Lifesize® Security for Cloud-based Service & Devices

Overview

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

Security

SECURE FOUNDATION

All Lifesize cloud-based calling capacity is hosted on dedicated machines within highly-secure IBM SoftLayer data centers. Account administration, software update delivery, and streaming and recording are hosted in Amazon Web Services data centers. Lifesize uses best-of-breed data centers with independent third-party security and privacy certifications to ensure the most secure and reliable foundation possible for our customers.

Compliance certifications for our data center partners can be found here:

http://www.softlayer.com/compliance

https://aws.amazon.com/compliance

Lifesize maintains staff dedicated to security and privacy as their primary and sole job function.

VIDEO CALLING

The Lifesize cloud-based solution room systems and client software provide secure and encrypted[1] video, audio, presentation (media) and call setup (signaling) in every call end-to-end. Media uses different ports for each call and is encrypted via SRTP/AES-128 (Secure RTP and Advanced Encryption Standard). Signaling uses a non-standard port and is secured via SIP+TLS (Transport Layer Security). Every caller's connection is encrypted using single-use encryption keys.

Lifesize also provides WebRTC clients, either natively in the browser or via plugin. Encryption is a mandatory component of WebRTC and applies to both signaling (via DTLS) and media (via SRTP/AES-128).

Third-party H.323 systems will join in a secure fashion if configured for H.235 encryption.

AUDIO CALLING

The Lifesize cloud-based solution offers a dial-in audio conferencing capability delivered via Twilio and Voxbone. These two leading providers deliver PSTN to VoIP connectivity with dedicated routes directly to the Lifesize infrastructure. Audio calls originating from the PSTN dialed towards the Lifesize cloud-based service will remain unencrypted, similar to other voice conferencing services.

MEETING SECURITY

Lifesize offers several features to keep your meetings secure:

- Passcodes can be used to secure your meetings
- Meetings can be created for one time events, then deleted
- Call escalation allows you to actively accept or reject new participants into a meeting
- During a meeting, a moderator can remove participants from a call
- During a meeting, a moderator may mute all participants
- During a meeting, a user may mute their own audio and/or video

[1] External calls are not encrypted in SIP.

Lifesize Security Overview

AUTHENTICATION

Lifesize supports single sign-on (SSO). SSO allows you to extend your own password retention, complexity and controls consistently to Lifesize. SSO also allows you to control which users have access to your Lifesize cloud-based subscription, and who does not. More importantly, with SSO, Lifesize authentication will occur directly between your users and your identity provider (IdP).

To provide SSO, Lifesize integrates with your IdP via SAML 2.0, which is the recognized standard for secure authentication to cloud services. Lifesize has validated interoperability with many top tier IdPs, including Microsoft ADFS, Azure AD, OneLogin, Ping Identity and Okta.

If you choose not to use SSO, secure and private alternatives are available for local user authentication and management. In this scenario, the connection between the Lifesize cloud-based apps and service is authenticated through https and registrations are secured via TLS. Administrators can grant or revoke user or room system access at any time.

ACCESS CONTROL

Licensed users can be assigned one of three roles within the Lifesize app. These roles and their capabilities are as follows. For a comprehensive list of permissions, visit our website.

User:

- Place and receive calls
- Mute your own audio or video
- Create and own a meeting
- Set or change a passcode for a meeting you own
- Add or remove participants in a meeting you own
- Mute all participants in a meeting you own
- Chat with users or a group (if the administrator has enabled chat)
- Live stream a meeting (if the administrator has enabled the meeting room for live streaming)
- Record a meeting (if the administrator has enabled recording)
- Specify who can view a recording for a recording you own

Superuser:

Same permissions as Users plus:

- View usage reports
- Promote a User to a Superuser
- Demote a Superuser to User
- Manage and delete Superusers and Users
- Manage and delete any meetings that aren't owned by the Administrator
- Enable or disable chat
- Enable or disable recording (if applicable with subscription level)
- Enable or disable live streaming on specific meetings (if applicable with subscription level)
- Enable or disable Lifesize Icon event alerts (if applicable with subscription level)
- Configure single sign-on (SSO) (if applicable with subscription level)
- Configure integration with common calendaring services
- Configure dial-in PSTN Phone numbers, Icon wallpaper (if applicable with subscription level), and meeting layouts
- Restrict the user email domains allowed to create new accounts in the Lifesize app

View additional details about Superuser permissions.

Administrator:

Same permissions as Users and Superusers plus:

- Administrator permissions and account cannot be changed or deleted by a User or Superuser.

