白皮书

InTouch[SM] 远程服务

IT 安全性问题

IT 安全性问题是梅特勒-托利多和客户使用远程服务时的主要关注点。梅特勒-托利多提供经过验证的远程服务解决方案，预防黑客攻击，并在标准的网络安全模式下，无需更改客户的 IT 安全基础设施就能支持梅特勒-托利多的智能产品。

由于梅特勒-托利多的产品连接在客户的网络中，因此还需确保远程服务解决方案支持客户的安全模式，对用户权限进行细化控制，并提供审核和可追溯功能。

我们的承诺：

- 维护和保护系统的完整性
- 对未经授权方屏蔽数据
- 确保系统用户经过身份验证
- 限制每名用户特定的数据、视图和运行
- 提供执行业务策略的灵活性与管控
- 审核和对过程及技术认证的解决方案由专业第三方提供

目录

1. IT 安全性问题 — 远程服务
2. 梅特勒-托利多对远程服务安全性的要求
3. 客户对远程服务安全性的要求
4. InTouch 远程服务如何工作?
5. 技术概览
6. 确保数据的机密性
7. 用户验证、访问控制和审核记录
8. 确保数据机密
9. 附加安全功能
10. 综述

METTLER TOLEDO

1 IT 安全性问题 — 远程服务

InTouch 远程服务提供梅特勒-托利多远程支持技术人员和客户环境中梅特勒-托利多智能产品之间的无缝连接。由于这些产品通常包含敏感的客户数据和其他受保护的内部信息，因此安全性与合规性是评估任何远程服务解决方案中最重要的要求。本白皮书详细描述了梅特勒-托利多和客户的安全要求，并解释了 InTouch 远程服务如何在您的网络环境中运行，以及如何满足您的技术安全要求。它还旨在解决通过防火墙和网络安全策略进行通信等关键问题。

我们的承诺

隐私和安全对于我们的客户而言至关重要。因此，梅特勒-托利多致力于以下安全原理：

- 维持和保护系统的完整性 — 网络、设备和数据
- 对未经授权方屏蔽数据
- 确保系统用户身份验证
- 限制每名用户特定的数据、视图和运行
- 提供执行业务策略的灵活性和与管控
- 审核和对过程及技术认证的解决方案由专业第三方提供

2 梅特勒-托利多的远程服务安全要求

梅特勒-托利多的解决方案需要满足最严苛的安全要求，以便高效地定期使用远程服务，让客户对其连接安全性信心十足。

梅特勒-托利多的要求包括：

经过企业验证的设计

将计算机连接至网络增加了安全担忧；连接智能产品也不例外。远程支持和监控系统必需保护不受任何网络安全威胁。

支持多台设备

梅特勒-托利多需要安全地支持大量不同类型的产品和复杂的客户配置，而无需客户进行大幅更改。

快速部署

客户要采用远程服务系统，安全功能必需已经在客户当前的网络安全模式中存在。

第三方安全公司验证

由授权第三方提供的安全审核官方认证，让梅特勒-托利多对供应商合作伙伴的能力、技术及其流程充满信心。

3 客户对远程服务安全的要求

智能产品连接至客户网络。每位客户都有自己的安全策略和网络保护，采用防火墙、代理服务器和寻址方案。连接至网络的产品必需受到这些安全保护。如果提供的远程服务需要更改至客户的网络保护，则可能无法被接受。正因如此，必须认真考虑客户要求，这包括：

保持当前的安全模式
梅特勒-托利多智能产品支持客户的 IT 部门管理安全运营方式、策略或流程，并应当遵守被认可的行业标准。

控制用户权限
根据客户的安全模式，InTouch 远程服务必须为客户提供细化控制，并设定可以在设备上执行操作的策略，如数据采集和软件更新等。可以为客户现场的所有连接设备集中定义这些策略。

