Secure Rooms

Version 3.11

Product Description

5.8.2021

Copyright © 2021 SSH Communications Security Corporation

This software and documentation are protected by international copyright laws and treaties. All rights reserved. SSH NQX® is a registered trademark of SSH Communications Security Corporation in certain jurisdictions.

SSH logos and names of products and services are trademarks of SSH Communications Security Corporation. Logos and names of products may be registered in certain jurisdictions.

All other names and marks are property of their respective owners.

No part of this publication may be reproduced, published, stored in an electronic database, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, for any purpose, without the prior written permission of SSH Communications Security Corporation.

THERE IS NO WARRANTY OF ANY KIND FOR THE ACCURACY, RELIABILITY OR USEFULNESS OF THIS INFORMATION EXCEPT AS REQUIRED BY APPLICABLE LAW OR EXPRESSLY AGREED IN WRITING.

Distributing, publishing and/or copying of this document is restricted, and requires a written statement from SSH Communications Security Corp.

SSH Communications Security Corporation
Karvaamokuja 2 B, FI-00380 Helsinki, Finland

Contents

1. Introduction **1**
2. User interface **2**
2.1 Top navigation bar 2
2.2 Main view 3
2.3 Room view 5
2.3.1 Breadcrumb 5
2.3.2 Instant messaging 7
2.3.3 Writing a message 8
2.3.4 Deleting a message 8
2.3.5 Appointments 8
2.3.6 Tasks 8
2.3.7 New poll 8
2.3.8 WIKI document 9
2.3.9 Board report 9
3. Configurations and user privileges **10**
3.1 Site configuration 10
3.2 Room settings 12
3.2.1 Configuration template used in a room 12
3.3 Site user settings 15
3.4 Room privileges 15
3.5 User settings 16
3.6 Configuration Template 16
4. User management **17**
4.1 Manual user management 17
4.2 User provisioning from AD via LDAP 17
4.3 User provisioning with REST API based to SCIM standard 18
5. Integration possibilities with other portals **18**
5.1 Single Sign-On 18
5.2 Information sharing via REST API 18
6. Requirements in operational environment **19**
6.1 Hardware and operating system requirements 19
6.1.1 Network connections and IP addresses 19
6.1.2 Cluster net (duplicated system) 19
6.1.3 SMS interface 19
6.1.4 Firewall settings 19

© 2021 SSH Communications Security Corporation

1. Introduction

CollabRoom combines secure file storing, sharing and messaging as well as other useful group functions into a single entity. The secure workspace enables you to share information with different groups easily and securely. Both internal and external users can be included. Workspace's security levels can be created according to the company's information security guidelines.

As for the user, collabRoom is fully responsive supporting different browsers and devices so that it works also with smart phones, for example. The use of the service can be restricted and users can be authenticated strongly with SSN based authentication*****, strongly with two-factor authentication****** or more flexible, for example, with a password or with a PIN code sent to GSM number. The collabRoom can be easily integrated with other portals with OpenID Connect based Single Sign-On.

The solution can be integrated with e-mail and sFTP interfaces so that the information can be transferred directly to various clients without laborious steps in between.

The service is used over protected TLS (HTTPS) connection with browser. The secure platform guarantees the information security and data protection in closed system.

***** *BankID (Sweden and Norway), Finnish Trust Network (banking recognition with Signicat or Telia), Generic OpenID Connect based SSN authentication, NemID, Suomi.fi*

****** *SMS-PIN + Password, MOTP and TOTP*

© 2021 SSH Communications Security Corporation

2. User interface

2.1 Top navigation bar

Top navigation bar is shown statically on each view. It includes the instance logo, user settings, logout button and help button. Depending on the admin privileges, site configurations, site users, admin view of the rooms and configuration templates can also be visible.

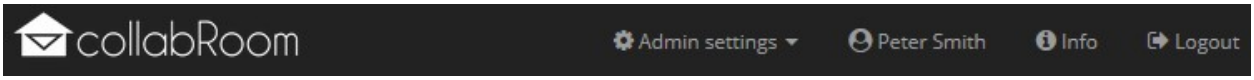


Figure 1. Top navigation bar

The following actions are available depending on privileges:

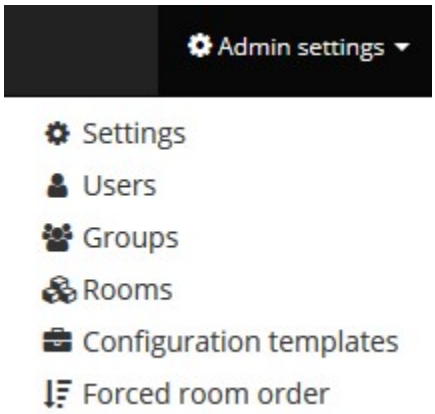


Figure 2. Actions available depending on privileges

Table 1. Descriptions of actions

	Settings	Site configuration can be used to set system-wide restrictions on, among other things, the method of sending notification messages.
	Users	In user management new users can be created and individual administrative privileges set.
	Groups	Toll for managing user groups and group privileges.
	Rooms	Tool for room management. Admin with privileges to see all rooms can change room settings and edit users without seeing the actual content of the room.
	Configuration templates	Configuration templates are used to create desired preset templates to a room. The template defines the default values for certain settings.
	Forced room order	Administrator can choose to globally override user-specific room order settings (alphabetical, rooms with new messages first).

