

# Services à distance InTouch<sup>SM</sup>

## Sécurité informatique

**Si la sécurité informatique est une priorité pour METTLER TOLEDO, cela en est également une pour nos clients qui utilisent les services à distance. La solution de service à distance éprouvée de METTLER TOLEDO protège les systèmes contre les virus et les pirates informatiques. Elle prend en charge les produits intelligents METTLER TOLEDO dans l'infrastructure informatique ou de sécurité existante du client et fonctionne avec les modèles de sécurité réseau standard.**

Pour une sécurité optimale de l'environnement des clients dans lequel sont connectés les produits METTLER TOLEDO, la solution de service à distance prend en charge le modèle de sécurité du client, permet un contrôle granulaire des droits des utilisateurs et offre des fonctionnalités d'audit et de suivi.

#### Notre engagement :

- Maintenir et protéger l'intégrité du système
- Dissimuler les données aux personnes non autorisées
- Garantir l'authentification des utilisateurs du système
- Limiter l'accès de chaque utilisateur à des données, des vues et des actions spécifiques
- Offrir la flexibilité et le contrôle nécessaires pour appliquer les politiques de l'entreprise
- Faire réaliser régulièrement un audit des procédés et de la solution technologique par un organisme tiers



#### Sommaire

1. Sécurité informatique – Services à distance
2. Mettler Toledo : critères de sécurité des services à distance
3. Clients : critères de sécurité des services à distance
4. Fonctionnement des services à distance InTouch
5. Présentation des technologies
6. Maintenance de l'intégrité et de la sécurité du réseau
7. Authentification de l'utilisateur, contrôle de l'accès et enregistrement des audits
8. Garantie de la confidentialité des données
9. Fonctionnalités de sécurité supplémentaires
10. Résumé

# 1 Sécurité informatique – Services à distance

Avec les services à distance InTouch, les techniciens METTLER TOLEDO sont connectés en toute transparence aux produits intelligents METTLER TOLEDO fonctionnant dans l'environnement du client. Compte tenu de la confidentialité et de la sensibilité des données généralement stockées sur ces produits, les fonctionnalités de sécurité et de compatibilité sont les principaux critères de choix d'une solution de service à distance. Ce livre blanc décrit les exigences de sécurité de METTLER TOLEDO et celles de nos clients. Il démontre également comment la plateforme sécurisée et éprouvée des services à distance InTouch répond à ces exigences.

## Notre engagement

La confidentialité et la sécurité sont deux critères essentiels pour nos clients. C'est pourquoi METTLER TOLEDO s'engage à respecter les principes de sécurité suivants :

- Maintenir et protéger l'intégrité du système (réseau, équipement et données)
- Dissimuler les données aux personnes non autorisées
- Garantir l'authentification des utilisateurs du système
- Limiter l'accès de chaque utilisateur à des données, des vues et des actions spécifiques
- Offrir la flexibilité et le contrôle nécessaires pour appliquer les politiques de l'entreprise
- Faire réaliser régulièrement un audit des procédés et de la solution technologique par un organisme tiers

## 2 Mettler Toledo : critères de sécurité des services à distance

La solution de METTLER TOLEDO doit répondre aux exigences de sécurité les plus strictes afin de garantir une utilisation efficace et régulière des services à distance et de rassurer les clients quant à la sécurité de leurs connexions.

Les exigences de METTLER TOLEDO sont les suivantes :

### Conception éprouvée

La sécurité informatique s'impose comme une priorité pour les entreprises qui utilisent des produits intelligents connectés. Un système de surveillance et de support à distance doit garantir la sécurité des systèmes informatiques.

### Prise en charge de plusieurs appareils

METTLER TOLEDO assure la prise en charge d'un nombre important de produits variés et de configurations client complexes de façon quasi-transparente pour les clients.

### Déploiement rapide

Il est impératif que les fonctionnalités de sécurité figurent dans le modèle de sécurité du réseau actuel du client pour simplifier l'adoption des systèmes de service à distance.

### Validation de sécurité réalisée par un tiers

METTLER TOLEDO fait appel à un organisme d'audit de sécurité tiers pour évaluer les capacités, la technologie et les procédures de nos partenaires.

