



Statement Clarifying Lifesize Access to Customer Environments

Lifesize customer environments are managed access environments; in which Lifesize's access is limited both in terms of business need as well as least required access levels. In other words, Lifesize personnel may only access customer environments if there is a valid business reason to do so, and only to the extent necessary to perform the assigned job function.

Customers who use Lifesize Icon room systems have the additional security option of using their own SSL certificate to manage connectivity.

To be clear, at Lifesize:

- We don't watch customer calls and do not have the technical ability to do so.
- We don't record any customer calls.
- We don't review customer-initiated call recordings or chat.

Real-time video conferencing is ethereal in nature, meaning that the content data exists only in flight. By default, Lifesize calls are encrypted end-to-end in flight when Lifesize room systems registered to the Lifesize cloud-based service and client software are used. Unless a customer specifically purchases and implements Lifesize's recording features, no content from a video conferencing call is recorded or stored in Lifesize's network or systems. If a customer elects to record and save video conferencing calls, then such recorded content is encrypted at rest.

During real-time video conferencing calls that are not recorded by the customer, the only data captured by Lifesize is transactional in nature, and includes:

- User display name
- User email address (username)
- User passwords (if SSO is not enabled)
- IP addresses
- Call log information (call participants, quality statistics, and duration)

Lifesize Record & Share is hosted on Amazon Web Services.

Lifesize does not have 'hidden' backdoors into customer data, real-time video conferencing calls, or recorded content stored in Lifesize's system. In the event that a Lifesize employee connected to a real-time video conferencing call, they would appear as a participant in the call just like anyone else, and that activity would be logged with the call data. Any unauthorized access is prohibited by Lifesize's policies and is grounds for immediate and appropriate corrective action.