© 2021 SSH Communications Security Corporation

Peter Smith	**User settings**	From user settings the user can change their own preferences and info, such as e-mail address, mobile phone number and password.
Info	**Help**	Toggles help window depending on the view.
Logout	**Logout**	Logouts securely from the system.

2.2 Main view

The main interface of collabRoom is a page where user lands after initial authentication. The main view is personal for each user. The main view shows rooms where the user has been given access rights to. In the main view the user can toggle to private files area. Rooms can be seen as boxes in the center of the view and they include, among other things, the name of the room and the number of messages and users. User can define from own settings if the rooms with new messages are shown first or whether the rooms are in alphabetical order.

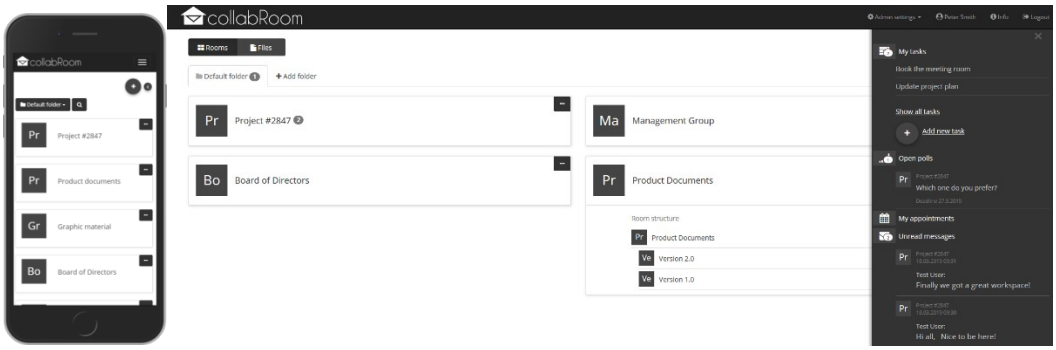


Figure 3. Main view of collabRoom as seen on a smartphone and with a browser. Example of a Rooms view

User can group the rooms into different folders. In the main view, the user can select by folder which rooms will be displayed. Folders are personal so that moving a room to a folder does not affect the view of other users. The main view also includes a search box that searches the message tags. As a result of the search, only rooms with corresponding message are shown in the main view.

Overview also contains meetings, tasks and polls that are pointed to current user. User is also able to find the latest activity in workspaces from Unread messages and Activity feed.

In a files view a user can add and manage private files. Those files can be kept in private files just for archiving purposes or can be used in rooms. The user can add files either from private files or from a local computer.

© 2021 SSH Communications Security Corporation

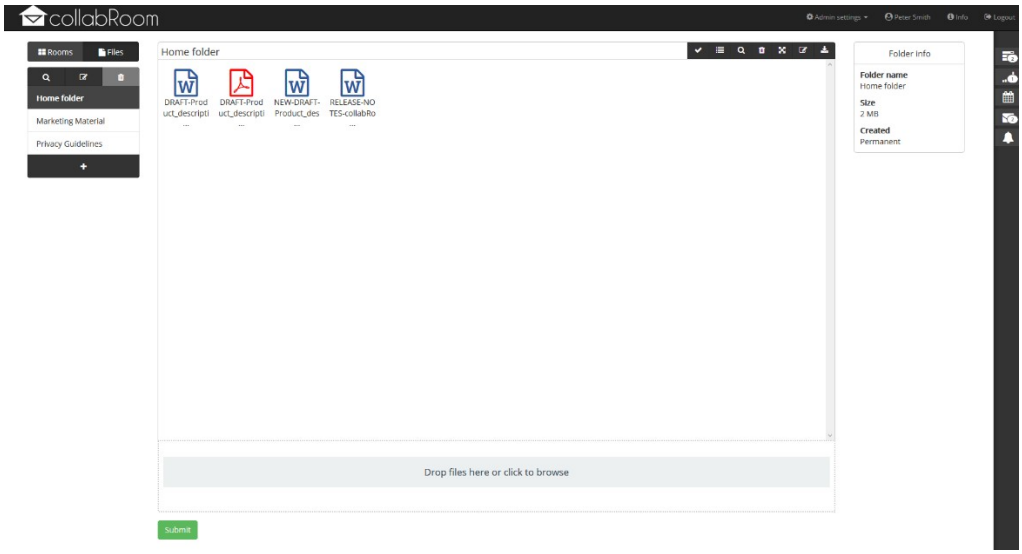
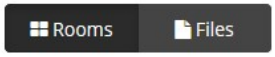
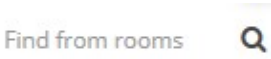
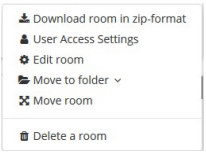
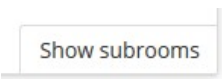


Figure 4. Main view of collabRoom as seen on a browser. Example of a Files view

The following actions are available in the main view:

Table 2. Actions in the main view

	**Rooms/Files toggle**	Rooms view is selected by default. By switching to Files view a user can add and manage private files. In a room the user can add files either from private files or from local computer.
	Folders	By selecting a folder all rooms in that folder can be seen. “Add folder” opens page where a new folder can be created.
	**Search bar**	Searches content / tags from rooms. As a result of the search, only rooms with corresponding message are shown in the main view.
	New room	Opens a wizard for creating a new room.
	**Actions**	Enables downloading, deleting or editing the room, as well as adding users or moving the room to a different folder/changing room structure.
	**Subroom indicator**	If room has subrooms, they are shown here.

