

Beschreibung Netzwerk, Ethernet und Wi-Fi (WLAN) für Cubis® MCA Waage

Dieses Dokument beschreibt die Verbindung der Waage mit einem Netzwerk per Ethernet und Wi-Fi (WLAN). In Beispielen werden das Einrichten und die Anwendung in der Praxis beschrieben.



Zusammenfassung

Die Cubis® MCA Premium Laborwaage bietet umfassende und flexible Konnektivitätsoptionen zur Integration der Waage in die Labor-IT. Eine große Anzahl an standardisierten IT-Protokollen, wie REST-Webservice, SMB oder LDAP, stehen über Ethernet und Wi-Fi zu Verfügung und ermöglichen die direkte Einbindung ohne die Verwendung einer zusätzlichen Middleware. Darüber hinaus kann die Cubis® mit einem Webbrowser über das Netzwerk ferngesteuert und Audit Trail und andere Statusinformationen eingesehen werden.

1	Netzwerkverbindung Ethernet und Wi-Fi	4
1.1	Allgemeine Einstellungen	4
1.2	Ethernet (LAN)	4
1.2.1	Protokoll IPv4	5
1.2.2	Protokoll IPv6	5
1.2.3	DNS 1 und DNS 2	5
1.3	Wi-Fi (WLAN)	5
1.3.1	Wi-Fi SSID und Passwort	6
1.3.2	Protokoll IPv4/IPv6 und DNS 1/2	6
2	Netzwerkdienste	6
2.1	Serielle Kommunikation	6
2.1.1	SBI Protokoll	6
2.1.2	xBPI Protokoll	7
2.1.3	SICS Protokoll	7
2.1.4	QAPP-Direkt	7
2.2	Netzwerkkonnectoren	7
2.2.1	YDP30-NET	7
2.2.2	Netzwerk-Drucker	7
2.2.3	FTP / FTPS	7
2.2.4	SMB Protokoll	8
2.3	Website	8
2.3.1	Webservices	8
2.4	NTP-Server für Datum und Zeit	8
2.5	Zertifikate	8
2.5.1	Betreiberpflichten	8
2.5.2	Gerätzertifikat zurücksetzen	9
2.5.3	Zertifikate installieren und aktualisieren	9
2.5.3.1	Client-Zertifikate	9
2.5.3.2	CA-Zertifikate	9
2.5.3.3	Zertifikatsdateitypen	9
2.5.4	Zertifikattypen	10
2.5.4.1	CA-Zertifikate	10
2.5.4.2	Unbekannte Zertifizierungsstellen	10
2.5.4.3	Gerätezertifikate	10
2.5.4.4	Wifi-Zertifikate	11
2.5.4.5	LDAPS-Zertifikate	11
2.5.5	Sichere Netzwerkverbindungen mit SSL/TLS	11
2.5.5.1	Unbekannte Zertifizierungsstellen	11
3	Anwendungsbeispiele	11
3.1	Report der Menü-Einstellungen auf Windows File Server	12
3.1.1	Einrichten	12
3.1.2	Anwenden	12
3.1.3	Fehlerbehandlung	12

3.2 Aktualisierung des QAPP Center von FTP Server	13
3.2.1 Einrichten	13
3.2.2 Anwenden	13
3.2.3 Fehlerbehandlung	14
3.3 Audit Trail Einträge per Webbrowser einsehen	14
3.3.1 Einrichten	14
3.3.2 Anwenden	14
3.3.3 Fehlerbehandlung	15
3.4 Datum und Zeit mit NTP Server synchronisieren	15
3.4.1 Einrichten	15
3.4.2 Fehlerbehandlung	16
4 Anhang	16
4.1 Kompatible Wi-Fi-Sticks	16
5. Abkürzungen	17

1 Netzwerkverbindung Ethernet und Wi-Fi

Der Anschluss einer Cubis® MCA-Waage an ein TCP-/IP-basiertes Netzwerk kann kabelgebunden über den Ethernet-Anschluss (RJ45 Buchse) und kabellos über einen Wi-Fi USB Adapter (WLAN-Stick) erfolgen.

Die Übertragungsraten der Netzwerkverbindung sind 10 Mbit/sec (10BASE-T, Ethernet) und 100 Mbit/sec (100BASE-TX, Fast Ethernet).

Der Ethernet-Anschluss erfolgt mit einem Verbindungskabel, CAT-5 oder höher, paarweise verdreht, abgeschirmt, 1:1, UTP / STP, Stecker RJ45; z. B. Patchkabel CAT-5 je nach Einsatz (straight/crossover).

Für eine kabellose Verbindung unterstützt die Cubis® MCA die gängigsten Wi-Fi USB Adapter (WLAN-Sticks) die auf dem Markt angeboten werden.

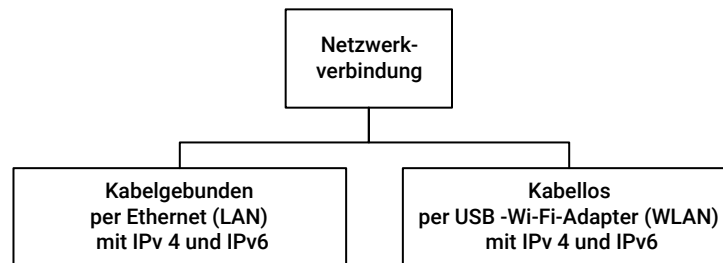


Abbildung 1: Netzwerkverbindung

Die Cubis® MCA-Waage kann auf Ethernet und Wi-Fi jeweils eine IPv4 und eine IPv6 Adresse haben, d. h. damit bis zu 4 Adressen.

Über die Netzwerkverbindungen Ethernet (LAN) und Wi-Fi (WLAN) bietet die Cubis® MCA-Waage gleichzeitig mehrere Netzwerkdienste.

1.1 Allgemeine Einstellungen

Der Hostname der Waage setzt sich ab Werk aus der Bezeichnung der Serie und den letzten 3 Bytes der MAC-Adresse zusammen, z. B. [cubis-1a477e]. Der Hostname kann frei gewählt werden, muss aber in einem Netzwerk eindeutig sein.

1.2 Ethernet (LAN)

Für den Ethernet-Anschluss der Waage kann das Protokoll IPv4 als auch IPv6 genutzt werden. Für jedes Protokoll ist getrennt einstellbar, ob die IP-Adresse automatisch bezogen werden soll oder ob die Waage dafür eine feste IP-Adresse erhält. Das jeweilige Protokoll kann auch ganz ausgeschaltet werden.

In der Übersicht der Einstellungen für Ethernet wird über den Status angezeigt, ob eine Verbindung zum Netzwerk besteht. Außerdem wird hier die eindeutige MAC-Adresse der Waage dargestellt, z. B. [00:30:D6:1F:77:569].

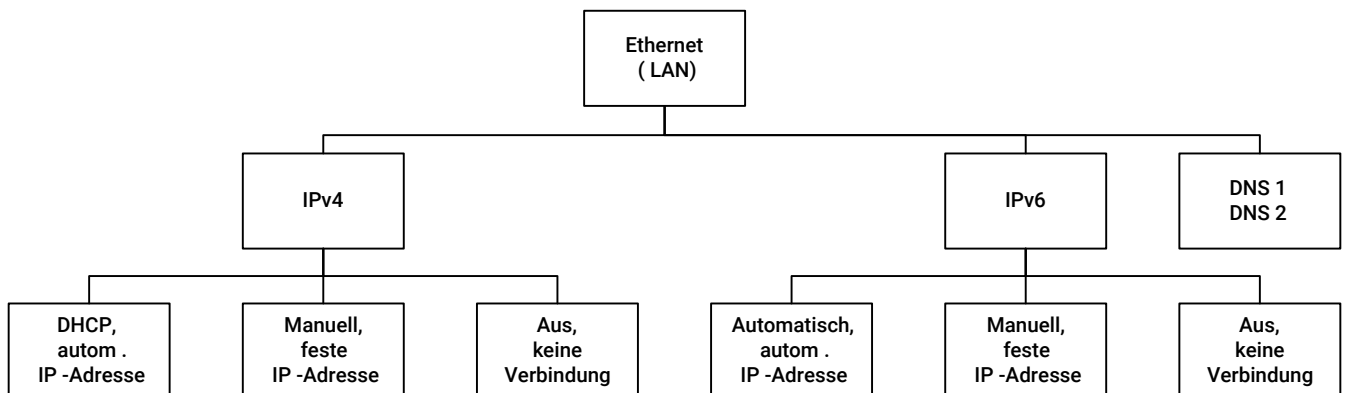


Abbildung 2: Ethernet mit IPv4/IPv6

Für den Betrieb mit einer festen IP-Adresse muss neben der IP-Adresse, je nach Protokoll, noch zusätzlich bei IPv4 die Subnetz-Maske und das Gateway bzw. bei IPv6 noch die Präfix-Länge und das Gateway manuell eingegeben werden.

werden. Die Eingabe des Gateways ist optional und nur erforderlich, wenn eine Verbindung zum Internet benötigt wird.

