Declaración de Seguridad

Fecha de revisión: 5 de marzo de 2024

Tabla de contenido

Introducción

Este documento proporciona información de seguridad relacionada con ISL Online - software de escritorio remoto. Hemos preparado este documento para revelar el trasfondo técnico y las capas de seguridad implementadas en los productos de ISL Online. Te invitamos a distribuir este documento libremente a tus colegas, socios o clientes para aclarar cualquier posible preocupación de seguridad.

Acerca de Nosotros

ISL Online es uno de los pioneros de la industria del escritorio remoto. Desde 2001, nuestro software de escritorio remoto está ayudando a profesionales de TI y técnicos de mesa de ayuda, desde empresas pequeñas y medianas, hasta compañías Fortune 500. El software ISL ("Internet Services Layer") está diseñado para hacer las sesiones de soporte remoto y acceso remoto seguras y eficientes.

ISL Online (XLAB) tiene su sede en el corazón de Europa, con oficinas en Alemania, Eslovenia, Suiza y el Reino Unido. Junto con Distriduidores Autorizados de Estados Unidos, Asia/Pacífico, Medio Oriente, África y América Latina, atendemos a clientes prácticamente en cualquier parte del mundo, siendo Japón nuestro mercado más fuerte.

Casa Matriz de ISL Online

XLAB d.o.o.

Pot za Brdom 100

SI-1000 Ljubljana

Slovenia

VAT ID: SI15779092

Reg. Number: 1639714

support@islonline.com

+386 1 2447760

Alemania	Suiza	Reino Unido
ISL Online GmbH Noetherstrasse 1 D-69115 Heidelberg VAT ID: DE347105357 Reg. Number: HRB 741430 verkauf@islonline.com +49 (0)6221 321 4990	ISL Online AG Aargauerstrasse 250 CH-8048 Zürich VAT ID: CHE-305.215.248 MWST Reg. Number: CHE-305.215.248 verkauf@islonline.com +41 (0)62 724 13 60	ISL Online Ltd. 22 Basepoint Business Centre Rivermead Drive, Westlea Swindon, Wiltshire SN5 7EX, UK VAT ID: GB942657990 Reg. Number: 06581089 sales@islonline.com +44 1793 608 7370

Puedes encontrar una lista de nuestros Distribuidores Autorizados en:
https://www.islonline.com/company/about-us.htm

Blinda tu soporte con la máxima seguridad

Para ISL Online la seguridad de tu empresa es lo más importante. Integramos tecnologías de seguridad estándares en la industria para proteger tus datos y cumplir con los estándares más estrictos. Bancos, instituciones de gobierno y marcas globales, todos eligen ISL Online por cumplir con los más altos niveles de seguridad.

ISL Online ofrece diferentes opciones de hospedaje (nube, on-premises, nube privada y nube privada administrada). Algunas medidas de seguridad descritas en este documento solo son aplicables a ciertas opciones de hospedaje. Contáctanos para conocer más detalles en support@islonline.com.

Te invitamos también a visitar el Glosario de ISL Online en https://www.islonline.com/help/glossary.htm que explica algunos de los términos utilizados en este documento.

RSA o ECDSA con Intercambio de Claves Diffie-Hellman

ISL Online utiliza la siguiente terminología al describir el establecimiento de sesiones de control remoto:

- **Conexión de Servidor** – la conexión TLS inicial que ISL Light establece con un servidor ISL Conference Proxy (ICP).
- **Conexión Estándar** – una conexión cifrada de extremo a extremo (TLS) entre dos puntos finales de ISL Light, donde los paquetes son retransmitidos por un servidor ISL Conference Proxy (ICP). Consiste en dos componentes lógicos: el Canal de Control y el Flujo de Datos de Escritorio Remoto.
- **Canal de Control** – terminología de ISL Online para el componente de la Conexión Estándar que mantiene la conexión activa entre dos puntos finales. El Flujo de Datos de Escritorio Remoto solo es posible mientras el Canal de Control está activo.
- **Flujo de Datos de Escritorio Remoto** – terminología de ISL Online para el componente de la **Conexión Estándar** que transfiere paquetes de datos cifrados de un punto final a otro. El **Flujo de Datos de Escritorio Remoto** incluye imágenes del escritorio remoto, archivos intercambiados entre los puntos finales durante la sesión y la comunicación audiovisual entre el Operador y el Cliente, entre otros datos. Consume la mayoría del ancho de banda. Si es posible, el Flujo de Datos de Escritorio Remoto se descarga a una **Conexión Directa**.
- **Conexión Directa** – una conexión directa cifrada de extremo a extremo (TLS) entre dos puntos finales de ISL Light. En ciertas configuraciones, es retransmitida por un servidor TURN.

Para establecer una sesión de escritorio remoto desde tu equipo local a un equipo remoto, necesitas iniciar la aplicación ISL Light, que posee la clave pública RSA de 2048 bits del servidor ISL Conference Proxy (ICP). La conexión TLS inicial (**Conexión de Servidor**) se establece una vez que la aplicación ISL Light confirma que se está conectando al servidor ISL Conference Proxy (ICP) usando la clave pública proporcionada.

Una vez que ambos puntos finales (Operador y Cliente) han establecido una Conexión de Servidor, utilizan claves RSA para establecer una Conexión Estándar entre ellos. Esto se logra negociando claves de cifrado simétrico AES de 256 bits mediante el algoritmo criptográfico Diffie-Hellman.

Si está disponible, se establecerá una **Conexión Directa** entre los dos puntos finales, permitiendo que el contenido de la sesión se envíe directamente de un punto final a otro sin ser retransmitido a través del servidor ISL Conference Proxy (ICP).

