

Description du réseau, d'Ethernet et de Wi-Fi (WLAN) pour la balance Cubis® MCA

Ce document décrit comment connecter la balance à un réseau via Ethernet et Wi-Fi (WLAN). Des exemples sont donnés pour illustrer comment configurer et utiliser la balance dans la pratique.



Résumé exécutif

La balance de laboratoire Cubis® MCA Premium offre des options de connectivité complètes et flexibles pour intégrer la balance dans l'informatique du laboratoire. Un grand nombre de protocoles informatiques standardisés, tels que le service web REST, SMB ou LDAP, sont disponibles via Ethernet et Wi-Fi, ce qui permet une intégration directe sans utiliser de logiciel intermédiaire supplémentaire. En outre, Cubis® peut être commandée à distance sur le réseau à l'aide d'un navigateur Web et il est possible de consulter la piste d'audit et d'autres informations d'état.

1	Connexion réseau Ethernet et Wi-Fi	4
1.1	Paramètres généraux	4
1.2	Ethernet (LAN)	4
1.2.1	Protocole IPv4	5
1.2.2	Protocole IPv6	5
1.2.3	DNS 1 et DNS 2	5
1.3	Wi-Fi (WLAN)	5
1.3.1	SSID et mot de passe Wi-Fi	6
1.3.2	Protocole IPv4/IPv6 et DNS 1/2	6
2	Services de réseau	6
2.1	Communication en série	6
2.1.1	Protocole SBI	6
2.1.2	Protocole xBPI	7
2.1.3	Protocole SICS	7
2.1.4	QAPP direct	7
2.2	Connecteurs de réseau	7
2.2.1	YDP30-NET	7
2.2.2	Imprimante réseau	7
2.2.3	FTP / FTPS	8
2.2.4	Protocole SMB	8
2.3	Site web	8
2.3.1	Webservices	8
2.4	Serveur NTP pour la date et l'heure	8
2.5	Certificats	8
2.5.1	Obligations de l'exploitant	8
2.5.2	Réinitialiser les certificats	9
2.5.3	Installer et mettre à jour les certificats	9
2.5.3.1	Certificats clients	9
2.5.3.2	Certificats CA	9
2.5.3.3	Types de fichiers de certificats	9
2.5.4	Types de certificats	10
2.5.4.1	Certificats CA	10
2.5.4.2	Autorités de certification inconnues	10
2.5.4.3	Certificats d'appareils	10
2.5.4.4	Certificats Wifi	11
2.5.4.5	Certificats LDAPS	11
2.5.5	Connexions réseau sécurisées avec SSL/TLS	11
2.5.5.1	Autorités de certification inconnues	11
3	Exemples d'application	11
3.1	Rapport sur les paramètres des menus sur le serveur de fichiers Windows	11
3.1.1	Mise en place	12
3.1.2	Application	12
3.1.3	Dépannage	12

3.2	Mise à jour du QAPP Center du serveur FTP	13
3.2.1	Mise en place	13
3.2.2	Application	13
3.2.3	Dépannage	14
3.3	Visualisation des entrées de la piste d'audit via un navigateur web	14
3.3.1	Mise en place	14
3.3.2	Application	14
3.3.3	Dépannage	15
3.4	Synchroniser la date et l'heure avec un serveur NTP	15
3.4.1	Mise en place	15
3.4.2	Dépannage	16
4	Annexe	16
4.1	Bâtons Wi-Fi compatibles	16
5.	Abréviations	17

1 Connexion réseau Ethernet et Wi-Fi

Une balance Cubis® MCA peut être connectée à un réseau basé sur TCP/IP par câble via la connexion Ethernet (prise RJ45) et sans fil via un adaptateur USB Wi-Fi (clé WLAN).

Les débits de transmission de la connexion réseau sont de 10 Mbit/sec (10BASE-T, Ethernet) et de 100 Mbit/sec (100BASE-TX Fast Ethernet).

La connexion Ethernet est réalisée à l'aide d'un câble de connexion, CAT 5 ou supérieur, torsadé par paires, blindé, 1:1, UTP/STP, fiche RJ45 ; par exemple, un câble patch CAT 5 en fonction de l'utilisation (droit/croisé).

Pour une connexion sans fil, Cubis® MCA supporte les adaptateurs USB Wi-Fi les plus courants (clés WLAN) proposés sur le marché.

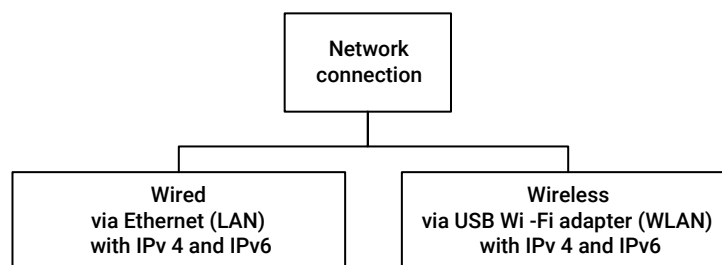


Figure 1 : Connexion au réseau

La balance Cubis® MCA peut avoir une adresse IPv4 et une adresse IPv6 sur Ethernet et Wi-Fi respectivement, soit jusqu'à 4 adresses.

Via les connexions réseau Ethernet (LAN) et Wi-Fi (WLAN), la balance Cubis® MCA offre simultanément plusieurs services réseau.

1.1 Paramètres généraux

Le nom d'hôte de la balance, ex-factory, est composé de la désignation de la série et des 3 derniers octets de l'adresse MAC, par exemple [cubis-1a477e]. Le nom d'hôte peut être choisi librement, mais il doit être unique dans un réseau.

1.2 Ethernet (LAN)

Pour la connexion Ethernet de la balance, les protocoles IPv4 ainsi que IPv6 peuvent être utilisés. Il est possible de définir séparément pour chaque protocole, si l'adresse IP doit être obtenue automatiquement ou si la balance reçoit une adresse IP fixe. Le protocole respectif peut également être complètement désactivé.

Dans l'aperçu des paramètres pour Ethernet, l'état indique si une connexion au réseau est établie. En outre, l'adresse MAC unique de la balance est également affichée ici, par exemple [00:30:D6:1F:77:569].

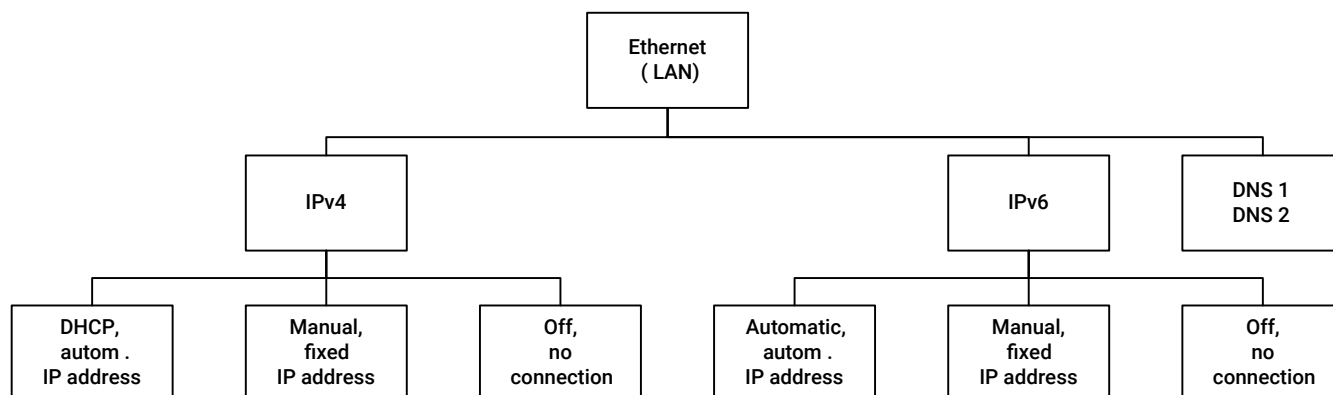


Figure 2 : Ethernet avec IPv4/IPv6

Pour le fonctionnement avec une adresse IP fixe, il faut saisir manuellement, en plus de l'adresse IP, selon le protocole, le masque de sous-réseau et la passerelle pour IPv4, ou la longueur du préfixe et la passerelle pour IPv6.

