islonline

Security Statement

Revision Date: 4 January 2018

Introduction

This document provides the security information related to ISL Online - remote desktop software. We have prepared this document to reveal the technical background and security layers implemented in the ISL Online products. You are welcome to distribute this document freely to your colleagues, partners or customers in order to clarify the possible security concerns.

About Us

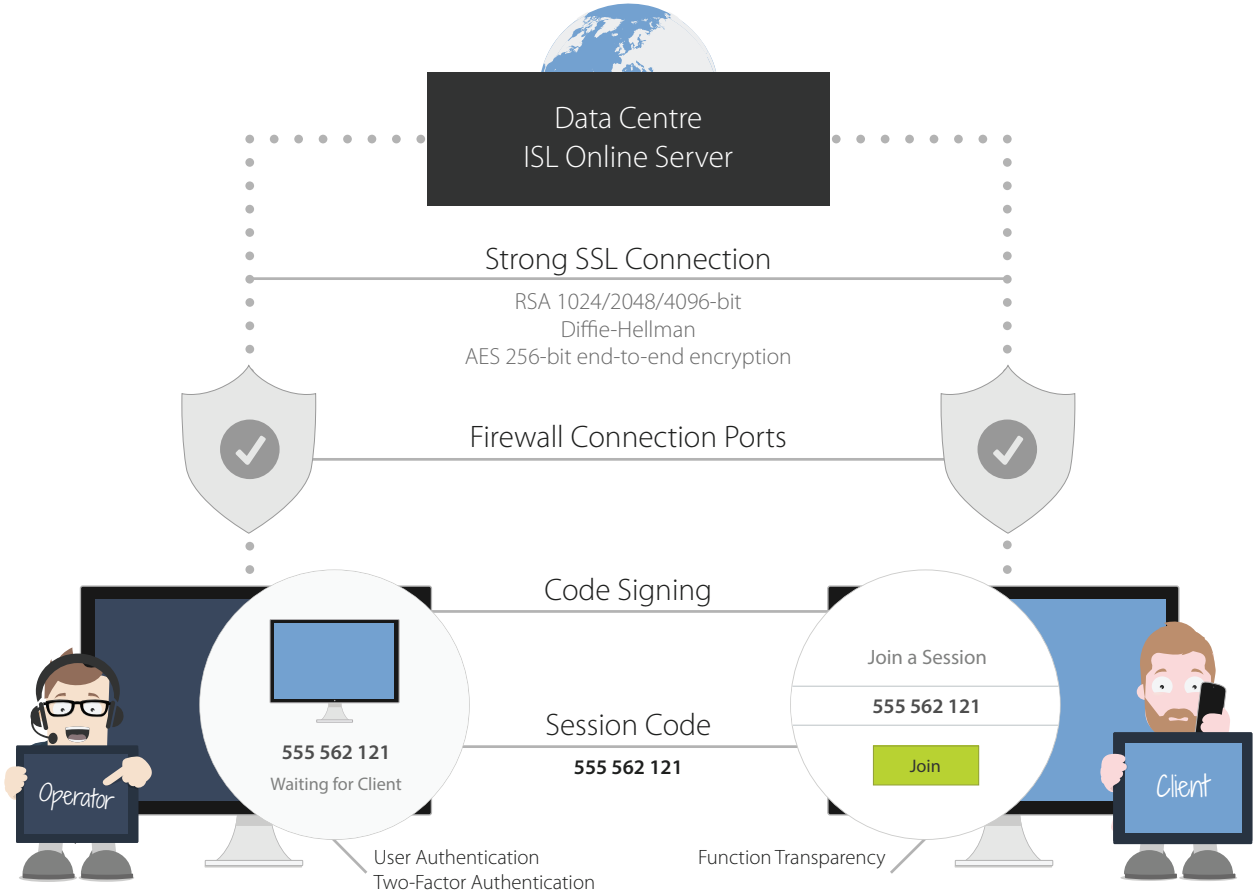
ISL Online is a pioneer in the remote desktop support industry. Since 2003, ISL Online has been providing remote control software to IT professionals and helpdesk technicians in more than 100 countries, with Japan being the strongest market.

Delivered via cloud or on-premises, ISL Online allows users to access and control Windows, Mac and Linux computers as well as mobile devices to provide ad hoc technical support and remote management. Banks, government bodies and global brands all choose ISL Online for our high level of security in the remote support software industry.

ISL Online is developed by XLAB, a software development company headquartered in Slovenia with offices located in Switzerland, the UK and the USA. We work with authorised partners across Europe, Asia/Pacific, Middle East, Africa, and Latin America. We serve customers virtually anywhere in the world. Visit us at www.islonline.com.