La **Conexión Directa** se crea utilizando claves del Algoritmo de Firma Digital de Curva Elíptica (ECDSA P-256) para negociar claves de cifrado simétrico AES de 256 bits, empleando el algoritmo criptográfico Diffie-Hellman. Mientras la **Conexión Estándar** inicial permanece activa, ahora sirve únicamente como Canal de Control, gestionando la conectividad de la sesión sin contener ninguna información sobre el contenido del Flujo de Datos de Escritorio Remoto.

Cifrado de Extremo a Extremo AES de 256 Bits

Independientemente del tipo de conexión (Conexión Estándar o Conexión Directa), el contenido del Flujo de Datos de Escritorio Remoto entre el equipo local y el remota se transfiere a través de un túnel seguro, protegido por un cifrado simétrico de extremo a extremo AES de 256 bits, para cumplir con los estándares de seguridad más altos.

Conexión Estándar

Cuando se utiliza una Conexión Estándar, todo el tráfico de datos, incluyendo tanto el Canal de Control como el Flujo de Datos de Escritorio Remoto, se retransmite a través de un servidor ISL Conference Proxy (ICP). El ICP no puede descifrar el contenido de las sesiones, sino que solo puede transferir paquetes de un lado a otro.

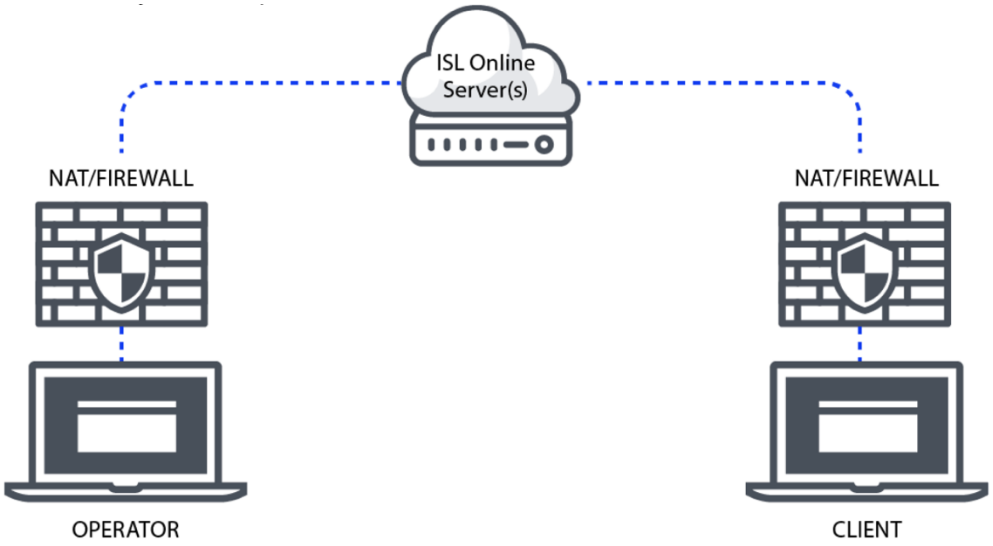

Diagrama de la Conexión Estándar utilizando un servidor ISL Conference Proxy (ICP) para gestionar tanto el Canal de Control como el Flujo de Datos de Escritorio Remoto.

Conexión Directa

En ciertos casos, está disponible una Conexión Directa, lo que significa que el flujo de datos evita el servidor ISL Conference Proxy (ICP) y se establece directamente entre el operador y el cliente. El servidor ISL Conference Proxy (ICP) entonces solo manejará el Canal de Control.

Si ambas están disponibles, ISL Light comparará qué opción de conexión ofrece mejor velocidad y calidad de sesión. Para verificar si la Conexión Directa está disponible, ISL Light realiza comprobaciones de candidatos ICE (Establecimiento de Conectividad Interactiva) una vez que el Canal de Control está establecido.

Los candidatos ICE (Establecimiento de Conectividad Interactiva) son direcciones de red potenciales que un dispositivo puede usar para establecer un canal de comunicación con otro dispositivo. Los candidatos ICE incluyen varios tipos de direcciones, y su propósito es ayudar a los dispositivos a descubrir la ruta más adecuada para la comunicación, especialmente cuando se trata de Traducción de Direcciones de Red (NAT) y firewalls. La conexión original al servidor ISL Conference Proxy (Canal de Control, utilizando transporte de Multiplexación (MUX)) sigue siendo necesaria para enviar metadatos, mientras que el Flujo de Datos de Escritorio Remoto se descarga a una Conexión Directa si está disponible.

Durante el proceso ICE, los dispositivos intercambian sus listas de candidatos y se realizan comprobaciones de conectividad para determinar el camino óptimo para la comunicación. La negociación y selección de candidatos son parte del protocolo ICE, permitiendo que los dispositivos se adapten a diferentes entornos de red y establezcan un canal de comunicación confiable. ISL Light evalúa la calidad del transporte MUX (Multiplexión) frente al transporte ICE. Esta evaluación considera factores como el tiempo de ping, determinando la calidad en base a la latencia en la comunicación. El sistema selecciona la conexión con el menor tiempo de ping para asegurar un rendimiento óptimo.

Los principales tipos de candidatos ICE son:

- **Candidatos Host**
- **Candidatos Server-Reflexive**
- **Candidatos de Relay**

Candidatos Host

Estas son las direcciones IP locales del propio dispositivo. Los candidatos Host representan las interfaces de red reales del dispositivo y se utilizan para la conexión directa cuando ambos dispositivos están en la misma red local.