© 2021 SSH Communications Security Corporation

2.3 Room view

Room view is a shared view for all users of the room. It is parallel to all room users. There are four icons on the right side of the room title that can change the message listing of the room view. Options are: message view, tree view, list view and file view. Listing determines the manner in which the messages/files are shown in the room.

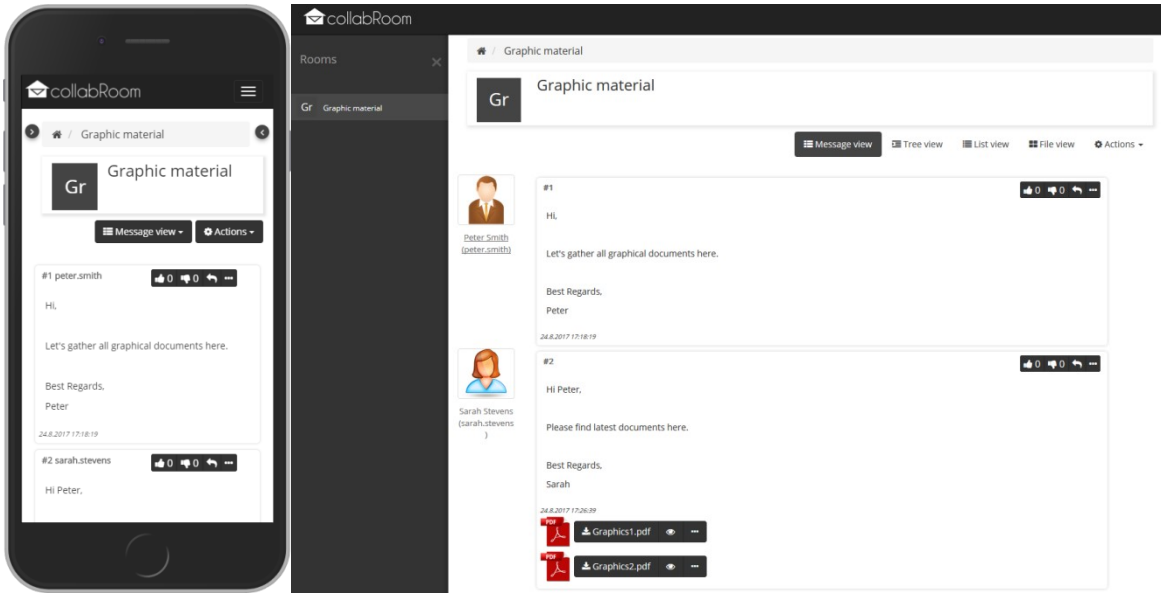


Figure 5. Room view

On the right side of the room view are the room specific appointments, tasks, polls and activity. The left side of the room view shows the name of the room that always takes back to the main room view. In addition, the sub-rooms are shown on the left-hand side

Figure 6. Example of file view

2.3.1 Breadcrumb

Navigation in the room can be done also with a breadcrumb (Figure 7) locating below the top navigation bar. User can return to main view by clicking the logo icon on the left side.

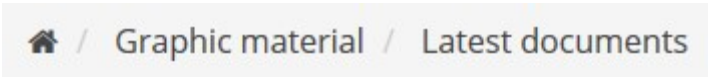
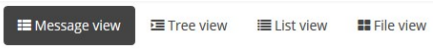
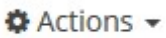
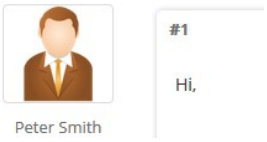
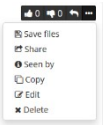
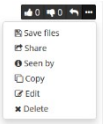
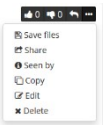
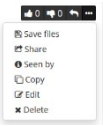


Figure 7. Breadcrumb

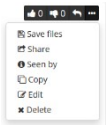
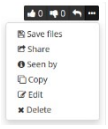
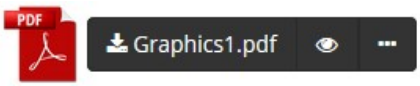
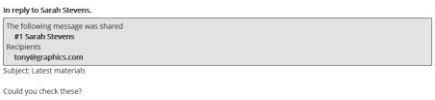
The following actions are available in the room view:

© 2021 SSH Communications Security Corporation

Table 3. UI components

	Title	Title of the room.
	**Views**	The message listing of the room view. Options are: message view, tree view, list view and file view. Selected view is remembered and used across all rooms (where available).
	**Room actions**	Depending on room privileges, user can access room settings and user access settings, room reporting, view room users, create new subrooms, view room tasks, create new appointments and polls, send message to nonmember of the room and create new wiki documents.
	**Message header**	Message header shows the writer's name and profile picture as well as the running number.
thumbs down	**Thumbs up /**	Users can like/unlike the messages. Others can see who has liked or unliked the message.
	**Save files**	A user can save files from own messages.
	**Share**	Depending on room privileges, user can share specific message to non-member of the room.
	**Seen by**	Depending on room settings, user can see a list of the users who have been visited the room after the message have been composed.
	**Copy**	Depending on room privileges, the user can copy messages to other rooms.