Alle nötigen Angaben dazu kann der zuständige Netzwerk-Administrator für das Firmen-Netzwerk liefern.

1.2.1 Protokoll IPv4

Die IP-Adresse beim Protokoll IPv4 (4*8 Bit=32 Bit) besteht aus 4 Dezimalzahlen zwischen 0 und 255, die durch einen Punkt voneinander abgetrennt werden, z. B. [123.4.56.123]. Für die Eingabe der festen IP-Adresse, der Subnet-Maske und das Gateway gilt dieses Format.

1.2.2 Protokoll IPv6

Die IP-Adresse beim Protokoll IPv6 (8*16Bit=128 Bit) besteht aus 8 alphanumerischen Hexa-Dezimalzahlen zwischen 0 und FFFF die durch einen Doppelpunkt voneinander abgetrennt werden, z. B. [ecb1:d583:6341:baf76:0:0:0:1].

Die ersten 4 Blöcke (64 Bit) bilden den Präfix und die letzten 4 Blöcke den Interface Identifier. An die Stelle der IPv4-Netzmaske und der IPv4-Netzwerkadresse treten bei IPv6 die Präfixlänge und das Präfix. Die Präfixlänge gibt die Anzahl der Bits an, die das Präfix bilden. Typische Präfixlänge ist 64. Das Präfix ersetzt bei IPv6 die Subnetzmaske.

1.2.3 DNS 1 und DNS 2

Das DNS (Domain Name System) dient in IP-basierten Netzwerken der Beantwortung von Anfragen zur Namensauflösung. Ein Netzwerk kann mehrere DNS-Server haben, die Cubis® MCA unterstützt die Eingabe von zwei Servern.

Für jeden DNS-Server kann die IP-Adresse oder der Servername eingegeben werden.

Bei DHCP werden die DNS-Server automatisch vom DHCP Server bereitgestellt. In diesem Fall werden DNS1 und DNS2 zusätzlich zu der DNS-Serverliste hinzugefügt.

1.3 Wi-Fi (WLAN)

An die MCA Waage kann ein Wi-Fi USB Adapter (WLAN-Stick) angeschlossen werden, mehrere Adapter dieser Art werden nicht unterstützt.

In der Übersicht der Einstellungen für Wi-Fi (WLAN) wird über den Status angezeigt, ob ein entsprechender Wi-Fi USB Adapter angeschlossen und mit dem Netzwerk verbunden ist.

Status Anzeige

- Kein Gerät vorhanden - Kein Wi-Fi USB Adapter angeschlossen.
- Getrennt - Keine Verbindung mit dem Wi-Fi Netzwerk, z. B. nicht mit Wi-Fi SSID und Passwort angemeldet.
- Bereit - Verbindung mit dem Wi-Fi Netzwerk vorhanden.
- Online - Verbindung mit dem Wi-Fi Netzwerk und zum Internet vorhanden.

Wenn eine Verbindung besteht, dann wird hier auch die eindeutige MAC-Adresse des Wi-Fi USB Adapters dargestellt, z. B. 34:C9:F0:89:6F:D6.

Im Anhang das Kapitel: Kompatible Wi-Fi-Sticks.

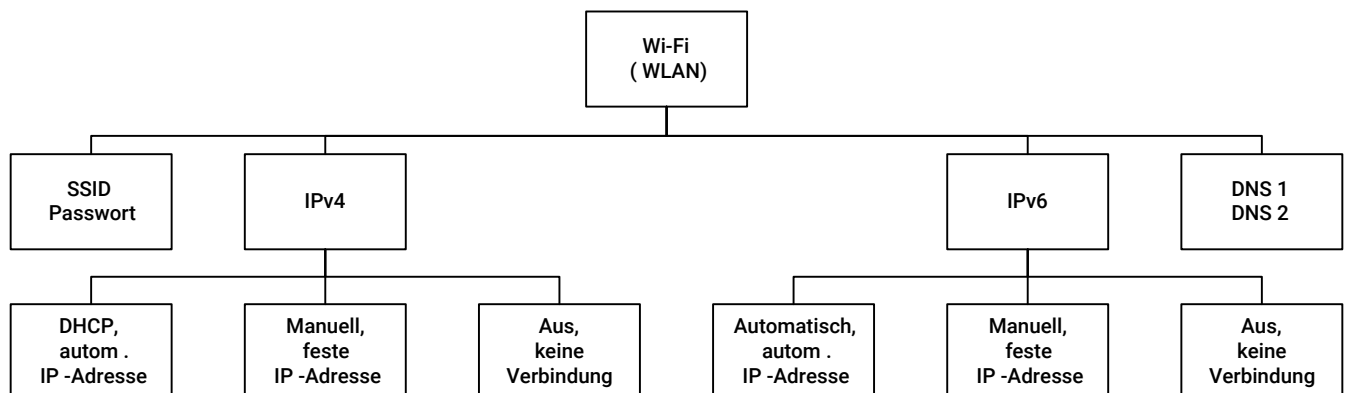


Abbildung 3: Wi-Fi mit IPv4/IPv6

Für den Betrieb mit einer festen IP-Adresse muss neben der IP-Adresse je nach Protokoll noch zusätzlich bei IPv4 die Subnetz-Maske und das Gateway bzw. bei IPv6 noch die Präfix-Länge und das Gateway manuell eingegeben werden. Die Eingabe des Gateways ist optional und nur erforderlich, wenn eine Verbindung zum Internet benötigt wird.

Alle nötigen Angaben dazu kann der zuständige Netzwerk-Administrator für das Firmen-Netzwerk liefern.

1.3.1 Wi-Fi SSID und Passwort

Zur Verbindung mit einem Wi-Fi Netzwerk muss die Wi-Fi SSID (der eindeutige Wi-Fi Netzwerkname) und das Wi-Fi Passwort (der Wi-Fi Netzwerkschlüssel) eingegeben werden.

Die MCA Waage unterstützt zur Authentifizierung die Standards WEP, WPA-PSK und WPA2-PSK und somit das PSK Verfahren zur Verschlüsselung.

1.3.2 Protokoll IPv4/IPv6 und DNS 1/2

Für das Protokoll IPv4 und IPv6 sowie für DNS 1 und DNS 2, gilt bei Wi-Fi (WLAN) die gleiche Beschreibung wie bei Ethernet (LAN).

2 Netzwerkdienste

Die Cubis® MCA-Waage bietet über das Netzwerk mehrere Dienste an: eine serielle Kommunikation mit verschiedenen Protokollen, Konnektoren zur Verbindung mit Netzwerk-Massenspeichern und Druckern, eine Website und Webservice für den Remote Zugriff (Fernbedienung) sowie den Anschluss an einen NTP Server zur Synchronisierung von Datum und Zeit.

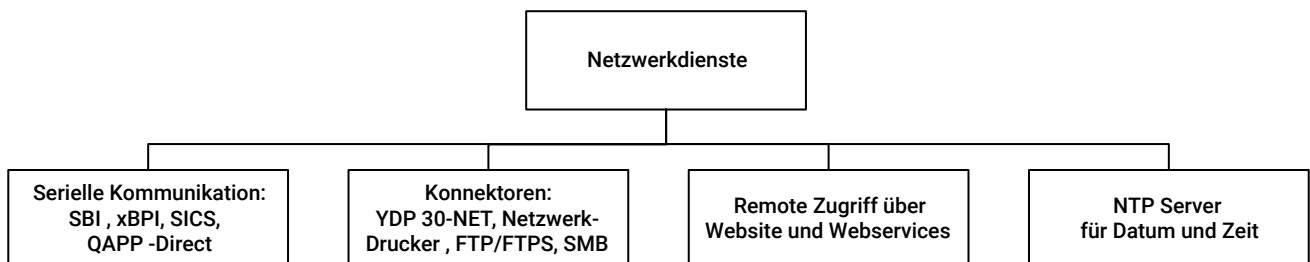


Abbildung 4: Netzwerkdienste

2.1 Serielle Kommunikation

Es besteht die Möglichkeit, über den Netzwerk-Anschluss die seriellen Kommunikations-Protokolle SBI, xBPI, SICS, miniSICS zu nutzen, die unabhängig von der aktiven Task und deren Anwendung betrieben werden können. Für diese Client/Server Verbindung ist die Einstellung von einem gemeinsamer TCP Port erforderlich.