审核和追溯活动
策略和符合法规要求通常指出远程服务系统必须能够轻松地审核和追溯所有的用户和管理活动。

数据集成与安全
从所连接的梅特勒-托利多设备发送至企业服务器的数据通过数据加密和 SSL/TLS 证书验证得到保护。仅收集有关监控、诊断和识别梅特勒-托利多设备的数据。在提交公司的数据集中没有客户敏感数据。

InTouch 远程服务凭借其卓越的性能、灵活性和可扩展性，提供最全面的数据保护措施和安全功能，从而满足梅特勒-托利多客户最广泛的需求。

4 InTouch 远程服务如何工作?

InTouch 远程服务能够监测在现场安装的梅特勒-托利多设备的状态、运行参数和配置。它通过一种基于软件的监控代理来实现这一功能，该代理能与托管的云企业服务器安全通信。

在云中运行的 InTouch 远程服务应用程序在收到数据和警报后，对设备的性能进行评估，并存储数据以便进行趋势分析。如果检测到问题，则云企业服务器会通知适当的服务人员。然后，远程支持技术人员会通过分析服务器数据远程诊断问题，而不会中断您的运营。

如需进一步诊断，则远程支持技术人员在获得您的许可后，远程访问设备，并直接在系统上工作。

诊断后即可立即纠正问题，例如进行必要的软件更新或其他配置调节等。经过您授权，远程服务技术人员可远程解决许多问题。

如果需要派服务人员至现场维修，通过 InTouch 收集的信息有助于确保他们在抵达现场前就准备好必要的资料和备件，从而解决问题。

5 技术概览

InTouch 远程服务系统包含两个主要组件: 在客户现场安装在梅特勒-托利多设备上运行的远程服务软件; 安装了提供访问设备信息的应用程序的托管云企业服务器。

客户现场的远程服务软件定期监控梅特勒-托利多设备，检查关键参数状态，提供系统状况和配置状况。此外，远程服务软件定期与云企业服务器通信，以提供最新的设备数据和状态信息。

InTouch 远程服务利用您现有的网络和安全基础设施。只要代理软件能够使用端口 443 打开云企业服务器的连接，无需更改即可建立远程连接。

安全 Firewall-Friendly™ 通信方法无需代理计算机，即可获得公开可见的固定 TCP/IP 地址。这是因为梅特勒-托利多绝不会在您的场所直接发起与代理的入站连接。代理软件利用托管的云企业服务器发起所有的通信，只有在发起和认证连接后，才会发生双向通信。

该代理软件监控特定参数集，并且仅将数据变化发送至云企业服务器。这可最大限度地减少数据流量。代理还会以“心跳”方式定期将小消息发送至云企业服务器，以确定代理激活。这些消息可使梅特勒-托利多支持人员分析请求信息。例如，支持人员会请求读取一个错误日志或者发起远程会话。代理软件“进入”后会提供请求的数据。

6 保持网络安全完整性

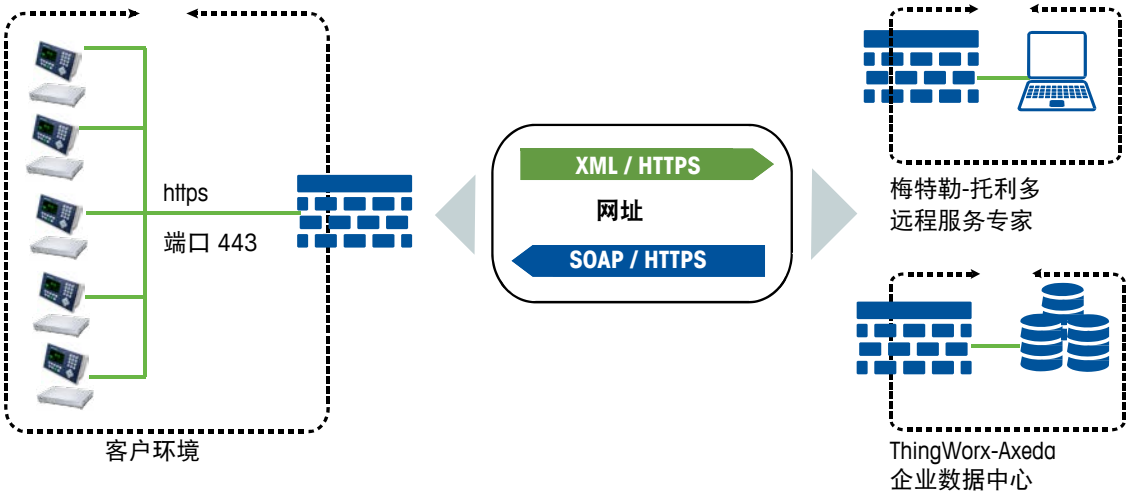
ThingWorx-Axeda 提供了加密信息交换的行业最佳实践。除了为全球公认的认证机构颁发 SSL 证书提供支持外，传输层安全 (TLS) 还用于提供通信级安全。使用高级加密的标准 (AES) 256 算法进一步确保信息安全。RSA 2048 算法用于密钥交换。