### 3 Clients : critères de sécurité des services à distance

Les produits intelligents sont connectés aux réseaux des clients. Chaque client applique ses propres politiques de sécurité et de protection du réseau par le biais de pare-feu, serveurs proxy et systèmes d'adressage. La protection des produits connectés aux réseaux des clients doit être assurée au-delà de ces couches de sécurité. Si la prise en charge de la solution de service à distance implique la modification de ses procédures de sécurité, le client risque de se montrer réticent. C'est pourquoi il est impératif de prendre en compte les exigences du client, y compris :

#### **Préserver le modèle de sécurité actuel**

Outre leur conformité aux normes industrielles en vigueur, les produits intelligents de METTLER TOLEDO doivent s'intégrer en toute transparence aux procédures, opérations et politiques de sécurité informatique du client.

#### **Contrôler l'accès des utilisateurs**

Les services à distance InTouch doivent permettre aux clients de définir des politiques conformes à leurs modèles de sécurité qui déterminent quelles actions, telles que la collecte de données et les mises à jour logicielles, peuvent être réalisées sur quels appareils et à quel moment. Ces politiques peuvent être définies de manière centralisée pour l'ensemble des appareils connectés sur le site du client.

#### **Activité d'audit et de suivi**

En raison des exigences de conformité aux règlements et politiques, la simplicité et la convivialité des fonctionnalités d'audit et de suivi des activités d'administration et des utilisateurs offertes par la solution de service à distance sont des critères déterminants.

#### **Intégrité et sécurité des données**

Les données envoyées depuis les appareils METTLER TOLEDO connectés vers notre serveur sont protégées par un certificat SSL/TLS et un système de cryptage des données. Nous collectons uniquement données dont nous avons besoin pour surveiller les appareils METTLER TOLEDO, identifier les problèmes et dépanner les appareils. Les données qui nous sont transmises n'incluent aucune donnée client confidentielle.

Grâce à leur large gamme de fonctionnalités de sécurité et de protection des données, les services à distance InTouch garantissent la performance, la flexibilité et l'évolutivité dont les clients METTLER TOLEDO de divers secteurs ont besoin.

## 4 Fonctionnement des services à distance InTouch

Les services à distance InTouch surveillent le statut, les paramètres d'exploitation et la configuration des appareils METTLER TOLEDO installés sur votre site. Pour cela, ils utilisent un agent de surveillance logiciel qui communique de façon sécurisée avec le serveur Cloud Enterprise hébergé.

L'application des services à distance InTouch fonctionnant dans le Cloud évalue les performances de vos appareils à partir des données et alarmes reçues, puis stocke les données pertinentes qui serviront à analyser les tendances. En cas de détection d'un problème, le serveur Cloud Enterprise avertit le personnel de maintenance. Les techniciens à distance analysent ensuite les données sur le serveur Cloud Enterprise pour identifier le problème à distance, sans aucune interruption de vos activités.

Si cette opération ne permet pas d'identifier correctement le problème, le technicien à distance peut, avec votre accord, accéder à distance à l'appareil pour intervenir directement sur celui-ci.

Une fois le problème détecté, le technicien le résout immédiatement, dans la mesure où cela est possible, par exemple dans le cas d'une mise à jour logicielle ou d'une modification de la configuration. Le technicien peut résoudre de nombreux problèmes en intervenant à distance, avec votre accord.

Si un technicien de maintenance doit se déplacer sur site pour effectuer une réparation, les informations collectées via InTouch l'aident à préparer efficacement son intervention.

## 5 Présentation des technologies

Les services à distance InTouch reposent sur deux principaux composants : le logiciel Agent des services à distance qui fonctionne sur un appareil ou un ordinateur sur le site du client, et le serveur Cloud Enterprise et les applications connexes qui permettent d'accéder aux informations sur l'appareil.

Le logiciel Agent installé sur le site du client surveille les appareils METTLER TOLEDO et vérifie le statut des principaux éléments de données pour avoir une vue d'ensemble de l'état de santé et de la configuration du système. Par ailleurs, l'Agent des services à distance envoie régulièrement une mise à jour des données et du statut des appareils au serveur Cloud Enterprise.

Les services à distance InTouch exploitent votre infrastructure réseau et de sécurité. À l'exception de la connexion sortante vers le serveur Cloud Enterprise via le port 443 initiée par l'Agent, la connexion à distance ne requiert aucune modification de votre environnement.

Grâce au processus de communication sécurisé Firewall-Friendly™, il n'est pas nécessaire d'attribuer une adresse TCP/IP fixe ou visible publiquement. En effet, METTLER TOLEDO n'a en aucun cas besoin de créer une connexion entrante vers l'Agent sur votre site. L'Agent communique uniquement avec les serveurs Cloud Enterprise et les communications bilatérales ne sont démarrées qu'après l'ouverture et l'authentification de la connexion.