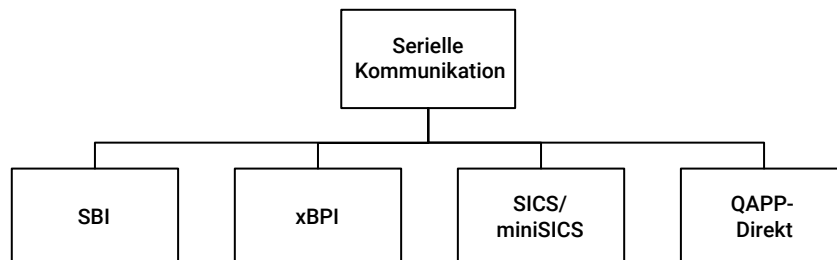


Abbildung 5: Serielle Kommunikation via Netzwerk

2.1.1 SBI Protokoll

Mit diesem einfachen ASCII-basierten Protokoll können die grundlegenden Funktionen der Waage mit ESC-Befehlen gesteuert werden. Die Ausgabe von Anzeigewerten kann einzeln durch ESC-Befehl angefordert werden oder automatisch mit jedem neuen Wägewert im Zyklus der Anzeigefolge oder automatisch in bestimmten Zeitintervallen erfolgen. Es kann eingestellt werden das die Ausgabe nur mit Stabilität oder ohne Stabilität vom Anzeigewert ausgeführt werden soll. Das Ausgabeformat kann mit oder ohne Kennzeichnung (Header) gewählt werden.

Die SBI Befehle und Ausgabeformate sind in einer separaten Schnittstellenbeschreibung zu finden.

2.1.2 xBPI Protokoll

Dieses binäre Protokoll bietet einen erweiterten Befehlsumfang. Damit können zahlreiche Funktionen der Waage gesteuert werden.

Zu den möglichen xBPI Befehlen gibt es eine separate Schnittstellenbeschreibung.

2.1.3 SICS Protokoll

Das Protokoll SICS (Standard Interface Command Set) stellt eine Kompatibilität zum MT-SICS Protokoll der Fa. Mettler her und ermöglicht es Befehle für die grundlegenden Funktionen an die Waage zu senden. Es ist zu beachten, dass es aber Unterschiede aufgrund der unterschiedlichen Hardware- / Softwareplattformen gibt.

Die in der MCA Waage realisierten SICS und miniSICS Befehle sind in einer separaten Schnittstellenbeschreibung zu finden.

2.1.4 QAPP-Direkt

Nur spezielle QAPPs, die durch eine Task gestartet werden, können die Schnittstelle für ihre Zwecke der Eingabe und Ausgabe nutzen. Die Möglichkeiten der Ein- und Ausgabe über die Schnittstelle sind in der jeweiligen speziellen QAPP beschrieben.

2.2 Netzwerkkonnektoren

In der Cubis® MCA stellen die Konnektoren die Verbindung zu Netzwerk-Servern her, die als Drucker oder Massenspeicher genutzt werden sollen.

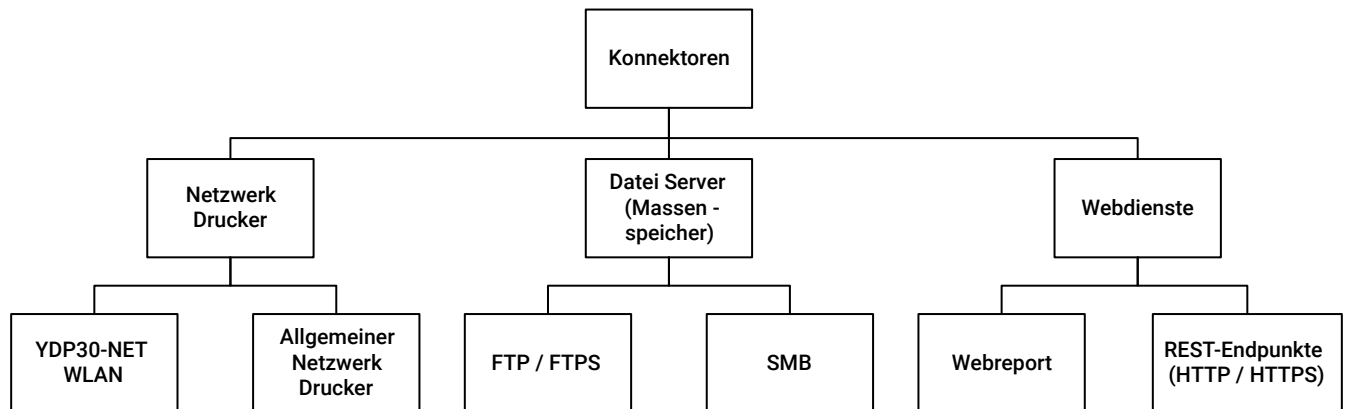


Abbildung 6: Netzwerk Konnektoren

Als Netzwerk-Drucker kann der YDP30-NET per WLAN oder ein allgemeiner Netzwerk-Drucker in einem unabhängigen Wi-Fi-Netzwerk oder Firmennetzwerk per DHCP angebunden werden.

Für die Verbindung zu einem Massenspeicher, wie Windows File Server, FTP/FTPS oder STARLIMS ist eine spezielle QAPP-Erweiterung erforderlich, die über das QAPP Center unter [Connectivity] freigeschaltet werden muss.

2.2.1 YDP30-NET

Dieser Konnektor ist für den Anschluss von einem Drucker YDP30-NET per Kabel (LAN) oder schnurlos (WLAN) vorgesehen. Für den Konnektor muss ein Konnektor Name, eine IP-Adresse oder ein Host Name vom Drucker sowie eine vereinbarte Port Nummer zwischen Drucker und Waage eingetragen werden.

Die schnurlose Anbindung des Druckers YDP30-NET per Wi-Fi ist in einer separaten Anleitung beschrieben.

2.2.2 Netzwerk-Drucker

Der Konnektor Netzwerk-Drucker ermöglicht die Verbindung zu in einem z. B. A4-Drucker in einem unabhängigen Wi-Fi-Netzwerk mit Standard-Wi-Fi-Komponenten oder in einem Firmennetzwerk per DHCP mit Standard-Authentifizierungsmethoden. Der Netzwerk-Drucker muss IPP (Internet Printing Protocol) unterstützen.

Für den Konnektor muss ein Konnektor Name, eine IP-Adresse oder ein Host Name vom Drucker eingegeben sowie das Protokoll für die Übertragung eingestellt werden.

In der separaten Beschreibung [Druckkonzept] ist das Einrichten und Anwenden eines Netzwerk-Druckers in einem Anwendungsbeispiel beschrieben.

2.2.3 FTP / FTPS

Das File Transfer Protocol (FTP) ist ein Standard-Netzwerkprotokoll für die Übertragung von Computerdateien

zwischen einem Client und einem Server in einem Computernetzwerk.

Die Waage ist der FTP-Client und kann über das Protokoll Dateien auf einen FTP-Server ablegen bzw. Dateien von einem FTP-Server holen. Bei FTPS ist die Verbindung zusätzlich verschlüsselt, die dafür erforderlichen Zertifikate sind separat beschrieben.

Für die Verbindung zu einem FTP / FTPS Server muss ein Konnektor erstellt werden mit einem eindeutigen Namen, der IP-Adresse und Port Nummer vom Netzwerk-Server, ggf. ein Unterverzeichnis auf dem Server und der Benutzername und das Passwort.