© 2021 SSH Communications Security Corporation

	**Edit**	Depending on room privileges, user can edit messages.
	**Delete**	Depending on room privileges, user can remove messages.
	Reply	Replying to a specific message.
	**Attachment**	Attachments are shown with their common file type icon and the name of the attachment. Files can be viewed as images and it can be defined which attachments may be downloaded.
	**Shared message indicator**	When a message is shared, all users of the room get a notification of it that is shown as a new message.

2.3.2 Instant messaging

From message writer's name opens a window for instant messaging with that user, if instant messaging is enabled in the room.

Users are able to send 1to1 instant messages by clicking the username above the message. A new chat window will open (*Figure 8)*.

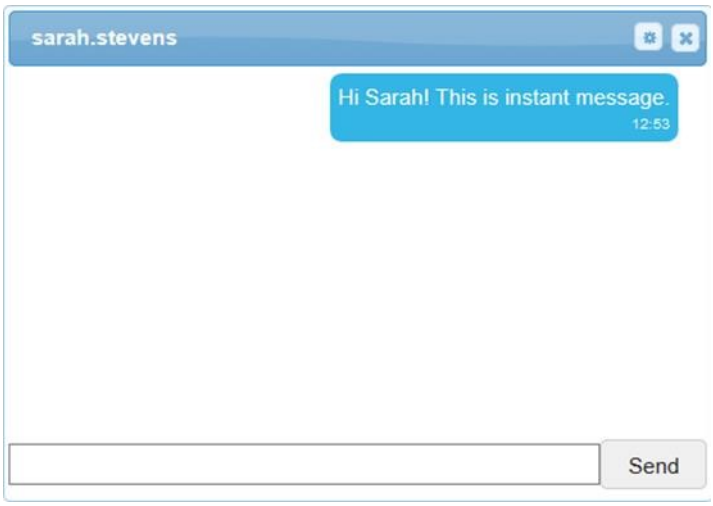


Figure 8. Instant message modal

2.3.3 Writing a message

On the bottom of the room view is message writing tool where you can write new messages. A message can be written using the standard formatting tools, such as bold, italic and underline. Message editor also enables special characters, making tables, adding pictures directly to text, and it is possible to create links, undo & redo and find & replace, for example.

Files are transferred either by dragging the file to the files field or by selecting the file from own computer. In the list view a file can be dragged and dropped directly to the middle of the view on top of a message, and the file is automatically sent to the room without separate function for sending a message.

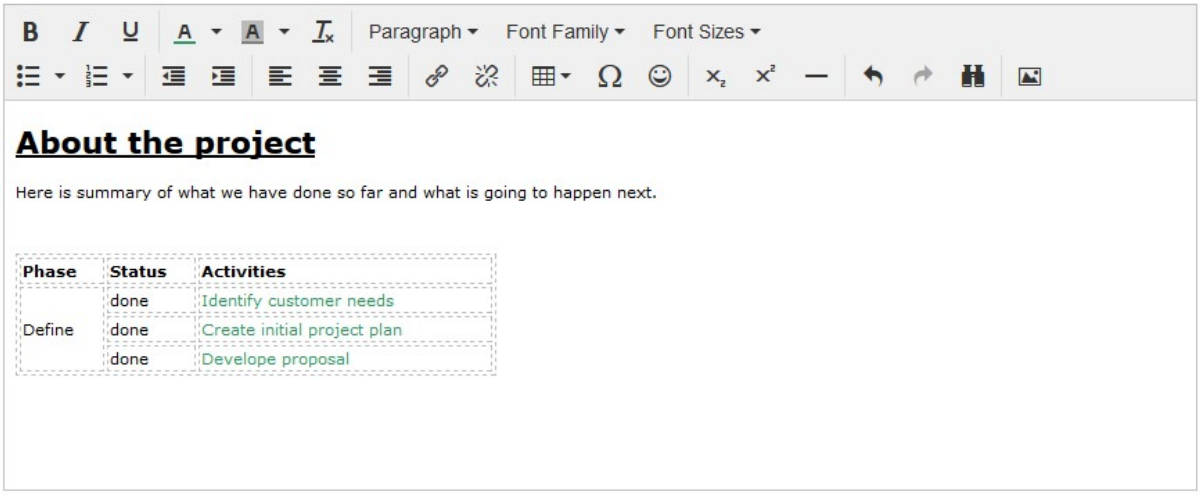


Figure 9. Message writing tool

2.3.4 Deleting a message

Own message can be removed from a room by choosing “Delete” icon under message “…”-menu. Only a moderator can delete other users’ messages.

2.3.5 Appointments

Purpose of room appointment is to establish a common time, for example, for a meeting. New suggestion for an appointment is added from room actions under “Appointments”. Appointment is always linked to a room so that a new meeting can only be created by going into a room first. Location, attendants and suggested times are entered to the appointments. After this, participants will be able to choose what time is suitable for them. When an option is suitable for all, then the meeting creator can lock this date as an agreed date.

2.3.6 Tasks

Different task can be created. Task can be assigned to a specific person. The task can be edited, marked as done or removed afterwards.

2.3.7 New poll

With polls it is possible to create quick surveys. Polls can be created under room actions. A poll is always given a question and the choices for answers. Choices are written with each option on a separate line.