L'Agent surveille un ensemble particulier de paramètres et n'envoie que les données qui ont été modifiées aux serveurs Cloud Enterprise. Cela réduit le trafic de données transmises à METTLER TOLEDO sur votre réseau.

Par ailleurs, l'Agent envoie régulièrement un message succinct aux serveurs Cloud Enterprise pour confirmer qu'il est actif. Ces messages permettent à au service technique METTLER TOLEDO d'envoyer les requêtes d'action dans la file d'attente. L'équipe peut, par exemple, demander un journal d'erreur ou démarrer une session à distance. La requête sera transmise lors de l'envoi du prochain message par l'Agent.

## 6 Maintenance de l'intégrité et de la sécurité du réseau

ThingWorx-Axeda met en œuvre les meilleures pratiques du secteur en matière de cryptage des messages. Outre la prise en charge de certificats SSL émis par des autorités de certification de renommée mondiale, le protocole TLS (Transport Layer Security) permet de sécuriser les communications. Le contenu des messages bénéficie d'une couche de sécurité supplémentaire avec l'algorithme Advanced Encryption Standard (AES) 256. L'algorithme RSA 2048 est utilisé pour les échanges les plus importants.

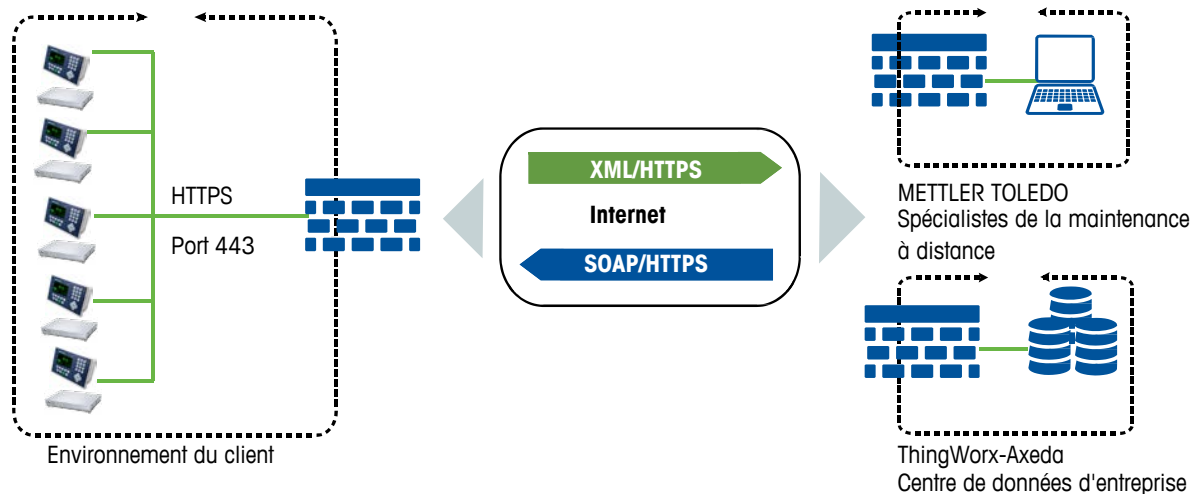
La technologie brevetée Firewall-Friendly™ d'ThingWorx-Axeda permet une communication bilatérale reposant sur des normes de services Web, notamment les protocoles HTTPS (Hypertext Transfer Protocol) et SOAP (Simple Object Access Protocol) et le langage XML (Extensible Markup Language). La prise en charge des appareils connectés n'entraîne aucune modification de l'infrastructure de sécurité informatique du client.

L'Agent des services à distance fonctionnant sur les appareils METTLER TOLEDO démarre toutes les communications avec le serveur Cloud Enterprise. Ce logiciel intelligent, qui permet aux appareils de se comporter comme des clients Web, envoie des messages au serveur Cloud Enterprise sous la forme de commandes HTTPS POST. Chaque message inclut des données cryptées au format XML envoyées via le protocole SSL sur le port 443. L'Agent ne peut accéder qu'aux serveurs associés aux services à distance InTouch.

Vous n'avez pas besoin de configurer de réseau virtuel privé pour mettre en œuvre les services à distance InTouch ni d'utiliser de communications par ligne téléphonique risquant de compromettre la sécurité de vos données puisque toutes les communications sont établies par l'appareil.