Hinweis: Durch mehrere auf der Waage angelegte Konnektoren zum selben Server, aber mit unterschiedlichen Unterverzeichnissen kann das Ablegen von Daten je nach Thema (Backup, Report, ...) leicht strukturiert werden.

2.2.4 SMB Protokoll

Der Konnektor Windows File Server verwendet das SMB-Netzwerkprotokoll. Dieses Protokoll ermöglicht den Zugriff auf freigegebene Netzlaufwerke von Windows- oder Linux-Rechnern, um dort Datendateien in ausgewählte Zielverzeichnisse abzulegen bzw. abzuholen.

2.3 Website

Die Website der MCA Waage kann einfach über die IP-Adresse der Waage mit einem Webbrowser angezeigt werden. Die Seite [Meine Cubis] (Homepage) zeigt die gesetzten Geräte IDs, allgemeinen Geräteinformationen der Waage und Informationen zum Service.

Über die Seite [Fernbedienung] kann je nach Einstellung im Menü entweder [Nur Anzeige] oder [Anzeige und Steuerung] der MCA Waage per Browser erfolgen.

Die Seite [Screenshot] erstellt eine PNG-Datei, von der aktuellen Anzeige, die gespeichert werden kann.

Falls im QAPP Center im Paket [Pharma] die QAPP-Erweiterung [Audit Trail] aktiviert wurde, dann wird noch die Website [Audit Trail] angezeigt. Die Einträge im Audit Trail können nach Themen gefiltert, sortiert und exportiert werden.

Der Zugang zur Website kann per Menü komplett deaktiviert werden und damit auch die Remote Bedienung per REST Webservice.

2.3.1 Webservices

Die Remote Bedienung (Fernbedienung) der grundlegenden Funktionen der MCA Waage kann auch über einen REST Webservice erfolgen.

Zu den verfügbaren REST-Webdiensten der MCA Waage gibt es eine separate Beschreibung.

2.4 NTP-Server für Datum und Zeit

Die Cubis® MCA bietet die Möglichkeit zur Synchronisierung von Datum und Zeit mit einem NTP-Server. Dazu kann in den Geräteeinstellungen der MCA, unter Datum/Zeit und NTP Konfiguration, die Verbindung mit dem Server aktiviert und die IP-Adresse für den Server eingegeben werden.

2.5 Zertifikate

Die Cubis® MCA Waage unterstützt die Verwendung von Zertifikaten für eine vertrauensvolle Integration in die lokale IT-Infrastruktur. Die MCA kann Zertifikate von vertrauenswürdigen Zertifizierungsstellen (CA) verarbeiten, um vertrauenswürdige Server zu identifizieren. Die MCA stellt außerdem eigene Gerätezertifikate zum Download bereit. Diese Gerätezertifikate werden vor allem für die sichere Kommunikation und Authentifizierung verwendet (z.B. FTPS, HTTPS, Webservices).

Stammzertifikate haben eine begrenzte Gültigkeitsdauer und müssen in regelmäßigen Abständen erneuert werden. Das Ablaufen eines Stammzertifikats hat keine Auswirkungen auf die Kernfunktionen oder Daten der Waage selbst. Die Waage zeigt einige Wochen vor Ablauf der Gültigkeit eine Warnung an.

Gerätezertifikate basieren auf dem X.509-Standard und nutzen die Public-Key-Kryptografie, bei der ein Schlüsselpaar aus öffentlichem und privatem Schlüssel zum Einsatz kommt. Dieses Schlüsselpaar ermöglicht die verschlüsselte Datenübertragung, die Überprüfung digitaler Signaturen sowie eine zuverlässige Identitätsauthentifizierung. Abhängig von der Art und Weise, wie der private Schlüssel erstellt und gespeichert wird, kann es erforderlich sein, ihn vor der Verwendung mit einer Passphrase zu entschlüsseln.

2.5.1 Betreiberpflichten

Sartorius Cubis® MCA Waagen werden mit vorinstallierten Gerätezertifikaten ausgeliefert, die eine beschränkte Gültigkeit haben. Die Betreiber haben die Möglichkeit, die ursprünglich installierten Zertifikate zu erneuern und

eigene Zertifikate zu importieren.

Die Verwaltung und Aktualisierung sowie die Sicherstellung der Gültigkeit liegt in der Pflicht des Betreibers. Um mögliche Sicherheitswarnungen oder Einschränkungen bei sicheren Verbindungen zu vermeiden, ist es wichtig, dass die Gültigkeit der Zertifikate regelmäßig überprüft und bei Bedarf erneuert wird.

Die Aktualisierung des Zertifikats hat weder Auswirkungen auf die Wägefunktion noch auf die Einbindung in die lokale IT-Infrastruktur. Daher ist bei der Aktualisierung der Zertifikate eine Requalifizierung oder Revalidierung der Geräte nicht erforderlich.

2.5.2 Gerätzertifikat zurücksetzen

Sollte nach dem Zurücksetzen des Zertifikats eine Warnung über den Zertifikatsablauf angezeigt werden, aktualisieren Sie das Zertifikat bitte gemäß Kapitel Zertifikate aktualisieren

1. Stellen Sie die Zertifikatsdateien so bereit, dass sie über einen Konnektor des Geräts erreicht werden können, beispielsweise auf einem USB-Speicher und dem USB-Konnektor
2. Navigieren Sie vom Hauptmenü aus zu den Einstellungen
3. Navigieren Sie im Menü Verbindungen in das Untermenü Zertifikate
4. Systemzertifikate und anschließend Gerätzertifikate auswählen
5. Wählen Sie das Symbol „Papierkorb“, um Zertifikate zu erneuern und bestätigen Sie die Meldung „Zertifikate zurücksetzen“ mit „Ja“.
6. Prüfen Sie, ob das neue Zertifikat „Sartorius Factory Authority“ verfügbar ist. Dieses Zertifikat wird im Jahr 2043 ablaufen.
7. Wenn „Sartorius Factory Authority“ in der Liste sichtbar ist, war die Aktualisierung erfolgreich, und es wird ein Audit Trail-Eintrag erstellt.

Sollte nach dem Zurücksetzen des Zertifikats eine Warnung über den Zertifikatsablauf angezeigt werden, aktualisieren Sie das Zertifikat bitte gemäß Kapitel Zertifikate aktualisieren

2.5.3 Zertifikate installieren und aktualisieren

Um ein Zertifikat zu installieren oder zu aktualisieren, folgen Sie dieser Anleitung.

2.5.3.1 Client-Zertifikate

1. Stellen Sie die Zertifikatsdateien so bereit, dass sie über einen Konnektor des Geräts erreicht werden können, beispielsweise auf einem USB-Speicher und dem USB-Konnektor
2. Navigieren Sie vom Hauptmenü aus zu den Einstellungen
3. Navigieren Sie im Menü Verbindungen in das Untermenü Zertifikate
4. Navigieren Sie in das entsprechende Menü, für das ein Zertifikat installiert werden soll. Die Unterscheidung und Erläuterung der Zertifikate finden Sie im Kapitel Zertifikatstypen
5. Betätigen Sie die Schaltfläche [IMPORT] und wählen den entsprechenden Konnektor, über den die zu installierenden Zertifikatsdateien erreichbar sind.
6. Wählen Sie [Zertifikat] und selektieren Sie die Zertifikatsdatei mit dem öffentlichen Schlüssel aus der Liste der über den Konnektor verfügbaren Dateien. Folgende Formate werden unterstützt: .pem und .crt
7. Wählen Sie [Privater Schlüssel] und selektieren Sie die Zertifikatsdatei mit dem privaten Schlüssel aus der Liste der über den Konnektor verfügbaren Dateien. Folgende Formate werden unterstützt: .key
8. Wählen Sie [Privater Schlüssel Passwort] und geben Sie das Passwort des privaten Schlüssels ein.
9. Bestätigen Sie den Import. Die Dateien werden nach erfolgreicher Prüfung in das System übertragen.