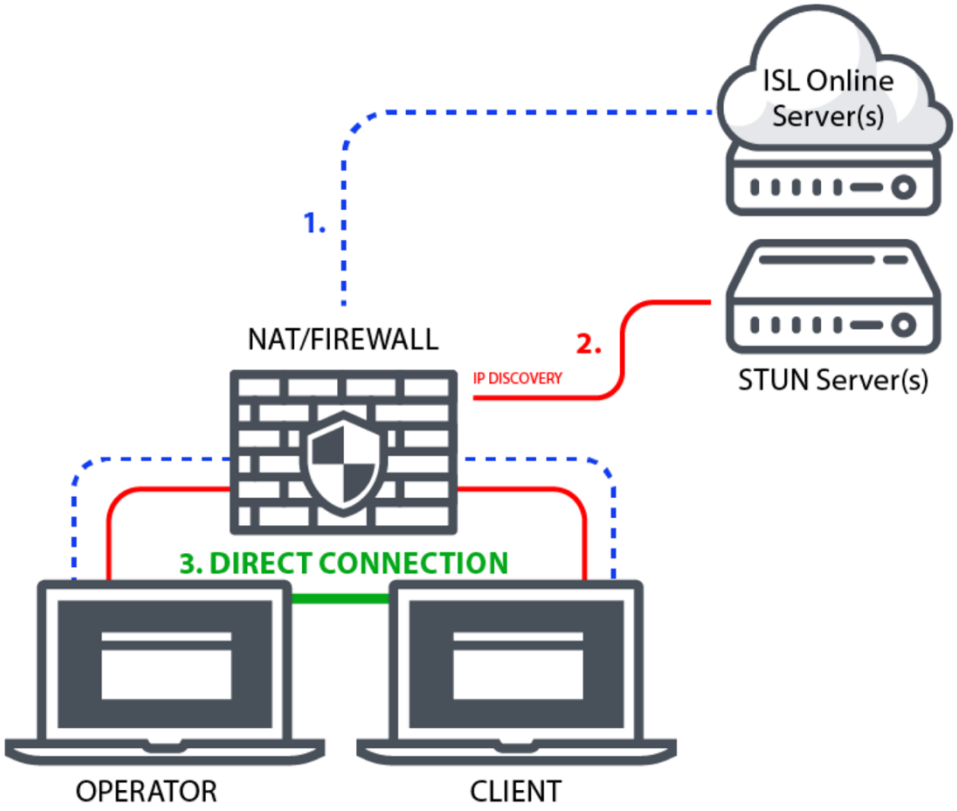

Diagrama de Conexión Directa mediante Candidatos Host en una Red de Área Local (LAN).

Para los candidatos Host, la conexión se origina (línea azul - representando el Canal de Control) desde el computador del operador pasando por NAT, luego al servidor ISL Conference Proxy (ICP). De manera similar, la conexión del cliente sigue una ruta comparable, atravesando el NAT para llegar al ISL Conference Proxy (ICP). A partir de ahí, la conexión continua (línea roja) desde los equipos del operador y del cliente, pasando por el

NAT hacia un servidor STUN. Tras un descubrimiento exitoso, se establece una sesión de conexión directa (línea verde, que representa el flujo de datos del escritorio remoto) entre los equipos del operador y del cliente.

Candidatos Server-Reflexive

Los candidatos Server-Reflexive se adquieren a través de servidores STUN (Utilidades de Travesía de Sesión para NATs). Los servidores STUN reflejan los paquetes UDP (Protocolo de Datagrama de Usuario) de vuelta al dispositivo, permitiéndole descubrir su dirección externa y puerto visibles a internet. Esto ayuda a establecer comunicación con dispositivos fuera de la red local, superando las barreras de NAT.

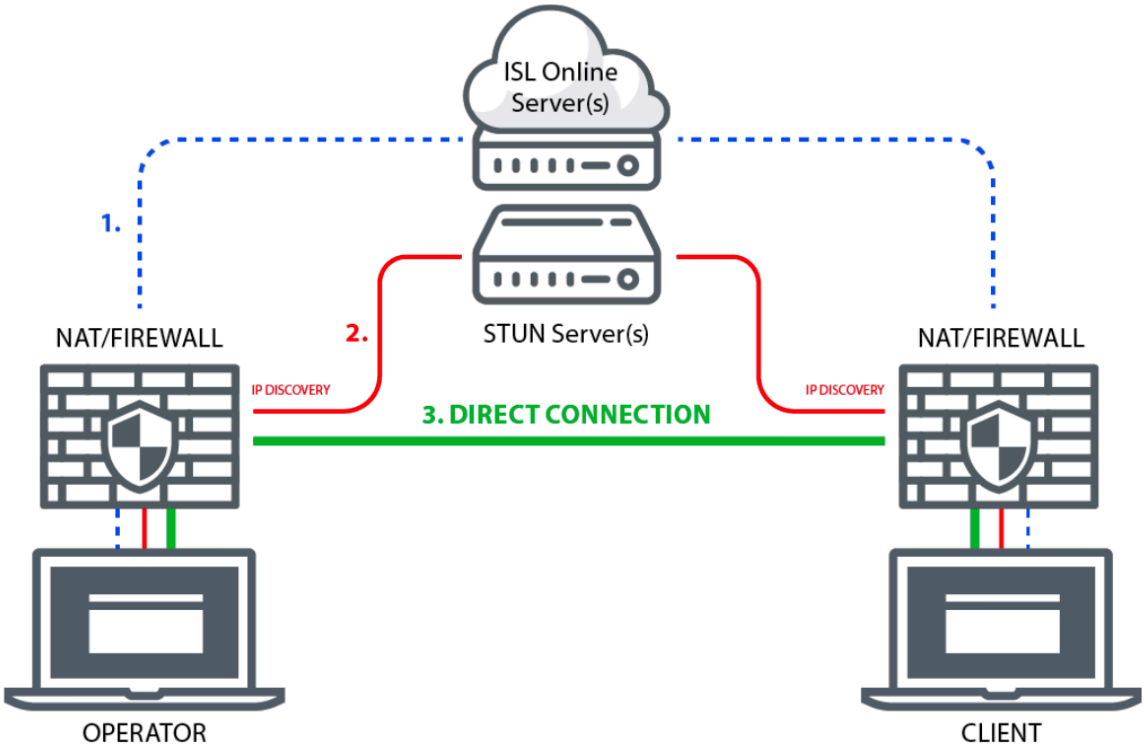

Diagrama de Conexión Directa a través de Candidatos Server-Reflexive (Servidor(es) STUN)

