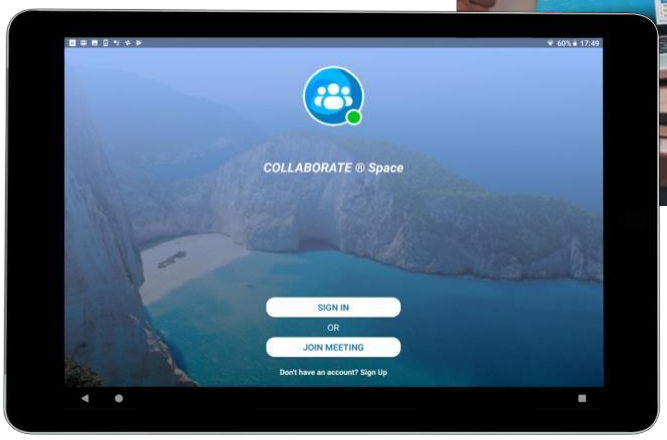
COLLABORATE® Space Security and Privacy



ClearOne

5225 Wiley Post Way

Suite 500

Salt Lake City, UT 84116

Telephone	1.801.975.7200
Tech Sales	1.801.974.3760
FAX	1.801.303.5711
E-mail	collaborate.support@clearone.com
On the Web	www.clearone.com

COLLABORATE® Live

USER GUIDE

CLEARONE DOCUMENT

DOC-0434-001REV 1.0 – April 11, 2020

TABLE OF CONTENTS

Chapter 1: Introduction

COLLABORATE Space Architecture

COLLABORATE Space was developed by ClearOne using a state of the art technology backbone which complies with all security requirements of our customers. COLLABORATE Space is a powerful collaboration application with a full suite of audio, video and meeting tools in a persistent space. This ClearOne video and audio communication system provides an ultra-high-quality, secure, and private collaboration experience. COLLABORATE Space can also easily be “white labeled” to match any partner or customer brand. The application is available in multiple licensing options.

Chapter 2: Security Model

The COLLABORATE Space Server security measures are constantly tested focusing on the security of client-server communication systems.

- Open-Source Security Testing Methodology Manual (OSSTMM);
- Information Systems Security Assessment Framework (ISSAF);
- Information Systems Security Assessment Framework (ISSAF);
- Application Security Project (OWASP)

Firewall/NAT Traversal

COLLABORATE Space allows you to keep your room systems and client software safely behind your firewall and manages firewall traversal through our global service.

Streaming, Recording and Sharing

Recorded calls are stored in secure Amazon Web Services facilities when using the COLLABORATE Space public cloud option. When using the On Premise server option, all of the information is stored on the user's enterprise server. In either option, access to view recordings may be globally restricted to users within your organization only by the administrator.

- Record and Share is available to COLLABORATE Space subscribers
- Recording and sharing is encrypted using AES.

Chapter 3: Security Analysis

Security analysis of Client/Server Component of COLLABORATE Space Server

This section describes the client server component security of COLLABORATE Space Server. This applies to both the cloud server option as well as the on-premise enterprise server option.

Administration and Web Access Interface

The following security measures apply to both the super-admin and admin accounts of individual instances of COLLABORATE Space entities:

- Authenticated access with username and password. Both the username and password must be alphanumeric and at least eight characters in length.
- Access credentials stored on the server database are encrypted.
- Invulnerability against SQL injection attacks.
- Secure transmissions using HTTPS (TLS 1.0, TLS 1.1, TLS 1.2 are the ones supported). A security certificate is required and must be enabled and configured within the COLLABORATE Space server.
- Log out capabilities to close web sessions.

Client Security Measures

- User authentication using access credentials (user/password login)
- Sharing/application control permission verification. The host is required to request permission before sharing a document or taking remote control of an application.
- File transfer control. Users need to authorize a file transfer to avoid receiving unwanted files or applications.

Server Security Measures

- Database encryption of sensitive data.
- Admin or Super-admin authentication required to access to session recordings.
- Safeguards to prevent OS level command execution with maximum access privileges.

Client/Server Communication

- All client/server communications are encrypted using a public key encryption algorithm.
- All client/server communications use the secure TCP port 443.

Server Access

It is strongly recommended to define a poll of source IPs for the SSH access in the firewall of the networks. Additionally, the SSH access to the server must require a private key file for the authentication purpose. It would be possible to define a poll of source IPs for the administration site.

Chapter 4: COLLABORATE Space Privacy

COLLABORATE Space is designed with both security and privacy in mind. Privacy is equally important within COLLABORATE Space. Here are few important privacy measures that were taken in designing the COLLABORATE Space application.

Personal Data

COLLABORATE Space Software may request that you enter personal data. This personal data may include your first and last name, an Avatar image that might be used to identify you, (which could be your photograph, if you choose to use that), and your email address. COLLABORATE Space uses this personal data, along with the video captured by the software, to identify you and to associate written and/or verbal communication you make with your personal data. ClearOne does not record or retain any data from COLLABORATE Space calls or instant messages that are exchanged through COLLABORATE Space or share any data with third parties.

Designed for Privacy

COLLABORATE Space is designed for organizational users in mind. In order to protect the privacy and security of users belonging to the organization, COLLABORATE Space allows users within the organization to chat among themselves as well as allows scheduling a meeting within the organization. Parties outside of the organization can be invited to join a meeting within the COLLABORATE Space application or by the application's webRTC portal.

Meeting Invitation

COLLABORATE Space meeting invitations are created by a random number generator issuing a new and unique personal ID for each participant for a meeting. Personal IDs cannot be shared with any other user and is even unknown to the user, host, or to ClearOne. With each personal ID, only one connection to the meeting is provided.

A COLLABORATE Space meeting invitation allows the host to secure the meeting so the participant invitee cannot join the meeting before host enters the meeting.

Participant Information

COLLABORATE Space always displays the name of each participant during the meeting in order to identify each of the participants.

Meeting Controls

COLLABORATE Space only allows the meeting host to invite any additional participants. This prevents uninvited guests to join COLLABORATE Space meetings without permission from the

meeting organizer.

Recording

When recording is enabled by any meeting participant, COLLABORATE Space always shows a message on each participant screen indicating which participants are recording.