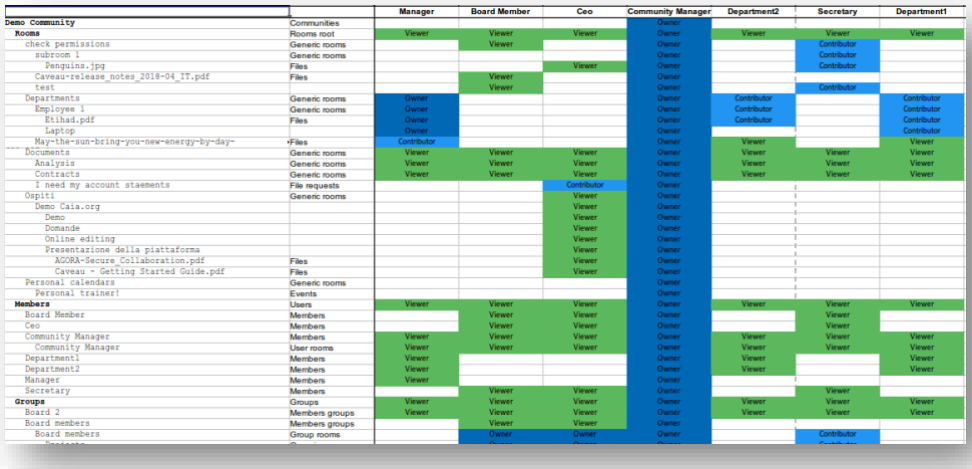
Conditions of use

You can define that the users have first to accept your conditions of use of the platform before being able to access it.

Trust Room Manager Guide

Permissions

Not sure about the permissions defined inside the Trust Room? To help you cross-check them you can export the Trust Room permissions (always from the "… Actions" button on the "Trust Room settings" page). You will get a spreadsheet with all your resources and the permissions owned on it by each user:



		Manager	Board Member	Ceo	Community Manager	Department2	Secretary	Department1
Demo Community	Communities				Owner			
Rooms	Rooms root	Viewer	Viewer	Viewer	Owner	Viewer	Viewer	Viewer
check permissions	Generic rooms		Viewer		Owner		Contributor	
subroom 1	Generic rooms				Owner		Contributor	
Penguins.jpg	Files			Viewer	Owner		Contributor	
Caveau-release_notes_2018-04_IT.pdf	Files		Viewer		Owner			
test			Viewer		Owner		Contributor	
Departments	Generic rooms	Owner			Owner	Contributor		Contributor
Employee 1	Generic rooms	Owner			Owner	Contributor		Contributor
Etihad.pdf	Files	Owner			Owner	Contributor		Contributor
Laptop		Owner			Owner			Contributor
May-the-sun-bring-you-new-energy-by-day-	Files	Contributor			Owner	Viewer		Viewer
Documents	Generic rooms	Viewer	Viewer	Viewer	Owner	Viewer	Viewer	Viewer
Analysis	Generic rooms	Viewer	Viewer	Viewer	Owner	Viewer	Viewer	Viewer
Contracts	Generic rooms	Viewer	Viewer	Viewer	Owner	Viewer	Viewer	Viewer
I need my account staements	File requests			Contributor	Owner			
Ospiti	Generic rooms			Viewer	Owner			
Demo Caia.org				Viewer	Owner			
Demo				Viewer	Owner			
Domande				Viewer	Owner			
Online editing				Viewer	Owner			
Presentazione della piattaforma				Viewer	Owner			
AGORA-Secure_Collaboration.pdf	Files			Viewer	Owner			
Caveau - Getting Started Guide.pdf	Files			Viewer	Owner			
Personal calendars	Generic rooms				Owner			
Personal trainer!	Events				Owner			
Members	Users	Viewer	Viewer	Viewer	Owner	Viewer	Viewer	Viewer
Board Member	Members		Viewer	Viewer	Owner		Viewer	
Ceo	Members		Viewer	Viewer	Owner		Viewer	
Community Manager	Members	Viewer	Viewer	Viewer	Owner	Viewer	Viewer	Viewer
Community Manager	User rooms	Viewer	Viewer	Viewer	Owner	Viewer	Viewer	Viewer
Department1	Members	Viewer			Owner	Viewer		Viewer
Department2	Members	Viewer			Owner	Viewer		Viewer
Manager	Members	Viewer			Owner			
Secretary	Members		Viewer	Viewer	Owner		Viewer	
Groups	Groups	Viewer	Viewer	Viewer	Owner	Viewer	Viewer	Viewer
Board 2	Members groups	Viewer	Viewer	Viewer	Owner	Viewer	Viewer	Viewer
Board members	Members groups		Viewer	Viewer	Owner			
Board members	Group rooms		Owner	Owner	Owner		Contributor	

