Getting started guide

AGORA is a highly secure, compliance driven data protection platform. Encrypted Trust Rooms provide the ultimate vehicle for secure content sharing, secure collaboration, and productivity.

With AGORA you can communicate and collaborate over the Internet with your colleagues, partners and clients in a secure and confidential way. You can share documents, plan meetings, chat and even more, with the certainty that only persons designated by you can access the information.

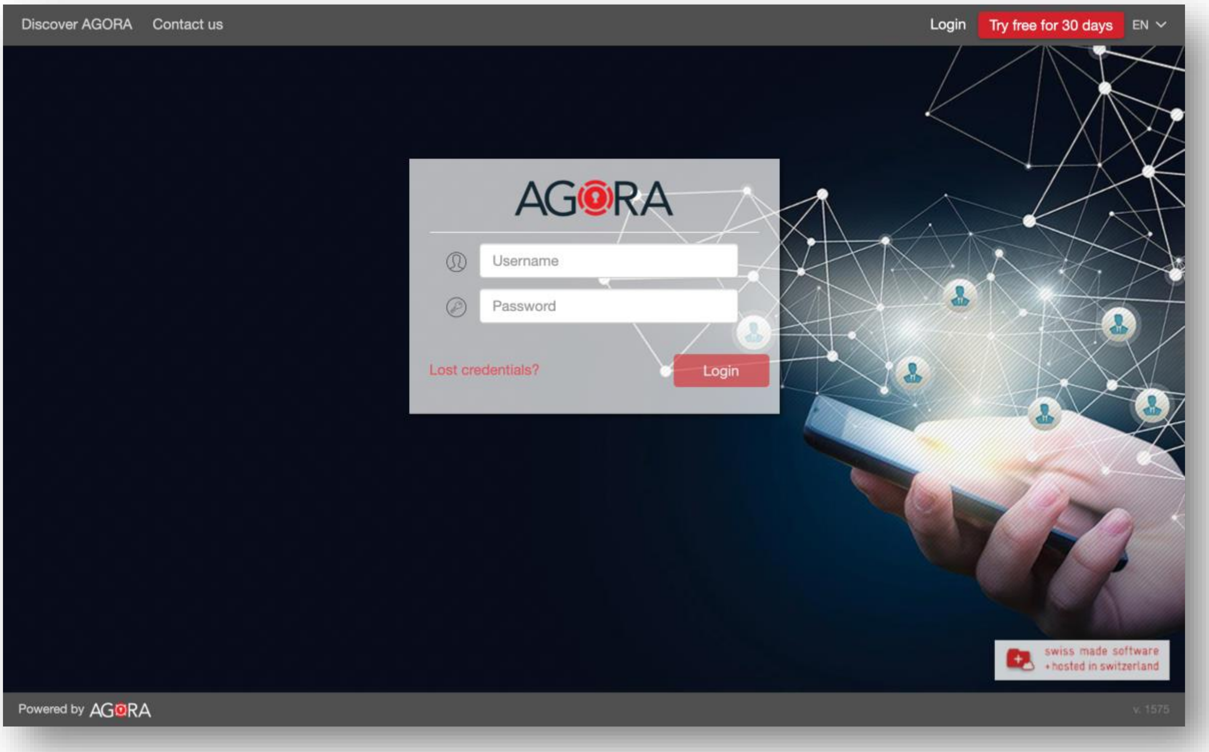
If you want to know more about AGORA, please visit: https://www.agora-secureware.com.

Introduction

This short guide will help you to access your Trust Room, understand the structure of the platform and perform the principal tasks… all this in a secure way.