La saisie de la passerelle est facultative et nécessaire uniquement lorsqu'une connexion à Internet est requise.

Toutes les informations nécessaires à cet effet peuvent être fournies par l'administrateur réseau responsable du réseau de l'entreprise.

1.2.1 Protocole IPv4

L'adresse IP pour le protocole IPv4 (4*8 bits = 32 bits) se compose de 4 nombres décimaux compris entre 0 et 255, séparés par un point, par exemple [123.4.56.123]. Ce format s'applique à la saisie de l'adresse IP fixe, de la marque de sous-réseau et de la passerelle.

1.2.2 Protocole IPv6

L'adresse IP pour le protocole IPv6 (8*16 bits = 128 bits) se compose de 8 nombres alphanumériques hexadécimaux compris entre 0 et FFFF, qui sont séparés par deux points, par exemple [ecb1:d583:6341:baf76:0:0:0:1].

Les 4 premiers blocs (64 bits) constituent le préfixe et les 4 derniers blocs l'identifiant de l'interface. Le masque de réseau IPv4 et l'adresse réseau IPv4 sont remplacés par la longueur du préfixe et le préfixe dans IPv6. La longueur du préfixe spécifie le nombre de bits qui constituent le préfixe. La longueur typique d'un préfixe est de 64. Le préfixe remplace le masque de sous-réseau dans le cas d'IPv6.

1.2.3 DNS 1 et DNS 2

Dans les systèmes de réseau basés sur IP, le DNS (Domain Name System) aide à répondre aux requêtes de résolution de noms. Un réseau peut avoir plusieurs serveurs DNS, le Cubis® MCA supporte l'entrée de deux serveurs.

L'adresse IP ou le nom du serveur peut être saisi pour chaque serveur DNS.

En cas de DHCP, le serveur DNS est fourni automatiquement par le serveur DHCP. De plus, dans ce cas, DNS1 et DNS2 sont ajoutés à la liste des serveurs DNS.

1.3 Wi-Fi (WLAN)

Un adaptateur USB Wi-Fi (clé WLAN) peut être connecté à la balance MCA ; plusieurs adaptateurs de ce type ne sont pas pris en charge.

Dans la vue d'ensemble des paramètres pour le Wi-Fi (WLAN), l'état indique si un adaptateur USB Wi-Fi correspondant est connecté et s'il est relié au réseau.

Affichage de l'état

- Aucun appareil disponible - Aucun adaptateur USB Wi-Fi n'est connecté.
- Déconnecté - Pas de connexion au réseau Wi-Fi, par exemple, pas de connexion avec le SSID et le mot de passe Wi-Fi.
- Prêt - Connexion établie avec le réseau Wi-Fi.
- En ligne - Connexion établie avec le réseau Wi-Fi et l'Internet.

Si une connexion a été établie, l'adresse MAC unique de l'adaptateur USB Wi-Fi est également indiquée ici, par exemple 34:C9:F0:89:6F:D6.

Dans l'annexe, la section : Compatible Wi-Fi sticks.

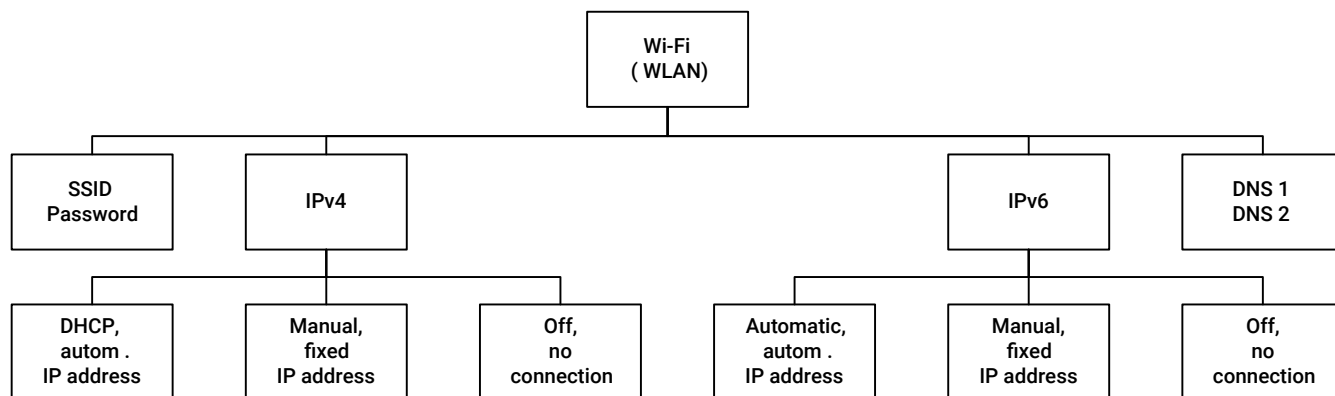


Figure 3 : Wi-Fi avec IPv4/IPv6

Dans le cas d'un fonctionnement avec une adresse IP fixe, il faut saisir manuellement, en plus de l'adresse IP, selon le protocole, le masque de sous-réseau et la passerelle pour IPv4, ou la longueur du préfixe et la passerelle pour IPv6. La saisie de la passerelle est facultative et nécessaire uniquement lorsqu'une connexion à Internet est requise.

Toutes les informations nécessaires à cet effet peuvent être fournies par l'administrateur réseau responsable du réseau de l'entreprise.

1.3.1 SSID et mot de passe Wi-Fi

Pour vous connecter à un réseau Wi-Fi, vous devez saisir le SSID Wi-Fi (le nom unique du réseau Wi-Fi) et le mot de passe Wi-Fi (la clé du réseau Wi-Fi).

Pour l'authentification, la balance MCA supporte les standards WEP, WPA-PSK et WPA2-PSK et donc aussi la méthode PSK pour le cryptage.

1.3.2 Protocole IPv4/IPv6 et DNS 1/2

Pour le protocole IPv4 et IPv6 ainsi que pour DNS 1 et DNS 2, la même description s'applique au Wi-Fi (WLAN) qu'en cas de Ethernet (LAN).

2 Services de réseau

Via le réseau, la balance Cubis® MCA offre plusieurs services simultanément, une communication série avec différents protocoles, connecteurs pour la connexion à des périphériques de stockage de masse en réseau et à des imprimantes, un site web et service web pour l'accès à distance, ainsi que la connexion à un serveur NTP pour la synchronisation de la date et de l'heure.

