Artículo técnico

Servicios remotos InTouch℠

Seguridad de TI

La seguridad de TI representa una de las principales preocupaciones para METTLER TOLEDO y nuestros clientes que utilizan servicios remotos. METTLER TOLEDO ofrece una solución de servicios remotos contrastada que protege frente a los piratas informáticos y respalda nuestros productos inteligentes sin modificar la infraestructura de seguridad o TI de nuestros clientes. Además, es compatible con los modelos de seguridad de la red estándares.

Como los productos de METTLER TOLEDO están conectados a las redes de nuestros clientes, estos también deben recibir la garantía de que nuestra solución de servicios remotos respalda el modelo de seguridad del cliente, proporciona un control exhaustivo de los derechos de los usuarios y ofrece funciones de auditoría y seguimiento.

Nuestro compromiso:

- mantener y proteger la integridad del sistema;
- ocultar datos a partes no autorizadas;
- garantizar que los usuarios del sistema se autentican;
- limitar a cada usuario a datos, vistas y acciones específicos;
- ofrecer flexibilidad y control para aplicar las políticas empresariales;
- auditar y certificar los procesos y la solución tecnológica con regularidad y por parte de un tercero.

Contenido

1.	Seguridad de TI: servicios remotos
2.	Requisitos de METTLER TOLEDO para la seguridad de los servicios remotos
3.	Requisitos de los clientes para la seguridad de los servicios remotos
4.	Funcionamiento de los servicios remotos InTouch
5.	Visión general de la tecnología
6.	Mantenimiento de la integridad de la seguridad de la red
7.	Autenticación de usuarios, control del acceso y registro de auditorías
8.	Garantía de la confidencialidad de los datos
9.	Funciones de seguridad adicionales
10.	Resumen

METTLER TOLEDO

1 Seguridad de TI: servicios remotos

Los servicios remotos InTouch permiten establecer una conexión ininterrumpida entre los técnicos de asistencia remota de METTLER TOLEDO y nuestros productos inteligentes dentro del entorno de un cliente. Como estos productos suelen contener datos confidenciales de clientes y otros tipos de información privada y protegida, las capacidades de seguridad y conformidad figuran entre los requisitos más importantes a la hora de evaluar cualquier solución de servicios remotos. En este artículo se detallan los requisitos de seguridad de METTLER TOLEDO y los de nuestros clientes; además, se explica cómo los servicios remotos InTouch funcionan en su entorno y cómo cumplen sus requisitos técnicos de seguridad. También está orientado a abordar preguntas sobre temas clave, como la comunicación a través de cortafuegos y la seguridad de la red.

Nuestro compromiso

Para nuestros clientes, la seguridad y la privacidad son primordiales. Por lo tanto, METTLER TOLEDO tiene el compromiso de regirse por los siguientes principios de seguridad:

- mantener y proteger la integridad del sistema (la red, el equipo y los datos);
- ocultar datos a partes no autorizadas;
- garantizar que los usuarios del sistema se autentican;
- limitar a cada usuario a datos, vistas y acciones específicos;
- ofrecer flexibilidad y control para aplicar las políticas empresariales;
- auditar y certificar los procesos y la solución tecnológica con regularidad y por parte de un tercero.

2 Requisitos de METTLER TOLEDO para la seguridad de los servicios remotos

La solución de METTLER TOLEDO debe cumplir los requisitos de seguridad más estrictos, para que se puedan utilizar los servicios remotos con eficacia y a diario y los clientes tengan la tranquilidad de que sus conexiones son seguras y privadas.

Entre los requisitos de METTLER TOLEDO se incluyen:

Diseño contrastado en empresas

Conectar un ordenador a Internet genera inquietudes en materia de seguridad; por tanto, lo mismo ocurre cuando se conectan productos inteligentes. Un sistema de supervisión y asistencia remotas debe proteger frente a todas las amenazas para la seguridad de TI.