Para el candidato Server-Reflexive, la conexión se origina (línea azul - representando el Canal de Control) desde el equipo del operador pasando a través de NAT, luego al servidor ISL Conference Proxy (ICP). De manera similar, la conexión del cliente sigue una ruta comparable. Desde allí, la conexión procede (línea roja) desde el ordenador del operador, pasando a través de NAT hasta un servidor STUN. El mismo proceso ocurre desde el extremo del cliente. Tras un descubrimiento exitoso, se establece una Conexión Directa (línea verde – representando el Flujo de Datos de Escritorio Remoto) entre el operador y el cliente.

Candidatos Relay

Los candidatos relay se obtienen a través de un servidor TURN (Traversar Utilizando Relevos alrededor de NAT). En casos donde la comunicación directa no es posible debido a firewalls restrictivos o NAT simétrico, los dispositivos pueden usar un servidor relay para transmitir sus datos a través de un servidor de terceros. Los candidatos TURN ayudan a establecer comunicación cuando otros métodos fallan.

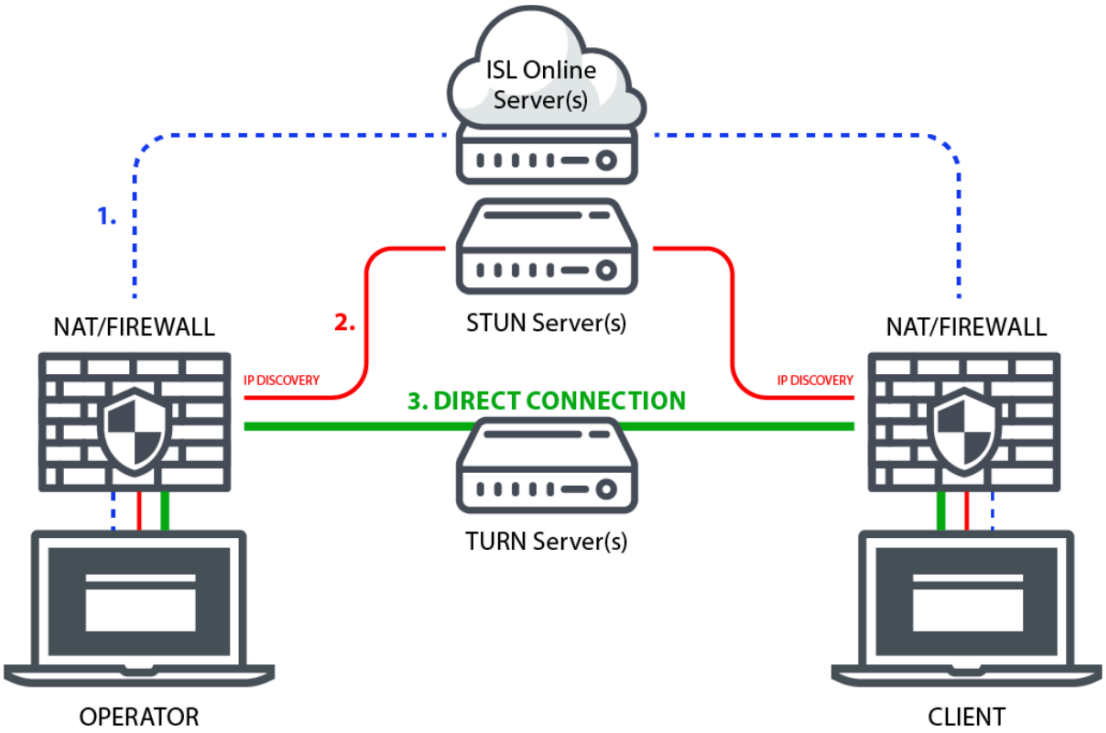

Diagrama de Conexión Directa a través de Candidatos Relay (Servidor(es) TURN)

Para los candidatos relay, la conexión se origina (línea azul - representando el Canal de Control) desde el ordenador del operador pasando a través de NAT, luego al servidor Proxy de Conferencia ISL (ICP). De manera similar, la conexión del cliente sigue una ruta comparable. Desde allí, la conexión procede (línea roja) desde el ordenador del operador, pasando a través de NAT hasta un servidor STUN. El mismo proceso ocurre desde el extremo del cliente. La diferencia clave respecto a los candidatos reflejados por el servidor es que la Conexión Directa (línea verde – representando el Flujo de Datos de Escritorio Remoto) se establece a través de un servidor TURN entre el operador y el cliente.

Dado que la sesión está cifrada de extremo a extremo, los servidores TURN no pueden descifrar el contenido de las sesiones; solo transfieren paquetes de datos de un lado a otro.

Verificación en Dos Pasos (2FA)

La Verificación en Dos Pasos (2FA) es una capa adicional de seguridad para los profesionales de TI. Con 2FA activado, los operadores solo pueden iniciar sesión en el sistema ISL Online pasando por un proceso de verificación de dos pasos proporcionando algo que saben (contraseña) y algo que tienen (token de 2FA). Este segundo factor aumenta la seguridad y hace mucho más difícil el acceso no autorizado.

Recomendamos usar la Verificación en Dos Pasos, especialmente en sistemas altamente sensibles. ISL Online permite configurar diferentes métodos para el segundo paso de verificación (correo electrónico, teléfono, aplicación de autenticación – TOTP, llave de seguridad – llaves Yubico basadas en el estándar FIDO U2F).