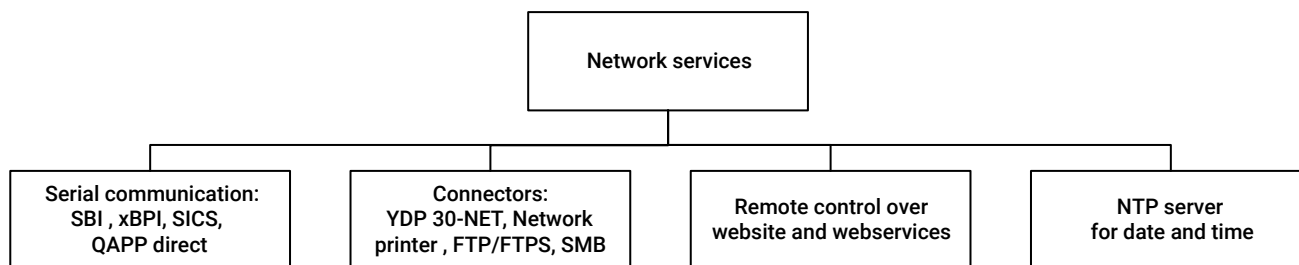


Figure 4 : Services de réseau

2.1 Communication en série

La connexion réseau permet d'utiliser les protocoles de communication série SBI, xBPI, SICS, miniSICS, qui peuvent être exploités indépendamment de la tâche active et de son utilisation. Cette connexion client/serveur nécessite le paramétrage d'un port TCP commun.

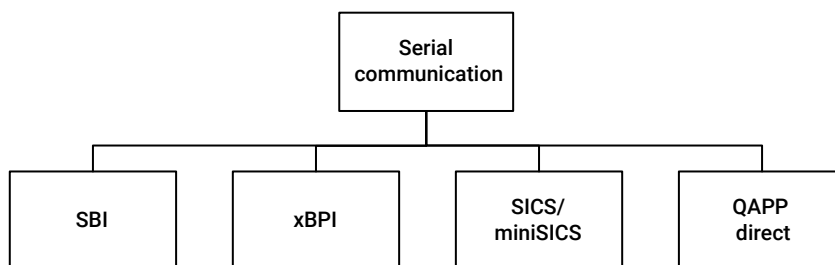


Figure 5 : Communication en série

2.1.1 Protocole SBI

Ce protocole simple, basé sur ASCII, permet de contrôler les fonctions de base de la balance à l'aide de commandes ESC. La sortie des valeurs d'affichage peut être demandée individuellement par une commande ESC, ou automatiquement avec chaque nouveau résultat de pesée dans le cycle de séquence d'affichage, ou automatiquement après des intervalles de temps spécifiques. Il est possible de choisir si la sortie est fournie uniquement avec une valeur d'affichage stable, ou également sans que la valeur d'affichage soit stable. Le format de sortie peut être sélectionné avec ou sans identifiant (en-tête).

Les commandes SBI et les formats de sortie sont donnés dans une description séparée de l'interface.

2.1.2 Protocole xBPI

Ce protocole binaire offre une gamme étendue de commandes. Il peut être utilisé pour contrôler de nombreuses fonctions de la balance.

Il existe une description séparée de l'interface des commandes xBPI possibles.

2.1.3 Protocole SICS

Le protocole SICS (Standard Interface Command Set) établit une compatibilité avec le protocole MT-SICS de Mettler et permet d'envoyer des commandes à la balance pour les fonctions de base. Cependant, il faut noter qu'il existe des différences dues aux différentes plateformes matérielles/logicielles.

Les commandes SICS et miniSICS implémentées dans la balance sont présentées dans une description séparée de l'interface.

2.1.4 QAPP direct

Seuls les QAPP spéciaux, qui sont lancés par une tâche, peuvent utiliser l'interface à des fins d'entrée et de sortie. Les possibilités d'entrée et de sortie via l'interface sont décrites dans le QAPP spécial correspondant.

2.2 Connecteurs de réseau

Dans Cubis® MCA, les connecteurs établissent la connexion avec les serveurs du réseau qui doivent être utilisés comme dispositifs de stockage de masse ou comme imprimantes.

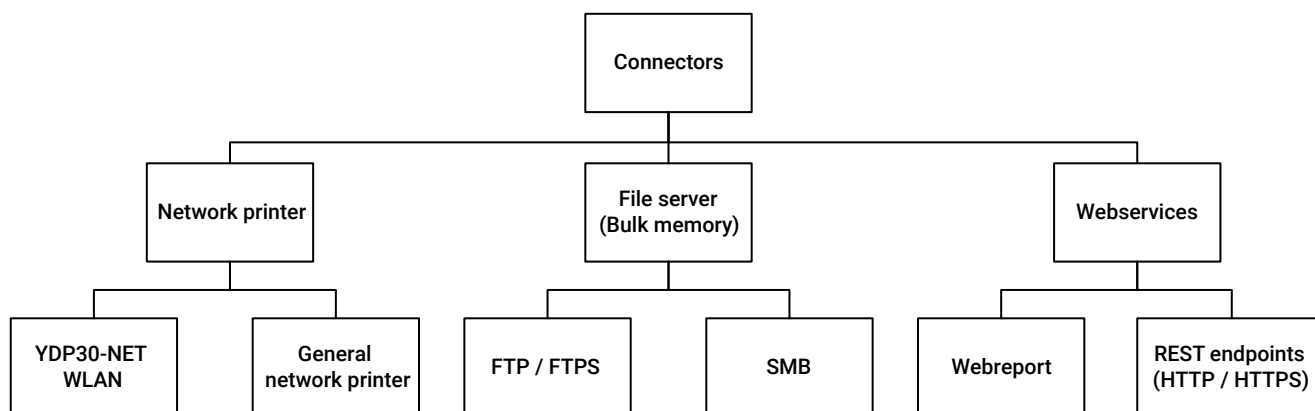


Figure 6 : connecteurs réseau

L'imprimante réseau YDP30-NET peut être connectée par WLAN ou comme une imprimante réseau générale avec un réseau Wi-Fi indépendant ou un réseau d'entreprise utilisant DHCP.

Pour se connecter à un dispositif de stockage de masse, tel qu'un serveur de fichiers Windows, FTP/FTPS ou STARLIMS, une extension QAPP spéciale est nécessaire, qui doit être activée via le QAPP Center sous [Connectivité].

2.2.1 YDP30-NET

Ce connecteur est destiné à raccorder une imprimante YDP30-NET avec un câble (LAN) ou une connexion sans fil (WLAN). Un connecteur requiert un nom de connecteur, une adresse IP ou un nom d'hôte à saisir sur l'imprimante, ainsi qu'un numéro de port convenu entre l'imprimante et la balance.

La connexion sans fil de l'imprimante YDP30-NET est décrite dans des instructions séparées.

2.2.2 Imprimante réseau

Le connecteur pour imprimante réseau permet, par exemple, de se connecter à une imprimante A4 dans un réseau Wi-Fi indépendant avec des composants Wi-Fi standard, ou dans un réseau d'entreprise par DHCP avec des méthodes d'authentification standard. L'imprimante réseau doit prendre en charge le protocole IPP (Internet Printing Protocol).

Un connecteur nécessite la saisie d'un nom de connecteur, d'une adresse IP ou d'un nom d'hôte sur l'imprimante, ainsi que du protocole de transfert.