Compatibilidad con varios dispositivos

METTLER TOLEDO debe respaldar de forma segura una amplia variedad y un gran número de distintos tipos de productos y configuraciones complejas de los clientes sin requerir que estos últimos realicen cambios significativos en su infraestructura.

Implementación rápida

Para que los clientes adopten sistemas de servicios remotos, su modelo actual de seguridad de la red ya debe incluir capacidades de seguridad.

Validación por parte de una compañía de seguridad externa

Una certificación oficial expedida por una empresa de seguridad externa acreditada previa realización de una auditoría permite que METTLER TOLEDO tenga plena confianza en las capacidades de nuestro socio proveedor, la tecnología, y sus procesos y procedimientos.

3 Requisitos de los clientes para la seguridad de los servicios remotos

Los productos inteligentes se conectan a las redes de nuestros clientes. Cada cliente cuenta con sus propias políticas de seguridad y mecanismos de protección de la red consistentes en cortafuegos, servidores proxy y esquemas de direcciones. Un producto que se conecte a su red debe estar protegido tras esas capas de seguridad. Si una solución de servicios remoto requiere que se efectúen cambios en la protección de la red de los clientes, es probable que estos no la acepten. Por este motivo, es importante considerar los requisitos del cliente, incluidos:

Conservar el modelo actual de seguridad
Los productos inteligentes de METTLER TOLEDO respaldan el modo en el que el departamento de TI del cliente gestiona las operaciones, las políticas o los procedimientos de seguridad, y deben respetar los estándares aceptados de la industria.

Controlar el acceso de los usuarios
De conformidad con el modelo de seguridad del cliente, los servicios remotos InTouch deben dotar al cliente de un control exhaustivo y establecer políticas relativas a las acciones que se pueden efectuar en el dispositivo, como la recogida de datos y las actualizaciones del software, y cuándo se pueden realizar. Estas políticas pueden definirse de forma centralizada para todos los dispositivos conectados en las instalaciones del cliente.

Auditar las actividades y realizar un seguimiento de ellas
Con frecuencia, los requisitos de políticas y conformidad con normativas dictan que el sistema de servicios remotos debe facilitar el proceso de auditoría y seguimiento de todas las actividades administrativas y de los usuarios.

Garantizar la seguridad y la integridad de los datos
Los datos enviados del equipo conectado de METTLER TOLEDO al servidor de la empresa se protegen mediante el cifrado y la validación de certificados SSL/TLS. Solo se recogen los datos necesarios para supervisar el equipo de METTLER TOLEDO, diagnosticar sus problemas y solucionarlos. Es decir, en el conjunto de datos que se envía a la empresa no se incluyen datos confidenciales de los clientes.

Los servicios remotos InTouch confieren el rendimiento, la flexibilidad y la escalabilidad necesarios para satisfacer las necesidades de la mayor variedad de clientes de METTLER TOLEDO proporcionando el abanico más amplio de protecciones de datos y funciones de seguridad.

4 Funcionamiento de los servicios remotos InTouch

Los servicios remotos InTouch supervisan el estado, los parámetros de funcionamiento y la configuración de los equipos de METTLER TOLEDO presentes en sus instalaciones. Esto lo consigue mediante un agente de supervisión basado en software que se comunica de forma segura con el servidor alojado en la nube empresarial.

La aplicación de los servicios remotos InTouch, que se ejecuta en la nube, evalúa el rendimiento de su equipo a medida que se reciban datos y alarmas, y almacena dichos datos para efectuar análisis de tendencias. Si se detecta algún problema, el servidor alojado en la nube empresarial notifica al personal de mantenimiento pertinente. A continuación, el técnico de asistencia remota diagnostica el problema analizando los datos del servidor alojado en la nube empresarial (de forma remota y sin interrumpir las operaciones del cliente).

Si se deben efectuar más tareas de diagnóstico, dicho técnico puede, con su permiso, acceder de forma remota al equipo y trabajar en el sistema directamente.

