Security Statement

Revision date: 15 August 2026

Security at a Glance

Introduction 3
About Us 3
Expect Maximum Security 4
RSA or ECDSA with Diffie-Hellman Key Exchange 4
AES 256-Bit End-to-End Encryption 5
Standard Connection 5
Direct Connection 5
  Host Candidates 6
  Server-Reflexive Candidates 7
  Relay Candidates 7
2-Step Verification (2FA) 8
ISO/IEC 27001:2022 Certification (Information Security Management) 8
Port Filtering 9
Allow/Deny List 9
Scheduled Sessions 9
Code Signing 10
External Security Audits and Penetration Testing 10
Function Transparency (No Stealth Mode) 10
Customizable Password Policy 11
Brute Force Intrusion Protection 11
Intranet (LAN-only) Setup 11
Reverse Proxy Support 11
Automatic Session Recording 11
Access Management 12
Incident Management System (IMS) 12
System and Audit Logs 12
Restriction of Features 13
External Authentication 13
Single Sign-On (SSO/SAML) 14
Verified Data Centres 14
Server Hardening 14
Compliance with Regulations and Security Standards 14
Data Minimization 15

Introduction

This document provides 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 to clarify any possible security concerns.

About Us

ISL Online is one of the pioneers of the remote desktop industry. Since 2001, we have been providing remote desktop software to IT professionals and help desk technicians from small and medium-size businesses to Fortune 500 companies. ISL ("Internet Services Layer") software is designed to make remote support and remote access sessions secure and efficient.

ISL Online (ISL Remote d.o.o.) is headquartered in the heart of Europe with offices in Germany, Slovenia, Switzerland and the United Kingdom. Together with Authorized Partners from the United States, Asia/Pacific, Middle East, Africa and Latin America we serve customers virtually anywhere in the world, with Japan being our strongest market.

Imprint:

ISL Online Headquarters

ISL Remote d.o.o.
Pot za Brdom 100
SI-1000 Ljubljana
Slovenia
VAT ID: SI24379905
Reg. Number: 7300514
support@islonline.com
+386 1 2447760

Germany	**Switzerland**	**United Kingdom**
ISL Online GmbH Noetherstrasse 1 D-69115 Heidelberg VAT ID: DE347105357 Reg. Number: HRB 741430 verkauf@islonline.com	ISL Online AG Aargauerstrasse 250 CH-8048 Zürich VAT ID: CHE-305.215.248 MWST Reg. Number: CHE-305.215.248 verkauf@islonline.com	ISL Online Ltd. 22 Basepoint Business Centre, Rivermead Drive, Westlea, Swindon, SN5 7EX, UK VAT ID: GB942657990 Reg. Number: 06581089 sales@islonline.com

You can find a list of Authorized Partners worldwide at: https://www.islonline.com/company/contact-us.htm

Expect Maximum Security

At ISL Online we address security very seriously. We apply industry-standard security technologies to protect your data and comply with the strictest security standards. Banks, government bodies and global brands choose ISL Online for its high level of security.

ISL Online offers different hosting options (cloud, on-premises, private cloud, and managed private cloud). Some security measures described in this document are only applicable to certain hosting options. Please contact us for details at support@islonline.com.

Please visit the ISL Online Glossary at https://www.islonline.com/help/glossary.htm to get acquainted with the terms used in this document.

RSA or ECDSA with Diffie-Hellman Key Exchange

ISL Online uses the following terminology when describing remote control session establishment:

- **Server Connection** – the initial TLS connection ISL Light establishes with an ISL Conference Proxy server (ICP)
- **Standard Connection** – an end-to-end encrypted connection (TLS) between two ISL Light endpoints, where packets are relayed by an ISL Conference Proxy (ICP) server. It consists of two logical components: the **Control Channel** and the **Remote Desktop Data Stream**.
- **Control Channel** – ISL Online's terminology for the component of the Standard Connection that keeps the connection between two endpoints active. The Remote Desktop Data Stream is only possible as long as the Control Channel is active.
- **Remote Desktop Data Stream** – ISL Online's terminology for the component of the **Standard Connection** that transfers encrypted data packets from one endpoint to another. The **Remote Desktop Data Stream** includes images of the remote desktop, files exchanged between the endpoints during the session, and audio/video communication between the Operator and the Client, among other data. It consumes the majority of the bandwidth. If possible, the Remote Desktop Data Stream is offloaded to a **Direct Connection**.
- **Direct Connection** – an end-to-end encrypted direct connection (TLS) between two ISL Light endpoints. In certain setups, it is relayed by a TURN server.