Login

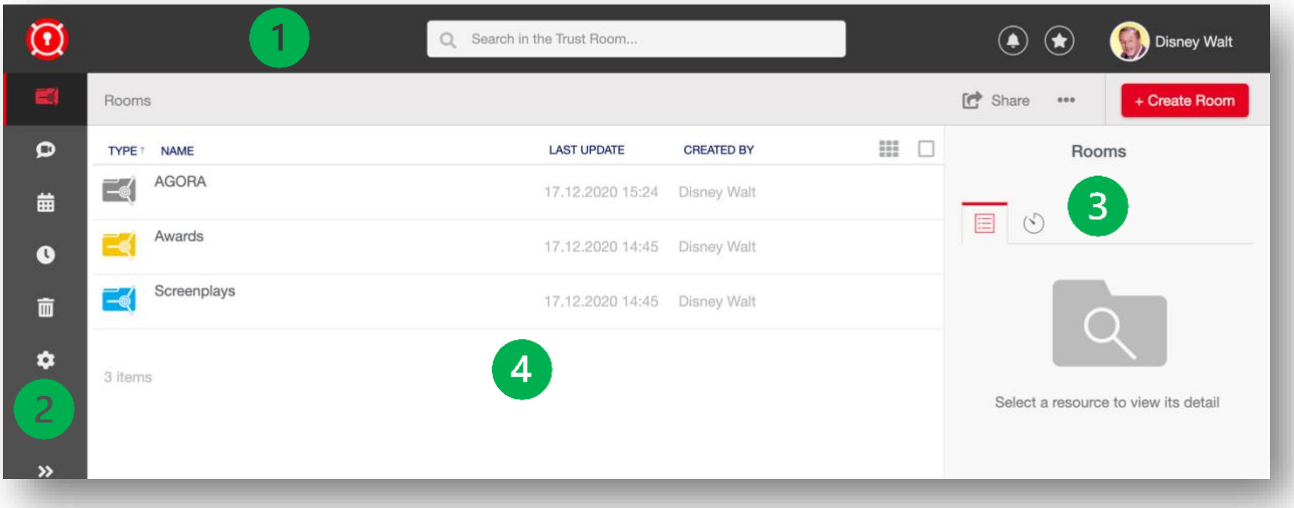
In order to access your Trust Room, go to the address https://collaboration.agora-secureware.ch and enter, in the login form, your username and password. In case your username is not an email address you are also asked to enter the name of your Trust Room.



If your account requires a two-factor authentication, you will be then asked to enter either a mobile TAN, sent to you by SMS, or a one-time password displayed on your mobile authentication App (like Google Authenticator, Duo, Authy or similar).

User interface structure

The platform’s user interface is structured as follows:

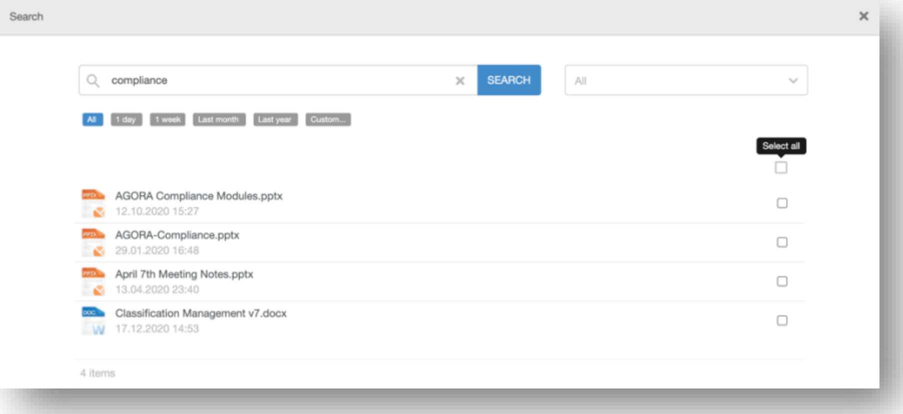

1
Search in the Trust Room...
Disney Walt
Rooms
Share
+ Create Room
2
3
4
Rooms
Select a resource to view its detail
3 items

TYPE	NAME	LAST UPDATE	CREATED BY
	AGORA	17.12.2020 15:24	Disney Walt
	Awards	17.12.2020 14:45	Disney Walt
	Screenplays	17.12.2020 14:45	Disney Walt

