

## Soporte y servicio remoto seguros para dispositivos inteligentes

La seguridad es un asunto fundamental para Leica Microsystems y sus clientes usuarios de los servicios remotos. Leica Microsystems requiere una solución probada de un servicio remoto que proteja contra virus y/o piratas informáticos dando un soporte a nuestros instrumentos, sin modificaciones importantes en la red por parte del usuario final, a la par que se trabaja en nuestro modelo de seguridad de red actual y se obtiene una certificación oficial mediante una empresa de seguridad de terceros. Puesto que los instrumentos de Leica Microsystems se conectan a las redes de nuestro cliente, los clientes finales necesitan tener la seguridad de que la solución de servicio remoto es compatible con su actual modelo de seguridad, proporcionando además un control gradual y total sobre el acceso de usuario, incluso ofrece posibilidades de seguimiento y auditoría de utilización sencilla (trazabilidad).

Para el nuevo sistema de servicio remoto (RemoteCare), Leica Microsystems, utiliza infraestructura de servidor y software Axeda® ServiceLink™. Axeda ServiceLink minimiza las preocupaciones en materia de seguridad de Leica y nuestros clientes, a la par que reduce de forma proactiva el tiempo de inactividad, gestiona los riesgos y garantiza que el equipo esté siempre habilitado para proporcionar resultados óptimos.

Mediante Axeda ServiceLink, RemoteCare de Leica Microsystems conecta perfectamente nuestra empresa con los instrumentos que fabricamos, en los propios entornos de nuestro cliente (conectando con el sistema operativo del usuario final). Puesto que estos instrumentos con frecuencia realizan el seguimiento de registros de pacientes y demás tipos de información privada y protegida, las capacidades de seguridad y conformidad se encuentran entre los requisitos más importantes evaluados en cualquier solución de servicio remoto. En este documento se examinan los requisitos de Leica Microsystems y de sus clientes, así como la forma en que Axeda ServiceLink proporciona el soporte y servicio remoto seguro y probado para tratar dichos requisitos.

### Requisitos de Leica Microsystems en materia de seguridad para el servicio remoto

Leica Microsystems eligió productos Axeda para RemoteCare a fin de cumplir los más estrictos requisitos de seguridad, tanto a nivel de nuestra empresa como nuestros clientes, para que puedan utilizar los servicios remotos de forma efectiva y rutinaria, teniendo la confianza de que todas las conexiones son seguras y privadas en todo momento.

Algunos de nuestros requisitos más comunes incluyen:

- **Diseño probado por la empresa:** al conectar un ordenador a Internet aumenta la preocupación por la seguridad, y ocurre lo mismo cuando se conectan dispositivos inteligentes. Ya sean piratas informáticos que estén intentando dañar un dispositivo con archivos corruptos, virus, robar datos que se transfieran entre el instrumento y Leica Microsystems, u obtener acceso no autorizado a información importante, un sistema de supervisión remota debe ofrecer protección contra éstas y otras amenazas.
- **Soporte para varios dispositivos:** Leica Microsystems necesita dar soporte de forma segura a distintos tipos de dispositivos y configuraciones complejas de clientes sin que sea necesario que el usuario final realice cambios importantes.
- **Implementación rápida:** para que los clientes adopten sistemas de servicio remoto, debe haber capacidades de seguridad en el modelo de seguridad de la red actual del cliente.
- **Validación firme de seguridad de terceros:** una certificación oficial mediante una auditoría de seguridad ofrece confianza a los clientes en las capacidades de la tecnología y el proveedor.

### Compromiso:

Leica Microsystems cree que la privacidad y la seguridad tienen una gran importancia para nuestros clientes.

RemoteCare mantiene los siguientes principios relativos a la seguridad:

- Proteger la integridad del sistema: red, equipos y datos
- Realizar el seguimiento del acceso y de la actividad para lograr la conformidad normativa
- Ofrecer flexibilidad y control para cumplir las políticas empresariales
- Auditar y certificar los procesos y soluciones de Leica Microsystems regularmente mediante un tercero