2.5.3.2 CA-Zertifikate

1. Stellen Sie die Zertifikatsdateien so bereit, dass sie über einen Konnektor des Geräts erreicht werden können, beispielsweise auf einem USB-Speicher und dem USB-Konnektor
2. Navigieren Sie vom Hauptmenü aus zu den Einstellungen
3. Navigieren Sie im Menü Verbindungen in das Untermenü Zertifikate
4. Navigieren Sie in das entsprechende Menü, für das ein Zertifikat installiert werden soll. Die Unterscheidung und Erläuterung der Zertifikate finden Sie im Kapitel Zertifikatstypen
5. Betätigen Sie die Schaltfläche [IMPORT] und wählen den entsprechenden Konnektor, über den die zu installierenden Zertifikatsdateien erreichbar sind.
6. Selektieren Sie die Zertifikatsdatei aus der Liste der über den Konnektor verfügbaren Dateien. Folgende Formate werden unterstützt: .pem und .crt

2.5.3.3 Zertifikatsdateitypen

Eine kurze Einführung in die PKI: Schlüssel bestehen aus zwei Hälften, einem öffentlichen und einem privaten Schlüssel. Der öffentliche Schlüssel kann öffentlich und weit verbreitet werden, und Sie können ihn verwenden, um

Informationen, die mit dem privaten Schlüssel erzeugt wurden, zu überprüfen, aber nicht zu vervielfältigen. Der private Schlüssel muss geheim gehalten werden.

- .key-Dateien sind im Allgemeinen der private Schlüssel, der vom Server zum Verschlüsseln und Verpacken von Daten zur Überprüfung durch die Clients verwendet wird.
- .pem-Dateien sind in der Regel der öffentliche Schlüssel, der vom Client zur Überprüfung und Entschlüsselung der von Servern gesendeten Daten verwendet wird. PEM-Dateien können auch verschlüsselte private Schlüssel sein.
- In .p12-Dateien sind beide Hälften des Schlüssels eingebettet, so dass Administratoren die Schlüsselhälften leicht verwalten können.
- .cert- oder .crt-Dateien sind die signierten Zertifikate mit einem öffentlichen Schlüssel, Informationen über den Schlüsselbesitzer und die digitale Signatur der Zertifizierungsstelle, die das Zertifikat ausgestellt hat. Damit kann ein System von einer dritten Partei als vertrauenswürdig eingestuft werden.
- In .cer-Dateien liegen die Zertifikate normalerweise in einem Binär- oder Base64-Format vor. Sie unterscheiden sich damit in ihrer Codierung zu .crt-Dateien.

2.5.4 Zertifikattypen

Für den sicheren Verbindung zu Netzdiensten benötigt die Waage unterschiedliche Zertifikate, die auf die Waage geladen werden können. Es wird zwischen folgenden Zertifikaten unterschieden:

- CA-Zertifikate (Vertrauenswürdige Zertifizierungsstellen)
- Gerätezertifikate
- WiFi-Authentifizierungszertifikat
- LDAPS-Zertifikat

2.5.4.1 CA-Zertifikate

Ein CA-Zertifikat (engl. Certificate Authority Certificate) ist ein digitales Zertifikat, das von einer vertrauenswürdigen Stelle – der sogenannten Zertifizierungsstelle oder Certificate Authority (CA) – ausgestellt wird. Sein Zweck besteht darin, die Echtheit und Vertrauenswürdigkeit eines Kommunikationspartners oder Dienstes zu bestätigen. Wenn zwei Geräte oder Programme über ein Netzwerk miteinander kommunizieren, ermöglicht ein CA-Zertifikat beiden Seiten, sicherzustellen, dass sie tatsächlich mit dem gewünschten Kommunikationspartner verbunden sind und nicht mit einem Angreifer, der sich als dieser ausgibt.

Wird ein CA-Zertifikat als vertrauenswürdig eingestuft, akzeptiert das Gerät automatisch alle davon abgeleiteten Zertifikate. Auf diese Weise entsteht eine sogenannte Zertifikatskette, die vom Root-CA-Zertifikat bis zum jeweiligen Gerätezertifikat zurückverfolgt werden kann. Eine Auswahl vertrauenswürdiger Zertifizierungsstellen ist bereits auf dem Gerät vorinstalliert.

2.5.4.2 Unbekannte Zertifizierungsstellen

Im Gerät besteht die Möglichkeit, auch Zertifikaten zu vertrauen, die nicht von einer bekannten Zertifizierungsstelle ausgestellt wurden. Aktiviert man diese Option, akzeptiert das Gerät solche Zertifikate, ohne deren Gültigkeit über eine Zertifikatskette zu prüfen. Das kann in Test- oder Entwicklungsumgebungen sinnvoll sein, birgt jedoch ein Sicherheitsrisiko im produktiven Einsatz, da die Authentizität und Vertrauenswürdigkeit der verwendeten Zertifikate nicht garantiert wird.

Diese Option kann unter Zertifikate, Systemzertifikate, [Unbekannten Zertifizierungsstellen vertrauen] aktiviert werden.

2.5.4.3 Gerätezertifikate

Gerätezertifikate verleihen einem Gerät eine eindeutige Identität, die es ermöglicht, sich gegenüber verbundenen Systemen zu authentifizieren. Dies stellt sicher, dass nur autorisierte Geräte auf Daten zugreifen können und die Kommunikation zwischen Geräten geschützt ist. Diese Zertifikate basieren auf X.509-Standards und werden durch Public-Key-Zertifikate (Public Key Infrastructure, PKI) erzeugt. Dadurch können Geräte andere vertrauenswürdige Geräte und Server identifizieren.

In der Regel wird ein Gerätezertifikat von der internen Zertifizierungsstelle (CA) einer Organisation ausgestellt. Das Zertifikat wird mit dem privaten Schlüssel des Stammzertifikats (CA-Zertifikat) der Organisation signiert, das als Basis für die Signierung weiterer Zertifikate dient.

Die Sicherung der Geräte obliegt dem Betreiber und ist keine Leistung des Herstellers Sartorius. Daher ist es wichtig, das Gerät mit einem eigenen Zertifikat zu sichern, sobald es in Ihrer Organisation eintrifft. Ab Werk werden die Geräte mit einem Standard-Zertifikat von Sartorius ausgeliefert.

Gerätezertifikate sollten intern in Ihrem System und Netzwerk erstellt werden, wofür eine private CA erforderlich ist. Es gibt zwei Ansätze:

1. Erstellen Sie eine eigene private CA mit Tools wie OpenSSL oder Microsoft CA.
2. Beauftragen Sie einen Managed PKI (mPKI)-Anbieter, der Ihre Authentifizierungs- und Verschlüsselungsanforderungen übernimmt.

2.5.4.4 Wifi-Zertifikate

Ein WiFi-Zertifikat ist ein digitales Zertifikat, das für die sichere Authentifizierung und Verschlüsselung in einem drahtlosen Netzwerk (WLAN) eingesetzt wird. Typischerweise kommen solche Zertifikate im Rahmen von WPA2-Enterprise oder WPA3-Enterprise zum Einsatz, bei denen das 802.1X-Authentifizierungsverfahren (z. B. EAP-TLS) verwendet wird.

Bei WPA2-Enterprise oder WPA3-Enterprise erfolgt die Authentifizierung in der Regel über den sogenannten RADIUS-Server, der häufig mit einem Verzeichnisdienst (LDAP/Active Directory) verbunden ist. Damit sich Clients und RADIUS-Server gegenseitig sicher identifizieren können, werden Zertifikate genutzt.

2.5.4.5 LDAPS-Zertifikate

LDAP-Server (Lightweight Directory Access Protocol) verwenden Zertifikate, um ihre Kommunikation mit Clients oder anderen Diensten abzusichern. Häufig sind LDAP-Server für die zentrale Benutzer- und Rechteverwaltung zuständig. Ist die Verbindung nicht gesichert, können sensible Benutzerdaten (z. B. Passwörter, Gruppen- oder Rolleninformationen) abgefangen oder manipuliert werden.

Indem der LDAP-Server über LDAPS (LDAP über SSL/TLS) kommuniziert, wird die Verbindung verschlüsselt. Zudem verifiziert der Client mithilfe des Serverzertifikats die Identität des LDAP-Servers. Auf dem Gerät muss deshalb das Zertifikat des LDAPS-Servers abgelegt werden.

2.5.5 Sichere Netzwerkverbindungen mit SSL/TLS

Um Daten sicher zu übertragen, werden Sicherheitsprotokolle wie SSL (Secure Sockets Layer) und TLS (Transport Layer Security) eingesetzt. Sie definieren, wie Verschlüsselungs- und Authentifizierungsalgorithmen zu verwenden sind, um eine abhör- und manipulationssichere Verbindung zu gewährleisten.