Expect Maximum Security

At ISL Online we understand that information security is of utmost importance to you when it comes to establishing connections with remote computers. We apply a number of measures and features which make ISL Online secure and help us comply with strict security standards our clients expect.



Two-factor authentication

Two-factor authentication is an extra layer of security which adds a second factor to the authentication process and makes unauthorised access near to impossible.

Session Code

The helpdesk operator passes a unique session code to the client. The session code is invalidated immediately after the connection is established.

Strongest Encryption

A remote desktop support connection with a client is established using the RSA 1024/2048/4096-bit public-private key exchange. Upon a successful RSA key exchange all data traffic is encrypted using symmetrical AES 256-bit keys.

Firewall-Friendly

ISL Online automatically initiates an outgoing connection through ports 7615, 80 and 443, therefore it works with your existing firewall and does not require any additional configuration.

Security at a Glance

RSA with Diffie-Hellman key exchange	✓
AES 256-Bit end-to-end encryption	✓
Two-factor authentication (2FA)	✓
ISO 27001:2013 Certification (information security management)	✓
Port filtering	✓
Blacklisting/whitelisting	✓
Code signing	✓
External security audits and penetration testing	✓
Function transparency (no stealth mode)	✓
Password encryption	✓
Brute force intrusion protection	✓
Intranet (LAN-only) option	✓
Reverse proxy support	✓
Automatic session recording option	✓
Access management	✓
Incident management system (IMS)	✓
Logs and accountability	✓
Features restriction	✓
External Authentication	✓
Data Centers & Metadata	✓

Please notice:

ISL Online offers different hosting options (Cloud, Server License, Private Cloud, Managed Private Cloud). Some security measures described in this document are only available for certain hosting options. Please contact us for details (support@islonline.com).

RSA with Diffie-Hellman Key Exchange

To establish a remote desktop support connection with a client, the helpdesk operator needs to start the ISL Light application, which carries an RSA 1024-bit public key of the ISL Online server. The initial connection is established when the public key of the ISL Light application and the private key of the ISL Online server are verified and exchanged. The industry standard X.509 certificates are used to guarantee the authenticity of a transmission. This PKI (Public Key Infrastructure) prevents the „Man-in-the-middle" attacks. Upon a successful RSA key exchange, the Diffie-Hellman cryptographic algorithm is used to exchange symmetrical AES 256-bit keys.

We are rolling out the RSA 2048-bit keys to our public cloud. They will gradually replace the 1024-bit keys. On the other hand, our Server License users that keep their ISL Online servers up to date can already start using 2048-bit keys. They are even able to configure their ISL Online servers to use 4096-bit crypto keys.

AES 256-Bit End-to-End Encryption

Once the remote desktop session is established between the operator (help desk technician) and the client (end-user) all data traffic is encrypted using symmetrical AES 256-bit keys. A secure SSL end-to-end tunnel is established between the operator and the client. This means that even the ISL Online servers cannot decrypt the content of the sessions but only transfer packets from one side to another.

Two-Factor Authentication (2FA)

Two-factor authentication (2FA) is an extra layer of security for help desk technicians and IT professionals. With 2FA enabled, operators can only log in to the ISL Online system by going through a two-step verification process by providing something they know (password) and something they have (2FA token). This second factor increases security and makes unauthorised access much more difficult.

We recommend using two-factor authentication, especially on highly sensitive systems. ISL Online allows you to configure different methods for the second step of verification (email, phone, authentication app - TOTP, security key - Yubico keys based on FIDO U2F standard).

ISO/IEC 27001:2013 Certification (Information Security Management)

The ISO 27001:2013 is internationally accepted and one of the most widely recognised information security standards. This certificate specifies the requirements for a comprehensive Information Security Management System (ISMS), and it defines how organisations manage and handle information securely. It is only awarded to organisations that follow stringent security practices, after a rigorous audit process.

The ISO/IEC 27001:2013 certificate validates ISL Online's expertise in information security management and our commitment to the highest level of security throughout the company. It is further proof that the data is well-protected and secure with ISL Online.

Beside the ISO 27001 compliance, ISL Online's internal playbooks and security policies are also periodically matched against best practices suggested by SSAE 16 (SOC 2).

Port Filtering

Good remote desktop software works without making any firewall adjustments.

With ISL Online your firewall can remain intact as ISL Light automatically initiates an outgoing connection, trying to connect using ports 7615, 80 and 443.

However, larger organisations normally have a certain policy about the configuration of their firewalls or proxies. System administrators might want to open port 7615 only to pass the ISL Online traffic through directly and keep filtering the rest. They can also configure DNS name exception or IP number exception.