Wipe Trust Room

If you are looking for a quick way to delete all the content of your Trust Room, the "Wipe Trust Room" function is what you were searching. You can find it in the "… Actions" button on the "Trust Room settings" page.

This function permanently deletes EVERYTHING (except your account and the Trust Room managers group) from your Trust Room, so as you can image, as to be used very carefully.

It can be used for example in case you use your Trust Room over the time for different projects (like mergers and acquisitions) each of them always with a different audience.

Trust Room Manager Guide

Users

To create and manage users, click in the top bar on the Administration icon and select "Users".

Members vs Guests

We have two types of users inside AGORA: members and guests.
The first ones are what we may also define as "power users"; they are typically your company employees. A member can potentially do everything inside the platform: create resources, setting permissions, create guest accesses and perform administrative tasks (like users and groups management). In order to simplify your job, inside AGORA you can also assign on the different resources a "default" permission to "every member of the Trust Room".
On the other hand, guests are typically external users, like customers or partners. If given the necessary permission a guest can access all the resources but only upload new documents, create requests, participate in chat and discussions and create new rooms. All this in a very controlled way: they are not able to modify the inherited permissions, notifications and approvals settings. In addition, since the "default" permission to "every member of the Trust Room" do not apply for guests, in order to access a resource, you will have to explicit assign him a permission to access something. In this way you don't have the risk that a guest can unintentionally see something he should not have been allowed to.

Create new users

To create a new user simply click on New and select the type of user (member or guest) that you would like to create. In the wizard you will have the possibility to define, beside the user data, also his groups' memberships, whether to create for him a personal room and whether to send him directly the login information.

Send login information

If one or your users forget his credentials you can send him a new password by entering his profile page and selecting "Send login information" from the "… Actions" button.
You can send either all credentials (username, Trust Room, address of the application plus a new password), only a new password or only the rest (without generating a new password).

Disable a user

If you want to suspend the access of a user, without deleting his account, you can simply enter his profile and select on "Disable" from the "… Actions" button.
To re-enable him select "Enable" from the same button.

Trust Room Manager Guide

Groups

To create and manage groups, click in the top bar on the Administration icon and select "Groups". In AGORA you can use groups to simplify your job: instead of assigning permissions to single users you assign them to groups. This is very useful for example in case of turnover.

Create new groups

To create a new group simply select "New" on the Groups page, select the type of members you would like to have in this group (members or guests), provide a name and an optional description and finally select its members.