SSL ist eine älteren Standards entsprechende Sicherheitstechnologie, die eine verschlüsselte Verbindung zwischen einem Server und einem Client herstellt. Im Fall der Waage (z. B. Cubis MCA) kann dies die verschlüsselte Kommunikation mit einem Webbrowser sein, der auf die Gerätewebseite zugreift. Inzwischen wurde SSL durch TLS (Transport Layer Security) als Nachfolgetechnologie abgelöst. Da aber SSL der bekanntere Begriff ist, wird in Bezug auf Zertifikate oder die Sicherung übertragener Daten von TLS/SSL gesprochen, auch wenn im Hintergrund nur TLS genutzt wird. Die Waage unterstützt derzeit TLS bis Version 1.3.

2.5.5.1 Unbekannte Zertifizierungsstellen

Im Gerät besteht die Möglichkeit, auch Zertifikaten zu vertrauen, die nicht von einer bekannten Zertifizierungsstelle ausgestellt wurden. Aktiviert man diese Option, akzeptiert das Gerät solche Zertifikate, ohne deren Gültigkeit über eine Zertifikatskette zu prüfen. Das kann in Test- oder Entwicklungsumgebungen sinnvoll sein, birgt jedoch ein Sicherheitsrisiko im produktiven Einsatz, da die Authentizität und Vertrauenswürdigkeit der verwendeten Zertifikate nicht garantiert wird.

Diese Option kann unter Zertifikate, Systemzertifikate, [Unbekannten Zertifizierungsstellen vertrauen] aktiviert werden.

3 Anwendungsbeispiele

Die Anwendungsbeispiele beziehen sich auf die MCA Version ab Package 09-03-04.01.xx mit den darin enthaltenen Einstellmöglichkeiten und Funktionalitäten. Für das Einrichten der Netzwerk Verbindungen, Konnektoren und Schnittstellen werden entsprechende Benutzerrechte benötigt.

Zum Konfigurieren der Ethernet- und Wi-Fi Schnittstelle sind grundlegende Kenntnisse von TCP-/IP-basierten Netzen und Netzwerk-Technologien im Allgemeinen erforderlich.

Voraussetzung für alle Beispiele ist eine Verbindung der Waage mit einem Netzwerk per Ethernet (LAN) oder Wi-Fi

(WLAN).

3.1 Report der Menü-Einstellungen auf Windows File Server

Dieses Beispiel beschreibt das Einrichten und Anwender der MCA Waage, damit aus dem Menü [Einstellungen] heraus eine Report-Datei mit allen Einstellungen der Waage im PDF-Format über den Konnektor [Windows File Server] per SMB-Netzwerkprotokoll, in das Zielverzeichnis eines freigegebenen Netzlaufwerks exportiert werden kann.

Für die Übertragung von Dateien per SMB-Protokoll ist die QAPP-Erweiterung [Verbindung zu Windows File Server] aus dem Paket [Connectivity] erforderlich. Die Erweiterung kann 30 Tage frei genutzt werden, danach muss sie lizenziert werden.

Voraussetzung für diese Aktion ist ein freigegebenes Laufwerk in ihrem Netzwerk mit SMB-Protokoll.

Einsatz dieser Anwendung kann damit die zentrale Ablage der Menü-Einstellungen aller vernetzten MCA Waagen sein.

3.1.1 Einrichten

Konfigurationsschritte:

1. Aktivieren Sie die QAPP-Erweiterung [Verbindung zu Windows File Server], falls noch nicht erfolgt.
 - a. Das Menü [Task-Verwaltung] und dann das [QAPP Center] öffnen.
 - b. Wählen Sie das Software-Paket [Connectivity] und darin die QAPP [Verbindung zu Windows File Server]. Es wird die Beschreibung und Version der QAPP angezeigt.
 - c. Aktivieren Sie mit der Schaltfläche [Lizenz] diese QAPP, die Bestell- und Lizenzinformationen werden angezeigt.
 - d. Falls diese QAPP nicht ab Werk freigeschaltet bestellt wurde, starten Sie die Testversion oder geben Sie den erworbenen Lizenzcode für diese QAPP ein.
2. Richten Sie einen Konnektor zu einem Windows File Server ein, z. B. [Mein SMB Server für Einstellungen].
 - a. Das Menü [Einstellungen] öffnen.
 - b. Zu [Verbindungen] -> [Konnektoren] -> [SMB] navigieren.
 - c. Aktivieren Sie mit der Schaltfläche [+] das Anlegen eines neuen Konnektors.
 - d. Vergeben Sie einen eindeutigen Namen für diesen Konnektor.
 - e. Geben Sie den Netzwerkpfad für Host und Share ein, achten Sie auf die richtige Schreibweise [//HostName/ShareName].
 - f. Für die Ablage der Dateien können Sie auch ein Unterverzeichnis auf dem Server mit angeben.
 - g. Geben Sie den Benutzernamen und das Passwort für den Zugriff auf das freigegebene Laufwerk in Ihrem Netzwerk ein. Achten sie hier ebenfalls auf die richtige Schreibweise, insbesondere auf Groß- und Kleinschreibung.

3.1.2 Anwenden

Benutzerschritte:

1. Vom Hauptmenü aus öffnen Sie mit der Schaltfläche [Einstellungen] das Menü für die Einstellungen der Waage.
2. Betätigen Sie die Schaltfläche [Export] in der Navigations- und Funktionsleiste.
3. Es wird eine Liste der Konnektoren angezeigt, über die der Export der Report-Datei erfolgen kann.
4. Wählen Sie Ihren angelegten Konnektor z. B. [Mein SMB Server für Einstellungen] aus. Die Report-Datei wird erstellt und über den Konnektor zum SMB Server exportiert.
5. Als Bestätigung für einen erfolgreichen Export erhalten Sie die Meldungen [Report gesendet] und [Prozess beendet]. Die Report-Datei im PDF Format mit der dazugehörigen Prüf-Datei liegt jetzt auf dem Server und kann angesehen werden.
6. Falls der Export der Report-Datei nicht erfolgen konnte, geht diese Datei nicht verloren, siehe Fehlerbehandlung.

Anmerkung: Das Dateiformat PDF ist ein plattformunabhängiges Dateiformat für Dokumente. Druckausgaben in diesem Format können damit auf jedem Rechner angesehen werden. Zu jeder Ausgabe-Datei in PDF-Format wird eine passende Prüf-Datei mit der Prüfsumme (MD5-Hashwert) der PDF-Daten angelegt. Diese Prüfsumme wird zusätzlich beim Übertragen der Datei im Audit Trail gespeichert. Über ein passendes Tool kann die PDF-Datei mit dieser Prüf-Datei verglichen werden und damit die Integrität der PDF-Daten sichergestellt werden.

3.1.3 Fehlerbehandlung

Keine Report-Datei in das Verzeichnis vom SMB File Server exportiert.

1. Stellen Sie sicher, dass alle oben genannten Konfigurationsschritte befolgt wurden.
2. Überprüfen Sie, ob die Waage z. B. per Ethernet-Kabel mit dem Netzwerk verbunden ist. Im [Status Center] muss unter [Geräteinformationen] die IP-Adresse der Waage im Netzwerk angezeigt werden.
3. Kontrollieren Sie im Konnektor den Netzwerkpfad und die richtige Schreibweise von Host und Share sowie Benutzername und Passwort für die Zugriffsrechte auf den SMB File Server.
4. Testen Sie die Verbindung des Konnektors mit dem SMB File Server, in dem Sie in der Übersicht der eingestellten Werte die Schaltfläche [Info] betätigen. Wenn alle Einstellungen richtig sind und der SMB File Server erreichbar, dann erhalten Sie die Meldung, dass der Konnektor verfügbar ist.
5. Wenn nicht, dann überprüfen Sie, ob sich der SMB File Server im Netzwerk befindet und von Ihrem PC aus eine Datei dort abgelegt werden kann.
6. Falls es zu Fehlermeldung [Übertragungsfehler] kommt, dann können Sie den Export:
 - a. Wiederholen: Die Ausgabe der Report-Datei zum Netzwerk-Server erfolgt erneut.
 - b. Später wiederholen: Die Ausgabe der Report-Datei wird automatisch wiederholt. Im [Status Center] unter [Nachrichten] werden ausstehenden Übertragungen angezeigt.
 - c. Umleiten: Sie können die Report-Datei auf einen anderen Konnektor umleiten.
 - d. Löschen: Der Export der Report-Datei wird aufgehoben und gelöscht.