Regardless of the network configuration ISL Online apps will automatically try different approaches to find working transport (detecting proxy settings, using WinINet, creating a tunnel, making use of the wildcard DNS etc.).

Blacklisting / Whitelisting

Remote desktop software is a very powerful tool which enables you to control remote computers. To prevent any misuse of remote desktop software in your company, the possibility of creating whitelists and blacklists is indispensable.

For security reasons you might want to restrict the use of ISL Online software within your organisation. You are able to limit the data access to ISL Online servers based on the IP and/or MAC addresses. You can use the "allow" function to specify the whitelist of IP/MAC addresses which are allowed to start a remote support session or access an unattended computer. On the other hand, you can use the "deny" function to specify the blacklist of IP/MAC addresses. These rules can be defined for a specific user or the entire domain on the ISL Online server.

For example, you can allow your employees to generate session codes for a remote support session from the office only (your company's range of IP addresses).

Code Signing

Code signing is widely used to protect software that is distributed over the Internet. Code signing doesn't make any changes in the software, it appends a digital signature to the executable code. This digital signature assures recipients that the remote desktop software does indeed come from the source you trust. It provides enough information to authenticate the signer as well as to ensure that the code has not been subsequently modified.

ISL Online applications are digitally signed by means of a code signing certificate, which reliably identifies ISL Online as the software publisher and guarantees that the code has not been altered or corrupted since it was signed with a digital signature.

External Security Audits and Penetration Testing

Regular systematic security audits and narrowly focused penetration tests are crucial for each remote desktop software provider responsible for information security. They allow a company to remedy in time potential weaknesses and vulnerabilities identified.

Independent security audits and penetration tests of the ISL Online system are conducted on a regular basis and reveal that ISL Online is a trustworthy service providing a very high level of security.

Function Transparency (No Stealth Mode)

It is important that a remote desktop application is designed in such a way that it can never run in the background without a client being aware of it. The functionality of the software should be totally transparent and the client should be able to follow the actions performed by the helpdesk operator all the time.

ISL Online is designed to provide remote support to clients over the Internet but only upon the client's explicit request. The client allows a helpdesk operator to start desktop sharing and can terminate the session anytime. When the operator has full remote desktop control over the client's computer, the client can easily take back control by simply moving the mouse. Once the session is terminated, the helpdesk operator cannot access the client's computer again with the same session code.

Password Encryption

The security of your data depends not only on the strength of the encryption method but also on the strength of your password, including factors such as length and composition of the password, and the measures you take to ensure that your password is not disclosed to any third party.

ISL Online password security policy is based upon the latest NIST specifications; the password must be at least 8 characters long; any leading and trailing spaces will be removed; allowed characters used in the password are any printable ASCII characters and spaces; the password is checked against the blacklist, which consists of the most common and simple passwords.

ISL Online does not store passwords in plaintext, but uses salted password hashing to protect passwords stored in user account databases.

Brute Force Intrusion Protection

To prevent unauthorised access, brute force protection should be applied to remote desktop software.

A brute-force attack is a trial-and-error method which calculates every possible combination that could make up a password or decrypt an encrypted file. In a brute force attack, automated software is used to generate a large number of consecutive guesses until the correct one is found.

ISL Online has configured rate limiting for login and connection attempts in order to prevent brute-force attacks. ISL Online servers prevent brute-force intrusion (login) attempts by limiting the maximum number of failed login attempts for a user or for a specific address in the defined period of time. A login can also be limited only in a specific time frame.

Intranet (LAN-only) Option

Some large organisations only use ISL Online for their internal support across different geographical locations. In such cases remote desktop software must allow establishing remote desktop sessions within a local area network (LAN) only.

If you plan to use ISL Online within your LAN (intranet) only, there is no need for a public IP address. You only need a private address in the range of private networks (as specified in RFC 1918).

Reverse Proxy Support

A reverse proxy can hide the topology and characteristics of your backend servers by removing the need for direct Internet access to them. You can place your reverse proxy in an Internet facing DMZ, but hide your web servers inside a private subnet. It diminishes the risks of unauthorised access to sensitive data. ISL Online allows you to install the server behind a reverse proxy without exposing it directly to the internet, terminating SSL on the reverse proxy.

Automatic Session Recording Option

Remote desktop software should not merely protect data transmission, but should also protect you as the remote desktop support provider and the client as its receiver. The best way to achieve this is session recording. This is particularly true for those companies that have trusted a third-party servicing company with computer maintenance by granting non-limited remote access to their computers.

ISL Online offers a powerful option to start recording automatically at the beginning of every remote access session in order to have full control over the remote access activity and prevent possible conflicts with clients.

Access Management

If there is only one person using remote desktop software in a company, setting up access permission is not something you would be worried about, however, this feature becomes very important from the security point of view once there are numerous users using the software to connect to remote computers.