La description séparée [Concept d'impression] décrit la configuration et l'application d'une imprimante réseau avec

un exemple d'application.

2.2.3 FTP / FTPS

Le protocole de transfert de fichiers (FTP) est un protocole réseau standard pour le transfert de fichiers informatiques entre un client et un serveur dans un réseau informatique.

La balance est le client FTP et peut stocker des fichiers sur un serveur FTP ou récupérer des fichiers d'un serveur FTP en utilisant le protocole. En cas de FTPS, la connexion est également cryptée ; les certificats nécessaires à cet effet sont décrits séparément.

Pour se connecter à un serveur FTP/FTPS, un connecteur doit être créé avec un nom unique, l'adresse IP et le numéro de port du serveur réseau, si nécessaire, un sous-répertoire sur le serveur et le nom d'utilisateur et le mot de passe.

Note : Avec plusieurs connecteurs sur le bilan vers le même serveur, mais avec des sous-répertoires différents, le stockage des données peut être facilement structuré en fonction du sujet (sauvegarde, rapport, ...).

2.2.4 Protocole SMB

Le connecteur du serveur de fichiers Windows utilise le protocole réseau SMB. Ce protocole facilite l'accès aux lecteurs réseau libérés des ordinateurs Windows ou Linux afin de stocker ou de récupérer des fichiers de données dans les répertoires cibles sélectionnés.

2.3 Site web

Le site Internet de la balance MCA peut être affiché simplement via l'adresse IP de la balance avec un navigateur Internet. La page [My Cubis] (page d'accueil) affiche les identifiants des appareils réglés, des informations générales sur les appareils de la balance et des informations sur le service.

En utilisant la page [Remote operation], selon les paramètres du menu, il est possible d'afficher [View only] ou [View and remote control] de la balance MCA via le navigateur.

La page [Screenshot] crée un fichier PNG de l'affichage actuel, qui peut être sauvegardé.

Si l'extension QAPP [Audit trail] a été activée dans le QAPP Center dans le package [Pharma], le site web [Audit trail] est également affiché. Les entrées de la piste d'audit peuvent être filtrées, triées et exportées en fonction des thèmes.

L'accès au site web peut être complètement désactivé via le menu et donc aussi la commande à distance via le service web REST.

2.3.1 Webservices

L'exploitation à distance des fonctions sous-jacentes de la balance MCA peut également se faire via un service web REST.

Il existe une description séparée des services web REST disponibles de la balance MCA.

2.4 Serveur NTP pour la date et l'heure

Cubis® MCA offre la possibilité de synchroniser la date et l'heure avec un serveur NTP. Pour ce faire, la connexion avec le serveur peut être activée et l'adresse IP du serveur peut être saisie dans les paramètres de l'appareil MCA sous Date/Time et NTP Configuration.

2.5 Certificats

Le Cubis® MCA balance supporte l'utilisation de certificats pour une intégration fiable dans l'infrastructure informatique locale. Le MCA peut traiter les certificats des agences de certification (CA) de confiance, afin d'identifier les serveurs de confiance. Le MCA fournit également ses propres certificats d'appareil à télécharger. Ces certificats sont importés dans les navigateurs pour l'accès à distance sécurisé au site Web de l'appareil.

Il existe une description distincte au sujet des [Certificats].

Les certificats de périphérique sont basés sur la norme X.509 et utilisent la cryptographie à clé publique, qui consiste à utiliser une paire de clés publique et privée. Cette paire de clés permet la transmission cryptée des données, la vérification des signatures numériques ainsi qu'une authentification fiable de l'identité. Selon la manière dont la clé privée est créée et stockée, il peut être nécessaire de la décrypter avec une phrase de passe avant de l'utiliser.

2.5.1 Obligations de l'exploitant

Les balances Sartorius Cubis® MCA sont livrées avec des certificats d'appareil préinstallés, dont la validité est

limitée. Les opérateurs ont la possibilité de renouveler les certificats installés à l'origine et d'importer leurs propres certificats.

La gestion et la mise à jour ainsi que la garantie de la validité sont du ressort de l'exploitant. Afin d'éviter d'éventuelles alertes de sécurité ou des restrictions de connexions sécurisées, il est important de vérifier régulièrement la validité des certificats et de les renouveler si nécessaire.

L'actualisation du certificat n'a aucune incidence sur la fonction de pesage ni sur l'intégration dans l'infrastructure informatique locale. Par conséquent, la mise à jour des certificats ne nécessite pas de requalification ou de revalidation des appareils.

2.5.2 Réinitialiser les certificats

Si un avertissement concernant l'expiration du certificat s'affiche après la réinitialisation du certificat, veuillez mettre à jour le certificat comme décrit dans la section Mise à jour des certificats

1. Fournir les fichiers de certificats de manière à ce qu'ils soient accessibles via un connecteur de l'appareil, par exemple sur une clé USB et le connecteur USB.
2. Naviguer vers les paramètres à partir du menu d'accueil
3. Naviguer dans le menu Connexions puis Certificats
4. Sélectionnez Device Certificates
5. Sélectionnez l'icône "Corbeille" pour renouveler les certificats et confirmez le message "Réinitialiser les certificats" par "Oui".
6. Vérifiez que le nouveau certificat "Sartorius Factory Authority" est disponible. Ce certificat expirera en 2043.
7. Si "Sartorius Factory Authority" est visible dans la liste, la mise à jour a été effectuée avec succès et une entrée dans la piste d'audit est générée.

Si un avertissement concernant l'expiration du certificat s'affiche après la réinitialisation du certificat, veuillez mettre à jour le certificat conformément au chapitre Mettre à jour les certificats.

2.5.3 Installer et mettre à jour les certificats

Pour installer ou mettre à jour un certificat, suivez ces instructions.

2.5.3.1 Certificats clients

1. Rendez les fichiers de certificat accessibles via un connecteur de l'appareil, par exemple sur une clé USB et le connecteur USB.
2. Naviguer vers les paramètres à partir du menu d'accueil
3. Naviguer dans le menu Connexions puis Certificats
4. Naviguez dans le menu correspondant pour lequel un certificat doit être installé. Vous trouverez la distinction et l'explication des certificats dans le chapitre Types de certificats.
5. Cliquez sur le bouton [IMPORT] et sélectionnez le connecteur correspondant par lequel les fichiers de certificat à installer sont accessibles.
6. Sélectionnez [Certificat] et choisissez le fichier de certificat avec la clé publique dans la liste des fichiers disponibles via le connecteur. Les formats suivants sont supportés : .pem et .crt.
7. Sélectionnez [Clé privée] et choisissez le fichier de certificat avec la clé privée dans la liste des fichiers disponibles via le connecteur. Les formats suivants sont pris en charge : .key.
8. Sélectionnez [Mot de passe de la clé privée] et saisissez le mot de passe de la clé privée.
9. Confirmez l'importation. Les fichiers seront transférés dans le système après avoir été vérifiés avec succès.