To establish a remote desktop session from your local computer to a remote computer, you need to start the ISL Light application, which possesses the RSA 2048-bit public key of the ISL Conference Proxy (ICP) server. The initial TLS connection (**Server Connection**) is established once the ISL Light application confirms it is connecting to the ISL Conference Proxy (ICP) server using the provided public key.

Once both endpoints (Operator and Client) have established a **Server Connection**, they use RSA keys to establish a **Standard Connection** between them. This is achieved by negotiating AES 256-bit symmetric encryption keys using the Diffie-Hellman cryptographic algorithm.

If available, a **Direct Connection** will be established between the two endpoints, allowing the contents of the session to be sent directly from one endpoint to the other without being relayed via the ISL Conference Proxy (ICP) server. The Direct Connection is created by using keys from the Elliptic Curve Digital Signature Algorithm (ECDSA P-256) to negotiate AES 256-bit symmetric encryption keys, employing the Diffie-Hellman cryptographic algorithm. While the initial **Standard Connection** remains active, it now serves solely as a Control Channel, managing the session connectivity without containing any information about the content of the Remote Desktop Data Stream.

AES 256-Bit End-to-End Encryption

Regardless of the connection type (Standard Connection or Direct Connection), the content of the Remote Desktop Data Stream between the local and remote computer is transferred through a secure tunnel, protected by symmetrical AES 256-bit end-to-end encryption, to meet the highest security standards.

Standard Connection

When a Standard Connection is used, all data traffic, including both the Control Channel and the Remote Desktop Data Stream, is relayed via an ISL Conference Proxy (ICP) server. The ICP cannot decrypt the content of the sessions but can only transfer packets from one side to another.

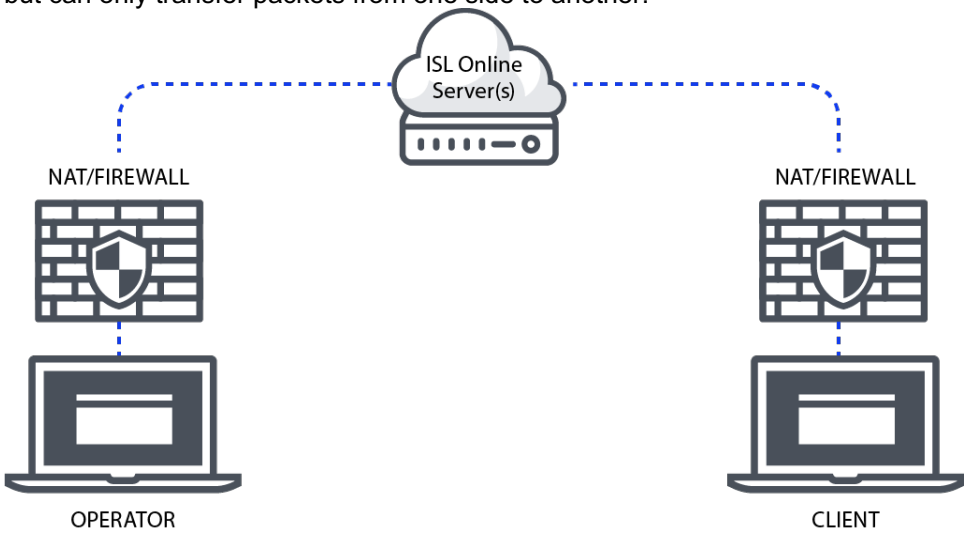


Diagram of Standard Connection using an ISL Conference Proxy (ICP) server to manage both the Control Channel and the Remote Desktop Data Stream.

Direct Connection

In certain cases, a Direct Connection is available, meaning that the data stream bypasses the ISL Conference Proxy server (ICP) and is established directly between the operator and the client. The ISL Conference Proxy server (ICP) will then only handle the Control Channel.

If both are available, ISL Light will compare which connection option offers better session speed and quality. To check if Direct Connection is available ISL Light conducts ICE (Interactive Connectivity Establishment) candidate checks once the Control Channel is established.