Aucune adresse IP n'est associée à l'appareil. Tous les appareils sont dissimulés derrière les pare-feu, serveurs proxy et systèmes d'adressage de l'infrastructure de sécurité informatique du client.

Pour schématiser, si un navigateur Web accède à Internet via l'infrastructure réseau du client, l'appareil connecté avec les services à distance InTouch utilise cette même connexion réseau pour communiquer avec le serveur Enterprise. Le fonctionnement des services à distance n'a donc aucun impact sur l'infrastructure de sécurité informatique du client.



## 7 Authentification de l'utilisateur, contrôle de l'accès et enregistrement des audits

### Authentification de l'utilisateur

Pour que nous puissions intervenir efficacement tout en protégeant vos données sensibles, l'accès aux applications des services à distance InTouch est exclusivement réservé au personnel compétent du support et de maintenance METTLER TOLEDO.

Pour accéder au système via le serveur Cloud Enterprise, les utilisateurs doivent saisir un ID unique et un mot de passe. Les mots de passe sont complexes et sont modifiés tous les 90 jours.

Si un utilisateur laisse une application ouverte sans surveillance, les données ne sont plus protégées. Pour éviter tout risque d'accès non autorisé, le système déconnecte automatiquement les utilisateurs après 20 minutes d'inactivité.

### Contrôle de l'accès des utilisateurs

L'accès des utilisateurs est contrôlé à l'aide de méthodes de contrôle d'accès basées sur les activités et sur les appareils. Il existe plusieurs combinaisons de ces méthodes grâce auxquelles les utilisateurs peuvent travailler efficacement tout en protégeant l'accès à vos données sensibles.

Le contrôle d'accès basé sur les activités permet à l'administrateur système de regrouper les utilisateurs accédant aux applications des services à distance InTouch, mais également de définir les activités qu'ils peuvent réaliser. L'autorisation d'accès aux applications des services à distance InTouch d'un groupe d'utilisateurs dépend de la fonction des utilisateurs et de leur niveau d'expérience avec les produits METTLER TOLEDO.

Le contrôle d'accès basé sur les appareils permet de déterminer les appareils auxquels chaque groupe d'utilisateur peut accéder. Ainsi, les utilisateurs ne peuvent consulter que les informations des appareils auxquels ils sont affectés.

#### **Enregistrement des audits**

Le système de l'entreprise crée un audit trail complet dans lequel sont consignés tous les événements et activités associés à la fois aux appareils intelligents et aux utilisateurs du support à distance. Le journal d'audit inclut des informations sur les interactions des utilisateurs au niveau du système et des appareils. Les données du journal d'audit sont stockées sur le serveur Cloud Enterprise et ne peuvent pas être supprimées. Les utilisateurs des services à distance InTouch peuvent consulter uniquement le journal d'audit des produits METTLER TOLEDO auxquels ils sont autorisés à accéder. Si un utilisateur ou un produit est supprimé du système, toutes les données le concernant demeurent dans le journal d'audit. Le système conserve ainsi une trace des informations concernant les activités, les utilisateurs et les appareils.

## **8 Garantie de la confidentialité des données**

Les services à distance InTouch sont fournis via une technologie reposant sur la norme SSL/TLS qui garantit une transmission sécurisée des données. Le protocole SSL/TLS permet de transmettre des données privées via Internet. Outre le cryptage des données, la norme SSL permet l'authentification de l'expéditeur et du destinataire. La norme SSL prend en charge les clés d'une longueur de 2 048 bits maximum et l'authentification mutuelle via des certificats. La norme SSL est celle utilisée par les banques pour crypter les transactions en ligne.

L'Agent des services à distance InTouch intégré aux produits intelligents METTLER TOLEDO surveille et analyse uniquement les éléments de données associés à l'exploitation et aux performances des produits. Les données surveillées dans le cadre du contrôle des performances des appareils n'incluent aucune donnée client confidentielle. Nous collectons et analysons uniquement les données dont nous avons besoin pour surveiller les appareils, identifier les problèmes et dépanner les appareils.

#### **Déclaration relative à l'utilisation et à la protection des données**

Les données collectées par METTER TOLEDO dans le cadre de l'utilisation des services à distance InTouch font l'objet d'un contrôle rigoureux et sont consultées uniquement par le personnel autorisé. Les éléments de données collectés lors de l'utilisation des services à distance InTouch et déterminés par un modèle spécifique incluent uniquement les paramètres requis pour identifier et résoudre les problèmes des appareils. En aucun cas METTLER-TOLEDO ne transférera, ne vendra ni ne divulguera à des tiers les données ou informations collectées par le biais des services à distance InTouch.