1 The **top bar**, which contains following elements:

The **logo** that can be replaced with a custom image for each Trust Room

Search: which allows you to look for any type of content inside your Trust Room



compliance

AGORA Compliance Modules.pptx 12.10.2020 15:27 □

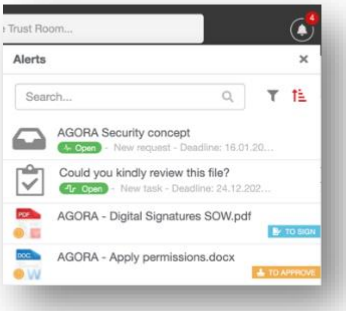
AGORA-Compliance.pptx 29.01.2020 16:48 □

April 7th Meeting Notes.pptx 13.04.2020 23:40 □

Classification Management v7.docx 17.12.2020 14:53 □

4 items

Alerts: this menu displays the list of what you are asked to: files to approve or sign, requests for documents, events invitations, tasks.



AGORA Security concept
Open - New request - Deadline: 16.01.20...

Could you kindly review this file?
Open - New task - Deadline: 24.12.202...

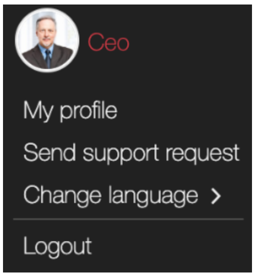
AGORA - Digital Signatures SOW.pdf

AGORA - Apply permissions.docx

★ The list of resources marked as **Favorites**.

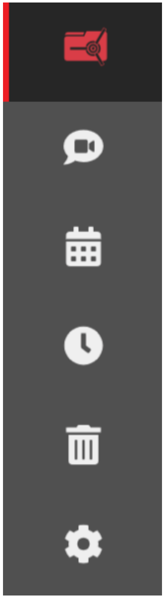
You can add resources to your favorites' list selecting "Add to favorites" from their "Actions" menu or simply clicking on the relative star inside the list view.

The **My profile** menu, where you can access your profile page, send a support request to your Trust Room manager, change the user interface language and also log out.

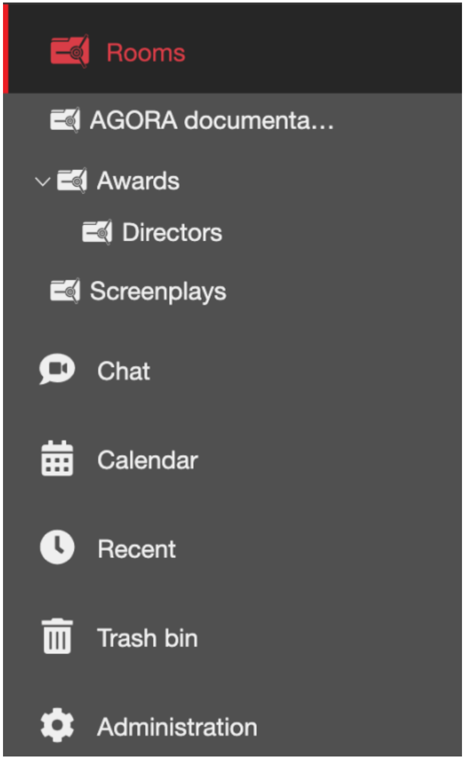


2 The **navigation bar**, where you can move between the different main sections of the application (the displayed options depend upon the configuration of your Trust Room and your permissions), and – once expanded – browse the tree structure of your rooms**.**

