White Paper

InTouch℠ Remote Services

IT Security

IT security is a primary concern for METTLER TOLEDO and our customers that employ remote services. METTLER TOLEDO offers a proven remote service solution that protects against hackers and supports METTLER TOLEDO intelligent products without changes to our customer's IT or security infrastructures while working within standard network security models.

Because METTLER TOLEDO products are connected within our customer's networks, they also need to be assured that the remote service solution supports our customer's security model, provides granular control over user rights and offers auditing and tracking capabilities.

Our commitment:

- Maintain and protect the integrity of the system
- Conceal data from unauthorized parties
- Ensure system users are authenticated
- Limit each user to specific data, views & actions
- Provide flexibility and control to enforce business policies
- Audit and certify the processes and technology solution regularly by a third party

Contents

METTLER TOLEDO

1 IT Security – Remote Services

InTouch Remote Services provide a seamless connection between METTLER TOLEDO remote support technicians and METTLER TOLEDO intelligent products within a customer's environment. Because these products often contain sensitive customer data and other types of private and protected information, security and compliance capabilities are among the most important requirements evaluated in any remote service solution. This paper details the security requirements of METTLER TOLEDO and those of our customers, and explains how InTouch Remote Services operates within your environment and how it meets your technical security requirements. It is also intended to address questions about key issues such as communication through firewalls and network security.

Our Commitment

Privacy and security are of the utmost importance to our customers. Therefore, METTLER TOLEDO is committed to the following security principles:

- Maintain and protect the integrity of the system – network, equipment and data
- Conceal data from unauthorized parties
- Ensure system users are authenticated
- Limit each user to specific data, views and actions
- Provide flexibility and control to enforce business policies
- Audit and certify the processes and technology solution regularly by a third party

2 Mettler Tolodo's Requirements for Remote Service Security

METTLER TOLEDO's solution needs to meet the most stringent security requirements so that remote services can be used effectively and routinely, leaving customers feeling confident that their connections are secure and private.

METTLER TOLEDO requirements include:

Enterprise proven design

Connecting a computer to the Internet raises security concerns; therefore, connecting intelligent products is no different. A remote support and monitoring system must safeguard against all IT security threats.

Support for multiple devices

METTLER TOLEDO needs to securely support a wide variety and large number of different product types and complex customer configurations without requiring significant changes for our customers.

Rapid deployment

For customers to adopt remote service systems, the security capabilities must already exist within the customer's current network security model.

Third-party security firm validation

Official certification by an accredited third-party security audit provides METTLER TOLEDO with the confidence in the capabilities of our vendor partner, the technology and their process and procedures.

3 Customers' Requirements for Remote Service Security

Intelligent products are connected to customers' networks. Each customer has their own security policies and network protection in the form of firewalls, proxy servers, and addressing schemes. A product connected to their network must be protected behind those layers of security. If a remote service offering requires changes to a customer's network protection, it will likely fail to gain acceptance. Because of that, it is important to consider the requirements of the customer, including:

Maintain current security model
METTLER TOLEDO intelligent products support the way the customer's IT organization manages security operations, policies, or procedures and should adhere to accepted industry standards.

Control user access
In compliance with the customer's security model, InTouch Remote Services must provide the customer with granular control and set policies the actions that can be performed on the device, such as data collection and software updates, and when they can be performed. These policies can be centrally defined for all connected devices at the customer's location.

Audit and track activity
Policy and regulatory compliance requirements often dictate that the remote service system must make auditing and tracking all user and administration activity easy.

Data integrity and security
Data sent from the connected METTLER TOLEDO equipment to the enterprise server is protected through data encryption and SSL/TLS certificate validation. Only the data necessary to monitor, diagnose and troubleshoot the METTLER TOLEDO equipment is collected. There is no sensitive customer data collected in the data set delivered to the enterprise.

InTouch Remote Services delivers the performance, flexibility and scalability required to meet the needs of the broadest range of METTLER TOLEDO customers by providing the widest range of data protection safeguards and security features.

4 How Does InTouch Remote Services Work?

InTouch Remote Services monitors the status, operating parameters and configuration of the METTLER TOLEDO equipment in your facility. It does this through a software-based monitoring Agent that communicates securely with the hosted Cloud Enterprise server.

The InTouch Remote Services application running in the cloud evaluates the performance of your equipment as data and alarms are received, storing the data for trend analysis. If a problem is detected, the hosted Cloud Enterprise server notifies appropriate service personnel. The remote support technician then diagnoses the issue by analyzing data on the hosted Cloud Enterprise server — remotely and without interruption to your operation.

If further diagnosis is required, the remote support technician can, with your permission, remotely access the equipment and work on the system directly.

Once diagnosed, the problem may then be corrected immediately, as in the case of a necessary software update or other configuration adjustment. With your authorization, the remote service technician can resolve many issues for you remotely.

If a service technician needs to be sent to your facility to repair the problem, the information collected through InTouch helps ensure that they arrive on site with the necessary parts and knowledge to resolve the issue.