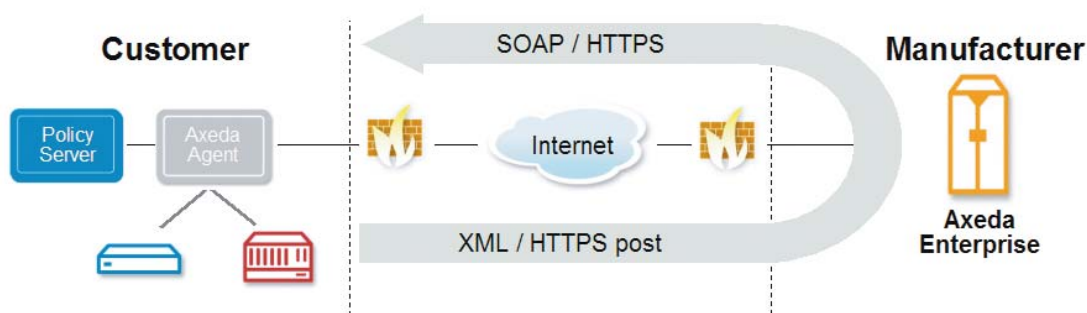
## Requisitos del cliente en materia de seguridad para el servicio remoto

Se conectan instrumentos inteligentes a las redes de nuestro cliente. Cada cliente tiene su propia política de seguridad y protección de red en forma de cortafuegos, servidores proxy y esquemas de direccionamiento. Un dispositivo conectado a su red estará protegido detrás de estas capas de seguridad. Si una oferta de servicio remoto requiere cambios en la protección de red de nuestro cliente, probablemente no tendrá aceptación. Por ello, es importante tener en cuenta los requisitos del cliente, incluyendo:

- El mantenimiento del modelo de seguridad actual: el dispositivo de Leica Microsystems debe ser compatible con la forma en que la organización gestiona las operaciones, las políticas o los procedimientos de seguridad, y debe cumplir las normas aceptadas del sector.
- El control del acceso de usuarios: siguiendo la línea del modelo de seguridad del cliente, el dispositivo de Leica Microsystems debe proporcionar al cliente (no a Leica Microsystems) control gradual y definir políticas sobre las acciones que se pueden realizar en el dispositivo, tales como recopilación de datos y actualizaciones de software, y cuándo se pueden realizar esas acciones. Estas políticas deben definirse centralmente para todos los instrumentos en una ubicación del cliente.
- La auditoría y seguimiento de la actividad: los requisitos de conformidad normativa y de políticas dictan que el sistema de la empresa debe facilitar la realización de la auditoría y el seguimiento de la actividad de administración y de todos los usuarios.

Axeda ServiceLink ofrece el rendimiento, flexibilidad y escalabilidad necesarios para satisfacer las necesidades del mayor rango posible de clientes de RemoteCare de Leica Microsystems proporcionando la más amplia gama posible de funciones de seguridad y garantías de protección de los datos.

Figura 1: Comunicaciones Firewall-Friendly™ de Axeda



## No se requieren cambios en las infraestructuras de seguridad o de TI

El uso de tecnología Firewall-Friendly™ permite que RemoteCare proporcione comunicación de dos vías basándose en estándares de servicios web, entre los que se incluyen Hypertext Transfer Protocol (HTTP), Simple Object Access Protocol (SOAP) y eXtensible Markup Language (XML). No es necesario realizar cambios en la infraestructura de seguridad de TI del cliente final para admitir diagnósticos y supervisión remota. Además, todas las comunicaciones entre el centro de datos de Leica o del proveedor de servicios y el sitio del cliente están cifradas mediante Secure Sockets Layer (SSL) hasta 168 bits.

## No se necesitan módems ni VPN

El agente de RemoteCare inicia todas las comunicaciones conforme al entorno informático seguro del sitio del dispositivo. Tampoco es necesario configurar costosas VPN para implementar RemoteCare o para poner en riesgo la seguridad al utilizar comunicaciones de conexión por módem. El único requisito es una conexión a Internet.

## Control de acceso y autenticación de usuarios de fácil gestión

El sistema RemoteCare utiliza la norma Lightweight Directory Access Protocol (LDAP) para autenticar usuarios.

El control de acceso de usuarios se gestiona mediante un control basado en la actividad y en el dispositivo. Estos métodos se combinan en una amplia variedad de formas para que los usuarios puedan realizar su trabajo de forma efectiva a la par que se protege todo acceso a información confidencial.

El control de acceso basado en la actividad permite al administrador del sistema RemoteCare asignar y clasificar usuarios mediante Axeda ServiceLink, así como definir las actividades que se pueden realizar. Cada grupo de usuarios recibe acceso controlado en la aplicación Axeda, página y niveles de función.