Navigation collapsed



Navigation expanded

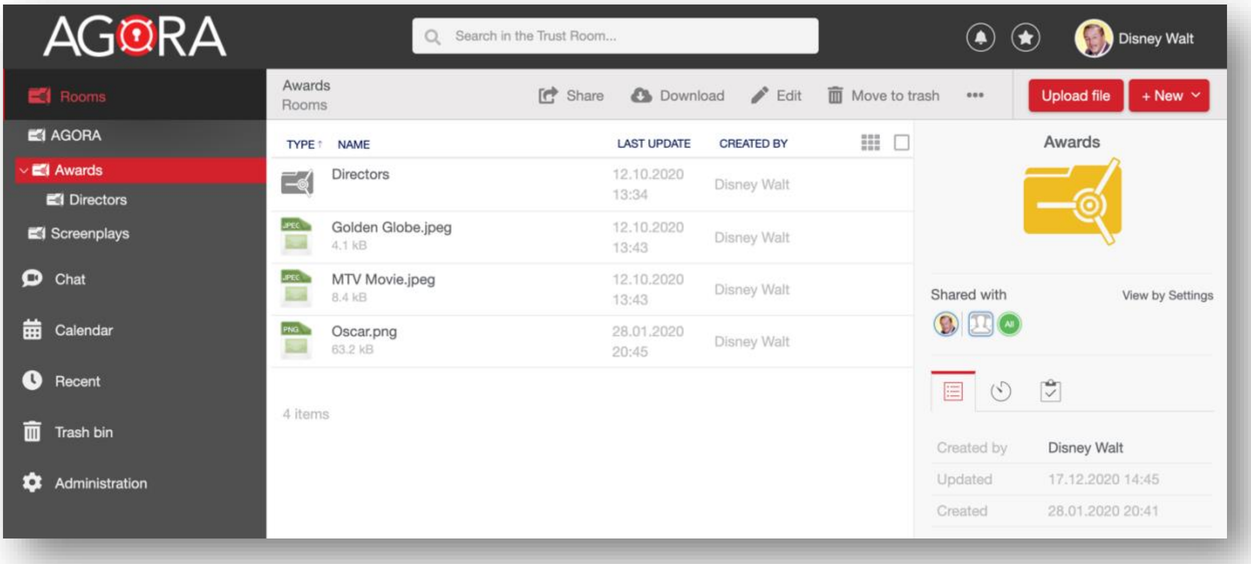


3 In the **detail bar**, on the right, are displayed the properties of the current resource (room, meeting, file, …) and also the users allowed to access it. The resource's owners are even allowed to view immediately the permissions that the single users/groups have on it.
If you select an element inside a room, you will see in this bar its detail (including the preview for files).

4 The **content**

Rooms

Inside this page you can browse all the information (Rooms, files, meetings, events, discussions, …) that were either shared with you or that you shared with others. You can drill down the rooms' hierarchy either clicking on the single list's elements or using the tree structure, displayed inside the navigation bar on the left.



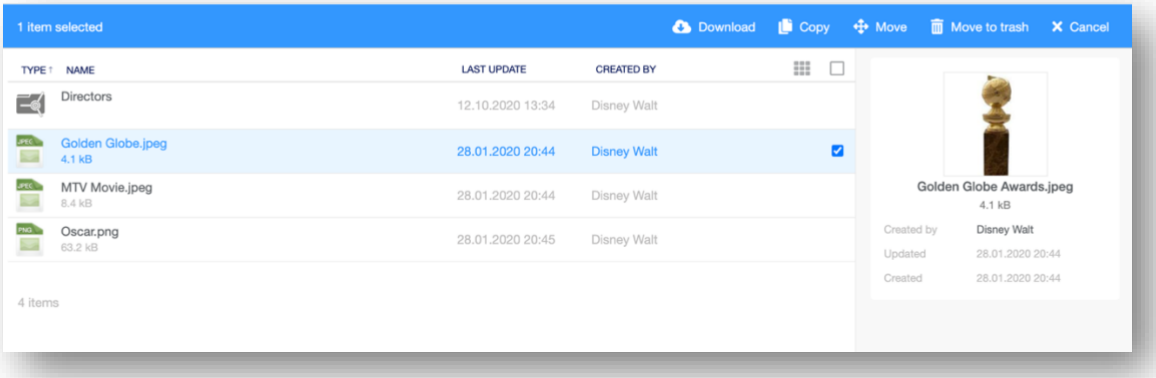
TYPE ↑	NAME	LAST UPDATE	CREATED BY
	Directors	12.10.2020 13:34	Disney Walt
	Golden Globe.jpeg 4.1 kB	12.10.2020 13:43	Disney Walt
	MTV Movie.jpeg 8.4 kB	12.10.2020 13:43	Disney Walt
	Oscar.png 63.2 kB	28.01.2020 20:45	Disney Walt

4 items

Awards

Created by	Disney Walt
Updated	17.12.2020 14:45
Created	28.01.2020 20:41

You are able to perform actions (like download, copy, move, delete) on multiple list's elements by performing a multiple selection, that can be done either by manually check the element's selection checkbox or holding Ctrl+Click (or Cmd+Click on Mac) and ranges with Shift+Click.



