Security Protocols Livecare Support Release 2.2

February 2023

www.livecare.it
Icona Srl Viale Brianza, 20 – 20092
Cinisello Balsamo (MI) ITALY

Table of contents

Setting up a support session

When you set up a support session using Livelet (an executable used by the customer to receive support), Livecare Support determines the optimal connection type.

The connection is routed through our network of servers, via TCP or https-tunnelling.

This communication occurs directly between Liveoperator and Livelet, via the ICONA SRL servers, without any information from this connection being stored on our servers. Even we, the routing server operators, are unable to read the flow of encrypted data.

Livelet remains on the customer's disc once the support session has ended, but is no longer running on the customer's computer, and no connection to the customers' computer can be established in any way.

Livelet can be configured to require a phone call between the operator and customer before activating the connection. In that case, the support session is launched according to the following steps:

- The customer makes contact with the operator to request support, using systems external to Livecare (telephone, chat, e-mail...),
- The operator provides the customer with the new, automatically generated session code,
- The customer enters the session code into Livelet,
- Livelet launches a connection with the operator's PC using the ICONA server as a bridge server for the connection.

During this process, no other operator can connect to the customer's Livelet at any time.

Data processing

Under no circumstances are the video files of support sessions performed and recorded by the Operators stored on Icona servers, even temporarily.

1. The connection logs between the operator, customer and Livecare server are stored for 30 days, and only record network events between the operator and the customer. Access to that data is only provided for diagnostics purposes if an operator discovers a problem and requests intervention from the technical support team, or in the event of a server malfunction.

2. The Liveoperator, Livelet and Internet Agent logs are saved locally on the devices on which they are installed, and access to technical support is only available to the operator via the "Report Problem" function.
3. The logs of text chats between the operator and the customer are stored on our server for an indefinite period. The server on which the logs are saved can be redirected using the dedicated function on the Liveoperator configuration page.

Under no circumstances can the logs referred to above be shared with third parties.

Support encryption, demos and file transfer

Livecare Support traffic is secure thanks to the use of the TLS protocol (1.2 or higher depending on the operating system) with 256 bit AES for session encryption. This technology is used in a similar form for https/SSL and is fully secure and complies with current security standards.

Code signing

As a further safety measure, all of our software is signed using Thawte Code Signing (a Symantec Group Company). This method allows the software creator to be reliably identified at all times. If the software is modified, the digital signature is automatically invalidated.

Audio and video communication encryption

Integrated audio and video communication is protected by encryption similar to that described in the encryption paragraph.

Absence of hidden mode

There is no function that allows Livelet to operate in the background.

Once the connection is established, a small control panel is visible at all times. This means that Livelet does not in any way allow background monitoring of customers' computers.

Location of the server

The Livecare Support server is located within the European Community.

Data centres and backbone

Livecare Support's physical servers are located in the European Union, in data centres certified in accordance with ISO 27001 and equipped with connections with multiple redundant carriers and redundant power supply systems.

Only brand name hardware is used.

Access to the data centres is only granted to authorized ICONA SRL personnel. The closed circuit video monitoring system, intrusion detection, and 24/7 monitoring internally protect our servers from attacks.

icona