FIREWALL/NAT TRAVERSAL

Our architecture allows you to keep your Lifesize room systems and client software safely behind your firewall and manages firewall traversal through our global calling nodes. Lifesize room systems and client software do not require any firewall ports to be opened inbound from the Internet. There's also no longer a need for static public IP addressing or complicated static NAT and port-forwarding firewall configurations. This allows you to maintain your existing perimeter posture and protects your users and devices from

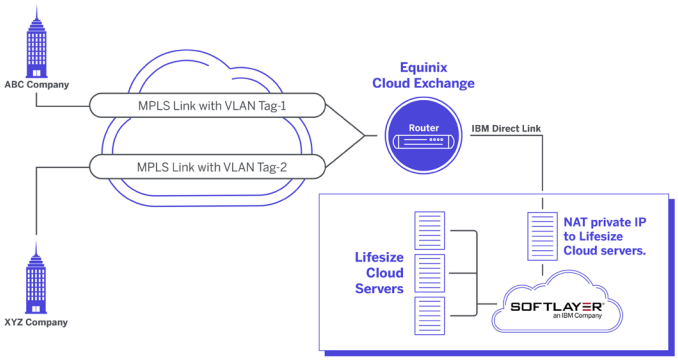
SIP and H.323 nuisance calls that are common on the open Internet.

Lifesize only makes use of outbound TCP/UDP connections for call set up and media. These TCP/UDP connections are always initiated by the Lifesize room system or client software in order to establish pinholes and dynamic port address translations. These connections are always directed to one of our global calling nodes on a specific list of published host IP addresses allowing for tightly crafted firewall rules.

FIREWALL CONFIGURATION
Information about opening ports and configuring your network is available on our website.

MPLS Connectivity

Our optional MPLS private link service provides you with the ability to connect to the Lifesize service by extending your MPLS network to select datacenters in which the Lifesize cloud service is operated. We recommend this service if you want the benefits of the Lifesize cloud service but need the dedicated connectivity that MPLS can provide. This program gives you the option of establishing private connections that allow media traffic to flow to and from Lifesize datacenters through your carrier's MPLS network.



Privacy

Lifesize maintains a Privacy Shield certification issued by the US Department of Commerce on November 3, 2016. Our data center partners maintain the same.

- Read more about Lifesize, IBM SoftLayer and Amazon Web Services Privacy Shield certifications.
- Review our publicly available Privacy Policy.

DATA RETENTION
Video communication data is transient in nature and encrypted in flight. Lifesize does not record, capture or store any video conference media (audio, video or presentation). We do maintain basic metadata of each call so that customer administrators can access usage reports and information. Similarly, server logging is retained for the purposes of technical support engagements and troubleshooting. This data does not include any media.

USER INFORMATION
As a part of consuming our service offering, Lifesize stores only the basic information below for each of our customers' user accounts. Should you choose to leave the service, this information will be permanently deleted 180 days following the end of your contract.

Administrator:

- Email address (which is also your username)
- Password (for non-SSO accounts only)
- First name, last name
- Display name
- Telephone
- Address
- Company

Users and Superusers:

- Display name
- Email address (which is also your username)
- Password (for non-SSO accounts only)

Lifesize Security Overview

LIFESIZE STREAM, RECORD AND SHARE

Lifesize offers streaming and recording services as an additional option for our customers. Recorded calls are stored in secure Amazon Web Services facilities. Access to view recordings may be globally restricted to users within your organization by your administrator.

- Lifesize Record & Share is included[2] with the Enterprise subscription for the Lifesize cloud-based service and may be available as an add-on for other subscription plans. Record & Share is disabled by default and must be purposefully enabled by an administrator before users are able to record any calls.
- Content distribution may be restricted to only your own organization.
- Lifesize Record & Share is encrypted using AES-128 for data in-flight (recording and playback) and AES-256 for data at rest (storage).
- Lifesize Record & Share is hosted on Amazon Web Services (AWS), which is designed for security across all geographies and verticals. Learn more about AWS Security.
- Initiation of recordings requires manual intervention whereby a user of the Lifesize cloud-based service must activate the feature to record the conference session.
- An on-screen notification will be displayed to all video participants taking part in the conference to notify users that the call is being recorded.

CHAT

Lifesize chat is hosted on Amazon Web Services (AWS), which is designed for security across all geographies and verticals. Learn more about AWS Security.

BILLINGS

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

Service Optimization & Availability

The Lifesize cloud-based service is operated in secure data centers in North America, Europe, Oceania and Asia, ensuring redundancy and failover. Lifesize calling capacity is hosted exclusively in IBM SoftLayer data centers. Lifesize room systems and client software will automatically register with the closest and least-busy cloud node in order to minimize public Internet traversal for your users regardless of their location. Calls between these users will leverage IBM SoftLayer's private network, rather than the Internet, to minimize latency and maximize quality.

In case of disruption, your Lifesize room systems and client software users will be routed to another available server, in some cases without disconnecting a live call. Our systems are backed up, ensuring that your configurations are protected and up to date.

Questions?

Have more questions about Lifesize cloud-based security? Contact your sales representative or email: support@lifesize.com

[2] Enterprise subscription includes 10 recording hours. Additional hours may be purchased.

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

APAC REGIONAL OFFICE
Singapore
+65 6631 2831

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

SS_CloudSecurity_US_0417