TYPE ↑	NAME	LAST UPDATE	CREATED BY	□
	Directors	12.10.2020 13:34	Disney Walt	
	Golden Globe.jpeg 4.1 kB	28.01.2020 20:44	Disney Walt	☑
	MTV Movie.jpeg 8.4 kB	28.01.2020 20:44	Disney Walt	
	Oscar.png 63.2 kB	28.01.2020 20:45	Disney Walt	

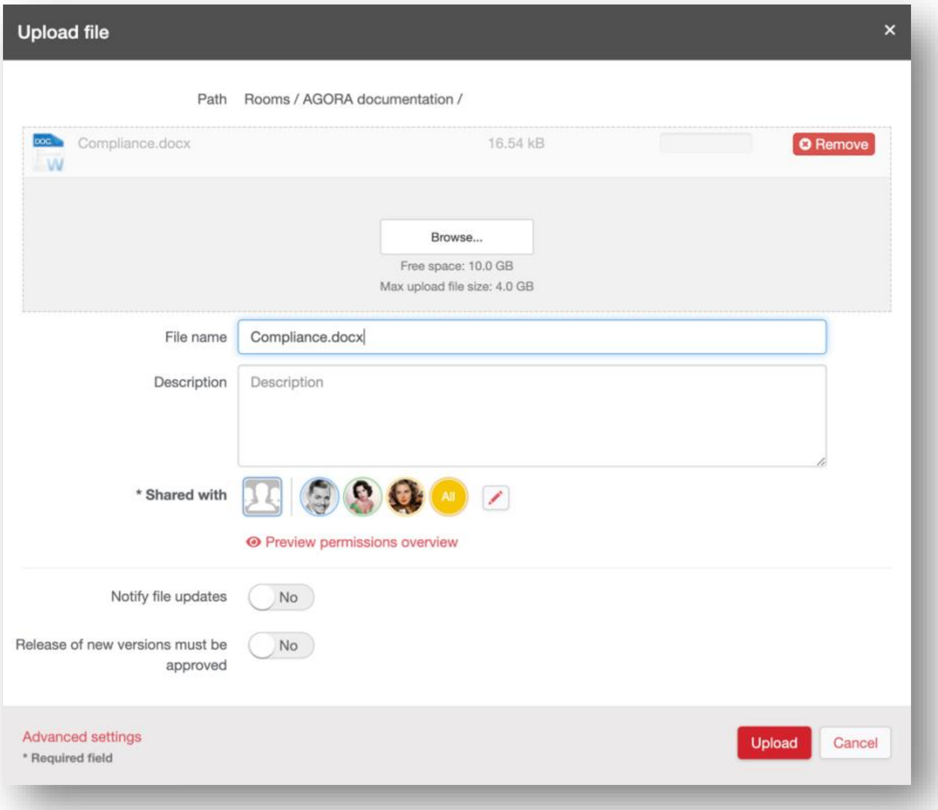
4 items

Golden Globe Awards.jpeg
4.1 kB

Created by	Disney Walt
Updated	28.01.2020 20:44
Created	28.01.2020 20:44

Upload a file

To upload a file, go to a room, where you own at least a “Contributor” permission (otherwise you are not allowed to do it) and either drag and drop from your system the desired file(s) or click on the “Upload file” button, you will see on the top right-hand corner of the screen.



Upload file

Path Rooms / AGORA documentation /

Compliance.docx 16.54 kB

Free space: 10.0 GB
Max upload file size: 4.0 GB

File name: Compliance.docx

Description: Description

* Shared with

Notify file updates: No

Release of new versions must be approved: No

* Required field

On the upload file form, in the most cases, you can simply confirm your action with "Upload" (since all the settings are inherited from the room).