ICE (Interactive Connectivity Establishment) candidates are potential network addresses that a device can use to establish a communication channel with another device. ICE candidates include various types of addresses, and their purpose is to help devices discover the most suitable path for communication, especially when dealing with Network Address Translation (NAT) and firewalls. The original connection to the ISL Conference Proxy server (Control Channel, using Multiplexing (MUX) transport) remains necessary for sending metadata, while the Remote Desktop Data Stream is offloaded to a Direct Connection if available.

During the ICE process, devices exchange their lists of candidates, and connectivity checks are performed to determine the optimal path for communication. The negotiation and selection of candidates are part of the ICE protocol, allowing devices to adapt to different network environments and establish a reliable communication channel. ISL Light assesses the quality of MUX (Multiplexing) transport versus ICE transport. This evaluation considers factors such as ping time, with quality determined based on the latency in communication. The system selects the connection with the lower ping time to ensure optimal performance.

The main types of ICE candidates are:

- **Host Candidates**
- **Server-Reflexive Candidates**
- **Relay Candidates**

Host Candidates

These are the local IP addresses of the device itself. Host candidates represent the device's actual network interfaces and are used for direct connection when both devices are on the same local network.

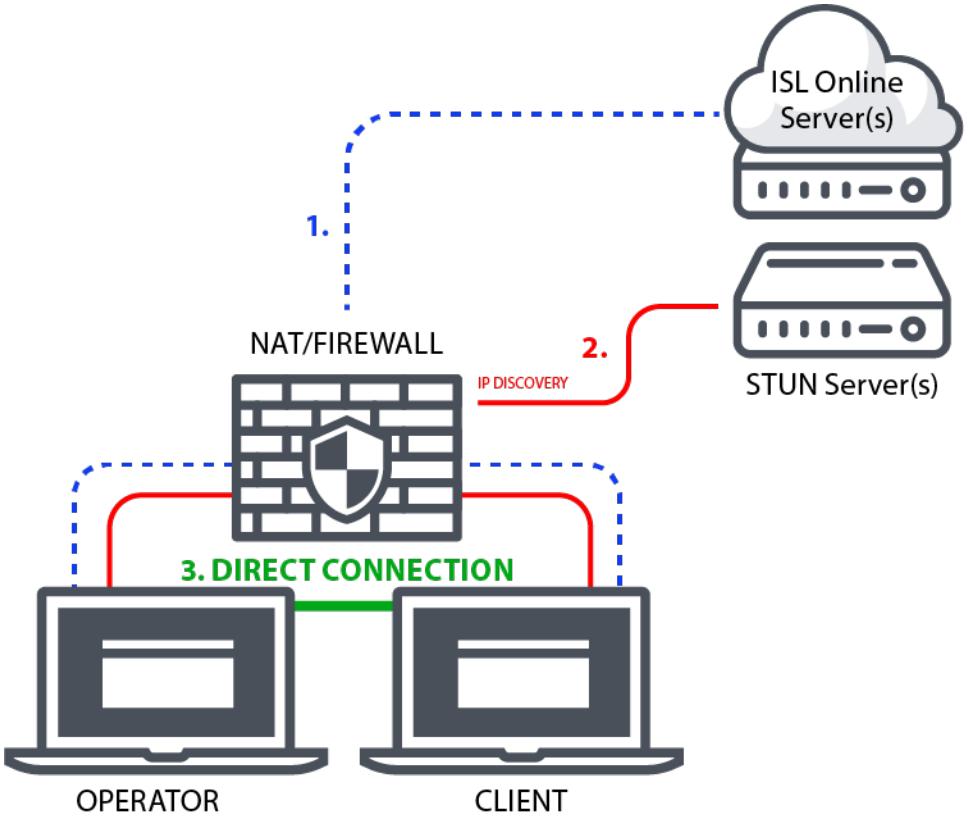


Diagram of Direct Connection via Host Candidates in a Local Area Network (LAN).

For the host candidate, the connection is initiated (blue line - representing the Control Channel) within the Local Area Network (LAN), originating from the operator's computer. It traverses NAT to reach the ISL Conference Proxy server (ICP). Likewise, the client's connection follows a comparable route, traversing NAT to reach the ISL Conference Proxy server (ICP). From there, the connection continues (red line) from the operator's and client's computer, passing through NAT to a STUN server. Following successful discovery a direct connection session

(green line – representing the Remote Desktop Data Stream) is established between the operator's and the client's computers.