Certificación ISO/IEC 27001:2022 (Gestión de Seguridad de la Información)

La ISO 27001:2022 es internacionalmente aceptada y uno de los estándares de seguridad de la información más reconocidos a nivel mundial. Este certificado especifica los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) integral y define cómo las organizaciones gestionan y manejan la información de manera segura. Solo se otorga a organizaciones que siguen prácticas de seguridad estrictas, después de un proceso de auditoría riguroso. El certificado ISO/IEC 27001:2022 valida la experiencia de ISL Online en gestión de seguridad de la información y nuestro compromiso con el más alto nivel de seguridad en toda la empresa. Es una prueba adicional de que los datos están bien protegidos y seguros con ISL Online. Además de cumplir con la ISO 27001, los manuales internos y políticas de seguridad de ISL Online también son revisados periódicamente en contra de las mejores prácticas sugeridas por SSAE 16 (SOC 2).

Filtrado de Puertos

Con ISL Online, su firewall puede permanecer intacto ya que ISL Light inicia automáticamente conexiones salientes, intentando conectar usando los puertos 7615, 80 o 443.

Sin embargo, las organizaciones más grandes normalmente tienen una política establecida respecto a la configuración de sus firewalls o proxies. Los administradores de sistemas podrían querer abrir solo el puerto 7615 para permitir el tráfico de ISL Online directamente y seguir filtrando el resto. También pueden configurar excepciones por nombre de DNS o dirección IP.

Independientemente de la configuración de la red, las aplicaciones de ISL Online intentarán automáticamente diferentes enfoques para encontrar un transporte funcional (detectando configuraciones de proxy, usando WinINet, creando un túnel, haciendo uso del DNS comodín, etc.).

En caso de que se use una Conexión Directa, el firewall debe permitir los puertos necesarios para los protocolos STUN y TURN. Comúnmente se utiliza el puerto 3478, sin embargo, las conexiones relay se realizan en puertos altos arbitrarios.

Lista de Accesos Permitidos / Denegados

El software de escritorio remoto es una herramienta muy potente que permite controlar equipos remotos. Para prevenir cualquier mal uso del software de escritorio remoto en su empresa, la posibilidad de crear listas de accesos permitidos y denegados es indispensable.

Por razones de seguridad, podrías querer restringir el uso del software ISL Online dentro de tu organización. Puedes limitar el acceso a los datos a los servidores ISL Conference Proxy (ICP) basado en las direcciones IP y/o MAC. Puedes usar la función "permitir" para especificar la lista de direcciones IP/MAC que están autorizadas para iniciar una sesión de soporte remoto o acceder a un ordenador desatendido. Por otro lado, puedes usar la función "denegar" para rechazar una lista de direcciones IP/MAC. Estas reglas pueden definirse para un usuario específico o para todo el dominio en el servidor ISL Conference Proxy (ICP).

Por ejemplo, puedes permitir que tus empleados generen códigos de sesión para una sesión de soporte remoto solo desde la oficina (el rango de direcciones IP de tu empresa).

Sesiones programadas

Puedes limitar aún más tu exposición a un posible mal uso restringiendo el marco de tiempo durante el cual se pueden establecer sesiones de soporte remoto o acceso no supervisado a equipos remotos.

Por ejemplo, si su horario laboral está especificado de 9 AM a 5 PM, puedes evitar que se inicien sesiones de soporte remoto fuera de ese intervalo de tiempo. Además, todas las sesiones activas se terminarán una vez que finalice el marco de tiempo designado.

Firma de Código

La firma de código es ampliamente utilizada para proteger el software que se distribuye a través de Internet. La firma de código no realiza cambios en el software, sino que añade una firma digital al código ejecutable. Esta firma digital asegura a los destinatarios que el software de escritorio remoto proviene efectivamente de una fuenta confiable. Proporciona suficiente información para autenticar al firmante, así como para asegurar que el código no ha sido modificado posteriormente.

Las aplicaciones de ISL Online están firmadas digitalmente mediante un certificado de firma de código, que identifica de manera fiable a ISL Online como el editor del software y garantiza que el código no ha sido alterado ni corrompido desde que fue firmado con una firma digital.

Auditorías de Seguridad Externas y Pruebas de Penetración

Las auditorías de seguridad sistemáticas regulares y las pruebas de penetración enfocadas son cruciales para cada proveedor de software de escritorio remoto responsable de la seguridad de la información. Permiten a una empresa remediar posibles debilidades y vulnerabilidades identificadas. Las auditorías de seguridad independientes y las pruebas de penetración del sistema ISL Online se realizan de manera regular y revelan que ISL Online es un servicio confiable que proporciona un nivel muy alto de seguridad.

Transparencia de Funcionamiento (Sin Modo Oculto)

Es importante que una aplicación de escritorio remoto esté diseñada de tal manera que nunca pueda funcionar en segundo plano sin que el cliente sea consciente de ello. La funcionalidad del software debe ser totalmente transparente, y el cliente siempre debe poder seguir las acciones realizadas por el técnico de soporte.

ISL Online está diseñado para proporcionar soporte remoto a clientes a través de Internet, pero solo a petición explícita del cliente. El cliente permite que un operador de soporte inicie el escritorio remoto y puede terminar la sesión en cualquier momento. Cuando el operador toma el control total del escritorio del cliente, este puede recuperar fácilmente el control simplemente moviendo el ratón. Una vez terminada la sesión, el operador de soporte no puede acceder nuevamente al equipo del cliente con el mismo código de sesión.

Política de Contraseñas Personalizable

La seguridad de sus datos no depende solo de la fortaleza del método de cifrado, sino también de la fortaleza de sus contraseñas, incluyendo factores como la longitud y composición de la contraseña, y las medidas que toma para asegurar que sus contraseñas no sean divulgadas a ningún tercero.