The creator of the poll can choose whether the answers are shown only to himself, the survey respondents, or all users of the room. The creator of the poll can also choose how the results are

© 2021 SSH Communications Security Corporation

displayed: so that the answers will show who voted what, or so that it is only shown how many votes each option has received. The creator of the poll can also choose if it possible to choose one or more options. The poll can also have a deadline after which voting is no longer possible.

2.3.8 WIKI document

With WIKI it is possible to create group documents that can be edited. WIKI shows the document version history. It can also be downloaded as a PDF document.

2.3.9 Board report

Users with sufficient privileges (moderators and admins) are able to view reporting from user actions within a room.

Figure 10. Reporting from user actions

3. Configurations and user privileges

Configurations and user privileges are divided into two levels: site and room levels. Site level configurations and user privileges can be seen and accessed only by users who have the appropriate admin privileges.

All the requests that are made to collabRoom are logged into Audit trail. This makes it possible to see who has made changes and when. The checksums of all uploaded or downloaded files are also saved to Audit trail.

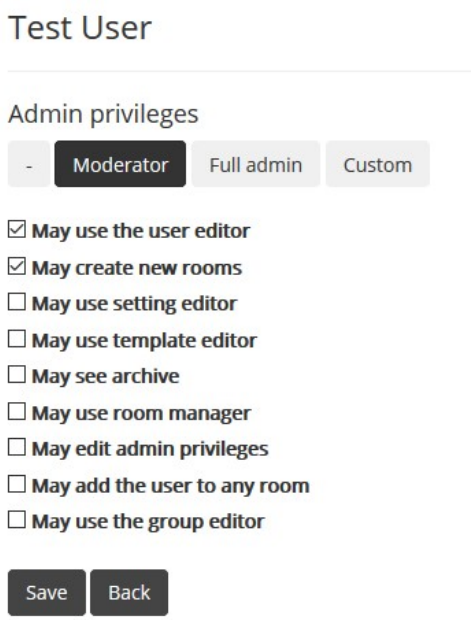


Figure 11. Site level privilege selector (Admin privileges)

3.1 Site configuration

Site configuration can be accessed from the top navigation bar (Admin settings). Site configuration can be used to set system-wide restrictions on, among other things, the method of sending notification messages.

- **Invitation sender email address:** Possible to define the e-mail address that is used as a sender of the invitation messages. By default the system generates a random string that is used as the sender address.
- **Login page logo file:** Organization's own logo can be entered. Logo will be shown in login page.
- **Navigation bar background image (default: none):** The top bar can have a background image. The image will appear on all pages.
- **Header logo file (default: none):** The top bar can have Organization's own logo.
- **CSS theme:** Select CSS theme from templates.
- **CSS:** Possible to define CSS specifications (such as colors and fonts) that affect the whole system.
- **Allow users to order password reset link:** Specify whether users can order a link to their e-mail to change their password in the login page. If this is not allowed and the user forgets their password, the administrator must set a new password.

© 2021 SSH Communications Security Corporation

-
- **Allow users to change TOTP application:** Specify whether users can change their TOTP authentication application.

  Prevent users from changing their GSM number: Specify whether users can change their GSM number (if relevant to authentication method)
- **Prevent users from changing their email address:** Specify whether users can change their email address (if relevant to authentication method)
- **Enable email notifications for all users:** Selecting this will enable email notification for all users by default.
- **Disable SMS notifications:** Prevent that users can order notifications with SMS.
- **Enable FTP rooms:** Select whether FTP room option will be shown in the new room creation modal.
- Hide user list from room moderators in room access settings: Select whether user list is shown for room moderators.
- **Include user ID in invitation and notification links:** If this is enabled, the links in invitation and notification messages includes the username so that the user only needs to enter their password in log in page. If this is disabled, the user needs to enter both username and password.
- **Limit allowed notification methods (default: off):** If the option is enabled, it can be individually configured from user settings who of the users are not able to receive notifications, or can only receive e-mail or SMS notifications, for example.
- **Send notifications in plaintext within own organization:** Notification messages are always sent encrypted to users outside the organization, but it is possible to choose whether e-mail notifications are sent encrypted or unencrypted to your organization’s users.
- **Encrypt message bodies in database:** By default, all messages are encrypted in the database. In this case, the search feature cannot retrieve data from messages, but only from message tags. If the messages are not encrypted, then the search will also search hits from the message body.
- **Minimum length of password:** The minimum length of password set by the user can be determined.
- **The password must contain at least one lowercase, uppercase, numeric and special character:** To increase security it can be required that the password must contain at least one lowercase letter, uppercase letter, number and special character.
- **Notification interval (default: 4 hours):** The default setting for notification interval of new actions in rooms can be defined. Each user can set this up for themselves, but the default value can be defined. Minimum value is one hour.
- **Lifetime for deleted room (default: 7 days):** A deleted room will be stored on the server for a limited time in case there is a need to recover it. It can be defined how many days the room information will remain after the removal. The room must be turned active during this period. After this time, the room will be permanently deleted and the information is not recoverable.
- **Get users from LDAP (default: off):** collabRoom can be integrated with company’s AD system. User accounts are made from the e-mail addresses located in AD. During initial authentication users must create their own passwords. LDAP user import also supports phone numbers and defining group memberships. Users with an attached phone number are created with pin-code login

© 2021 SSH Communications Security Corporation

- enabled.With group memberships users can have permissions assigned to them automatically. Specific LDAP settings can be found in D-Center.
- **Convert URL-addresses in messages to links (default: on):** All URL addresses (http, https) in messages can be turned into links automatically.
- **Remove attached files when removing a message (default: on):** It can be defined what happens to files attached to a message if the message is deleted. If this is not selected, the files remain on the server even when the actual message is deleted.