Server-Reflexive Candidates

Server-reflexive candidates are acquired through STUN (Session Traversal Utilities for NATs) servers. STUN servers reflect UDP (User Datagram Protocol) packets back to the device, allowing it to discover its external address and port visible to the internet. This helps in establishing communication with devices outside the local network, overcoming NAT barriers.

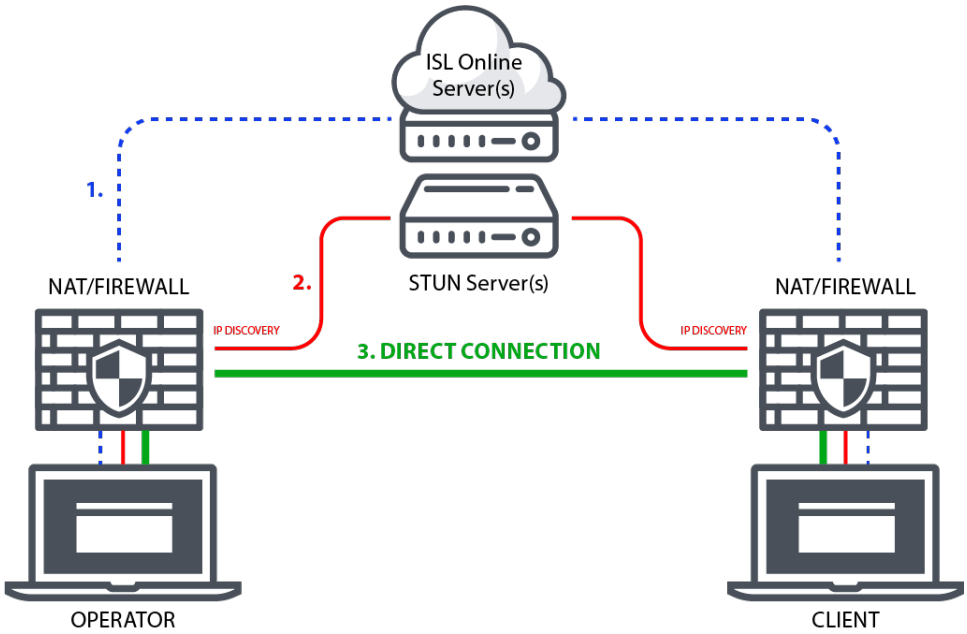


Diagram of Direct Connection via Server-Reflexive Candidates (STUN Server(s)).

For the server-reflexive candidate, the connection originates (blue line - representing the Control Channel) from the operator's computer passing through NAT, then to the ISL Conference Proxy server (ICP). Likewise, the client's connection follows a comparable route. From there, the connection proceeds (red line) from the operator's computer, passing through NAT to a STUN server. The same process occurs from the client's end. Following a successful discovery, a Direct Connection (green line – representing the Remote Desktop Data Stream) is established between the operator and the client.

Relay Candidates

Relayed candidates are obtained through a TURN (Traversal Using Relays around NAT) server. In cases where direct communication is not possible due to restrictive firewalls or symmetric NAT, devices can use a relay server to relay their data through a third-party server. TURN candidates help in establishing communication when other methods fail.