3.2 Aktualisierung des QAPP Center von FTP Server

In diesem Beispiel wird das Einrichten und Anwenden der Cubis® MCA Waage beschrieben, um die Aktualisierung für das QAPP Center von einem FTP Server zu laden.

Für die Übertragung von Dateien von einem FTP Netzwerk Server ist eine QAPP-Erweiterung [Verbindung zu FTP/FTPS] aus dem Paket [Connectivity] erforderlich. Die Erweiterung kann 30 Tage frei genutzt werden, danach muss Sie ebenfalls lizenziert werden.

Voraussetzung für diese Anwendung ist ein entsprechend eingerichteter FTP Server in Ihrem Netzwerk.

Diese Anwendung ermöglicht für vernetzte MCA Waagen das Aktualisieren des QAPP Centers von einer zentralen Quelle aus.

3.2.1 Einrichten

Konfigurationsschritte:

1. Aktivieren Sie die QAPP-Erweiterung [Verbindung zu FTP/FTPS], falls noch nicht erfolgt.
 - a. Das Menü [Task-Verwaltung] und dann das [QAPP Center] öffnen.
 - b. Wählen Sie das Software-Paket [Connectivity] und darin die QAPP [Verbindung zu FTP/FTPS]. Es wird die Beschreibung und Version der QAPP angezeigt.
 - c. Aktivieren Sie mit der Schaltfläche [Lizenz] diese QAPP, die Bestell- und Lizenzinformationen werden angezeigt.
 - d. Falls diese QAPP nicht ab Werk freigeschaltet bestellt wurde, starten Sie die Testversion oder geben Sie den erworbenen Lizenzcode für diese QAPP ein.
2. Richten Sie einen Konnektor zu einem FTP Server ein, z. B. [Mein FTP Server für Update QAPP Center].
 - a. Das Menü [Einstellungen] öffnen.
 - b. Zu [Verbindungen] -> [Konnektoren] -> [FTP] navigieren.
 - c. Aktivieren Sie mit der Schaltfläche [+] das Anlegen eines neuen Konnektors.
 - d. Vergeben Sie einen eindeutigen Namen für diesen Konnektor.
 - e. Geben Sie die IP-Adresse vom Netzwerk-Server ein, achten Sie auf die richtige Schreibweise.
 - f. Für die Verbindung ist eine Port-Nummer erforderlich, vorgegeben ist die Nummer 21. Falls erforderlich, können Sie eine andere Port-Nummer eingeben.
 - g. Sie können für die auf dem Server abgelegten Dateien zur Aktualisierung des QAPP Centers auch ein Unterverzeichnis angeben.
 - h. Geben Sie den Benutzernamen und das Passwort für den Zugriff auf den FTP Server ein. Achten sie hier ebenfalls auf die richtige Schreibweise, insbesondere auf Groß- und Kleinschreibung.

3.2.2 Anwenden

Benutzerschritte:

1. Öffnen Sie vom Hauptmenü aus mit der Schaltfläche [Einstellungen] das Menü für die Einstellungen der Waage.
2. Navigieren Sie zum Punkt [Gerätewartung] -> [QAPP Center installieren]. Es wird eine Liste der Konnektoren angezeigt, über die ein Paket für die Aktualisierung vom QAPP Center geladen werden kann.
3. Wählen Sie Ihren angelegten Konnektor z. B. [Mein FTP Server für Update QAPP Center] aus. Die Verbindung zum

FTP Server wird aufgebaut und eine Liste der verfügbaren Pakete für das Aktualisieren vom QAPP Center wird angezeigt.

4. Wählen Sie die gewünschte Version vom QAPP Center aus und bestätigen Sie die Meldung zur Aktualisierung.
5. Das QAPP Center wird vom FTP Server auf die Waage kopiert und dort aktualisiert. Als Bestätigung erhalten Sie die Anzeige der aktualisierten Version des QAPP Centers.
6. Siehe Fehlerbehandlung, falls die Aktualisierung nicht erfolgen konnte.

3.2.3 Fehlerbehandlung

Keine Aktualisierung des QAPP Center über den Konnektor möglich.

1. Stellen Sie sicher, dass alle oben genannten Konfigurationsschritte befolgt wurden.
2. Überprüfen Sie, ob die Waage z. B. per Ethernet-Kabel mit dem Netzwerk verbunden ist. Im [Status Center] muss unter [Verbindungen] die IP-Adresse der Waage im Netzwerk angezeigt werden.
3. Kontrollieren Sie im Konnektor die IP-Adresse und Port-Nummer des FTP Servers sowie Benutzername und Passwort für die Zugriffsrechte auf den Server.
4. Testen Sie die Verbindung des Konnektors mit dem FTP Server, in dem Sie in der Übersicht der eingestellten Werte die Schaltfläche [Info] betätigen. Wenn alle Einstellungen richtig sind und der FTP Server erreichbar, dann erhalten Sie die Meldung, dass der Konnektor verfügbar ist.
5. Überprüfen Sie mit Ihrem PC, ob sich auf dem FTP Server im Netzwerk das angegebene Unterverzeichnis und auch die Datei für die Aktualisierung des QAPP Center befindet.

3.3 Audit Trail Einträge per Webbrowser einsehen

Dieses Beispiel beschreibt das Einrichten und Anwenden der MCA Waage, damit Einträge im Audit Trail der Waage per Webbrowser eingesehen werden können.

Für die Fernbedienung der MCA Waage wird der [Chrome] Webbrowser empfohlen.

Eine sichere Verbindung der Waage mit dem Browser über das Protokoll HTTPS setzt bestimmte Gerätezertifikate voraus.

Die MCA Waage stellt dafür eigene Gerätezertifikate zum Download bereit. Diese Gerätezertifikate müssen für den sicheren Remotezugriff auf die Geräthewebsite in Browser importiert werden. Zum Thema [Zertifikate] gibt es eine separate Beschreibung.

Erst nach der Aktivierung der QAPP-Erweiterungen [Audit Trail] im QAPP Center unter [Pharma (QP1)] ist der volle Umfang vom Audit Trail nutzbar.

Einsatz dieser Anwendung ist z. B. die zentrale Fernüberwachung von Einstellungen an allen vernetzten MCA Waagen.

3.3.1 Einrichten

Konfigurationsschritte:

1. Aktivieren Sie die QAPP-Erweiterung [Audit trail], falls noch nicht erfolgt.
 - a. Das Menü [Task-Verwaltung] und dann das [QAPP Center] öffnen.
 - b. Wählen Sie das Software-Paket [Pharma] und darin die QAPP [Audit trail]. Es wird die Beschreibung und Version der QAPP angezeigt.
 - c. Aktivieren Sie mit der Schaltfläche [Lizenz] diese QAPP, die Bestell- und Lizenzinformationen werden angezeigt.
 - d. Falls diese QAPP nicht ab Werk freigeschaltet bestellt wurde, starten Sie die Testversion oder geben Sie den erworbenen Lizenzcode für diese QAPP ein.
2. Aktivieren Sie die Website der MCA-Waage, falls noch nicht erfolgt.
 - a. Das Menü [Einstellungen] öffnen.
 - b. Zu [Verbindungen] -> [Website / Webservices] navigieren.
 - c. Stellen Sie den Punkt [Webseitenzugang] auf [Aktiviert, ohne Authentifizierung] ein.
3. Falls erforderlich, aktivieren Sie den Remotezugriff auf die Website der MCA-Waage.
 - a. Das Menü [Einstellungen] öffnen.
 - b. Zu [Verbindungen] -> [Website / Webservices] navigieren.
 - c. Wählen Sie unter dem Punkt [Remote Zugang] die Einstellung [Anzeige und Steuerung].