  Disk space reserved for the instance (MB), empty (default: unlimited): An instance-specific quota can be set that determines how much space all rooms can take. If the quota is met, files can no longer be uploaded.
- **Enable personal storage:** Select whether personal file storage is available for all users.
- **Allow external users to use personal storage:** Select whether personal file storage is available for external users.
- **Disk space reserved for each users's personal files (MB):** Define a quota in MB for each users personal file storage.
- **Limit amount of users shown in user editor:** Limit amount of users shown on user administration page.
- **Show disclaimer for new users when logging in: (default: off):** Disclaimer page is shown to all users the first time they log in. Users need to accept it or their access will be denied. Users can be asked to accept it again if the disclaimer text is changed.
- **Hide user list from room moderators in room user access settings:** Select whether room administrators are able to view the list of user names within their rooms.
- **Restrict room moderators from changing room notification alias:** Select whether room moderators can change the email address used for sending room notifications.
- **Reset all room notification aliases to their default values:** Reset to pre-generated defaults.
- **Invitation and notification e-mail templates:** The template for sending invitations to the site or to a room as well as notifications of changes to a room can be defined. Settings include the message subject, e-mail body, text on links and e-mail address for SMS notifications.
- **Default setting for email notifications:** E-mail notifications can include the body texts of the new messages posted, message sender information or no data (default).

3.2 Room settings

From room settings it is possible to set, for example, room configuration template, topic of the room, content of notification messages, need for additional protection, room logo and room e-mail address.

3.2.1 Configuration template used in a room

Configuration templates are predefined room settings defined by administrator. Editing configuration templates takes place in the top menu under Admin Settings - "Configuration templates". Configuration

•
templates should be executed based on the company's or organization's information security policy. Configuration template also defines what default settings can be changed from room settings.

- **Beginning part of notification message sending e-mail address:** Room's private e-mail address can be defined. Room notifies the room users of any changes from this address. Replying to a room by e-mail is also done by using this address as the receiver. As default, individual address has been generated to the room.
- **Enable email notifications (default: off):** The room can notify of new messages and activities to users but only if a users' personal notifications are enabled. Notifications may include the message body or only sender data.
- **Default privilege when adding user to room:** Select a default privilege template for users when they are added to a room.
- **Invitation and notification message settings:** Invitation message and notification messages can have room specific subject lines and texts.

  Show this many messages (default: 25): It can be defined how many messages are displayed in the room view at a time.
- **Additional room protection (default: off):** In addition to system authentication, the room can be determined to require strong SSN based authentication* or password authentication. This authentication is required when user chooses the room from main view. If room's additional protection is "Shared password", the password must be given to the "New password" and "Confirm password" fields.
  ** BankID (Sweden and Norway), Finnish Trust Network (banking recognition with Signicat or Telia), Generic OpenID Connect based SSN authentication, NemID, Suomi.fi*
- **Prevent administrators' access to room settings and user management:** Deny access to the room and it's settings for admin users. If this is not enabled an administrator who has rights to add users to any room can add or remove users from a room without asking permissions from room owner. If this setting is enabled in a room an administrator cannot add or remove users from the room.
- **Allowed components (default: all):** It can be chosen which components are available in the room. Options are wiki, polls, instant messaging and files.
- **Allowed room views (default: all):** It can be defined what room views the user can use. Options are message, tree, list and file view.
- **Default view:** Select a default view, that will be used always when a user enters a room. It is also possible to override user preference (user preference being the previous option used by a user).
- **External users allowed (default: on):** External users are those whose e-mail address is not included in the e-mail domains of this instance. By selecting "Yes", the room can have users also from other organizations.
- **Show files as images (default: off):** If the file is of the correct type (for example an image or a PDFfile) and this setting is enabled, the file is shown in a dialog on the web page one page at time, without the file being downloadable. If the file cannot be converted or the conversion fails, the file remains downloadable. It is possible to view files as images even if the room does not have the

© 2021 SSH Communications Security Corporation

- setting “change files to images” enabled. As default, ImageMagick is used as the underlying file to image conversion tool but PDFBox is also available.
- **Attachment download restrictions:** Define which attachments may be downloaded. Attachment downloading options are: allow attachment downloading, disable attachment downloads and only allow downloads for files that cannot be converted to preview images.
- **Allow messages to guests (default: on):** Users of a room can send an e-mail message in the name of the room or in their own name. Receiver can reply to this message and the reply will be shown to all users in the room or as an e-mail only to the person who sent the message.
- **Allow users to see who has seen their messages (default: off):** By enabling this all room users are able to check a list of the users visited the room after the message have been composed. Some files can be converted to images. For example docx files can be seen as picture instead of having to use Microsoft Office. Converted images can be commented. Comments can be either public or private and they are page specific.
- **Message sharing allowed (default: on):** It is possible to allow a user to share specific message to non-member of the room. The non-member can also reply to this message and the reply will be shown to all users in the room. When a message is shared, all users of the room get a notification of it that is shown as a new message. Text in the notification message template can be edited.
- **Attachment allowed in reply of shared message**: It is possible to allow a user to add attachment/s for shared message.