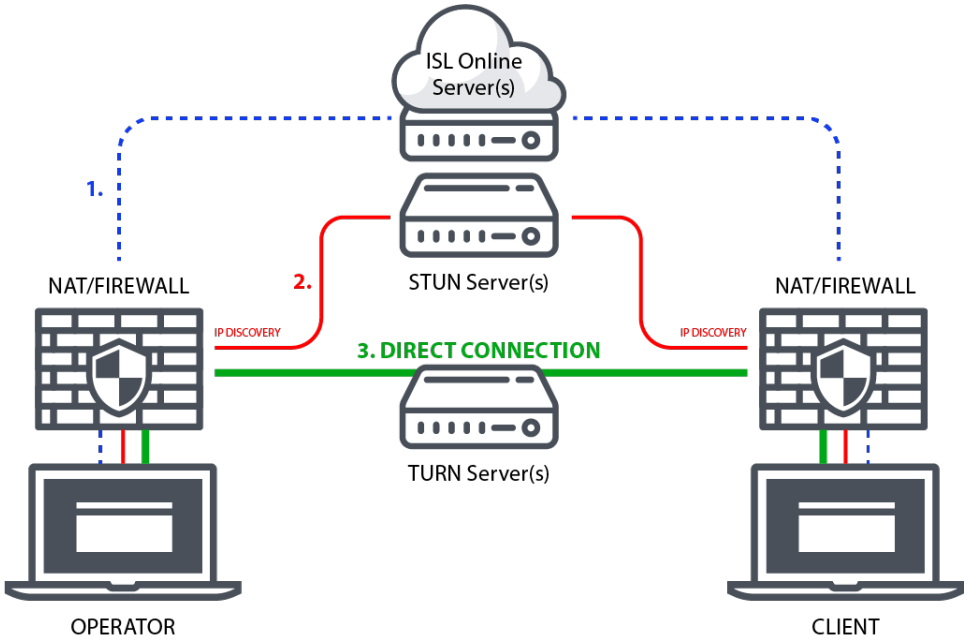


Diagram of Direct Connection via Relay Candidates (TURN Server(s)).

For Relay candidates, the connection originates (blue line - representing the Control Channel) from the operator's computer passing through NAT, then to the ISL Conference Proxy server (ICP). Likewise, the client's connection follows a comparable route. From there, the connection proceeds (red line) from the operator's computer, passing through NAT to a STUN server. The same process occurs at the client's end. The key difference from server-reflexive candidates is that the Direct Connection (green line – representing the Remote Desktop Data Stream) is established via a TURN server between the operator and client.

Since the session is end-to-end encrypted, the TURN server(s) cannot decrypt the content of the sessions; they only transfer data packets from one side to another.

2-Step Verification (2FA)

2-Step Verification (2FA) is a mandatory extra layer of security for help desk technicians and IT professionals. All operators must log in to the ISL Online system through a two-step verification process, providing something they know (a password) and something they have (a second factor). This second factor increases security and makes unauthorized access much more difficult.

ISL Online supports the following methods for the second verification step: passkeys, authentication apps (TOTP), and physical security keys. Email and phone-based verification are also supported, though we consider them less secure than the other methods and recommend using a passkey, authenticator app, or security key wherever possible.

ISO/IEC 27001:2022 Certification (Information Security Management)

The ISO 27001:2022 is internationally accepted and one of the most widely recognized information security standards. This certificate specifies the requirements for a comprehensive Information Security Management System (ISMS), and it defines how organizations manage and handle information securely. It is only awarded to organizations that follow stringent security practices, after a rigorous audit process.

The ISO/IEC 27001:2022 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.

Besides being ISO 27001 compliant, ISL Online's internal playbooks and security policies are also periodically reviewed against best practices suggested by SSAE 18 (SOC 2).

Port Filtering

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

However, larger organizations normally have a policy in place regarding 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 address 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.)

In case a Direct Connection is used the firewall must allow ports needed for STUN and TURN protocols. Most commonly the port 3478 is used, however relay connections are made on arbitrary high ports.

Allow/Deny List

Remote desktop software is an immensely powerful tool which enables you to control remote computers. To prevent any misuse of remote desktop software in your company, the possibility of creating Allow and Deny lists is indispensable.

For security reasons you might want to restrict the use of ISL Online software within your organization. You can limit the data access to ISL Conference Proxy servers (ICP) based on the IP and/or MAC addresses. You can use the "allow" function to specify the Allow list 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 reject a list of IP/MAC addresses. These rules can be defined for a specific user or the entire domain on the ISL Conference Proxy server (ICP).

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).

Scheduled Sessions

You can further limit your exposure to potential misuse by restricting the timeframe during which remote support sessions or unattended access to remote computers can be established.

For example, if your working hours are specified from 9 AM to 5 PM, you can prevent any remote support sessions from being initiated outside of that timeframe. Additionally, all active sessions will be terminated once the designated timeframe ends.

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 altered or corrupted.

ISL Online uses Google Cloud Key Management Service (Cloud KMS), including its Hardware Security Module (HSM) functionality, to securely manage the cryptographic signing keys used for our software.
Two code-signing certificates are in use: one with the Common Name (CN) "PDQ.com Corporation" (our parent company) and one with the Common Name "ISL Online Ltd.". Both certificates are used exclusively for the signing of ISL Remote software.

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 potential weaknesses and vulnerabilities identified.