Tras el diagnóstico, es posible solucionar el problema de inmediato, como en el caso de precisarse una actualización de software u otro ajuste de la configuración. Con su autorización, el técnico de asistencia remota puede resolverle muchos problemas a distancia.

Si se debe enviar un técnico de mantenimiento a sus instalaciones para corregir el problema, la información recogida a través de InTouch ayuda a garantizar que, cuando lleguen allí, lo hagan equipados con las piezas y los conocimientos necesarios para solucionar la situación.

5 Visión general de la tecnología

El sistema de servicios remotos InTouch consta de dos componentes esenciales: el software de agente de servicio remoto que se ejecuta en los equipos de METTLER TOLEDO de las instalaciones del cliente y el servidor alojado en la nube empresarial con las aplicaciones que permiten acceder a la información de dichos equipos.

El software de agente de servicio remoto que se ejecuta en las instalaciones del cliente supervisa los equipos de METTLER TOLEDO con regularidad y comprueba el estado de determinados datos esenciales que permiten hacernos una idea de la configuración y el estado del sistema. Además, el software de agente de servicio remoto se comunica periódicamente con el entorno del servidor de la nube empresarial para ofrecer actualizaciones sobre el estado y los datos del equipo.

Los servicios remotos InTouch aprovechan su infraestructura de seguridad y red actual. Siempre que el agente pueda establecer una conexión saliente con el servidor de la nube empresarial mediante el puerto 443, no se precisará ningún cambio para garantizar la conectividad remota.

El método de comunicación segura Firewall-Friendly™ no requiere que el equipo con el agente tenga una dirección TCP/IP fija o visible al público. Esto se debe a que METTLER TOLEDO nunca iniciará una conexión entrante con el agente que se ejecuta en el equipo de sus instalaciones. El agente inicia todas las comunicaciones con los servidores alojados en la nube empresarial y la comunicación bidireccional solo tendrá lugar después de que se haya iniciado y autenticado la conexión.

El agente supervisa un conjunto de parámetros específicos y solo envía los cambios que se produzcan los datos a los servidores de la nube empresarial. De esta forma, se minimiza el tráfico de su red que recibe METTLER TOLEDO.
Periódicamente, el agente también envía un pequeño mensaje a los servidores de la nube empresarial, una especie de "latido", para confirmar que dicho agente se encuentra activo. Estos mensajes permiten que el personal de asistencia de METTLER TOLEDO ponga en cola una solicitud de acción. Por ejemplo, el personal de asistencia podría solicitar un registro de errores o la autorización para iniciar una sesión remota. La próxima vez que el agente transmita dicha señal, se entregará la solicitud.