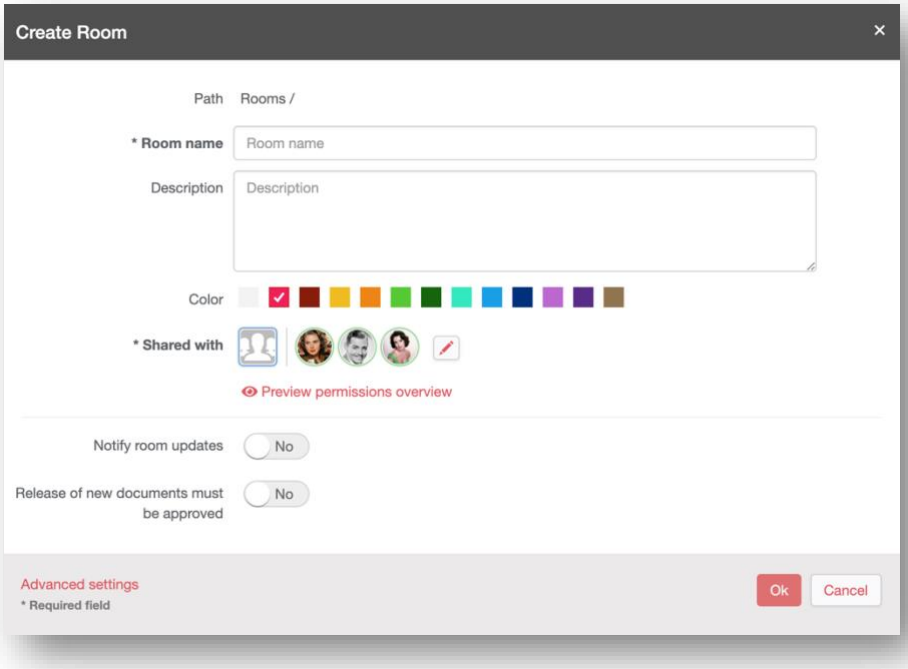
Trust Room Manager Guide

Rooms

A Room is the basic collaboration element of AGORA: it is the place that you set up to start collaborating with someone. It acts like a classical file folder but offers much more capabilities: in fact, you can store there not only files, but also sub-rooms (to better organize your data), events, discussions and much more. On a Room, you define the general rules for the collaboration: who can participate and with which permissions, the default notification settings, whether the files have to be first approved, whether there is a maximal lifetime for the document stored there, etc.

Create new Rooms

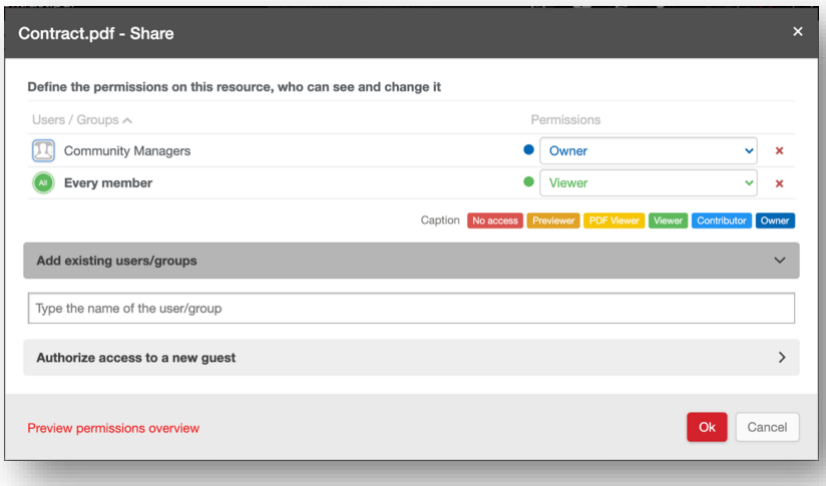
To create a new Room, go to a Room, where you own at least a “Contributor” permission and click on the "New" button on the top right-hand corner a select "Room" from the drop-down menu. You can either enter simply the new Room's name and confirm with "OK" or, similar to the file, define additional information. The settings you define on the Room will then be the default ones applied on the resources (files, sub-rooms, …) saved inside this Room.