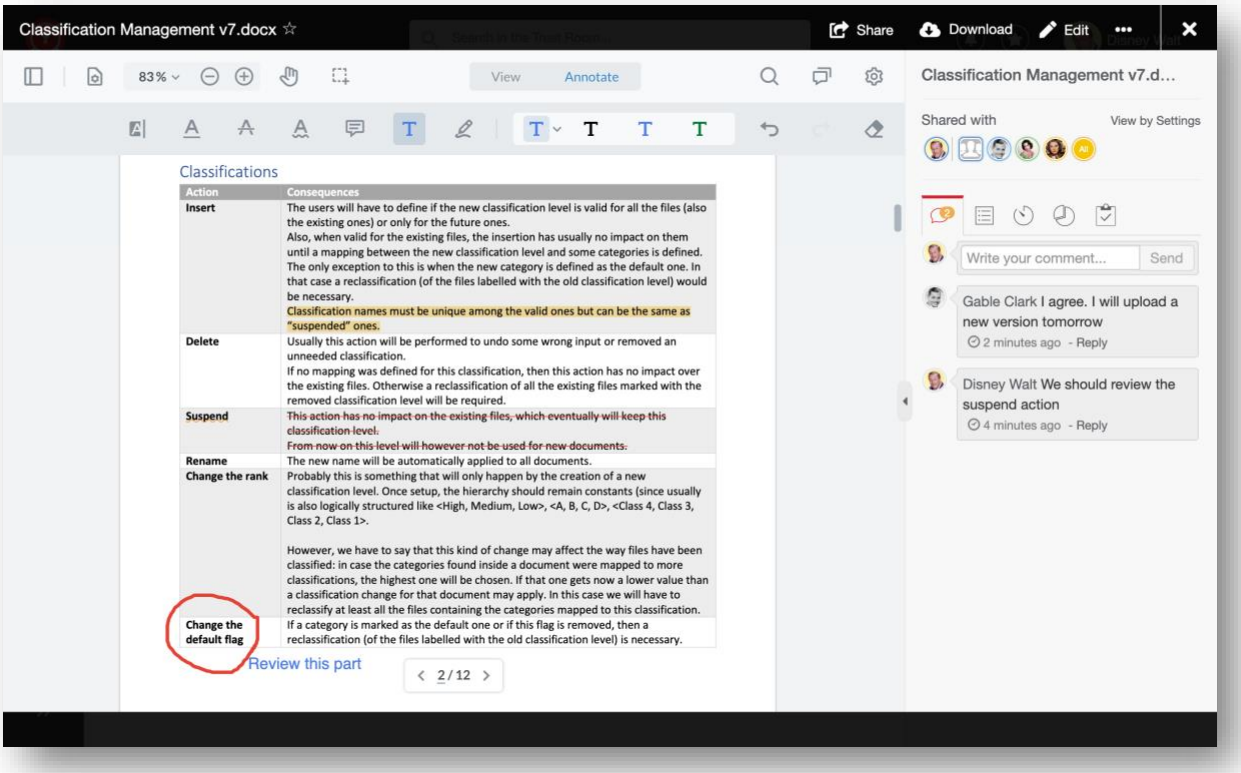
This form, however, enables to set more properties like:

- A description of the file
- The users/groups who can access this file and their permissions on it (Shared with)
- If someone has to be notified upon the publication of the file
- If someone has to approve the file prior its publication
- The lifetime of the file (when this file should be made visible and when it should be deleted)

File

When you open a file inside AGORA you get a powerful document reader[1] that offers many collaboration possibilities:

1. Share comments on the document
2. Add private annotations (text highlight, underline, strikethrough, free hand, free text and comments)
3. Search inside the document
4. View document's version history
5. View access statistic (only for the owners of the document)
6. View the history of the file (only for the owners of the document)
7. Assign tasks for this file



