Lifesize® Security Overview

With a proven history of innovation and years of experience with real-time collaborative video and audio communication solutions, at Lifesize we know what it takes to deliver.

As the first vendor to introduce HD video calling and now the first to introduce UHD (4K), it is no coincidence that we are still pushing the boundaries of what is possible. But what is most important to us is ensuring that we meet or exceed the essential security and robustness requirements of our customers while offering the flexibility and value that businesses demand in today's fast-paced and competitive SaaS (Software as a Service) world.

Our unique combination of industry-leading hardware products coupled with our award-winning software backed by our global cloud service and customer obsession make Lifesize unique in the industry and a name you can trust.

Architecture

Lifesize employs a truly modern, global cloud architecture designed from the ground up to meet the functionality, security and continually evolving communication needs of our customers. Delivering real-time collaborative video and audio communications in HD and UHD (4K) requires a

no-compromise infrastructure design approach along with application and protocol intelligence to handle the inevitable client-side variations associated with internet bandwidth and connectivity.

The Lifesize service, room systems and client software are designed and developed in the United States. Our cutting- edge microservice-based architecture embraces the latest protocols, technologies and application design concepts to provide the core foundation of our cloud-based products and services.

By conscious design, our solution intelligently splits different workloads into central and regionalized tasks with resources strategically positioned across the globe to provide proximity and presence worldwide. The same mindful dispersal of resources geographically also increases resilience and reduces the potential impact of localized failures, while keeping in mind regulatory, legal and privacy concerns.

Modern public clouds allow us to deploy infrastructure quickly to meet customer growth and address maintenance needs. Our architecture is designed to scale dynamically to always provide the best video conferencing experience for our customers. It is designed to allow the Lifesize service to change quickly without requiring customers to make frequent changes to their networking infrastructure.

Lifesize works with industry-leading technology partners and providers with world-class data center facilities to operate our service and provide the capability for local voice connectivity in more than 60 countries.

Benefits

- Industry-leading 4K call quality and content sharing
- Highest service availability and reliability
- Improved resilience and performance on low bandwidth networks
- Accelerated feature development

Lifesize Security Overview

Security

Security is an important consideration when considering any solution, cloud-based services included. Lifesize has emphasized security and privacy since launching our service in 2014.

Secure Foundation

All Lifesize cloud-based calling capacity is hosted within highly secure Amazon Web Services (AWS) data centers. Lifesize leverages AWS's independent third-party security and privacy certifications to ensure the most secure and reliable foundation possible for our customers. Compliance certifications for AWS can be found here:
https://aws.amazon.com/compliance/programs/

Lifesize chose AWS because it is the most mature public cloud offering. AWS is constantly innovating by providing new and improved cloud services. Video conferencing is a very elastic workload, so the capabilities of a public cloud partner like AWS allow Lifesize to adjust to customer needs quickly.

Colocation solutions are attractive and cost-effective if the applications you deploy do not change very often and your application has static workloads that have constant load requirements. However, if you are constantly innovating like Lifesize, a data center solution that is constantly innovating enables you to focus on building better products for customers rather than attempting to extract the most from an equipment investment that takes years to depreciate.

Hybrid public/colocation cloud solutions present different problems, as service providers must have two ways to do everything — one for the colocation part of their service and one for the public cloud part of their service. As a result, neither one is properly optimized or secured. A service provider's solution is only as secure as its weakest link. When you use a solution from a service provider with a hybrid cloud, you should ask where your workloads are running.

Lifesize has chosen to use AWS, the premier public cloud offering, and to focus on optimizing our operational efforts around a single solution implementation not a colocation or hybrid solution.

Secure Operation

The Lifesize production service operates separately and independently from the Lifesize corporate IT environment. The systems used for source control, build and continuous integration (CI) and the staging environment for quality assurance (QA) are each also maintained in separate and independent environments.