Independent security audits and penetration tests of the ISL Online system are performed on a regular basis. Identified issues are remediated according to the following service levels, based on severity:

- **Critical**: within 72 hours
- **High**: within 7 days (up to 30 days with justification)
- **Medium**: within 30 days (up to 90 days with justification)
- **Low**: within 180 days (up to 364 days with justification)

Summaries of our penetration test results are available at trust.pdq.com. Additional detail can be provided under NDA to corporate clients who need to validate these statements.

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 always be able to follow the actions performed by the helpdesk operator.

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.

Customizable Password Policy

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.

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

Additionally, ISL Online offers you to completely customise the password policy you have in place. You can set it globally or on per-user basis, allowing you to meet stricter security standards you may have in place.

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

A brute-force attack is a trial-and-error method which calculates every 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 to prevent brute-force attacks. ISL Conference Proxy servers (ICP) 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.

Intranet (LAN-only) Setup

Some large organizations 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 unauthorized 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

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. The recording is carried out locally and not by the server, meaning that session recording does not compromise the end-to-end encryption of the session.

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 reduce their reoccurrence.

System and Audit Logs

To comply with regulations in most industries, remote desktop software should enable users to keep logs of system activity as well as audit logs showing clear accountability.

ISL Online allows IT administrators to identify unique users, show which systems were accessed 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. Logging level, specifying how detailed the system logs are, can be customized depending on the customer’s needs.

Information contained in system logs corresponds to data listed in “Data Minimization” section together with additional information: “action” – event that caused the log to be written.

Furthermore, client-side debug logs can be enabled allowing ISL Online or customer’s IT administrator to investigate the root cause of an issue. Logs are highly detailed and can contain sensitive information (e.g. local system paths). These logs require highly specific instructions to be enabled and are stored on local machines only. They need to be manually transferred to ISL Online or IT Administrator ensuring the client is fully aware of their contents and who has access to this information.

Additionally, an audit log is available allowing administrator to review configuration changes and other actions carried out by users within the system – audit logs will include information regarding which user carried out what action and when.

Integration with a third-party log aggregation / reporting solution is also possible.

Restriction of 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. As such the software may contain features that are not needed or approved under different security standards.

ISL Online offers you complete control over which features are available to your users allowing you to restrict usage of features that are not needed for your specific case. You may: completely prevent the operator from taking control of the remote computer, disable the file sharing option, disable the audio or video communication and many other options.

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

External authentication is a method of user authentication where an external system or service is used to verify the identity of a user attempting to access a system or application.

ISL Conference Proxy servers (ICP) support two main types of external authentication:

- **Type 1** (Traditional Authentication - **LDAP, RADIUS**): The login flow remains fully managed by ISL Conference Proxy servers (ICP), but instead of verifying the entered credentials against a local user database, the authentication module contacts an external system (e.g. LDAP, Active Directory, NetIQ eDirectory, RADIUS), attempts to authenticate there with the provided credentials and then allows or denies the login attempt based on the response of that external system.
- **Type 2** (Federated Authentication - **SAML 2.0**): The login flow changes and ISL Conference Proxy servers (ICP) redirect the user to the configured identity provider's login page. Upon successful authentication, the user is redirected back to ISL Conference Proxy servers (ICP) and logged in automatically.

Please refer to the next point for more information about SSO through the SAML 2.0 protocol.

Single Sign-On (SSO/SAML)

Eligible users (administrators) can configure a Single Sign-On (SSO) method that enables users from their organizations to securely authenticate and log into their ISL Online accounts through third-party SSO identity providers (e.g., Microsoft Entra ID, Okta, etc.) via the secure SAML 2.0 protocol.

When an organization configures SSO, the users' login flow is changed. When a user wants to log into ISL Online products and services, ISL Conference Proxy servers (ICP) redirect them to an external Identity Provider (IdP) for user authentication. A user needs to enter their SSO credentials provided to them by the organization. Upon successful login the IdP uses SAML 2.0 protocol to redirect the user back and confirm to the ISL Conference Proxy server (ICP) that the user has been authenticated and is authorized to continue.

Verified Data Centres

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 senior system administrators following strict policies and workflows. Due to the AES 256-bit end-to-end encryption security policy, even our server administrators can not access or view the contents of the sessions.

When offering the Managed Private Cloud (MPC) solution the data centre selection is carried out and approved by the customer, meaning the customer has full control over where the servers are located.

