



Security concerns are a big reason companies dismiss using cloud-based services for any application. Video conferencing is no exception. At Lifesize, we understand the importance of security, and we built Lifesize Cloud to provide customers with a secure experience from the meeting room to the office and on the go.

## Data storage

We store the following basic information:

### ACCOUNT MANAGER

- Email address (which is also your username)
- Password
- First name
- Last name
- Telephone
- Address
- Company

### USERS

- Display name
- Email address (which is also your username)
- Password

### BILLINGS

We leverage a third-party PCI-compliant partner for direct sales and our Lifesize Partners for channel sales; therefore, no user billing information is stored in our systems.

### OTHER DATA

We never record, capture or store any unencrypted video/media stream or chat conversations.

## Security

### ACCOUNT SECURITY

- We send an authentication email before activating an account.
- Each account (admin and users) is secured with a password.
- We never send passwords via email. If you forget your password, you will be able to reset it.
- Passwords are not shown in the licensing database.

### MEETING SECURITY

- Passcode—You can add a passcode to secure your meetings.
- Remove participant—During a meeting, any participant can be easily removed from the call.

## Authentication

The connection between the Lifesize Cloud apps and Lifesize® Icon™ and the Lifesize Cloud service is authenticated through https at provisioning. Registrations are secured via TLS.

## Encryption

Lifesize Cloud lets you connect instantly with anyone, anywhere on any device. This means that some of your calls will be conducted over the public Internet. Rest assured that we support state-of-the-art encryption:

- 128-bit AES (Advanced Encryption Standard) encryption for media
- TLS (Transport Layer Security) encryption for signaling

NOTE: PSTN/audio-only calls, by their nature, are not encrypted.

# Overview

## Firewall/NAT traversal

You don't have to place devices outside your firewall to enable communications through Lifesize Cloud. Our architecture lets you keep your apps and meeting room video systems behind your firewall and manages the traversal through our authenticated servers.

### FIREWALL CONFIGURATIONS

Lifesize Cloud uses the following TCP/UDP ports against lifesizecloud.com to enable the service.

Lifesize Cloud apps and Lifesize Icon:

PROTOCOL	DESTINATION PORT	DESCRIPTION
TCP	80	HTTP: Lifesize Cloud app download (NOTE: will redirect to web console download page)
TCP	443	HTTPS: Lifesize Cloud app provisioning
TCP	35060/35061	Lifesize Cloud app signaling (SIP/TLS)
UDP	10000-16000	RTP media

For any SIP video endpoints:

PROTOCOL	DESTINATION PORT	DESCRIPTION
TCP/UDP	5060/5061	SIP/TLS

For any H.323 video endpoints:

PROTOCOL	DESTINATION PORT	DESCRIPTION
TCP	1720	H.225: call signaling
UDP	1719	H.225: RAS
TCP	10000-16000	H.245: Control channel

#### HEADQUARTERS

Austin, Texas, USA  
+1 512 347 9300  
Toll Free US +1 877 543 3749

#### EMEA REGIONAL OFFICE

Munich, Germany  
+49 89 20 70 76 0  
Toll Free Europe +00 8000 999 09 799

#### APAC REGIONAL OFFICE

Singapore  
+65 6303 8370



www.lifesize.com  
E-mail: info@lifesize.com

## Service availability

Lifesize Cloud is operated in secure Tier 1 data centers in North America, Europe and Asia, ensuring redundancy and failover. In case of disruption, your calls will be routed to another available server. Our systems are backed up, ensuring that your configurations are protected and up to date.

## Questions?

Have more questions about Lifesize Cloud security? Contact us at [support@lifesize.com](mailto:support@lifesize.com)

# lifesize

© 2014 Lifesize, a division of Logitech. All rights reserved. Information contained in this document is subject to change without notice. Lifesize is the registered trademark or trademark of Logitech. All other trademarks are the property of their respective owners.

SS\_Cloud\_Security\_0514