## 9 Fonctionnalités de sécurité supplémentaires

### ISO/IEC 27001:2013

ThingWorx-Axeda applique une stratégie de sécurité de bout en bout couvrant la totalité de l'environnement de sécurité, y compris le réseau, les applications, les utilisateurs et les données. ThingWorx-Axeda a obtenu la certification ISO 27001:2013, une performance qui s'inscrit dans les efforts de l'entreprise pour atteindre les niveaux de sécurité, de performance et de disponibilité les plus élevés pour le service Cloud M2M d'ThingWorx-Axeda.

Les fonctions du service Cloud M2M d'ThingWorx-Axeda permettent de résoudre les principaux problèmes de sécurité des informations :

- **Maintenir la sécurité du réseau sur le site des clients** – Basée sur la technologie brevetée Firewall-Friendly™ d'ThingWorx-Axeda, la solution ThingWorx-Axeda exploite l'infrastructure de sécurité des clients.
- **Dissimuler les données aux personnes non autorisées** – Toutes les communications entre vous et vos clients sont sécurisées grâce à la norme de cryptage SSL, une norme qui est également utilisée par les banques pour sécuriser les transactions en ligne.
- **Fournir une infrastructure sécurisée et évolutive à la demande** – Les centres de données ThingWorx-Axeda ont reçu la certification ISO 27001:2013 et sont soumis chaque année à la norme d'audit SAS 70. Ils font l'objet d'investissements importants dans les nouvelles technologies et sont équipés d'un matériel à la pointe de la technologie. Les centres de données utilisent des sous-systèmes redondants et des systèmes d'alimentation, de climatisation et de câblage réseau. Ils peuvent offrir une disponibilité supérieure à 99,95 %.
- **Garantir l'authentification des utilisateurs du système** – Tous les accès au système sont contrôlés de manière centralisée et requièrent une authentification par mot de passe. Les actions exécutées par les utilisateurs font l'objet d'un audit à des fins de traçabilité.
- **Limiter l'accès de chaque utilisateur à des données, des vues et des actions spécifiques** – Une fois que l'utilisateur a été authentifié, les actions qu'il peut effectuer se limitent aux produits qui lui ont été attribués et au niveau d'accès correspondant à son rôle.

### Déploiements reconnus

La technologie utilisée par les services à distance InTouch a été déployée par de nombreux fabricants dans divers secteurs, notamment la sécurité nationale, la médecine, les sciences de la vie, l'informatique, les télécommunications, l'impression et l'imagerie, les kiosques, les semi-conducteurs et l'automatisation industrielle. Le haut niveau de sécurité et de protection des données fourni par ThingWorx-Axeda à ces fabricants et à leurs clients correspond à celui auquel s'attendent nos clients.

Les centres de données utilisent généralement des solutions fournies par des entreprises telles que 3PAR, Egenera, EMC2, Inilon, NetApp, Quantum ou Teradata, qui proposent des services de support à distance. Si votre service informatique a recours à ces solutions, vous connaissez certainement la technologie Adexa utilisée par METTLER TOLEDO puisqu'elle est également employée dans les solutions en question.



## 10 Résumé

METTLER TOLEDO s'est associé à ThingWorx-Axeda pour mettre en œuvre les services à distance InTouch et garantir à ses clients le niveau de sécurité le plus élevé sans impact sur leur infrastructure de sécurité informatique. De nombreuses entreprises du monde entier font confiance à ThingWorx-Axeda pour offrir des services à distance à leurs clients. La conception et l'exploitation de l'infrastructure et des services fournis par ThingWorx-Axeda reposent sur l'association minutieuse de normes et de principes de sécurité.

La priorité absolue pour METTLER TOLEDO : atteindre le niveau de sécurité le plus rigoureux pour garantir à nos clients une utilisation efficace et sécurisée des services à distance InTouch. Nos clients choisissent les produits METTLER TOLEDO en toute confiance en sachant qu'ils bénéficieront d'une disponibilité et de performances optimales, et obtiendront des résultats ultraperformants.

[www.mt.com/service](http://www.mt.com/service)

Pour plus d'informations

**Mettler-Toledo AG**

Industrie  
CH 8606 Greifensee  
Suisse  
Téléphone : +41-44-944 22 11  
Fax : +41-44-944 30 60

Sous réserve de modifications techniques.  
© 10/2015 Mettler-Toledo AG  
MTSI 30254016