ThingWorx-Axeda 获得专利的 Firewall-Friendly™ 技术基于网络服务标准提供双向通信，包括超文本传输协议 (HTTPS)、简单对象存储协议 (SOAP) 和可扩展标记语言 (XML)。无需对客户的 IT 安全基础设施进行更改，以支持其连接的设备。

梅特勒-托利多设备上的远程服务代理软件通过托管的云企业服务器发起所有通信。该智能代理软件可使设备作为网络客户端，发起消息并作为 HTTPS POST 指令发送至企业服务器。每个消息均包含通过端口 443 使用 SSL 编码以 XML 格式进行编码的数据。代理软件仅可访问识别用于 InTouch 远程服务的特定服务器。

由于设备发起所有的通信，因此无需设置和保持 VPN 以实施 InTouch 远程服务，否则使用拨号通信会影响安全性。
该设备无公共 IP 地址。所有的设备都安全地隐藏在客户的防火墙、路由器和代理服务器 IT 安全基础设施后。

从本质上讲，如果网络浏览器能够使用客户当前的网络基础设施访问网络，那么通过 InTouch 远程服务启用的设备也能够使用相同的网络连接与企业服务器通信。因此，IT 安全基础设施无需更改。



7 用户验证、访问控制和审核记录

用户身份验证

访问 InTouch 远程服务的应用只能由梅特勒-托利多训练有素的服务和支持人员操作，以便高效完成任务，并保护敏感信息的访问。

托管的云企业服务器需要每位用户有独特的用户名 ID 和密码以访问系统。需要很强的安全级别密码，每位用户必须每 90 天更改一次密码。

当电脑开启、应用打开却无人值守时，数据会面临风险。为防止这种情况，系统在 20 分钟后自动退出未激活用户，以防止未经授权使用。

用户访问控制

通过基于活动和设备访问的控制解决用户访问控制问题。这些方法以各种方式组合，以便让用户高效地工作，并保护对敏感信息的访问。

基于活动的访问控制可使系统管理员在 InTouch 远程服务应用中进行用户分配和分类，以定义可以执行的活动。每个用户组基于自己的职业角色和梅特勒-托利多产品经验，均享有 InTouch 远程服务应用控制访问权限。

基于设备的访问控制提供定义可访问每个用户组的特定设备。此控制方法将设备信息仅限于那些用户负责的设备。

审核记录

并且企业系统创建全面的审核追溯，记录智能设备和远程支持用户的每个活动和事件。审核记录包含关于系统内用户互动以及与机器互动的信息。审核记录数据保存在托管的云企业服务器，无法从系统删除。InTouch 远程服务用户只能查看授权访问的梅特勒-托利多产品的审核记录。如果用户或产品从系统移除，那么关于用户或产品的所有数据都会继续在审核记录中保留。因此，系统保留全部维护日志。