El control de acceso basado en el dispositivo proporciona un método para definir los dispositivos específicos a los que puede acceder cada grupo de usuarios. Este método de control limita la visualización de información de dispositivos a sólo los dispositivos de los que es responsable un usuario.

## Comunicaciones seguras y confidencialidad de los datos

Mucha de la información que se transmite por el Internet público utiliza texto sencillo encapsulado en mensajes HTTP estándar. Los piratas informáticos pueden obtener acceso a la red en un punto cercano a la fuente o destino del mensaje y, a continuación, capturar y ver el texto de estos mensajes HTTP con herramientas que se pueden conseguir fácilmente.

RemoteCare, a través del software Axeda e infraestructura de servidor, es compatible con el mismo cifrado SSL estándar que utilizan los bancos para realizar transacciones en línea. SSL admite longitud de clave de hasta 168 bits y autenticación mutua utilizando certificados. RemoteCare puede también habilitar cifrado de mensajes AES de 256 bits de clave secreta, que se puede utilizar con SSL para cifrar datos más allá de la zona desmilitarizada (DMZ).

## Implementaciones probadas

El sistema RemoteCare es implementado en todo el mundo por fabricantes de varios sectores, incluyendo la seguridad nacional, ciencias de la vida, industria médica, tecnología de la información, telecomunicaciones, impresión y captura y procesamiento de imágenes, cabinas telefónicas, semiconductores, automatización de edificios y entornos industriales.

## Lo más destacado en seguridad de RemoteCare:

- Comunicaciones Firewall-Friendly™
- No se requieren cambios en las infraestructuras de seguridad y de TI
- No se precisan módems ni VPN
- Control completo del cliente final para cumplir las políticas empresariales
- Fácil de implementar y gestionar la seguridad de usuarios, aplicaciones y dispositivos
- Datos de cifrado SSL de 128 bits, HTTPS y PKI

## Características y ventajas en materia de seguridad

La tecnología Axeda proporciona a RemoteCare las siguientes características de seguridad y ventajas

### Seguridad de red

Características:

- La tecnología Firewall-Friendly™ está basada en estándares de servicios web, incluyendo HTTP, SOAP y XML.
- El Axeda Agent inicia todas las comunicaciones, por lo que los dispositivos no requieren direcciones IP públicas y no son visibles desde fuera del cortafuegos.

Ventajas:

- Los clientes no necesitan realizar cambios en la configuración del cortafuegos ni en los servidores proxy, de modo que se facilita la implementación y se tratan los objetivos de conformidad.
- No es necesario realizar conexiones de módem ni VPN.

### Seguridad del sistema y de los datos

Características:

- El cifrado SSL admite longitud de clave de hasta 168 bits y autenticación mutua utilizando certificados digitales bidireccionales.
- Cifrado de mensajes AES de 256 bits de clave secreta, que se puede utilizar con SSL para cifrar datos detrás de la DMZ.

Ventajas:

- Sólo las partes autorizadas pueden acceder a datos y dispositivos designados. Los clientes finales pueden limitar el acceso, vistas e, incluso, acciones según la función del usuario, lo cual les proporciona control sobre usuarios y acciones.
- Las comunicaciones probadas basadas en normas garantizan la conformidad con los requisitos normativos.

### Seguridad de la aplicación y del usuario

Características:

- El acceso al sistema se controla centralmente y se autentifica con respecto a un sistema LDAP de empresa.
- Las contraseñas de gran seguridad – imponen el uso de un mínimo de seis caracteres con una combinación de letras, números y símbolos.
- Se realiza el seguimiento y se registra cualquier actividad de acceso remoto.

Ventajas:

- Los clientes pueden aprovechar cuentas de usuario LDAP existentes, lo cual facilita la puesta en funcionamiento.
- Los usuarios finales disponen de una completa pista de auditoría al analizar la actividad del proveedor por necesidades de conformidad.

### Resumen

Leica Microsystems eligió Axeda ServiceLink para RemoteCare a fin de ofrecer el nivel más alto posible de seguridad. Empresas de todo el mundo proporcionan servicio remoto a sus clientes mediante Axeda ServiceLink. Esto es así gracias a que Axeda incorpora cuidadosamente principios y normas de seguridad en el diseño y funcionamiento de sus infraestructuras y servicios. Al igual que en Leica Microsystems, una prioridad principal en Axeda es la consecución de un nivel de seguridad estricto que permita a los clientes lograr sus objetivos de servicio remoto de forma segura y eficaz.