2.5.3.2 Certificats CA

1. Rendez les fichiers de certificat accessibles via un connecteur de l'appareil, par exemple sur une clé USB et le connecteur USB.
2. Naviguez vers les paramètres depuis le menu principal
3. Dans le menu Connexions, naviguez jusqu'au sous-menu Certificats
4. Naviguez vers le menu correspondant pour lequel un certificat doit être installé. La différenciation et l'explication des certificats se trouvent dans le chapitre Types de certificats.
5. Appuyez sur la touche [IMPORT] et sélectionnez le connecteur correspondant permettant d'accéder aux fichiers de certificat à installer.
6. Sélectionnez le fichier de certificat dans la liste des fichiers disponibles via le connecteur. Les formats suivants sont pris en charge : .pem et .crt

2.5.3.3 Types de fichiers de certificats

Une brève introduction à la PKI : les clés sont composées de deux moitiés, une clé publique et une clé privée. La clé publique peut être publique et largement diffusée, et vous pouvez l'utiliser pour vérifier les informations générées

par la clé privée, mais pas pour les reproduire. La clé privée doit être gardée secrète.

- Les fichiers .key sont généralement la clé privée utilisée par le serveur pour chiffrer et emballer les données en vue de leur vérification par les clients.
- Les fichiers .pem sont généralement la clé publique utilisée par le client pour vérifier et décrypter les données envoyées par les serveurs. Les fichiers PEM peuvent également être des clés privées cryptées.
- Les deux moitiés de la clé sont intégrées dans les fichiers .p12, ce qui permet aux administrateurs de gérer facilement les moitiés de clé.
- Les fichiers .cert ou .crt sont les certificats signés contenant une clé publique, des informations sur le propriétaire de la clé et la signature numérique de l'autorité de certification qui a délivré le certificat. Cela permet à un système d'être considéré comme fiable par une tierce partie.
- Dans les fichiers .cer, les certificats sont généralement au format binaire ou Base64. Ils se distinguent donc des fichiers .crt par leur encodage.

2.5.4 Types de certificats

Pour une connexion sécurisée aux services de réseau, la balance a besoin de différents certificats qui peuvent être chargés sur la balance. Une distinction est faite entre les certificats suivants :

- Certificats CA (autorités de certification de confiance).
- Certificat d'appareil
- Certificat d'authentification Wi-Fi
- Certificat LDAPS.

2.5.4.1 Certificats CA

Un certificat CA (en anglais Certificate Authority Certificate) est un certificat numérique délivré par une autorité de confiance, appelée autorité de certification ou Certificate Authority (CA). Son but est de confirmer l'authenticité et la fiabilité d'un partenaire de communication ou d'un service. Lorsque deux appareils ou programmes communiquent entre eux via un réseau, un certificat CA permet aux deux parties de s'assurer qu'elles sont effectivement connectées au partenaire de communication souhaité et non à un attaquant se faisant passer pour ce dernier.

Si un certificat CA est jugé digne de confiance, l'appareil accepte automatiquement tous les certificats qui en découlent. Il en résulte ce que l'on appelle une chaîne de certificats qui peut être retracée depuis le certificat CA racine jusqu'au certificat de l'appareil concerné. Une sélection d'autorités de certification fiables est déjà préinstallée sur l'appareil.

2.5.4.2 Autorités de certification inconnues

L'appareil offre également la possibilité de faire confiance aux certificats qui n'ont pas été émis par une autorité de certification connue. Si cette option est activée, l'appareil accepte de tels certificats sans vérifier leur validité au moyen d'une chaîne de certificats. Cette option peut être utile dans les environnements de test ou de développement, mais présente un risque de sécurité dans le cadre d'une utilisation productive, car l'authenticité et la fiabilité des certificats utilisés ne sont pas garanties.

Cette option peut être activée sous Certificats, Certificats système, [Faire confiance à des autorités de certification inconnues].

2.5.4.3 Certificats d'appareils

Les certificats de périphérique confèrent à un périphérique une identité unique qui lui permet de s'authentifier auprès des systèmes connectés. Cela garantit que seuls les appareils autorisés peuvent accéder aux données et que la communication entre les appareils est protégée. Ces certificats sont basés sur les normes X.509 et sont générés par des certificats à clé publique (infrastructure à clé publique, PKI). Cela permet aux appareils d'identifier d'autres appareils et serveurs de confiance.

En règle générale, un certificat de périphérique est délivré par l'autorité de certification (AC) interne d'une organisation. Le certificat est signé avec la clé privée du certificat racine (certificat AC) de l'organisation, qui sert de base pour la signature d'autres certificats.

La sécurisation des appareils incombe à l'exploitant et n'est pas une prestation du fabricant Sartorius. Il est donc important de sécuriser l'appareil avec son propre certificat dès qu'il arrive dans votre organisation. Au départ de l'usine, les appareils sont livrés avec un certificat standard de Sartorius.

Les certificats de périphérique doivent être créés en interne dans votre système et votre réseau, ce qui nécessite une AC privée. Il existe deux approches :

1. Créez votre propre CA privée avec des outils comme OpenSSL ou Microsoft CA.
2. Engagez un fournisseur de Managed PKI (mPKI) qui prendra en charge vos besoins d'authentification et de cryptage.

2.5.4.4 Certificats Wifi

Un certificat WiFi est un certificat numérique utilisé pour l'authentification et le cryptage sécurisés dans un réseau sans fil (WLAN). Typiquement, de tels certificats sont utilisés dans le cadre de WPA2-Entreprise ou WPA3-Entreprise, qui utilisent la méthode d'authentification 802.1X (par exemple EAP-TLS).

Avec WPA2-Entreprise ou WPA3-Entreprise, l'authentification se fait généralement via le serveur RADIUS, qui est souvent relié à un service d'annuaire (LDAP/Active Directory). Pour que les clients et le serveur RADIUS puissent s'identifier mutuellement de manière sûre, on utilise des certificats.

2.5.4.5 Certificats LDAPS

Les serveurs LDAP (Lightweight Directory Access Protocol) utilisent des certificats pour sécuriser leur communication avec les clients ou d'autres services. Souvent, les serveurs LDAP sont responsables de la gestion centrale des utilisateurs et des droits. Si la connexion n'est pas sécurisée, les données sensibles des utilisateurs (par exemple les mots de passe, les informations sur les groupes ou les rôles) peuvent être interceptées ou manipulées.

En communiquant avec le serveur LDAP via LDAPS (LDAP via SSL/TLS), la connexion est cryptée. De plus, le client vérifie l'identité du serveur LDAP à l'aide du certificat du serveur. Le certificat du serveur LDAPS doit donc être déposé sur l'appareil.

2.5.5 Connexions réseau sécurisées avec SSL/TLS

Pour transmettre des données en toute sécurité, on utilise des protocoles de sécurité tels que SSL (Secure Sockets Layer) et TLS (Transport Layer Security). Ils définissent la manière dont les algorithmes de cryptage et d'authentification doivent être utilisés afin de garantir une connexion à l'abri des écoutes et des manipulations.

SSL est une technologie de sécurité conforme à des normes plus anciennes, qui établit une connexion cryptée entre un serveur et un client. Dans le cas de la balance (par ex. Cubis MCA), il peut s'agir de la communication cryptée avec un navigateur web qui accède au site web de l'appareil. Entre-temps, SSL a été remplacé par TLS (Transport Layer Security) comme technologie de suivi. Mais comme SSL est le terme le plus connu, on parle de TLS/SSL en ce qui concerne les certificats ou la sécurisation des données transmises, même si seul TLS est utilisé en arrière-plan. La balance supporte actuellement TLS jusqu'à la version 1.3.