8 确保数据机密

提供 InTouch 远程服务所用的技术使用安全套接层/传输层安全协议 (SSL/TLS) 提供安全的数据传输。SSL/TLS 通过互联网提供传输隐私数据的协议。除了加密数据外，SSL 标准还提供身份验证，以确保彼此知道数据发送者和接受者。SSL 使用证书支持 2048 位密码长度和交互认证。SSL 是银行进行在线交易时使用的相同加密标准。

内置于梅特勒-托利多智能产品的 InTouch 远程服务代理软件仅监控和分析纳入产品运行和性能的特定数据项。数据集中不包含客户的敏感数据公司仅收集和分析为监控、诊断相关称重设备所需要的数据。

数据保护和使用声明

梅特勒-托利多通过使用 InTouch 远程服务收集的数据受到严格控制，并且只能由授权用户访问。通过使用 InTouch 远程服务收集、并且由型号类型定义的数据项仅包含诊断和修复设备问题需要的设备参数。梅特勒-托利多在任何情况下都不会通过使用 InTouch 远程服务，将收集到的任何数据或信息传输、销售或揭示给外部的第三方。

9 附加安全功能

ISO/IEC 27001:2013

ThingWorx-Axeda 结合涵盖网络、应用、用户和数据安全所有级别的端到端安全策略。ThingWorx-Axeda 已经获得 ISO 27001:2013 认证，支持梅特勒-托利多提供最高级别的 ThingWorx-Axeda M2M 云服务性能。

ThingWorx-Axeda M2M 云服务设计用于解决关键信息安全担心，功能如下：

- **在客户场所保持网络安全性** — 使用 ThingWorx-Axeda 获得专利的防火墙友好的通信，ThingWorx-Axeda 解决方案利用您的客户现有的安全基础设施。
- **隐藏未经授权的数据** — 利用 SSL 加密让您和您的客户之间的所有通信保持安全，利用相同的方法库实现安全的在线交易。
- **提供安全、可扩展的按需基础设施** — ThingWorx-Axeda 经过 ISO 27001:2013 认证的数据中心进行年度 SAS 70 检查，构建与最先进的设备、技术投资和运营经验之上。数据中心包括冗余子系统、能源供应、空调和网络电缆。大于 99.95% 的有效性。
- **确保系统用户经过身份验证** — 所有系统访问均受到集中控制，需要密码验证。所有的用户操作都经过完全审核用于可追溯性。
- **限制针对每名用户的具体数据、视图和运行** — 经过身份验证后，用户的操作限制为所负责的产品及其角色适当的访问级别。

经过验证的应用

目前世界各地的制造商在各种环境中应用的 InTouch 远程服务使用相同的技术，包括开发用于国土安全、医药、生命科学、信息技术、通信、打印和成像、终端机亭、半导体、工业和建筑自动化。ThingWorx-Axeda 按客户预期为制造商和客户提供相同的安全级别和数据保护。

ThingWorx-Axeda 也是许多关键网络存储和 IT 基础设施硬件的主要远程服务解决方案供应商。因此，您的 IT 部门使用这些公司的解决方案，您可能已经熟悉 ThingWorx-Axeda 技术，因为这些公司与梅特勒-托利多使用相同的 ThingWorx-Axeda 技术。

10 综述

梅特勒-托利多选择 ThingWorx-Axeda 作为我们远程服务基础设施供应商，使 InTouch 远程服务能为客户提供最高水平的安全性，而无需更改当前的 IT 安全基础设施。世界各地的公司正在使用 ThingWorx-Axeda 为客户提供远程服务。这是结合了 ThingWorx-Axeda 提供的基础设施、服务设计、运行安全原理和标准的结果。

梅特勒-托利多的首要任务是严格的 IT 安全，让客户相信我们能安全、高效地提供 InTouch 远程服务。这最终会提供给梅特勒-托利多客户更高的可靠性，更优良的产品性能。

Mettler-Toledo GmbH
Industrial
CH 8606 Greifensee
Switzerland
电话 +41-44-944 22 11
传真 +41-44-944 30 60

www.mt.com/service
访问网站，了解更多信息

MTSI 30259897