Server Hardening

All servers are provisioned automatically using hardened system images maintained in our internal repository. These images are configured to disable or remove non-essential services and software, ensuring that only approved components and processes required for the operation of our software are permitted to run.

Servers are continuously monitored for configuration changes and anomalous activity. Any findings are reported to the on-duty System Monitoring team and, where appropriate, escalated to the Incident Management team for further investigation and response. Monitoring is performed using a combination of custom built tooling and industry recognized endpoint protection solutions.

Compliance with Regulations and Security Standards

ISL Online is based in the European Union, which makes us subject to one of the world's most stringent data protection and privacy regulations. Stemming from Regulation (EU) 2016/679 (GDPR), ISL Online has implemented numerous safeguards and features allowing our users to exercise their privacy rights, and ensuring that ISL Online's handling and processing of data is carried out in accordance with the principles of GDPR.

ISL Online's information security practices are independently certified against the ISO/IEC 27001 standard, covering the design, development, sales, management, and support of our IT products and services. Our controls substantially overlap with the requirements of other major frameworks. The software is well-suited for companies and organizations that need to adhere to HIPAA (Health Insurance Portability and Accountability Act) requirements, and our dedicated data protection team can assist you with the documentation required to demonstrate your own HIPAA compliance. Likewise, our controls can support our clients' own SOC 2 compliance efforts.

Our team closely monitors the evolving legal and regulatory landscape in which we operate, including impactful new legislation such as the NIS-2 Directive and the Digital Operational Resilience Act (DORA), to keep our practices aligned with emerging requirements.

For a full overview of our certifications and compliance posture, visit https://www.islonline.com/compliance.htm. For any further inquiries, a dedicated privacy team is reachable at: dataprotection@islonline.com

Data Minimization

The data (session content) transferred between operators and clients during remote desktop sessions is NOT stored on ISL Online's servers. Servers will store the data listed in the Metadata table. ISL Online strives to handle and store only the minimal required data necessary for our service to operate and to provide our customers with session reports and history necessary for their business needs.

Please note, the metadata listed in this chapter is used as part of the Control Channel meaning it is created regardless of the type of connection used for a remote session (Standard Connection or Direct Connection).

Additionally, the metadata listed in this chapter is only stored on ISL Online's servers when session is created as part of our Hosted Service. For more security delicate organizations such as banks, national agencies, corporate environments... we offer the Self-Hosted models (Server License, Managed Private Cloud) where the ISL Online system is installed on dedicated servers or within privately owned datacenters. In such cases, all data (including metadata) remains in a closed corporate environment.

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	Custom name of the session (optional – if set by operator).
Username	Operator's username.
Client Email	Client's email address (optional – if provided by client).
Session Duration	Duration of the session in HH:MM:SS.
Status	Descriptive status of the session (running, paused, finished…).
Session Type	Remote Support (Attended) or Remote Access (Unattended).
Session Start	Timestamp – a date and time when the operator connected to the remote device.
Bytes	Number of bytes transferred 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.
Client Hostname	Hostname of the client's machine.

Client Description	Custom description of the client machine in ISL Light (optional – if set by operator)
Desk Hostname	Hostname of the operator's machine
Client MAC Address	MAC Address of the client's machine
Desk MAC Address	MAC Address of the operator's machine
Geo IP (Country, Region, City)	Estimated location inferred from IP Address, used by our Customer Protection Service (CPS) to prevent suspected fraudulent sessions.
Proxy, VPN	True/False values denoting if IP is a known proxy or a VPN address. Used by CPS to prevent suspected fraudulent sessions.
PPU Minutes Used	Number of Pay Per Use minutes consumed (optional – if PPU were used during the session).
Desk Comment	Comment provided by the Operator at the end of the session in the End of Session dialog (optional – dialog can be turned on or off)
Client Comment	Comment provided by the Client at the end of the session in the End of Session dialog (optional – dialog can be turned on or off)
Chat Transcript	Chat between the operator and the client during the session. By default, it is set to **Off**. It can be turned on upon request. Enabling the End Of Session dialog will turn on the Chat Transcript.
Notes	Notes about the session (optional – if added by the operator)
Multi-session ID	Hashed MAC addresses of device
Desk Network Interfaces	Network interfaces on the operator's side.
Client Network Interfaces	Network interfaces on the client's side.
Desk Transport	Network Transport used on the operator's side.
Client Transport	Network 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.
System Paths	Local system path where ISL Online executable file is ran from.