  Allow files to be shared to external users via link (default: off): Any file attached to a message can be shared with a generated link to users outside of collabRoom.
- **Disable list of room users:** Select whether room user list is visible in the room action menu. (Affects also administrators and room moderators)
- **Share notification message:** Email notification sent to recipients of a share can be modified.
- **Set expiration date for the room:** A room can be set to expire on a pre-defined date. NOTE: all room data will be permanently removed!
- **Delete posts after days:** Posts older than the set date date will be automatically deleted.
- **Allowed file extensions (default: all):** It is possible to specify the file types that can be added to a room. Allowed file extensions are separated by commas, for example “ppt,pdf,doc”.
- **Allowed IP networks (default: unlimited):** It is possible to specify the IP address space that has access to the room. For example, a room can be entered from internal network only.
- **Disk space reserved for the room (default: unlimited):** It is possible to set a limit on how much space the room’s files can take in total. The limit is set in megabytes.
- **Room logo:** Room can have a logo, picture or an icon with chosen color to easily separate it from other rooms.
- **Room order:** Administrator can decide how the room order is shown to all users in main view. Moderator can also decide how the room order with subrooms is shown. For example, some rooms can always be on top. This can be done under Admin settings – “Forced room order”.

© 2021 SSH Communications Security Corporation

•

3.3 Site user settings

In user management new users can be created and individual administrative privileges set. Users can be added one by one or several at a time. Users can also be removed, and disabled users can be restored unless permanently deleted. In addition, the invitation link can be sent to users.

3.4 Room privileges

Room users and their privileges can be changes. The default roles are: moderator, writer and reader. In addition it is possible to customize the privileges, such as the right to delete the messages posted by others and change room settings.

Administrator can set a validity period for room-specific user access. This gives the possibility to define fixed term access without needing to manually delete the user from a room.

© 2021 SSH Communications Security Corporation

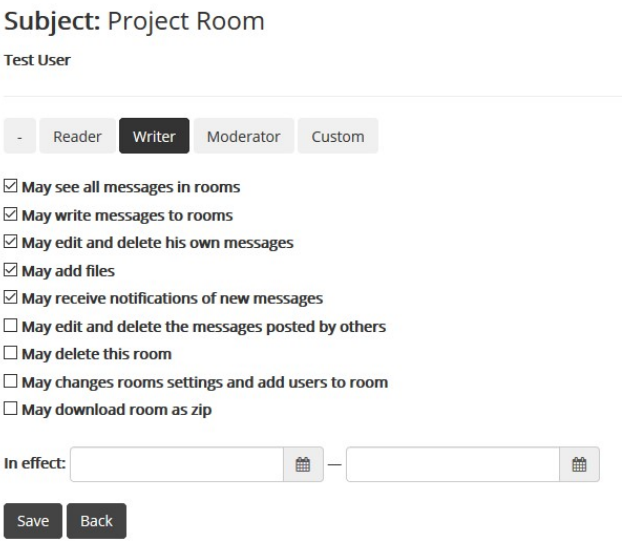


Figure 12. Room user-privilege selector

By defining different user groups and group privileges bulk privilege management is easy. For example, feature can be utilized when needing to add new admins, moderators or project managers to multiple rooms at once. Groups can be defined under Admin settings – “Groups”.

3.5 User settings

From user settings the user can change the user interface language (Danish, Deutsch, English, Estonian, Finnish, Latvian, Lithuanian, Norwegian, Russian, Swedish), own e-mail address, mobile phone number and password. In addition, the user can specify notification settings for new actions in the room, create new folders or delete them and also move rooms to folders. From additional settings the user can define, among other things, the interval for notifications and room order as well as change own profile image.

3.6 Configuration Template

Configuration templates are used to create desired preset templates to a room. Whenever a room is created, it must be chosen what configuration template it uses. The template defines the default values for settings, such as, if additional room protection is required, what are the allowed IP networks, are email notifications enabled, what extra features (instant messaging, polls, wiki etc.) are enabled, are external users allowed and what room views the users can choose from. In addition, the template defines if the presets can be changed when the room is created.

© 2021 SSH Communications Security Corporation

User management

4.1 Manual user management

collabRoom contains flexible and easy to use user management editor. The editor allows an administrator to create, edit and delete users in the collabRoom. Users can be added one by one or in a large group with CSV.