2.5.5.1 Autorités de certification inconnues

L'appareil offre également la possibilité de faire confiance aux certificats qui n'ont pas été émis par une autorité de certification connue. Si cette option est activée, l'appareil accepte de tels certificats sans vérifier leur validité au moyen d'une chaîne de certificats. Cette option peut être utile dans les environnements de test ou de développement, mais présente un risque de sécurité dans le cadre d'une utilisation productive, car l'authenticité et la fiabilité des certificats utilisés ne sont pas garanties.

Cette option peut être activée sous Certificats, Certificats système, [Faire confiance à des autorités de certification inconnues].

3 Exemples d'application

Les exemples d'application concernent la version du MCA à partir du package 09-03-04.01.xx, ainsi que les options de paramétrage et les fonctionnalités qu'elle contient. Des droits d'utilisateur appropriés sont nécessaires pour configurer les connexions, les connecteurs et les interfaces du réseau.

Pour configurer l'interface Ethernet et l'interface Wi-Fi, des connaissances de base sur les réseaux basés sur TCP/IP et les technologies de réseau en général sont nécessaires.

La condition préalable pour tous les exemples est une connexion de la balance à un réseau via Ethernet (LAN) ou Wi-Fi (WLAN).

3.1 Rapport sur les paramètres des menus sur le serveur de fichiers Windows

Cet exemple décrit la configuration et l'utilisation de la balance MCA afin qu'un fichier de rapport avec tous les paramètres de la balance puisse être exporté du menu [Paramètres] au format PDF, via le connecteur [serveur de fichiers Windows] en utilisant le protocole de réseau SMB, vers le répertoire cible d'un lecteur de réseau libéré.

Pour transférer des fichiers via le protocole SMB, une extension QAPP [Connexion au serveur de fichiers Windows] du paquet [Connectivité] est nécessaire. Cette extension peut être utilisée gratuitement pendant 30 jours, après quoi elle doit faire l'objet d'une licence.

Un lecteur libéré avec le protocole SMB dans votre réseau est une exigence pour cette application.

Cette application peut donc être utilisée pour stocker de manière centralisée les paramètres du menu de toutes les balances MCA en réseau.

3.1.1 Mise en place

Étapes de configuration :

1. Activez l'extension QAPP [Connexion au serveur de fichiers Windows], si cela n'a pas encore été fait.
 - a. Ouvrez le menu [Gestion des tâches], puis le [Centre QAPP].
 - b. Choisissez le progiciel [Connectivité], et à l'intérieur de celui-ci le QAPP [Connexion au serveur de fichiers Windows]. La description et la version du QAPP s'affichent.
 - c. Utilisez le bouton [Licence] pour activer ce QAPP ; les informations relatives à la commande et à la licence s'afficheront.
 - d. Si ce QAPP n'a pas été commandé en tant que [licence d'usine], démarrez la version de test ou entrez le code de licence que vous avez acheté pour ce QAPP.
2. Configurez un connecteur vers un serveur de fichiers Windows, par exemple, [Mon serveur SMB pour les paramètres].
 - a. Ouvrez le menu [Paramètres].
 - b. Allez dans [Connexions] -> [Connecteurs] -> [SMB].
 - c. Utilisez le bouton [+] pour activer la création d'un nouveau connecteur.
 - d. Attribuez un nom unique à ce connecteur.
 - e. Saisissez le chemin d'accès réseau pour l'hôte et le partage, en veillant à utiliser l'orthographe correcte [/Nom de l'hôte/Nom du partage].
 - f. Saisissez également le nom d'un sous-répertoire sur le serveur, dans lequel enregistrer les fichiers.
 - g. Entrez le nom d'utilisateur et le mot de passe pour l'accès au lecteur autorisé dans votre réseau. Faites attention à la notation correcte ici aussi, en particulier, les lettres majuscules/minuscules.

3.1.2 Application

Les étapes de l'utilisateur :

1. Dans le menu principal, utilisez le bouton [Setup] pour ouvrir le menu des réglages de la balance.
2. Appuyez sur le bouton [Export] dans la barre de navigation et d'outils.
3. Une liste des connecteurs est affichée, via lesquels le fichier de rapport peut être exporté.
4. Sélectionnez le connecteur que vous avez créé, par exemple, [Mon serveur SMB pour les paramètres]. Le fichier de rapport est créé et exporté vers le serveur SMB via le connecteur.
5. Vous obtenez les messages [Rapport envoyé] et [Processus terminé] comme confirmation d'une exportation réussie. Le fichier de rapport au format PDF, avec le fichier de contrôle associé, est maintenant présent sur le serveur et peut être consulté.
6. Si le fichier de rapport n'a pas pu être exporté, alors ce fichier n'est pas perdu, voir Dépannage.

Remarque : le format de fichier PDF est un format de données indépendant de la plate-forme pour les documents. La sortie imprimée dans ce format peut être visualisée sur chaque ordinateur. Pour chaque fichier de sortie PDF, un fichier test correspondant contenant la somme de contrôle (valeur de hachage MD5) des données PDF est créé. Lorsque le fichier est transféré, cette somme de contrôle est enregistrée dans la piste d'audit. À l'aide d'un outil approprié, ce fichier PDF peut être comparé au fichier de contrôle pour garantir l'intégrité des données PDF.

3.1.3 Dépannage

Aucun fichier de rapport exporté vers le répertoire du serveur de fichiers SMB.

1. Assurez-vous que toutes les étapes de configuration mentionnées ci-dessus ont été suivies.
2. Vérifiez que la balance est connectée au réseau, par exemple via un câble Ethernet. L'adresse IP de la balance dans le réseau doit être affichée dans le [Centre d'état] sous [Informations sur l'appareil].
3. Vérifiez le chemin d'accès au réseau dans le connecteur et l'orthographe correcte de Host et Share, ainsi que le

nom d'utilisateur et le mot de passe pour les droits d'accès au serveur de fichiers SMB.

4. Testez la connexion des connecteurs avec le serveur de fichiers SMB en activant le bouton [Info] dans l'aperçu des valeurs définies. Si tous les paramètres sont corrects et que le serveur de fichiers SMB est accessible, vous recevrez un message indiquant que le connecteur est disponible.
5. Si ce n'est pas le cas, vérifiez que le serveur de fichiers SMB est présent sur le réseau et qu'un fichier peut y être enregistré à partir de votre PC.
6. Si le message d'erreur [Échec du transfert] s'affiche, vous pouvez procéder comme suit pour l'exportation :
 - a. Retenter : Réessayer d'exporter le fichier de rapport vers le serveur réseau.
 - b. Réessayer plus tard : L'exportation du fichier de rapport est répétée automatiquement. Les transferts en suspens sont affichés dans le [Centre d'état] sous [Messages].
 - c. Redirection : Vous pouvez rediriger le fichier de rapport vers un autre connecteur.
 - d. Supprimer : L'exportation du fichier de rapport est annulée et supprimée.

3.2 Mise à jour du QAPP Center du serveur FTP

Cet exemple décrit la configuration et l'application de la balance Cubis® MCA, afin de charger la mise à jour du QAPP Center d'un serveur FTP.

Pour transférer des fichiers à partir d'un serveur réseau FTP, une extension QAPP [Connexion à FTP/FTPS] du paquet [Connectivité] est nécessaire. Cette extension peut être utilisée gratuitement pendant 30 jours, après quoi elle doit également faire l'objet d'une licence.

La condition préalable à cette application est un serveur FTP correctement configuré dans votre réseau.

Pour les balances MCA en réseau, cette application permet la mise à jour du QAPP Center à partir d'une source centrale.