5 Technology Overview

The InTouch Remote Services system is composed of two major components: the Remote Services Agent software running on the METTLER TOLEDO equipment at the customer site and the hosted Cloud Enterprise server with the applications that provide access to the equipment information.

The Remote Service Agent software at the customer site monitors the METTLER TOLEDO equipment on a regular basis, checking the status of key data elements that provide a picture of system health and configuration. Additionally, the Remote Services Agent periodically communicates with the Cloud Enterprise server environment to provide updates on equipment data and status.

InTouch Remote Services leverages your existing network and security infrastructure. As long as the Agent can open an outbound connection to the Cloud Enterprise server using port 443, no changes are required to establish remote connectivity.

The secure Firewall-Friendly™ communication method does not require the Agent computer to have a fixed or publicly visible TCP/IP address. That is because METTLER TOLEDO will never initiate an inbound connection to the Agent at your site. The Agent initiates all communications with the hosted Cloud Enterprise servers and two-way communication will only occur after the connection has been initiated and authenticated.

The agent monitors a specific set of parameters and sends only data changes to the Cloud Enterprise servers. This minimizes the traffic to METTLER TOLEDO on your network.
Periodically, the agent also sends a small message to the Cloud Enterprise servers as a form of "heartbeat" to confirm the agent is active. These messages enable METTLER TOLEDO support personnel to queue an action request. For example, support staff could request an error log or initiate a remote session. The next time the agent "checks in," the request is delivered.

6 Maintaining Network Security Integrity

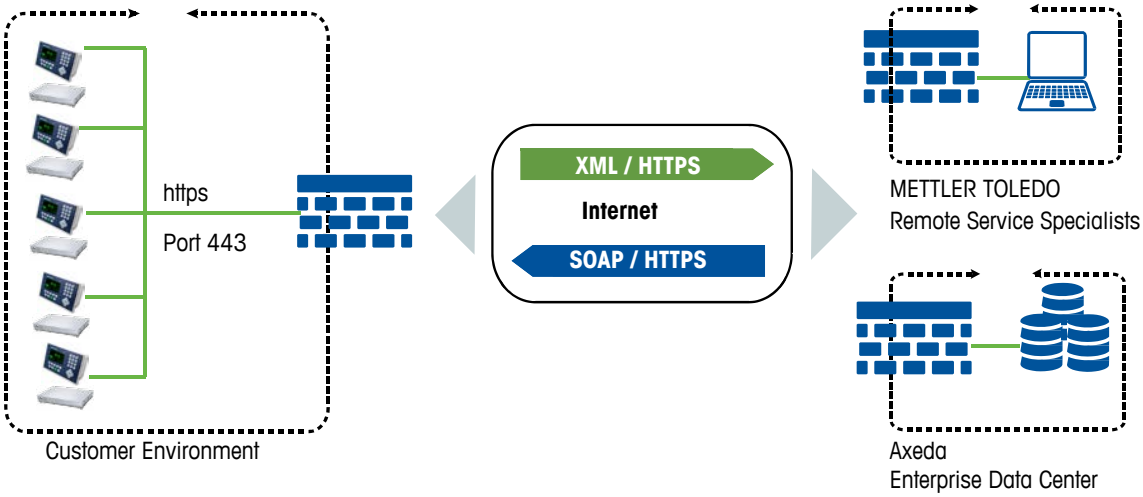
Axeda implements industry best practices for encrypting its message traffic. In addition to providing support for SSL certificates from globally recognized certificate authorities, Transport Layer Security (TLS) is used to provide security at the communications level. The content of the messages is then further secured using the Advanced Encryption Standard (AES) 256 algorithm. The RSA 2048 algorithm is used for key exchanges.

Axeda's patented Firewall-Friendly™ technology provides two-way communication based on Web services standards, including Hypertext Transfer Protocol (HTTPS), Simple Object Access Protocol (SOAP), and Extensible Markup Language (XML). No changes to the customer's IT security infrastructure are required to support their connected equipment.

The Remote Services Agent on the METTLER TOLEDO devices initiates all communication with the hosted Cloud Enterprise server. This intelligent agent software enables the device to act as a web client, and initiates messages to the enterprise server that are sent as HTTPS POST commands. Each message contains data encoded in XML format sent using SSL encryption across port 443. The software agent only can access the specific servers identified for InTouch Remote Services.

Because the device initiates all communications, there is also no need to set up and maintain VPNs to implement InTouch Remote Services or to compromise security by using dial-up communications.
The device does not have a public IP address. All devices remain securely hidden behind the customer's IT security infrastructures of firewalls, routers, and proxy servers.

Essentially, if a Web browser can access the Internet using the customer's current network infrastructure, the device enabled with InTouch Remote Services can communicate with the enterprise server using that same network connection. Therefore, no changes are required to the IT security infrastructure.



7 User Authentication, Access Control, & Audit Logging

User Authentication

Access to InTouch Remote Services' applications is limited exclusively to highly trained METTLER TOLEDO service and support staff so they may do their jobs effectively while protecting access to sensitive information.

The hosted Cloud Enterprise server requires each user to have a unique user name ID and password to access the system. Strong passwords are required and each user must change their password every 90 days.