Por defecto, la política de seguridad de contraseñas de ISL Online se basa en las últimas especificaciones del NIST (Instituto Nacional de Estándares y Tecnología) - la contraseña debe tener al menos 8 caracteres de longitud; se eliminarán los espacios iniciales y finales; los caracteres permitidos usados en las contraseñas son

cualquier carácter ASCII imprimible y espacios; la contraseña se verifica contra la lista negra, que consta de las contraseñas más comunes y simples.

Además, ISL Online le ofrece la posibilidad de personalizar completamente la política de contraseñas que tiene establecida. Puede configurarla globalmente o por usuario, lo que le permite cumplir con estándares de seguridad más estrictos que pueda tener.

ISL Online no almacena contraseñas en texto plano, primero aplica la técnica de Salted Password y después realiza un hashing a toda la cadena para proteger las contraseñas almacenadas en las bases de datos de cuentas de usuario.

Protección contra Intrusión por Fuerza Bruta

Un ataque de fuerza bruta es un método de prueba y error que calcula cada combinación que podría formar una contraseña o descifrar un archivo encriptado. En un ataque de fuerza bruta, se utiliza software automatizado para generar un gran número de conjeturas consecutivas hasta encontrar la correcta.

ISL Online ha configurado la limitación de velocidad para los intentos de incio de sesión y de conexión para prevenir ataques de fuerza bruta. Los servidores ISL Conference Proxy (ICP) previenen intentos de intrusión (inicio de sesión) por fuerza bruta limitando el número máximo de intentos fallidos de inicio de sesión para un usuario o para una dirección específica en un período de tiempo definido.

Configuración de Intranet (Solo LAN)

Algunas organizaciones grandes solo utilizan ISL Online para su soporte interno en diferentes ubicaciones geográficas. En tales casos, el software de escritorio remoto debe permitir establecer sesiones de escritorio remoto solo dentro de una red de área local (LAN).

Si planeas usar ISL Online solo dentro de su LAN (intranet), no es necesario una dirección IP pública. Solo necesita una dirección privada en el rango de redes privadas (como se especifica en el RFC 1918).

Soporte de Proxy Inverso

Un proxy inverso puede ocultar la topología y características de sus servidores backend al eliminar la necesidad de acceso directo a Internet a los mismos. Puedes colocar tu proxy inverso en una DMZ con acceso a Internet, pero ocultar sus servidores web dentro de una subred privada. Esto disminuye los riesgos de acceso no autorizado a datos sensibles. ISL Online le permite instalar el servidor detrás de un proxy inverso sin exponerlo directamente a Internet, terminando SSL en el proxy inverso.

Grabación Automática de Sesiones

El software de escritorio remoto no solo debe proteger la transmisión de datos, sino también protegerte a ti como proveedor de soporte y al cliente como su receptor. La mejor manera de lograr esto es la grabación de sesiones. Esto es particularmente importante para aquellas empresas que han confiado en una compañía de servicios externa para el mantenimiento de sistemas otorgando acceso remoto no limitado a sus equipos.

ISL Online ofrece una potente opción para comenzar a grabar automáticamente al inicio de cada sesión de acceso remoto con el fin de tener un control total sobre la actividad de acceso remoto y prevenir posibles conflictos con los clientes. La grabación se lleva a cabo localmente y no por el servidor, lo que significa que la grabación de la sesión no compromete el cifrado de extremo a extremo de la sesión.

Gestión de Accesos

Si solo una persona utiliza el software de escritorio remoto en la empresa, establecer permisos de acceso no es algo que te preocuparía, sin embargo, esta característica se vuelve muy importante desde el punto de vista de la seguridad una vez que hay numerosos usuarios utilizando el software para conectarse a equipos remotos. Con ISL Online, el administrador de la cuenta puede asignar a sus usuarios de dominio diferentes derechos y limitaciones, incluyendo permitir o deshabilitar el acceso a equipos específicos. Para cada usuario individual también puedes establecer un número máximo de sesiones concurrentes, deshabilitar derechos para usar audio, video, impresión remota, transferencia de archivos y compartir escritorio.

Sistema de Gestión de Incidentes (IMS)

Los proveedores de software de escritorio remoto deberían tener un sistema de gestión de incidentes (IMS) que garantice una restauración rápida de la operación normal del servicio después de una interrupción no planificada. ISL Online utiliza nuestro propio IMS, un conjunto de procedimientos, desarrollados por ISL Online, para mitigar los incidentes reportados. Siempre que se informa un incidente, se gestiona en nuestro sistema de tickets. Cada incidente normalmente incluye los siguientes elementos:

- Cronología UTC (un registro de eventos en orden cronológico en zona horaria UTC)
- Resumen ejecutivo (una descripción breve del incidente)
- Causa raíz (una explicación de la causa raíz del incidente)
- Resolución y recuperación (una descripción del proceso de mitigación del incidente)
- Medidas correctivas y preventivas (una explicación de las acciones tomadas para prevenir tales incidentes en el futuro)
- Otra información relevante

El IMS nos ayuda a mantener niveles de servicio continuos, medir la disponibilidad del servicio de TI, documentar los eventos no deseados y reducir su recurrencia.

Registros de Sistema y Auditoría

Para cumplir con las regulaciones en la mayoría de las industrias, el software de escritorio remoto debe permitir a los usuarios mantener registros de actividad del sistema así como registros de auditoría que muestren una responsabilidad clara.

ISL Online permite a los administradores de TI identificar usuarios únicos, mostrar qué sistemas fueron accedidos y, con una grabación de sesión activa, rastrear qué acciones se realizaron sobre la conexión remota. Dichos registros pueden profundizar en cada sesión individual, exponiendo la información sobre un operador, un cliente, direcciones IP, etc. El nivel de registro, especificando cuán detallados son los registros del sistema, puede ser personalizado dependiendo de las necesidades del cliente. La información contenida en los registros del sistema corresponde a los datos listados en la sección “Minimización de Datos” junto con información adicional: “acción” – evento que causó que se escribiera el registro.