With ISL Online, the account admin can assign its domain users different rights and limitations, including allowing or disabling access to specific computers. For each individual user you can also set a maximum number of concurrent sessions, disable rights to use audio, video, remote printing, file transfer, and desktop sharing.

Incident Management System (IMS)

Remote desktop software providers should have an incident management system (IMS) which guarantees a rapid restoration of normal service operation after an unplanned interruption.
ISL Online uses our own IMS, a set of procedures, developed by ISL Online, to mitigate the reported incidents. Whenever an incident is reported, it is managed in our ticketing system.

Each incident normally includes the following elements:
• Timeline UTC (a log of events in the chronological order in UTC time zone)
• Executive summary (a brief description of the incident)
• Root cause (an explanation of the root cause of the incident)
• Resolution and recovery (a description of the incident mitigation process)
• Corrective and preventative measures (an explanation of the actions taken to prevent such incidents in the future)
• Other relevant information

IMS helps us to maintain continuous service levels, measure the IT service availability, document the undesired events and protect their reoccurrence.

Logs and Accountability

To comply with regulations in most industries, remote desktop software should permit users to keep logs of a remote support activity and grant clear accountability.

ISL Online allows IT administrators to identify unique users, show which systems were connected and, with an active session recording, trace what actions were taken over the remote connection. Such records can dive into each individual session, exposing the information about an operator, a client, IP addresses, etc.

Integration with a third-party log aggregation / reporting solution (such as Kibana) is also possible.

Restriction on Features

Remote desktop software is a universal tool, used virtually in all industries. Accordingly, there are countless different use cases, which call for very flexible solutions that allow restriction on features to adhere to distinct security standards.

ISL Online allows you to restrict features that are available within a session: taking control of the remote computer, transferring files between customer and operator and many other features.

An example of where restricting a feature is essential: a bank employee should be able to see a client's computer screen, but should never be able to start sharing his/her own desktop. In this case, desktop sharing on the desk side can be disabled.

External Authentication

Different types of authentication schemes can be integrated within the ISL Online system, like the OpenLDAP, Microsoft Active Directory, Novell eDirectory or RADIUS. When external authentication is configured, operators' access rights and permissions to use ISL Online software are managed by IT administrators using their enterprise user management directories.

Data Centres & Metadata

ISL Online's servers (Public Cloud) are hosted by professional data centres all over the globe. We only choose highly reliable and industry-proven data centres with modern facilities and equipment, such as redundant or backup power supplies, redundant data communication connections, environmental controls (e.g. air conditioning, fire suppression) and security devices. ISL Online's master servers are located within the European Union in ISO 27001-certified data centres.

ISL Online servers are exclusively managed by our system administrators who need to follow a strict password storage policy. Due to the AES 256-bit end-to-end encryption security policy, even the administrators of the network cannot see the content of the sessions.

The data transferred between operators and clients during remote desktop sessions is NOT stored on ISL Online's servers. Only the basic session parameters (metadata) are stored on ISL Online's servers.

Metadata	Comment
Date	Timestamp – a date and time when the session was initiated by the operator.
Session Code	Unique session code used to establish the session.
Session Name	Name of the session (optional).
Username	Operator's username.
Client Email	Client's email address (optional).
Session Duration	Duration of the session in HH:MM:SS.
Status	Status of the session (e.g. running, paused, finished, etc.).
Session Start	Timestamp – when the session was started – operator connected to the remote device.
Bytes	Bytes transferred between the operator and the client during the session.
Server	ID of the server hosting the session.
Desk Platform	Operating system used by the operator.
Desk Version	ISL Light / ISL Light Desk version used by the operator.
Desk IP	Operator's IP address.
Client Platform	Operating system used by the client.
Client Version	ISL Light Client version used by the client.
Client IP	Client's IP address.
PPU Minutes Used	Number of Pay Per Use minutes used (optional).
Notes	Notes about the session (optional).
Multi-session ID	MAC address of device using multisession feature (optional).
Desk Network Interfaces	Network interfaces on the operator's side.
Client Network Interfaces	Network interfaces on the client's side.
Desk Transport	Transport used on the operator's side.
Client Transport	Transport used on the client's side.
Desk Language	Language used on the operator's side.
Client Language	Language used on the client's side.

For most security delicate organisations such as banks, national agencies, corporate environments, we offer the Self-Hosted models (Server License, Private Cloud) where the ISL Online system is installed on the server within such an organisation. In this case, all remote desktop connections are established through the server running within the organisation. As the self-hosted installation is a stand-alone system, the organisation is solely responsible for the server's administration. In this case, all data (including metadata) remains in a closed corporate environment.