Our processes and controls include the following:

- Source code scans for common vulnerabilities and exposures (CVE) based on constantly updated lists.
- A build and CI process that only accesses our external source code repository, never repositories on engineers' computers. The resulting container images (source code and operating system) are scanned for known CVEs again.
- CI environment promotes container images to staging QA environment, which is completely isolated from the production environment.
- CI environment promotes container images to production environment after approvals.
- Very constrained access control to all systems in the code development pipeline.
- Regular penetration testing by an industry-recognized and independent third party on our production environment.



Lifesize Security Overview

Secure Room Systems

Lifesize designs and builds the conference room hardware, the software and the service that ties it all together. Lifesize Icon conference room systems are built upon decades of security knowledge.

- Our hardware and software are built from the ground up with security as one of the main architectural requirements.
- Our systems are engineered exclusively for video communications as opposed to component-based kits based on general-purpose operating systems. The closed-box design does not allow others to use and/or add their own software applications.
- From the onset of power to the system, the system is protected by secure boot, and the software that resides in the system has secured signed software images.
- Our secure software is encrypted as it is downloaded to the system.
- Our software releases include third-party intrusion testing using industry-recognized tools.
- Our award-winning user interface and our Lifesize room systems APIs are the only available interfaces to the system for third-party integrations and for diagnostics.
- Complete, best-in-class solution with one point of contact for help if needed.

Video Calling

The Lifesize service, room systems and client software provide secure and encrypted video, audio, presentation (media) and call setup (signaling) in every call. Encryption cannot be disabled by either administrator or user. Video calls are encrypted with no trade-off in quality.

The Lifesize service, room systems and client software employ WebRTC. Encryption is a mandatory component of WebRTC and applies to both signaling (via DTLS and secure WebSockets) and media (via SRTP/AES-128).

Third-party H.323 systems will join video calls in a secure fashion when configured for H.235 encryption. Third-party SIP systems will join in a secure fashion when configured for SIP TLS.

Note:

Feature availability and price vary by subscription plan, selected options, and paired devices

Audio Calling

The Lifesize cloud-based solution offers a dial-in audio conferencing capability delivered in partnership with industry leading providers, enabling PSTN-to-VoIP connectivity with dedicated routes directly to the Lifesize infrastructure. Audio calls originating from the PSTN dialed toward the Lifesize cloud-based service will remain unencrypted, similar to other voice conferencing services.

Meeting Security

Lifesize offers several features to keep meetings secure:

- Passcodes can be used to secure meetings.
- One-time meetings allow for a single-use meeting that is deleted following the event and cannot be reused. One-time meetings are always hidden from the directory.
- Permanent meetings can be hidden from the directory.
- Call escalation allows users to actively accept or reject new participants into a meeting.
- During a meeting, a moderator can remove or mute individual participants from a call.
- During a meeting, a moderator can remove or mute all participants from a call.
- During a meeting, a user may mute their own audio and/ or video.

Authentication

Lifesize supports single sign-on (SSO), and it is offered as an additional option for customers. 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 which do not. More importantly, when using SSO with Lifesize, 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, Microsoft Entra ID, 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.

Lifesize Security Overview

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

As a User, you can:

- 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
- Hide a meeting you own from the directory
- Add or remove individual or all participants in a meeting you own
- Mute individual or all participants in a meeting you own
- Chat with users or a group (if the Administrator has enabled chat)
- Live stream a meeting in a meeting you own (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

As a Superuser, you have the same permissions as a User plus you can:

- View usage reports
- Promote a User to a Superuser
- Demote a Superuser to a User
- Manage and delete Superusers and Users
- Manage and delete any meetings
- Hide any meeting from the directory
- Hide any User or Superuser from the directory
- Hide any room system from the directory that is not associated with 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
- Configure single sign-on (SSO) (if applicable with subscription level)
- Configure integration with common calendaring services for one-click calling
- Configure dial-in PSTN phone numbers for meeting invites (if applicable with subscription options)
- Configure call details for meeting invites
- Customize Lifesize Icon wallpaper and Lifesize® Phone™ HD user interface
- Configure meeting layouts
- Restrict the user email domains allowed to create new accounts in the Lifesize app

Administrator

As an Administrator, you have the same permissions as a User and a Superuser plus:

- Your account and permissions cannot be changed or deleted by a User or Superuser
- You can hide yourself from the directory
- You can hide room systems associated with your own user account from the directory

Lifesize Security Overview

Firewall/NAT Traversal

The Lifesize architecture allows you to keep your Lifesize room systems and client software safely behind your firewall and manages firewall traversal through our global service. Lifesize room systems and client software do not require any firewall ports to be opened inbound from the internet.