6 Mantenimiento de la integridad de la seguridad de la red

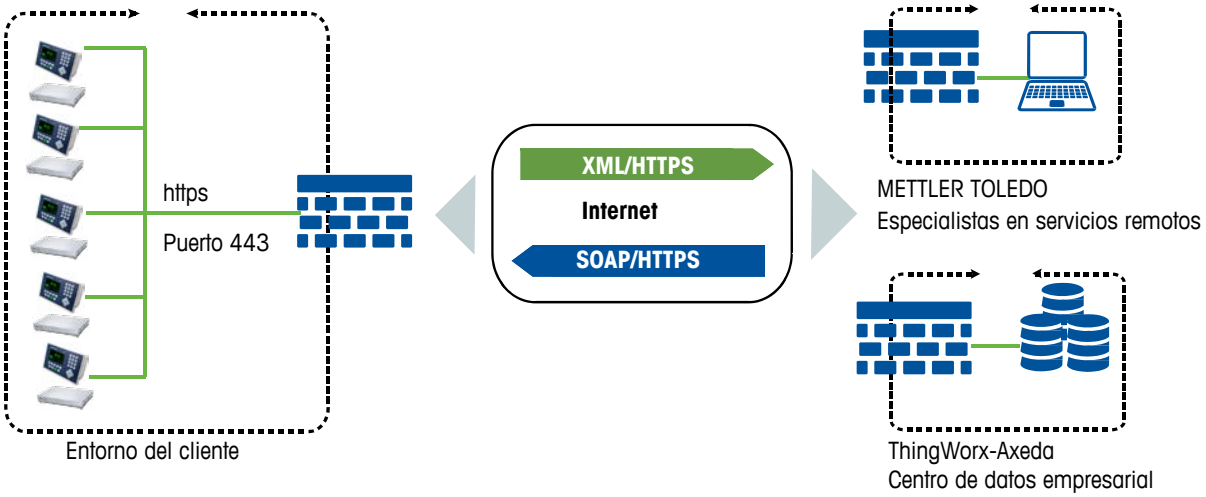
ThingWorx-Axeda implementa buenas prácticas del sector para cifrar su tráfico de mensajes. Además de admitir certificados SSL de autoridades de certificación reconocidas en todo el mundo, se utiliza el protocolo de seguridad de la capa de transporte (TLS) para dotar de seguridad a las comunicaciones. A continuación, se mejora la seguridad del contenido de los mensajes con el algoritmo Advanced Encryption Standard (AES) de 256 bits. Se utiliza el algoritmo RSA 2048 para intercambios de información clave.

La tecnología patentada Firewall-Friendly™ de ThingWorx-Axeda ofrece una comunicación bidireccional basada en estándares de servicios web, incluido el protocolo de transferencia de hipertexto (HTTPS), el protocolo simple de acceso a objetos (SOAP) y el lenguaje de marcado extensible (XML). No se precisa realizar ningún cambio en la infraestructura de seguridad de TI del cliente para integrar el equipo conectado.

El agente de servicio remoto incluido en los dispositivos de METTLER TOLEDO inicia todas las comunicaciones con el servidor alojado en la nube empresarial. Este agente de software inteligente permite que el dispositivo haga las veces de un cliente web e inicie la comunicación con el servidor empresarial con mensajes que se envían como comandos POST de HTTPS. Cada mensaje contiene datos codificados en formato XML que se envían a través del puerto 443 con un cifrado SSL. El agente de software solo puede acceder a servidores específicos identificados para los servicios remotos InTouch.

Puesto que es el dispositivo el que inicia todas las comunicaciones, no se necesita configurar o mantener redes VPN para implementar los servicios remotos InTouch ni poner en peligro la seguridad utilizando comunicaciones de acceso telefónico.
El dispositivo no cuenta con una dirección IP pública. Todos los dispositivos permanecerán ocultos de forma segura tras las infraestructuras de seguridad de TI del cliente, ya sean cortafuegos, routers y servidores proxy.

Básicamente, si un navegador web puede acceder a Internet con la infraestructura de red actual del cliente, el dispositivo equipado con los servicios remotos InTouch podrá comunicarse con el servidor empresarial a través de la misma conexión de red. Por lo tanto, no se precisa realizar ningún cambio en la infraestructura de seguridad de TI.



7 Autenticación de usuarios, control del acceso y registro de auditorías

Autenticación de usuarios

El acceso a las aplicaciones de los servicios remotos InTouch está limitado exclusivamente a personal de asistencia y mantenimiento altamente cualificado de METTLER TOLEDO, para que puedan desempeñar sus trabajos con eficacia a la vez que se protege el acceso a la información confidencial.

El servidor alojado en la nube empresarial requiere que cada usuario tenga un ID único, compuesto por un nombre de usuario y una contraseña, para acceder al sistema. Se exigen contraseñas seguras y cada usuario debe cambiar la suya cada 90 días.

Los datos se encuentran en riesgo siempre que se deja un ordenador encendido y sin supervisión con una aplicación abierta. Para evitar que se produzca esta situación, el sistema cierra automáticamente la sesión de los usuarios inactivos tras 20 minutos para impedir que alguien lo utilice sin autorización.