Además, los registros de depuración del lado del cliente pueden habilitarse permitiendo que ISL Online o el administrador de TI del cliente investiguen la causa raíz de un problema. Los registros son altamente detallados y pueden contener información sensible (por ejemplo, rutas del sistema local). Estos registros requieren instrucciones muy específicas para ser habilitados y se almacenan solo en máquinas locales. Necesitan ser transferidos manualmente a ISL Online o al Administrador de TI asegurando que el cliente está completamente consciente de su contenido y quién tiene acceso a esta información.

Adicionalmente, un registro de auditoría está disponible permitiendo al administrador revisar los cambios de configuración y otras acciones realizadas por los usuarios dentro del sistema - los registros de auditoría

incluirán información sobre qué usuario realizó qué acción y cuándo. También es posible la integración con una solución de agregación de registros/informes de terceros.

Restricción de Funcionalidades

El software de escritorio remoto es una herramienta universal, utilizada prácticamente en todas las industrias. En consecuencia, existen innumerables casos de uso diferentes, que requieren soluciones muy flexibles. Como tal, el software puede contener características que no son necesarias o no están aprobadas bajo diferentes estándares de seguridad.

ISL Online le ofrece control completo sobre qué características están disponibles para sus usuarios, permitiéndote restringir el uso de características que no son necesarias para su caso específico. Puede: prevenir completamente que el operador tome control del ordenador remoto, deshabilitar la opción de compartir archivos, deshabilitar la comunicación de audio o video y muchas otras opciones.

Un ejemplo de donde es esencial restringir una característica: un empleado de banco debería poder ver la pantalla del ordenador del cliente, pero nunca debería poder comenzar a compartir su propio escritorio. En este caso, la compartición de escritorio en el lado del escritorio puede ser deshabilitada.

Autenticación Externa

La autenticación externa es un método de autenticación de usuario donde se utiliza un sistema o servicio externo para verificar la identidad de un usuario que intenta acceder a un sistema o aplicación. Los servidores

ISL Conference Proxy (ICP) admiten dos tipos principales de autenticación externa:

- **Tipo 1** (Autenticación Tradicional - LDAP, RADIUS): El flujo de inicio de sesión se mantiene completamente gestionado por los servidores ISL Conference Proxy (ICP), pero en lugar de verificar las credenciales ingresadas contra una base de datos de usuarios local, el módulo de autenticación contacta a un sistema externo (por ejemplo, LDAP, Active Directory, NetIQ eDirectory, RADIUS), intenta autenticarse allí con las credenciales proporcionadas y luego permite o deniega el intento de inicio de sesión basado en la respuesta de ese sistema externo.
- **Tipo 2** (Autenticación Federada - SAML 2.0): El flujo de inicio de sesión cambia y los servidores ISL Conference Proxy (ICP) redirigen al usuario a la página de inicio de sesión del proveedor de identidad configurado. Tras una autenticación exitosa, el usuario es redirigido de nuevo a los servidores ISL Conference Proxy (ICP) e inicia sesión automáticamente.

Por favor, consulte el siguiente punto para obtener más información sobre el SSO a través del protocolo SAML 2.0.

Inicio de Sesión Único (SSO/SAML)

Los usuarios elegibles (administradores) pueden configurar un método de Inicio de Sesión Único (SSO) que permite a los usuarios de sus organizaciones autenticarse y acceder de manera segura a sus cuentas de ISL Online a través de proveedores de identidad SSO de terceros (por ejemplo, Microsoft Entra ID, Okta, etc.) mediante el protocolo seguro SAML 2.0.

Cuando una organización configura SSO, el flujo de inicio de sesión de los usuarios cambia. Cuando un usuario desea iniciar sesión en los productos y servicios de ISL Online, los servidores ISL Conference Proxy (ICP) los redirigen a un Proveedor de Identidad externo (IdP) para la autenticación del usuario. El usuario necesita ingresar sus credenciales SSO proporcionadas por la organización. Tras un inicio de sesión exitoso, el IdP

utiliza el protocolo SAML 2.0 para redirigir al usuario de vuelta y confirmar al servidor ISL Conference Proxy (ICP) que el usuario ha sido autenticado y está autorizado para continuar.

Centros de Datos Verificados

Los servidores de ISL Online (Nube Pública) están alojados en centros de datos profesionales en todo el mundo. Solo elegimos centros de datos altamente confiables y probados en la industria con instalaciones y equipos modernos, como suministros de energía redundantes o de respaldo, conexiones de comunicación de datos redundantes, controles ambientales (por ejemplo, aire acondicionado, supresión de incendios) y dispositivos de seguridad.

Los servidores maestros de ISL Online están ubicados dentro de la Unión Europea en centros de datos certificados ISO 27001.

Los servidores de ISL Online son gestionados exclusivamente por nuestros administradores de sistemas sénior siguiendo políticas y flujos de trabajo estrictos. Debido a la política de seguridad de cifrado de extremo a extremo AES de 256 bits, incluso nuestros administradores de servidores no pueden acceder o ver el contenido de las sesiones.

Cuando se ofrece la solución de Nube Privada Administrada (MPC), la selección del centro de datos se lleva a cabo y es aprobada por el cliente, lo que significa que el cliente tiene control total sobre la ubicación de los servidores.

Cumplimiento de Regulaciones y Estándares de Seguridad

ISL Online es una empresa con sede en la Unión Europea, lo que nos hace sujetos a una de las regulaciones de protección de datos y privacidad más estrictas del mundo. Derivado del Reglamento (UE) 2016/679 (GDPR), ISL Online ha implementado numerosas salvaguardias y características que permiten a nuestros usuarios ejercer sus derechos de privacidad, así como asegurar que el manejo y procesamiento de datos realizado por ISL Online se lleve a cabo de acuerdo con los principios del GDPR.