Data is at risk whenever a computer is left on and unattended with an application open. To prevent that situation, the system automatically logs off inactive users after 20 minutes to prevent unauthorized use.

User Access Control

User access control is addressed through activity-based and device-based access control. Those methods are combined in a wide variety of ways to allow users to do their jobs effectively while protecting access to sensitive information.

Activity-based access control enables the system administrator to assign and classify users in InTouch Remote Services applications, and to define the activities that can be performed. Each user group is given controlled access to the InTouch Remote Services applications based on their job role and experience level with METTLER TOLEDO products.

Device-based access control provides a method for defining the specific devices accessible to each user group. This method of control limits the view of device information to only those devices for which a user is responsible.

Audit Logging
Furthermore, the enterprise system creates a full audit trail, which documents every activity and event from both the intelligent devices and the remote support users. The audit log contains information about user interactions within the system and with machines. The audit log data is kept on the hosted Cloud Enterprise server and cannot be removed from the system. InTouch Remote Services users can only see the audit log for the METTLER TOLEDO products they are permitted to access. If a user or product is removed from the system, all data about the user or product will continue to be kept in the audit log. Therefore, the system maintains records of who did what, when, and against which devices.

8 Ensuring Data Confidentiality

The technology utilized to provide InTouch Remote Services uses Secure Sockets Layer/Transport Layer Security Protocol (SSL/TLS) to provide secure transmission of data. SSL/TLS provides a protocol for transmitting private data via the Internet. In addition to encrypting data, the SSL standard also provides authentication to ensure that both the sender and receiver of data are known to each other. SSL supports 2048 bit key length and mutual authentication using certificates. SSL is the same encryption standard used by banks for online transactions.

The InTouch Remote Service agent embedded into METTLER TOLEDO intelligent products, monitors and analyses only specific data items that are pertinent to operation and performance of the product. Customer sensitive data is not included in the data set, which is routinely monitored for product performance. Only the data needed to monitor, diagnose, and troubleshoot the specific product is collected and analyzed at the enterprise.

Data Protection and Usage Statement
Data collected by METTER TOLEDO though the use of InTouch Remote Services is strictly controlled and accessible only to authorized personnel. The data items which are collected through the use of InTouch Remote Services and defined by model type contain only device parameters required to diagnose and repair equipment problems. Under no circumstances will METTLER-TOLEDO transfer, sell or disclose any data or information collected through the use of InTouch Remote Services to third parties.

9 Additional Security Features

ISO/IEC 27001:2013

Axeda incorporates an end-to-end security strategy covering all levels, including network, application, user and data security. Axeda has attained ISO 27001:2013 certification, supporting the company's focus on delivering the highest levels of security, performance and availability of the Axeda M2M Cloud Service.

The Axeda M2M Cloud Service is designed to address key information security concerns with features that:

- **Maintain network security at customer sites** – Utilizing Axeda's patented Firewall-Friendly communication, the Axeda solution leverages your customers' existing security infrastructure.
- **Conceal data from unauthorized parties** – All communication between you and your customers is kept secure using SSL encryption, the same method banks use for secure online transactions.
- **Provide a secure and scalable on-demand infrastructure** – Axeda's ISO 27001:2013-certified data centers undergo an annual SAS 70 examination and are built on state-of-the-art equipment, technology investments, and operational expertise. The data centers include redundant subsystems, energy supply, air conditioning and network cabling. This provides for greater than 99.95% availability.
- **Ensure that system users are authenticated** – All access to the system is centrally controlled, requiring password authentication. All user actions are fully audited for traceability.
- **Limit each user to specific data, views, and actions** – Once authenticated, the user's actions are limited to the products for which they are responsible and the level of access appropriate to their roles.

Proven Deployments

InTouch Remote Services utilize the same technology that is currently deployed around the world by manufacturers in a wide range of environments, including those developed for applications in homeland security, medical, life sciences, information technology, telecommunications, print and imaging, kiosks, semiconductor, industrial and building automation. Axeda supplies those manufacturers and their customers the same high level of security and data protection as expected by our customers.

Axeda is also a major supplier of Remote Service solutions to many key supplies of network storage and IT infrastructure hardware. Therefore your IT department utilizes solutions from those companies, then you might already be familiar with Axeda's technology, as these companies employ the same technology from Axeda that METTLER TOLEDO uses.

10 Summary

METTLER TOLEDO has chosen Axeda as our remote service infrastructure provider to enable InTouch Remote Services to provide customers with the highest level of security without changing their current IT security infrastructure. Companies throughout the world are providing remote services to their customers using Axeda. This is a result of careful incorporation of security principles and standards in the design and operation of the infrastructure and services Axeda provides.

A top priority for METTLER TOLEDO is stringent IT security, providing our customers with the confidence we can deliver InTouch Remote Services securely and efficiently. This ultimately provides customers with higher product availability, improved product performance, and it allows them to deliver the highest quality output from their METTLER TOLEDO products.

www.mt.com/service

For more information

Mettler-Toledo AG
Industrial
CH 8606 Greifensee
Switzerland
Phone +41-44-944 22 11
Fax +41-44-944 30 60

MTSI 30254015