Control del acceso de los usuarios

Se controla el acceso de los usuarios por medio de una serie de mecanismos que rigen el acceso en función de las actividades y los dispositivos. Estos métodos se combinan de numerosas formas para permitir que los usuarios puedan desempeñar sus trabajos con eficacia y, a la vez, proteger el acceso a la información confidencial.

El control de acceso basado en las actividades permite que el administrador del sistema asigne y clasifique usuarios en las aplicaciones de los servicios remotos InTouch, así como que defina las actividades que se pueden desempeñar. Cada grupo de usuarios recibe un acceso controlado a las aplicaciones de los servicios remotos InTouch según su cargo y nivel de experiencia con los productos de METTLER TOLEDO.

Por su parte, el control de acceso basado en los dispositivos proporciona un método para definir los dispositivos concretos a los que puede acceder cada grupo de usuarios. Este método de control limita la visualización de información del dispositivo a solo el equipo del que sea responsable un usuario.

Registro de auditorías
Además, el sistema empresarial crea un Audit Trail completo, que documenta cada actividad y evento que se produzca en los dispositivos inteligentes o estén derivados de los usuarios de asistencia remota. El registro de auditorías contiene información sobre las interacciones de los usuarios dentro del sistema y con las máquinas. Estos datos se guardan en el servidor alojado en la nube empresarial y no se pueden eliminar del sistema. Los usuarios de los servicios remotos InTouch solo pueden ver el registro de auditorías de los productos de METTLER TOLEDO a los que se les haya concedido acceso. Si se elimina un usuario o producto del sistema, se seguirán conservando los datos sobre el usuario o producto en el registro de auditorías. Por lo tanto, el sistema lleva un registro de quién hizo qué, cuándo y en qué dispositivos.

8 Garantía de la confidencialidad de los datos

La tecnología utilizada para prestar los servicios remotos InTouch emplea el protocolo de capa de sockets seguros y seguridad de la capa de transporte (SSL/TLS) para garantizar la transmisión segura de los datos. SSL/TLS constituye un protocolo para transmitir datos privados mediante Internet. Además de cifrar datos, el estándar SSL ofrece funciones de autenticación para garantizar que tanto el remitente como el destinatario de los datos se conocen. SSL admite las claves de 2048 bits de longitud y la autenticación mutua mediante certificados. SSL es el mismo estándar de cifrado que utilizan los bancos para las transacciones on-line.

El agente de servicios remotos InTouch incorporado en los productos inteligentes de METTLER TOLEDO supervisa y analiza únicamente datos específicos que sean pertinentes al funcionamiento y rendimiento del producto. Es decir, no se incluyen datos confidenciales de los clientes en el conjunto de datos, el cual se supervisa con frecuencia para determinar el rendimiento del producto. La empresa solo recoge y analiza los datos necesarios para supervisar el producto específico, diagnosticar sus problemas y solucionarlos.

Protección de los datos y declaración de uso
Los datos que recoge METTLER TOLEDO a través de los servicios remotos InTouch están estrictamente controlados y solo puede acceder a ellos personal autorizado. Estos datos, que se recogen a través de los servicios remotos InTouch y se establecen según el tipo de modelo, contienen únicamente los parámetros del dispositivo necesarios para diagnosticar los problemas del equipo y corregirlos. METTLER TOLEDO no transferirá, venderá ni revelará a terceros ningún dato o información recogidos a través de los servicios remotos InTouch en ninguna circunstancia.

9 Funciones de seguridad adicionales

ISO/IEC 27001:2013

ThingWorx-Axeda incorpora una estrategia de seguridad integral que abarca todos los aspectos, incluidos la red, las aplicaciones, los usuarios y los datos. ThingWorx-Axeda ha logrado una certificación ISO 27001:2013, que respalda la prioridad de la empresa de ofrecer el mayor nivel de seguridad, rendimiento y disponibilidad posible con el servicio ThingWorx-Axeda M2M Cloud Service.