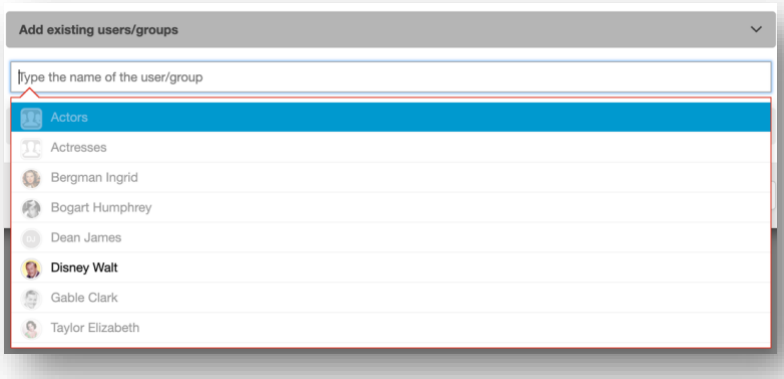
Trust Room Manager Guide

Share a resource

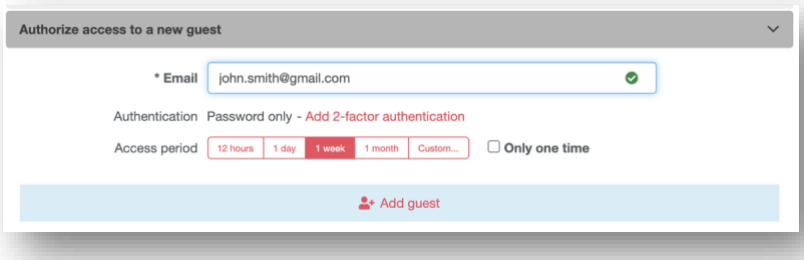
Sharing a resource (File, Meeting, Room, etc.) is a principal purpose of the platform. This share functionality is for both Internal Users being granted access, as well as occasional external trusted guests or third parties.



By using "**Add existing users/groups**" you can select the users/groups already defined in your Trust Room that you would like to authorize access to the resource. Users/Groups which have already access to the hierarchy of this resource (for example, who can see the Room where this file is saved) are written in black. In grey are instead displayed Users/Groups without this access.



In the "**Authorize access to a new guest**" section, you can grant access to your resource for an external person (guest). To accomplish this, simply enter their email address, and optionally setup a 2-factor authentication, the desired access period and if you want that the guest will be able to access that resource only one or multiple times. Once the guest account is added, you will have to assign him/her the desired permission level on the resource.



Permissions

When a user tries to access a resource, the system will first check if for that user a permission on this resource was assigned and in case this one will be applied. Otherwise the system will check if a permission was assigned to one of the groups in which that user is member of. If any is found the greater permission will be applied. If nothing was found, in case the user is a Trust Room's member, the system will check if a general permission for all Trust Room's members exists: if found this last will be applied otherwise the user has no access to this resource.

Permissions levels

The available permissions levels are:

Role	What you can do
Previewer	See all resources on the screen + display the content of files on the screen (with a watermark)
PDF viewer	Same as above + download a PDF copy of the original files (with a watermark)
Viewer	Same as above + download the original files
Contributor	Same as above + add content to the current resource (in case of a Room: upload files, create sub-rooms, events, …; in case of a file: upload new versions; …)
Owner	Same as above + modify the settings and the permissions and delete the resource

You can also assign to a user the special permission "No access". Since "No access" is the default permission, this level is only to be used for defining an "exception" to another permission defined (for example the file should be visible by all the group Marketing members BUT NOT by one of them).

Permissions' inheritance

On the "Permissions settings" form for "container" resources (resources where you can store other sub-elements, like rooms and events) you can also optionally define the inheritance behavior of the defined permissions. In other words, you can define how this permission should be propagated to the new elements saved inside the current resource. The available options are:

- **Apply** (default option): this permission will be proposed by the creation of new elements, but the author will be able to change or remove it
- **Lock**: this permission will be applied also on the new elements and the author will not be able to change or remove it
- **Don't apply**: this permission won't be proposed by the creation of new elements. The author can however add it manually

Trust Room Manager Guide

Reporting

As a Trust Room manager, you can see several kinds of reports about the use of your Trust Room:

- Daily logins (the daily number of accesses into your Trust Room)
- Login frequency (the frequency with which your users use the platform (here you may see that someone is using it daily whereas others have never had access)
- Activities (the different activities done in your Trust Room).
  You can export this list into a PDF or Excel file.
- Users activities (same as before, but the data is first grouped by user).
  Even this data can be exported into a PDF or Excel file.