3.2.1 Mise en place

Étapes de configuration :

1. Activez l'extension QAPP [Connexion à FTP/FTPS], si cela n'a pas encore été fait.
 - a. Ouvrez le menu [Gestion des tâches], puis le [Centre QAPP].
 - b. Sélectionnez le progiciel [Connectivité], et à l'intérieur de celui-ci, le QAPP [Connexion à FTP/FTPS]. La description et la version du QAPP s'affichent.
 - c. Utilisez le bouton [Licence] pour activer ce QAPP ; les informations relatives à la commande et à la licence s'afficheront.
 - d. Si ce QAPP n'a pas été commandé en tant que [licence d'usine], démarrez la version de test ou entrez le code de licence que vous avez acheté pour ce QAPP.
2. Configurez un connecteur vers un serveur FTP, par exemple, [Mon serveur FTP pour la mise à jour du QAPP Center].
 - a. Ouvrez le menu [Paramètres].
 - b. Allez dans [Connexions] -> [Connecteurs] -> [FTP].
 - c. Utilisez le bouton [+] pour activer la création d'un nouveau connecteur.
 - d. Attribuez un nom unique à ce connecteur.
 - e. Saisissez l'adresse IP du serveur réseau, en veillant à l'orthographe correcte.
 - f. Un numéro de port est nécessaire pour la connexion : le numéro 21 a été attribué. Si nécessaire, vous pouvez saisir un autre numéro de port.
 - g. Pour la mise à jour du QAPP Center, vous pouvez également spécifier un sous-répertoire pour les fichiers stockés sur le serveur.
 - h. Entrez le nom d'utilisateur et le mot de passe pour accéder au serveur FTP. Faites attention à la notation correcte ici aussi, en particulier, les lettres majuscules/minuscules.

3.2.2 Application

Les étapes de l'utilisateur :

1. Dans le menu principal, utilisez le bouton [Setup] pour ouvrir le menu des réglages de la balance.
2. Naviguer vers l'article de menu [Device maintenance] -> [Install QAPP Center]. Une liste de connecteurs est affichée, à l'aide de laquelle un paquet peut être chargé pour mettre à jour le QAPP Center.
3. Sélectionnez le connecteur que vous avez créé, par exemple, [Mon serveur FTP pour la mise à jour du Centre QAPP]. La connexion au serveur FTP est établie et une liste des paquets disponibles pour la mise à jour du QAPP Center est affichée.
4. Sélectionnez la version souhaitée du QAPP Center et confirmez le message de mise à jour.

5. Le QAPP Center est maintenant copié dans la balance depuis le serveur FTP et mis à jour. Comme confirmation, vous obtenez l'affichage de la version mise à jour du QAPP Center.
6. Consultez la section Dépannage, si la mise à jour n'a pas pu être effectuée.

3.2.3 Dépannage

La mise à jour du QAPP Center n'est pas possible via le connecteur.

1. Assurez-vous que toutes les étapes de configuration mentionnées ci-dessus ont été suivies.
2. Vérifiez que la balance est connectée au réseau, par exemple via un câble Ethernet. L'adresse IP de la balance dans le réseau doit être affichée dans le [Centre d'état] sous [Informations sur l'appareil].
3. Vérifiez l'adresse IP et le numéro de port du serveur FTP, ainsi que le nom d'utilisateur et le mot de passe pour les droits d'accès au serveur dans le connecteur.
4. Testez la connexion des connecteurs avec le serveur FTP en activant le bouton [Info] dans l'aperçu des valeurs définies. Si tous les paramètres sont corrects et que le serveur FTP est accessible, vous recevrez un message indiquant que le connecteur est disponible.
5. Vérifiez avec votre PC si le sous-répertoire spécifié ainsi que le fichier de mise à jour du QAPP Center sont présents sur le serveur FTP du réseau.

3.3 Visualisation des entrées de la piste d'audit via un navigateur web

Cet exemple décrit la configuration et l'utilisation de la balance MCA afin que les entrées de la piste d'audit de la balance puissent être consultées à l'aide du navigateur Web.

Le navigateur web [Chrome] est recommandé pour le fonctionnement à distance de la balance MCA.

Une connexion sécurisée de la balance avec le navigateur via le protocole HTTPS nécessite certains certificats de dispositif.

Pour cela, le MCA balance fournit ses propres certificats de dispositif à télécharger. Ces certificats d'appareil doivent être importés dans le navigateur pour l'accès à distance sécurisé au site Web de l'appareil. Il existe une description séparée sur le sujet des [Certificats].

Le champ complet de la piste d'audit ne peut être utilisé qu'après avoir activé l'extension QAPP [piste d'audit] dans le QAPP Center sous [Pharma (QP1)].

Une utilisation de cette application est, par exemple, la télésurveillance centrale des réglages de toutes les balances MCA en réseau.

3.3.1 Mise en place

Étapes de configuration :

1. Activez l'extension du QAPP [Audit trail], si ce n'est pas encore fait.
 - a. Ouvrez le menu [Gestion des tâches], puis le [Centre QAPP].
 - b. Sélectionnez le progiciel [Pharma] et le QAPP [Audit trail] dans celui-ci. La description et la version du QAPP s'affichent.
 - c. Utilisez le bouton [Licence] pour activer ce QAPP ; les informations relatives à la commande et à la licence s'afficheront.
 - d. Si ce QAPP n'a pas été commandé en tant que [licence d'usine], démarrez la version de test ou entrez le code de licence que vous avez acheté pour ce QAPP.
2. Activez le site web du solde du MCA, si ce n'est pas encore fait.
 - a. Ouvrez le menu [Paramètres].
 - b. Allez dans [Connexions] -> [Site Web / services Web].
 - c. Réglez l'élément de menu [Website access] sur [Enabled, no authentication].
3. Si nécessaire, activez l'accès à distance au site web de la balance MCA.
 - a. Ouvrez le menu [Paramètres].
 - b. Allez dans [Connexions] -> [Site web / services web].
 - c. Sous l'élément de menu [Accès à distance], sélectionnez le paramètre [Affichage et télécommande].

3.3.2 Application

Les étapes de l'utilisateur :

1. Démarrez le navigateur web, par exemple [Chrome], sur votre PC.
2. Saisissez l'adresse IP de votre balance, qui est affichée dans le [Centre d'état] sous [Informations sur le

périphérique].

3. Si vous n'avez pas encore importé les certificats de dispositif de la balance dans le navigateur, vous verrez le message [This is not a secure connection] dans le navigateur.
4. En utilisant le bouton [Avancé] et le lien [Suivant...], vous pouvez maintenant accéder à l'adresse IP de la balance, qui dans ce cas est considérée comme non sûre, ou bien vous devez d'abord importer les certificats d'appareil de votre balance dans votre navigateur. Vous trouverez une description séparée au sujet des [Certificats].
5. Sinon, la page [My Cubis] (page d'accueil) est maintenant affichée dans le navigateur.
6. Sélectionnez la page [Audit trail] pour l'exemple.
7. Vous pouvez maintenant trier la liste des entrées selon l'ID, l'horodatage et l'utilisateur.
8. La liste des entrées peut être affichée par ordre croissant ou décroissant.
9. Vous pouvez également définir des filtres, afin de ne visualiser que des groupes spécifiques d'entrées.