There is 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 does not require inbound firewall rules. To establish TCP/UDP media connections, checks are made in both directions; the client's outbound checks establish NAT/firewall state for when inbound connectivity is unavailable. Media either flows directly between participants in two-party calls or to the Lifesize media service in multiparty calls. A Lifesize TURN relay is available over TLS as a fallback for restrictive networks.

Connections to Lifesize services are directed only to our global resources on a specific list of published FQDNs, allowing for tightly crafted firewall rules. Lifesize manages these FQDNs and controls their Time to Live (TTL) so they are always current.

Firewall Configuration

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

Privacy

For a complete overview of Enghouse Interactive privacy resources and collateral, please visit our website.

Call Data Retention

Video communication data is transient in nature and encrypted in flight. Enghouse Interactive does not view, record or otherwise store any video conference media (audio, video or presentation).

Call Information

Lifesize stores basic metadata of each call so that customer administrators can access usage reports and information.

This data does not include any media. Should you choose to leave the Lifesize service, this information will be permanently deleted as per the terms in your contract.

Similarly, server logging is retained for the purposes of technical support engagements and troubleshooting for 15 days and archived for 90 days. This data does not include any media.

User Information

Lifesize stores only basic information for each of our customers' user accounts. Should you choose to leave the service, this information will be deleted as per the terms in your contract.

Administrator:

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

User and Superuser:

- Display name
- Email address (which is also the 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 only by the administrator.

- Lifesize Record and Share is available to subscribers of the Lifesize cloud-based service. Record and 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 Live Stream and Record and Share are encrypted using AES-128 for data in-flight (streaming, recording, or playback) and AES-256 for data at rest (storage).
- Lifesize Record and Share is hosted on AWS, which is designed for security across all geographies and verticals. Learn more about AWS Security.
- Lifesize Live Stream Q&A feature is hosted on Twilio Conversations, designed to keep data secure and prevent malicious activity. Learn more about Twilio 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 and by whom.

Chat

Lifesize chat is encrypted in flight (AES-128) and at rest (AES-256), which is designed for security across all geographies and verticals.

Service Optimization & Availability

The Lifesize cloud-based service is operated in secure AWS data centers in North America, Europe, and Asia. Lifesize calling capacity is hosted exclusively in AWS. Lifesize room systems and client software will automatically create conferences in the optimal AWS data center based on the location of the initial members of the conference. Recordings of conferences are stored in the AWS data center where the conference was hosted. They are not replicated outside of that AWS data center.

In case of a service failure, your Lifesize room systems and client software users will be routed to another available part of the service, in some cases without disconnecting a live call. Failed services are automatically replaced without any manual intervention by Lifesize staff, returning the service to full capacity within minutes. 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:

https://www.enghousevideo.com/company/contact-us

Corporate Office
Enghouse Systems Limited
80 Tiverton Court, Suite 800
Markham, Ontario L3R 0G4 Canada
Tel: +1-905-946-3200

Europe
Enghouse Video
Imperium, Imperial Way
Reading, RG2 0TD UK
Tel: +44 20 3357 3040

North America
Enghouse Video
27 Madison Avenue Suite 040
Paramus, NJ 07652 United States
Tel: +1-866-998-4396

Copyright © 2026 Enghouse Interactive. All Rights Reserved. Information contained in this document is subject to change without notice. Lifesize, the Lifesize logo, and Enghouse Video logo are registered trademarks of Enghouse Systems Limited. All other trademarks are the property of their respective owners.