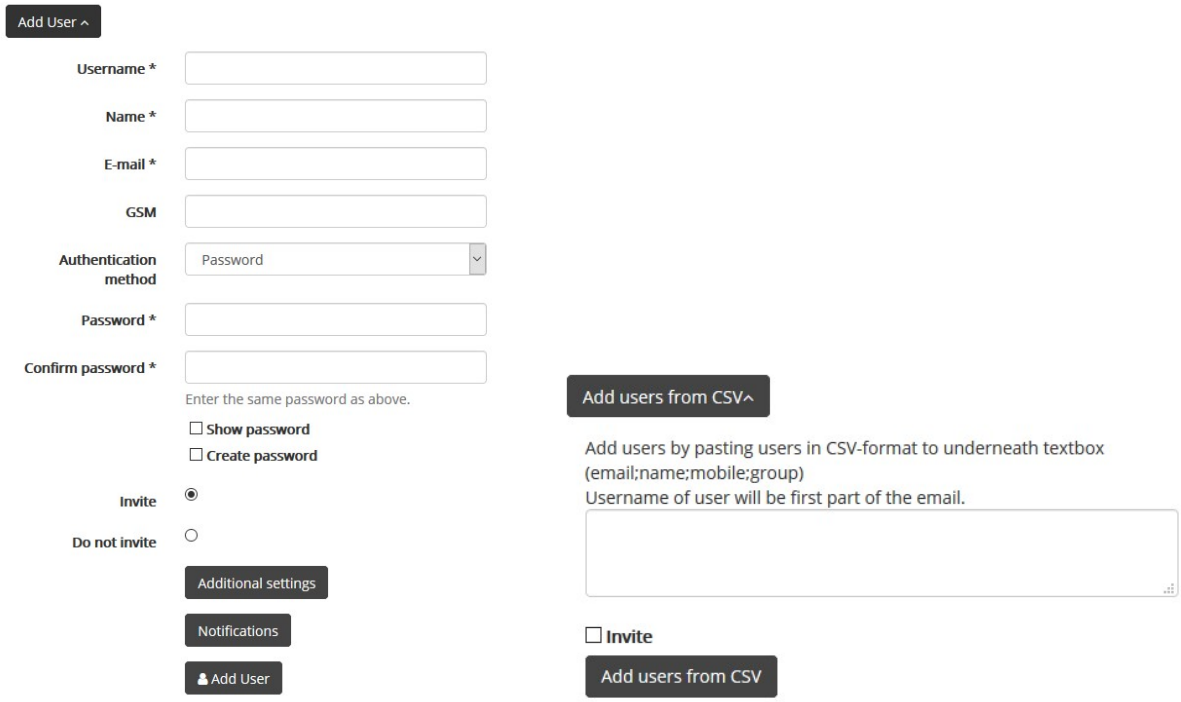


Figure 13. On the left image of a user editor which allows to add users one by one. On the right image of a user editor which allows to add users in a large group with CSV.

4.2 User provisioning from AD via LDAP

collabRoom supports user provisioning from AD via LDAP. Users can be created/deleted automatically. Users authentication method will be set according to LDAP query.

© 2021 SSH Communications Security Corporation

4.3 User provisioning with REST API based to SCIM standard

collabRoom users can be added with REST API which is based to SCIM standard v2. The API supports creating, editing and deleting of users and groups.

5. Integration possibilities with other portals

5.1 Single Sign-On

OpenID Connect based Single Sign-On as a stand-alone authentication method is supported and recommended if the collabRoom is intended to use together with other organization's portals. With SingleSign-On users can access the collabRoom from other portals without any additional authentication requirements. Room specific access management has to be always configured in collabRoom.

5.2 Information sharing via REST API

collabRoom contains “provider of external info” REST API which offers some basic information about events and happenings in collabRoom. This API can be used to fetch information about collabRoom to other organization’s portals.

© 2021 SSH Communications Security Corporation

SSH.COM Requirements i

6. Requirements in operational environment

6.1 Hardware and operating system requirements

Operating system is either RedHat Enterprise Linux 8 or Centos 8 with postfix –mail delivery system and Apache Web Server.

Recommended virtual hardware 4 -n CPU (2000MHz), 8 GB RAM, 146 GB HDD, two network adapters (if clustered).

6.1.1 Network connections and IP addresses

Servers are placed in to the network (typically to DMZ) Sec@GW server requires one to three public IP addresses. One IP address (eth0:0 adapter) will be used as a cluster address through which e-mail traffic is relayed. This IP address is used by the active machine. If NAT is used in address translation, information of both public and network address translated addresses is needed.

6.1.2 Cluster net (duplicated system)

Servers are in constant contact with each other concerning data and setting replication as well as automated monitoring. In order for the two servers to monitor each other, a dedicated connection is required (minimum of 100mbit full-duplex). Connection can be made with direct cable connection or connection through clutches. Usually, network uses addresses 10.0.0.20 (node 1) and 10.0.0.50 (node 2).

6.1.3 SMS interface

Users who log in using SMS authentication received a SMS message to the mobile phone. Sec@GW server creates an SMS message and sends it to the customer’s chosen SMS gateway in the net using email or http(s) interface. Next, customer’s SMS gateway sends the message forward to the receiver’s mobile phone.

6.1.4 Firewall settings

Firewall must allow the required connections. The following table shows requirements for basic installation; rules must be specified.

Table 4. Firewall settings

Connections to Sec@GW system (firewall settings)	

© 2021 SSH Communications Security Corporation

Port	Type	Source	Destination	Protocol / usage
443	TCP	*	Sec/c	HTTPS
25	TCP	Sec/c	* / SMTP GW	SMTP, shared messages
53	UDP	n1, n2	Nameservers	DNS
123	NTP	n1, n2	NTP servers	NTP
22	TCP	193.184.14.150	n1, n2	SSH, Reporting & updates, Deltagon's maintenance
443	TCP	n1, n2	193.184.14.150	Deltagon monitoring
443	TCP	n1, n2	193.184.14.151	Deltagon updateserver
80	TCP	n1, n2	Centos updateservers	CentOS updates
443	TCP	n1, n2	Redhat updateservers	Redhat updates

n1 = server 1

n2 = server 2 c

= cluster