3.3.3 Dépannage

La page d'accueil de la balance ne s'affiche pas dans le navigateur.

1. Vérifiez que la balance est connectée au réseau, par exemple via un câble Ethernet. L'adresse IP de la balance dans le réseau doit être affichée dans le [Centre d'état] sous [Informations sur l'appareil].
2. Assurez-vous que l'élément de menu [Accès au site Web] est réglé sur [Activé].

La connexion à la balance est affichée comme [Unsecure] dans le navigateur.

1. Importez les certificats d'appareil de la balance dans votre navigateur. Il existe une description séparée sur le sujet des [Certificats].

La page [Audit trail] ne peut pas être sélectionnée sur la page d'accueil de la balance.

1. Assurez-vous que toutes les étapes de configuration mentionnées ci-dessus ont été suivies. En particulier, l'extension QAPP [Audit trail] a été activée et la licence correspondante est toujours valide.

3.4 Synchroniser la date et l'heure avec un serveur NTP

Cet exemple décrit la configuration et l'application de Cubis® MCA, afin de permettre une synchronisation de la date et de l'heure de la balance avec un serveur NTP.

La condition préalable à cette utilisation est l'accès à un serveur NTP dans votre réseau d'entreprise ou dans le réseau public.

L'écart de temps entre la balance et le serveur NTP est vérifié toutes les 10 minutes. Si l'écart est supérieur à 3 secondes, l'heure de la balance est alors corrigée et la modification est inscrite dans l'audit trail.

Cette application permet une mise à jour et une synchronisation automatiques de la date et de l'heure sur toutes les balances MCA en réseau.

3.4.1 Mise en place

Étapes de configuration :

1. Mettre en place une configuration NTP active.
 - a. Ouvrez le menu [Paramètres].
 - b. Naviguez jusqu'à [Paramètres du périphérique] -> [Date et heure] -> [Configuration NTP].
 - c. Activez la configuration des paramètres du serveur NTP à l'aide du bouton [Edit].
 - d. Réglez l'élément de menu [NTP operating status] sur [Enabled].
 - e. Dans le champ [Server IP], entrez l'adresse du serveur NTP au format IPv4, par exemple 192.53.103.108. (Il s'agit d'un serveur NTP de l'Institut fédéral physico-technique de Braunschweig, en Allemagne).
 - f. Confirmez la configuration du NTP en cliquant sur le bouton [OK].
 - g. Testez la connexion au serveur NTP en activant le bouton [Info] dans l'aperçu de la configuration NTP.
2. Réglez le fuseau horaire correspondant à votre emplacement.
 - a. Ouvrez le menu [Paramètres].
 - b. Naviguez jusqu'à [Paramètres du périphérique] -> [Date et heure] -> [Définir la date et l'heure].
 - c. Activez les paramètres de date et d'heure à l'aide du bouton [Modifier].
 - d. Réglez votre emplacement en utilisant l'élément de menu [Fuseau horaire], [UTC +/- heure, lieu]. Ensuite, l'heure et la date s'affichent en fonction de votre heure locale.

Remarque : après avoir réglé la date, l'heure et le fuseau horaire, le MCA balance vous demande de redémarrer le système.

3.4.2 Dépannage

Aucune connexion possible avec le serveur NTP.

1. Assurez-vous que toutes les étapes de configuration mentionnées ci-dessus ont été suivies.
2. Vérifiez que la balance est connectée au réseau, par exemple via un câble Ethernet. L'adresse IP de la balance dans le réseau doit être affichée dans le [Centre d'état] sous [Informations sur l'appareil].
3. Vérifiez avec votre PC, si vous pouvez accéder à l'adresse IP du serveur NTP.

4 Annexe

4.1 Bâtons Wi-Fi compatibles

Cubis® MCA supporte les clés Wi-Fi les plus courantes (adaptateurs WLAN USB) disponibles sur le marché.

Gardez à l'esprit les éléments suivants lors du choix d'une clé Wi-Fi :

1. Évitez les bâtons Wi-Fi sans nom. Achetez toujours une marque connue.
2. Si possible, vérifiez la fiche technique de la clé Wi-Fi pour vous assurer qu'elle contient l'un des jeux de puces pris en charge suivants.

Les jeux de puces Wi-Fi pris en charge sont les suivants :

- Atheros - AR5523, AR9271, AR6004
- Atmel - at76c503, at76c505 or at76c505a
- Broadcom - BCM43235 (Revision 3), BCM43236 (Revision 3), BCM43238 (Revision 3), BCM43143, BCM43242, BCM43566, BCM43569
- Intersil's Prism54 chips - ISL38xx
- Marvell - Libertas 8388, Libertas 8682, 8766/8797/8897
- Ralink - RT2571, RT2571W, RT2572, RT2573 & RT2671 (no firmware), RT2770, RT2870 & RT3070, RT3071 & RT3072 & RT3370 (rt2870.bin)
- Realtek - RTL8192CU/RTL8188CU, RTL8712U/RTL8192SU, RTL8188EU, RTL8187 and RTL8187B
- Redpine Signals Inc - 91x
- ZyDAS - ZD1201, ZD1211/ZD1211B

5. Abréviations

DHCP	Dynamic Host Configuration Protocol	Un protocole de communication dans le domaine de l'informatique. Il permet l'attribution de la configuration du réseau aux clients par un serveur.
DNS	Domain Name System	Système de résolution des noms d'ordinateurs en adresses IP et vice versa.
FTP	File Transfer Protocol	Protocole réseau standard pour le transfert de fichiers entre un client et un serveur au sein d'un réseau.
FTPS	FTP over TLS	Une méthode pour crypter le protocole de transfert de fichiers (FTP).
HTTPS	Hypertext Transfer Protocol Secure	Un protocole de communication avec lequel les données peuvent être transmises sous forme cryptée.
IPv4	Internet Protocol version 4	Protocole Internet de la version 4.
IPv6	Internet Protocol version 6	Protocole Internet de la version 6.
MAC address	Media Access Control address	Adresse matérielle physique, identifiant unique du dispositif dans le réseau.
NTP	Network Time Protocol	Une norme pour la synchronisation des horloges dans les systèmes informatiques.
PNG	Portable Network Graphics	Portable network graphics, un format graphique matriciel avec compression des données sans perte.
PSK	Pre-shared key	Méthode de cryptage dans laquelle la clé doit être connue des deux participants avant la communication.
REST	Representational State Transfer	Paradigme de programmation pour les systèmes distribués, notamment pour les services web.
SMB	Server Message Block	Protocole réseau pour les services de fichiers, d'impression et d'autres serveurs dans les réseaux informatiques.
SSID	Service Set Identifier	Nom de réseau librement sélectionnable, par exemple pour le Wi-Fi.
URL	Uniform Resource Locator	Identification pour les adresses Internet ou Web.
UTC	Universal Time, Coordinated	Le temps mondial, également appelé temps terrestre ou temps universel.
WEP	Wired Equivalent Privacy	Protocoles de cryptage standard pour WLAN.
Wi-Fi	Wireless Fidelity	Réseau sans fil, synonyme de WLAN.
WLAN	Wireless Local Area Network	Sans fil, réseau local.
WPA	Wi-Fi Protected Access	Méthodes de cryptage pour un réseau sans fil. Successeur de WEP.
WPA2	Wi-Fi Protected Access 2	Mise en place d'une norme de sécurité pour les réseaux radio. Successeur du WPA.