Classifications

Action	Consequences
Insert	The users will have to define if the new classification level is valid for all the files (also the existing ones) or only for the future ones. Also, when valid for the existing files, the insertion has usually no impact on them until a mapping between the new classification level and some categories is defined. The only exception to this is when the new category is defined as the default one. In that case a reclassification (of the files labelled with the old classification level) would be necessary. Classification names must be unique among the valid ones but can be the same as "suspended" ones.
Delete	Usually this action will be performed to undo some wrong input or removed an unneeded classification. If no mapping was defined for this classification, then this action has no impact over the existing files. Otherwise a reclassification of all the existing files marked with the removed classification level will be required.
Suspend	~~This action has no impact on the existing files, which eventually will keep this classification level.~~ ~~From now on this level will however not be used for new documents.~~
Rename	The new name will be automatically applied to all documents.
Change the rank	Probably this is something that will only happen by the creation of a new classification level. Once setup, the hierarchy should remain constants (since usually is also logically structured like <High, Medium, Low>, <A, B, C, D>, <Class 4, Class 3, Class 2, Class 1>. However, we have to say that this kind of change may affect the way files have been classified: in case the categories found inside a document were mapped to more classifications, the highest one will be chosen. If that one gets now a lower value than a classification change for that document may apply. In this case we will have to reclassify at least all the files containing the categories mapped to this classification.
Change the default flag	If a category is marked as the default one or if this flag is removed, then a reclassification (of the files labelled with the old classification level) is necessary.

Review this part

Gable Clark I agree. I will upload a new version tomorrow
2 minutes ago - Reply

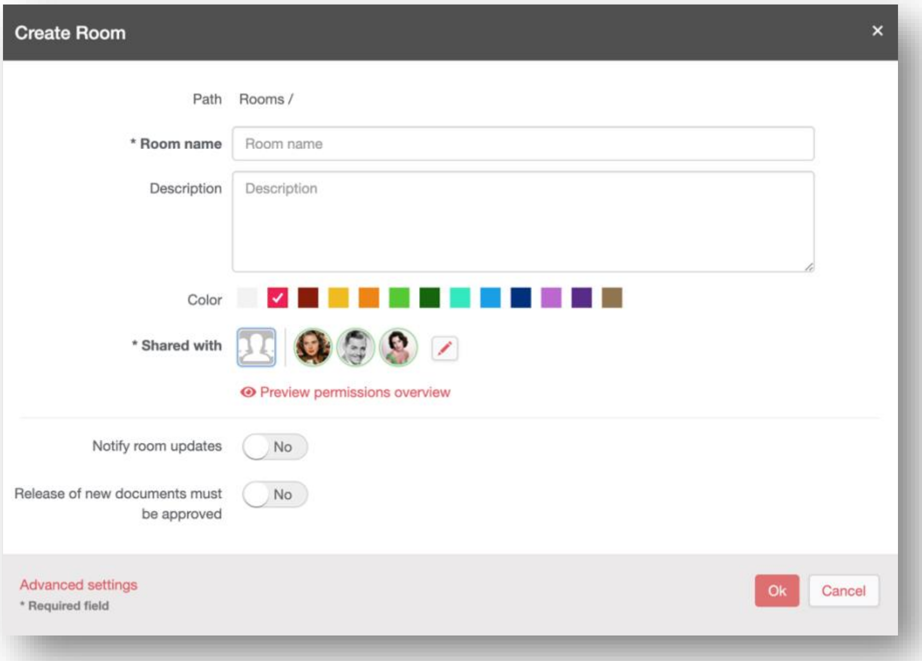
Disney Walt We should review the suspend action
4 minutes ago - Reply

[1] The preview of a document is available for the following file formats: Microsoft Office documents (Word, Excel, PowerPoint), PDF, images, text documents

Create a Room

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), notes, events, discussions and much more. On a Room, you define the general rules for the collaboration: who can participate and with which permission, the default notification settings, whether the files have to be first approved, whether there is a maximal lifetime for the documents stored there, etc.

To create a new Room, go to “Rooms” or select an existing 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.