Además, ISL Online permite el acceso remoto, el soporte remoto y las herramientas de colaboración en línea en el nivel de seguridad más alto, comprobado por la certificación contra el estándar de seguridad ISO 27001. El software también es adecuado para empresas y organizaciones que necesitan adherirse a los estrictos requisitos de HIPAA (Ley de Portabilidad y Responsabilidad de Seguros de Salud) y auditar su cumplimiento. ISL Online también incorpora las prácticas de ISO 27001 dentro de las herramientas proporcionadas a sus clientes. Dado que los requisitos de ISO 27001 superan los requisitos esbozados por HIPAA, ISL Online permite a sus clientes mantener o lograr el cumplimiento con HIPAA. Un equipo dedicado de protección de datos puede ayudarlo con la documentación y las pruebas requeridas para demostrar el cumplimiento.

Del mismo modo, debido a la superposición entre ISO 27001 y SOC 2, ISL Online permite a nuestros clientes mantener el cumplimiento con las regulaciones SOC-2. El alcance de nuestra certificación ISO 27001 cubre lo siguiente:

Diseño, desarrollo, ventas, gestión y soporte de productos y servicios de TI

y debería cubrir suficientemente las necesidades de nuestros clientes que intentan demostrar su cumplimiento con el estándar SOC 2.

Para cualquier consulta adicional, puedes contactar al equipo especializado en la siguiente dirección: dataprotection@islonline.com

Minimización de Datos

Los datos (contenido de la sesión) transferidos entre operadores y clientes durante las sesiones de escritorio remoto NO se almacenan en los servidores de ISL Online. Los servidores almacenarán los datos enumerados en la tabla de Metadatos. ISL Online se esfuerza por manejar y almacenar solo los datos mínimos necesarios para que nuestro servicio funcione y para proporcionar a nuestros clientes informes de sesiones e historial necesarios para sus necesidades comerciales.

Ten en cuenta que los metadatos enumerados en este capítulo se utilizan como parte del Canal de Control, lo que significa que se crean independientemente del tipo de conexión utilizada para una sesión remota (Conexión Estándar o Conexión Directa).

Además, los metadatos enumerados en este capítulo solo se almacenan en los servidores de ISL Online cuando se crea la sesión como parte de nuestro Servicio Hospedado. Para organizaciones más delicadas en seguridad, como bancos, agencias nacionales, entornos corporativos... ofrecemos los modelos Autoalojados (Licencia de Servidor, Nube Privada Gestionada) donde el sistema ISL Online está instalado en servidores dedicados o dentro de centros de datos de propiedad privada. En tales casos, todos los datos (incluidos los metadatos) permanecen en un entorno corporativo cerrado.

Metadatos	**Comentario**
Fecha	Timestamp - Fecha y hora en la que el operador inició la sesión.
Código de sesión	Código único utilizado para establecer la sesión.
Nombre de la sesión	Nombre personalizado de la sesión (opcional – si lo establece el operador).
Nombre de usuario	Nombre de usuario del operador.
Correo electrónico del cliente	Correo electrónico del cliente (opcional – si lo proporciona el cliente).
Duración de la sesión	Duración de la sesión en HH:MM
Estado	Estado descriptivo de la sesión (en curso, en pausa, finalizada…).
Tipo de sesión	Soporte Remoto (Asistido) o Acceso Remoto (No Asistido).
Inicio de la sesión	Fecha y hora de conexión del operador: Fecha y hora en la que el operador se conectó al dispositivo remoto.
Bytes	Número de bytes transferidos durante la sesión.
Servidor	ID del servidor que aloja la sesión.
Plataforma del escritorio	Sistema operativo utilizado por el operador.
Versión del escritorio	Versión de ISL Light / ISL Light Desk utilizada por el operador.
IP del escritorio	Dirección IP del operador.
Plataforma del cliente	Sistema operativo utilizado por el cliente.
Versión del cliente	Versión de ISL Light Cliente utilizada por el cliente.
IP del cliente	Dirección IP del cliente.
Nombre de host del cliente	Nombre de host de la máquina del cliente.
Descripción del cliente	Descripción personalizada de la máquina del cliente en ISL Light (opcional – si lo establece el operador).
Nombre de host del escritorio	Nombre de host de la máquina del operador.

Dirección MAC del cliente	Dirección MAC de la máquina del cliente.
Dirección MAC del escritorio	Dirección MAC de la máquina del operador.
Minutos PPU utilizados	Número de minutos de Pago Por Uso consumidos (opcional – si se utilizaron durante la sesión).
Comentario del escritorio	Comentario proporcionado por el Operador al final de la sesión en el diálogo de fin de sesión (opcional – el diálogo puede activarse o desactivarse).
Comentario del cliente	Comentario proporcionado por el Cliente al final de la sesión en el diálogo de fin de sesión (opcional – el diálogo puede activarse o desactivarse).
Transcripción del chat	Chat entre el operador y el cliente durante la sesión. Por defecto, está desactivado. Puede activarse a solicitud. Habilitar el diálogo de fin de sesión activará la transcripción del chat.
Notas	Notas sobre la sesión (opcional – si las añade el operador).
ID de multi-sesión	Direcciones MAC cifradas del dispositivo.
Interfaces de red del escritorio	Interfaces de red del lado del operador.
Interfaces de red del cliente	Interfaces de red del lado del cliente.
Transporte de red del escritorio	Transporte de red utilizado del lado del operador.
Transporte de red del cliente	Transporte de red utilizado del lado del cliente.
Idioma del escritorio	Idioma utilizado del lado del operador.
Idioma del cliente	Idioma utilizado del lado del cliente.
Rutas del sistema	Ruta del sistema local donde se ejecuta el archivo ejecutable de ISL Online.