3.3.2 Anwenden

Benutzerschritte:

1. Starten Sie auf Ihrem PC den Webbrowser, z. B. [Chrome].
2. Geben Sie die IP-Adresse Ihrer Waage ein, die im [Status Center] unter [Geräteinformationen] angezeigt wird.
3. Falls Sie die Gerätezertifikate der Waage noch nicht in Browser importiert haben, erhalten Sie auf dem Browser die Meldung [Dies ist keine sichere Verbindung].
4. Sie haben jetzt die Möglichkeit mit der Schaltfläche [Erweitert] und dem Link [Weiter ...] auf die IP-Adresse der Waage zu gehen, die in diesem Fall noch als unsicher angesehen wird oder Sie müssen die Gerätezertifikate der Waage erst in ihrem Browser importiert. Zum Thema [Zertifikate] gibt es eine separate Beschreibung.
5. Ansonsten wird jetzt im Browser die Seite [Meine Cubis] (Homepage) angezeigt.
6. Wählen Sie für das Beispiel die Seite [Audit-Trail].
7. Sie können jetzt die Liste der Einträge sortieren nach ID, Zeitstempel und Benutzer.
8. Die Liste der Einträge kann auf- oder absteigend angezeigt werden.
9. Sie können auch Filter setzen, um sich damit nur bestimmte Gruppen von Einträgen anzeigen zu lassen.

3.3.3 Fehlerbehandlung

Die Homepage der Waage wird im Browser nicht angezeigt.

1. Überprüfen Sie, ob die Waage z. B. per Ethernet-Kabel mit dem Netzwerk verbunden ist. Im [Status Center] muss unter [Geräteinformationen] die IP-Adresse der Waage im Netzwerk angezeigt werden.
2. Stellen Sie sicher, dass der Punkt [Webseitenzugang] auf [Aktiviert] eingestellt ist.

Die Verbindung zur Waage wird im Browser als [Unsicher] angezeigt.

1. Importieren Sie die Gerätezertifikate der Waage in ihren Browser. Zum Thema [Zertifikate] gibt es eine separate Beschreibung.

Auf der Homepage der Waage ist die Seite [Audit-Trail] ist nicht anwählbar.

1. Stellen Sie sicher, dass alle oben genannten Konfigurationsschritte befolgt wurden. Insbesondere die Aktivierung der QAPP-Erweiterung [Audit trail] erfolgt und die Lizenz dafür noch gültig ist.

3.4 Datum und Zeit mit NTP Server synchronisieren

In diesem Beispiel wird das Einrichten und Anwenden der Cubis® MCA beschrieben, um eine Zeitsynchronisation von Datum und Zeit der Waage mit einem NTP Server zu ermöglichen.

Voraussetzung für diese Anwendung ist der Zugang auf einen NTP Server in Ihrem Firmen-Netzwerk oder im öffentlichen Netz.

Alle 10 Minuten wird die Abweichung der Zeit zwischen der Waage und dem NTP Server geprüft. Ist die Abweichung größer als 3 Sekunden, dann wird die Zeit in der Waage korrigiert und die Änderung im Audit Trail eingetragen.

Diese Anwendung ermöglicht eine einfache automatische Aktualisierung und Synchronisierung von Datum und Zeit auf allen vernetzten MCA Waagen.

3.4.1 Einrichten

Konfigurationsschritte:

1. Richten Sie eine aktive NTP Konfiguration ein.
 - a. Das Menü [Einstellungen] öffnen.
 - b. Zu [Geräteeinstellungen] -> [Datum und Zeit] -> [NTP Konfiguration] navigieren.
 - c. Aktivieren Sie mit der Schaltfläche [Bearbeiten] die Konfiguration der NTP Server Einstellungen.
 - d. Stellen Sie den Punkt [NTP Betriebszustand] auf [Aktiviert] ein.
 - e. Geben Sie über [Server IP] die Adresse des NTP Servers im Format IPv4 ein, z. B. 192.53.103.108. (Das ist ein NTP-Server der Physikalisch-Technischen Bundesanstalt in Braunschweig Deutschland.)
 - f. Bestätigen Sie die NTP Konfiguration mit der Schaltfläche [OK].
 - g. Testen Sie die Verbindung zum NTP Server in dem Sie in der Übersicht der NTP Konfiguration die Schaltfläche [Info] betätigen.
2. Stellen Sie für Ihren Standort die richtige Zeitzone ein.
 - a. Das Menü [Einstellungen] öffnen.
 - b. Zu [Geräteeinstellungen] -> [Datum und Zeit] -> [Datum und Zeit einstellen] navigieren.
 - c. Aktivieren Sie mit der Schaltfläche [Bearbeiten] die Einstellungen für Datum und Zeit.
 - d. Stellen Sie über den Punkt [Zeitzone] ihren Standort ein, [UTC +/- Zeit, Ort]. Die Anzeige von Datum und Uhrzeit erfolgt anschließend sofort passend in Ihrer lokalen Zeit.

Anmerkung: Nach dem Stellen von Datum, Zeit und Zeitzone fordert die MCA Waage zum Neustart des Systems auf.

3.4.2 Fehlerbehandlung

Keine Verbindung zum NTP Server möglich.

1. Stellen Sie sicher, dass alle oben genannten Konfigurationsschritte befolgt wurden.
2. Überprüfen Sie, ob die Waage z. B. per Ethernet-Kabel mit dem Netzwerk verbunden ist. Im [Status Center] muss unter [Geräteinformationen] die IP-Adresse der Waage im Netzwerk angezeigt werden.
3. Überprüfen Sie mit Ihrem PC, ob sich auf die IP-Adresse des NTP Servers zugreifen können.

4 Anhang

4.1 Kompatible Wi-Fi-Sticks

Die Cubis® MCA unterstützt die gängigsten Wi-Fi-Sticks (USB-WLAN-Adapter) die auf dem Markt angeboten werden.

Für die Auswahl eines Wi-Fi-Sticks beachten Sie folgende Punkte:

1. Vermeiden Sie namenlose Wi-Fi-Sticks. Kaufen Sie bei einer bekannten Marke.
2. Überprüfen Sie nach Möglichkeit das Datenblatt des Wi-Fi-Sticks, um sicherzustellen, dass er einen der folgenden unterstützten Chipsätze enthält.

Unterstützte Wi-Fi-Chipsätze sind:

- 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. Abkürzungen

DHCP	Dynamic Host Configuration Protocol	Ein Kommunikationsprotokoll in der Computertechnik. Es ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server.
DNS	Domain Name System	System zur Auflösung von Computernamen in IP-Adressen und umgekehrt.
FTP	File Transfer Protocol	Standard-Netzwerkprotokoll für die Übertragung von Dateien in einem Netzwerk zwischen einem Client und einem Server.
FTPS	FTP over TLS	Eine Methode zur Verschlüsselung des File Transfer Protocol (FTP).
HTTPS	Hypertext Transfer Protocol Secure	Ein Kommunikationsprotokoll, mit dem Daten verschlüsselt übertragen werden können.
IPv4	Internet Protocol version 4	Internet Protokoll der Version 4.
IPv6	Internet Protocol version 6	Internet Protokoll der Version 6.
MAC address	Media Access Control address	Physikalische Hardware Adresse, eindeutiger Identifikator des Geräts in einem Netzwerk.
NTP	Network Time Protocol	Ein Standard zur Synchronisierung von Uhren in Computersystemen.
PNG	Portable Network Graphics	Portable Netzwerkgrafik, ein Rastergrafikformat mit verlustfreier Datenkompression.
PSK	Pre-shared key	Verschlüsselungsverfahren bei dem die Schlüssel vor der Kommunikation beiden Teilnehmern bekannt sein müssen.
REST	Representational State Transfer	Programmierparadigma für verteilte Systeme, insbesondere für Webservices.
SMB	Server Message Block	Ein Netzprotokoll für Datei-, Druck- und andere Serverdienste in Rechnernetzen.
SSID	Service Set Identifier	Frei wählbarer Netzwerkname, z. B. bei Wi-Fi.
URL	Uniform Resource Locator	Identifikationsbezeichnung für Internet- oder Webadressen.
UTC	Universal Time, Coordinated	Die Weltzeit, auch Erdzeit oder Universalzeit.
WEP	Wired Equivalent Privacy	Standard-Verschlüsselungsprotokoll für WLAN.
Wi-Fi	Wireless Fidelity	Kabelloses Netzwerk, Synonym für WLAN.
WLAN	Wireless Local Area Network	Kabelloses, lokales Netzwerk.
WPA	Wi-Fi Protected Access	Verschlüsselungsmethode für ein Drahtlosnetzwerk. Nachfolger von WEP.
WPA2	Wi-Fi Protected Access 2	Implementierung eines Sicherheitsstandards für Funknetzwerke. Nachfolger von WPA.