Create Room

Path Rooms /

* Room name

Description

Color

* Shared with

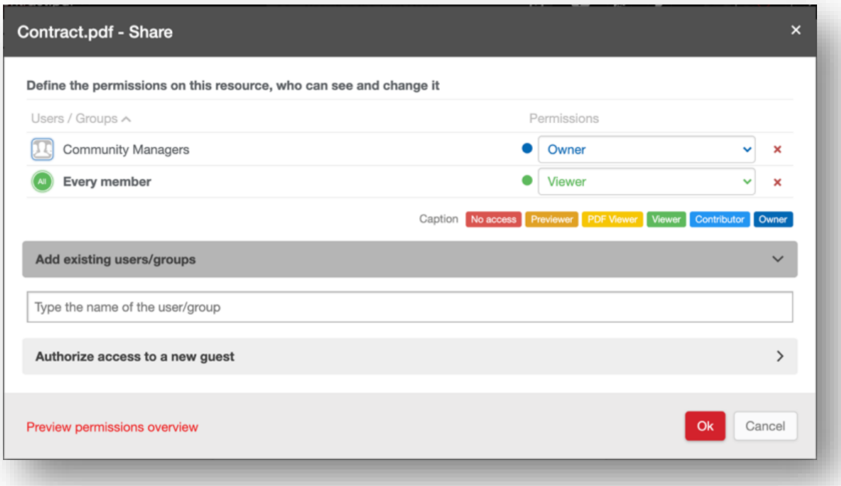
Notify room updates No

Release of new documents must be approved No

* Required field

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.



Contract.pdf - Share

Define the permissions on this resource, who can see and change it

Users / Groups	Permissions
Community Managers	Owner
Every member	Viewer

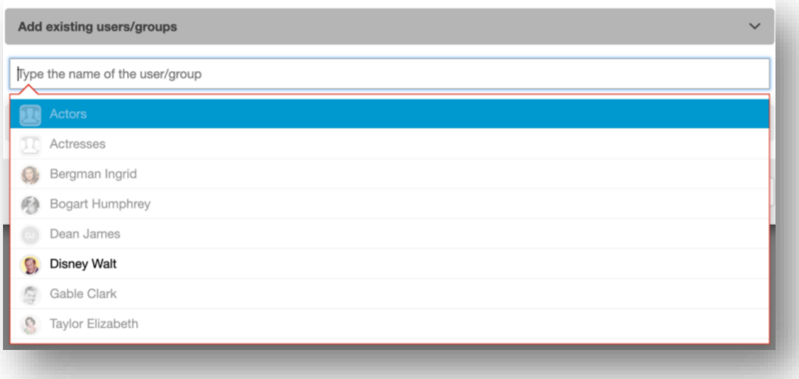
Caption: No access, Previewer, PDF Viewer, Viewer, Contributor, Owner

Add existing users/groups

Type the name of the user/group

Authorize access to a new guest

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.

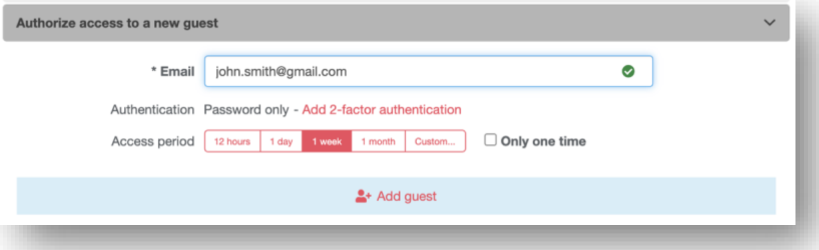


Add existing users/groups

Type the name of the user/group

- Actors
- Actresses
- Bergman Ingrid
- Bogart Humphrey
- Dean James
- Disney Walt
- Gable Clark
- Taylor Elizabeth

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.



Authorize access to a new guest

* Email: john.smith@gmail.com

Authentication: Password only - Add 2-factor authentication

Access period: 12 hours | 1 day | 1 week | 1 month | Custom...

□ Only one time

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