ThingWorx-Axeda M2M Cloud Service está diseñado para solucionar problemas de seguridad de la información esenciales con funciones que:

- **Mantener la seguridad de la red en las instalaciones del cliente:** mediante la tecnología de comunicación patentada Firewall-Friendly de ThingWorx-Axeda, la solución de ThingWorx-Axeda aprovecha la infraestructura de seguridad existente de sus clientes.
- **Ocultar datos a partes no autorizadas:** se protegen todas las comunicaciones entre su empresa y sus clientes con el cifrado SSL, el mismo método que utilizan los bancos para garantizar la seguridad de las transacciones on-line.
- **Proporcionar una infraestructura segura y escalable a petición:** los centros de datos certificados según la norma ISO 27001:2013 de ThingWorx-Axeda se someten a un examen SAS 70 anual y están construidos con equipo de última generación, inversiones en tecnología y experiencia operativa. Estos centros de datos incorporan subsistemas, fuentes de alimentación, aire acondicionado y cableado de red redundantes. De esta forma, se consigue una disponibilidad superior al 99,95 %.
- **Garantizar que los usuarios del sistema se autentican:** todo el acceso al sistema se controla de forma centralizada y requiere una autenticación mediante contraseña. Se registran todas las acciones de los usuarios para garantizar la trazabilidad.
- **Limitar a cada usuario a datos, vistas y acciones específicas:** una vez que se haya autenticado, las acciones del usuario están limitadas a los productos de los que sean responsables y al nivel de acceso adecuado para sus roles.

Implementaciones probadas

Los servicios remotos InTouch utilizan la misma tecnología que usan fabricantes en todo el mundo en una amplia gama de entornos, incluidos los desarrollados para aplicaciones de seguridad nacional, médicas, ciencias de la vida, tecnología de la información, telecomunicaciones, imagen e impresión, quioscos, semiconductores, industriales, y automatización de edificios. ThingWorx-Axeda proporciona a esos fabricantes y a sus clientes el mismo alto nivel de seguridad y protección de los datos que esperan nuestros propios clientes.

ThingWorx-Axeda también es un importante proveedor de soluciones de servicios remotos para muchas empresas de almacenamiento de red y hardware de infraestructura de TI. Por lo tanto, si su departamento de TI utiliza soluciones de estas compañías, es posible que ya esté familiarizado con la tecnología de ThingWorx-Axeda, ya que dichas empresas utilizan la misma tecnología de ThingWorx-Axeda que utiliza METT-

10 Resumen

METTLER TOLEDO ha elegido a ThingWorx-ThingWorx-Axeda como nuestro proveedor de infraestructura de servicios remotos para permitir que los servicios remotos InTouch ofrezcan a los clientes el mayor grado de seguridad sin modificar su infraestructura de seguridad de TI actual. Empresas de todo el mundo prestan servicios remotos a sus clientes utilizando la tecnología de ThingWorx-Axeda. Este es el resultado de una incorporación minuciosa de principios y estándares de seguridad en el diseño y el funcionamiento de la infraestructura y los servicios que ofrece ThingWorx-Axeda.

Para METTLER TOLEDO, proporcionar una seguridad de TI estricta constituye una importante prioridad, de forma que nuestros clientes puedan tener la tranquilidad de que les prestamos los servicios remotos InTouch de manera segura y eficaz. En última instancia, esto permite que los clientes disfruten de una mayor disponibilidad de los productos y un mejor rendimiento de los equipos; además, podrán obtener unos resultados de la mayor calidad gracias a sus productos de METTLER TOLEDO.

www.mt.com/service

Para más información

Mettler-Toledo GmbH
Industrial
CH 8606 Greifensee
Suiza
Teléfono: +41-44-944 22 11
Fax: +41-44-944 30 60

MTSI 30259896