

Descrizione della rete, Ethernet e Wi-Fi (WLAN) per la bilancia Cubis® MCA

Questo documento descrive come collegare la bilancia a una rete via Ethernet e Wi-Fi (WLAN). Vengono forniti esempi per illustrare come impostare e utilizzare la bilancia nella pratica.



Riassunto esecutivo

La bilancia da laboratorio Cubis® MCA Premium offre opzioni di connettività complete e flessibili per integrare la bilancia nell'IT del laboratorio. Un gran numero di protocolli IT standardizzati, come il servizio web REST, SMB o LDAP, sono disponibili tramite Ethernet e Wi-Fi, consentendo l'integrazione diretta senza l'uso di middleware aggiuntivi. Inoltre, il Cubis® può essere controllato a distanza attraverso la rete utilizzando un browser web e possono essere visualizzate le tracce di controllo e altre informazioni di stato.

1	Connessione di rete Ethernet e Wi-Fi	4
1.1	Impostazioni generali	4
1.2	Ethernet (LAN)	4
1.2.1	Protocollo IPv4	5
1.2.2	Protocollo IPv6	5
1.2.3	DNS 1 e DNS 2	5
1.3	Wi-Fi (WLAN)	5
1.3.1	SSID e password Wi-Fi	6
1.3.2	Protocollo IPv4/IPv6 e DNS 1/2	6
2	Servizi di rete	6
2.1	Comunicazione seriale	6
2.1.1	Protocollo SBI	6
2.1.2	protocollo xBPI	7
2.1.3	Protocollo SICS	7
2.1.4	QAPP diretto	7
2.2	Connettori di rete	7
2.2.1	YDP30-NET	7
2.2.2	Stampante di rete	7
2.2.3	FTP / FTPS	7
2.2.4	Protocollo SMB	8
2.3	Sito web	8
2.3.1	Webservices	8
2.4	Server NTP per data e ora	8
2.5	Certificati	8
2.5.1	Obblighi dell'operatore	8
2.5.2	Azzeramento dei certificati	9
2.5.3	Installare o aggiornare i certificati	9
2.5.3.1	Certificati del cliente	9
2.5.3.2	Certificati CA	9
2.5.3.3	Tipi di file di certificato	9
2.5.4	Tipi di certificati	10
2.5.4.1	Certificati CA	10
2.5.4.2	Autorità di certificazione sconosciute	10
2.5.4.3	Certificati del dispositivo	10
2.5.4.4	Certificati Wifi	10
2.5.4.5	Certificati LDAPS	11
2.5.5	Connessioni di rete sicure con SSL/TLS	11
2.5.5.1	Autorità di certificazione sconosciute	11
3	Esempi di applicazioni	11
3.1	Segnalazione delle impostazioni dei menu sul file server di Windows	11
3.1.1	Impostazione	11
3.1.2	Applicazione	12
3.1.3	Risoluzione dei problemi	12

3.2	Aggiornare il centro QAPP del server FTP	12
3.2.1	Impostazione	13
3.2.2	Applicazione	13
3.2.3	Risoluzione dei problemi	13
3.3	Visualizza le voci della traccia di controllo tramite browser web	13
3.3.1	Impostazione	14
3.3.2	Applicazione	14
3.3.3	Risoluzione dei problemi	14
3.4	Sincronizzare data e ora con il server NTP	15
3.4.1	Impostazione	15
3.4.2	Risoluzione dei problemi	15
4	Appendice	15
4.1	Bastoni Wi-Fi compatibili	15
5	Abbreviazioni	17

1 Connessione di rete Ethernet e Wi-Fi

Una bilancia Cubis® MCA può essere collegata a una rete basata su TCP/IP con un cavo tramite la connessione Ethernet (presa RJ45) e senza fili tramite un adattatore USB Wi-Fi (WLAN stick).

Le velocità di trasmissione della connessione di rete sono 10 Mbit/sec (10BASE-T, Ethernet) e 100 Mbit/sec (100BASE-TX Fast Ethernet).

Il collegamento Ethernet viene effettuato con un cavo di collegamento, CAT 5 o superiore, intrecciato a coppie, schermato, 1:1, UTP/STP, spina RJ45; ad esempio, cavo patch CAT 5 a seconda dell'uso (dritto/cross-over).

Per una connessione senza fili, Cubis® MCA supporta i più comuni adattatori USB Wi-Fi (WLAN sticks) che si trovano sul mercato.

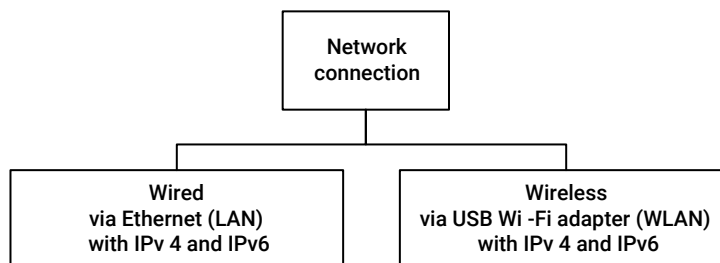


Figura 1: Connessione alla rete

La bilancia Cubis® MCA può avere un indirizzo IPv4 e uno IPv6 ciascuno su Ethernet e Wi-Fi rispettivamente, cioè fino a 4 indirizzi.

Attraverso le connessioni di rete Ethernet (LAN) e Wi-Fi (WLAN), la bilancia Cubis® MCA offre contemporaneamente diversi servizi di rete.

1.1 Impostazioni generali

Il nome host della bilancia, ex-fabbrica, è composto dalla denominazione della serie e dagli ultimi 3 byte dell'indirizzo MAC, ad esempio, [cubis-1a477e]. Il nome dell'host può essere scelto liberamente, ma deve essere unico in una rete.

1.2 Ethernet (LAN)

Per il collegamento Ethernet della bilancia si possono usare i protocolli IPv4 e IPv6. Si può impostare separatamente per ogni protocollo, se l'indirizzo IP deve essere ottenuto automaticamente o se al saldo viene dato un indirizzo IP fisso. Il rispettivo protocollo può anche essere disabilitato completamente.

Nella panoramica delle impostazioni per Ethernet, lo stato mostra se è stata stabilita una connessione alla rete. Inoltre, qui viene mostrato anche l'indirizzo MAC unico della bilancia, ad esempio [00:30:D6:1F:77:569].

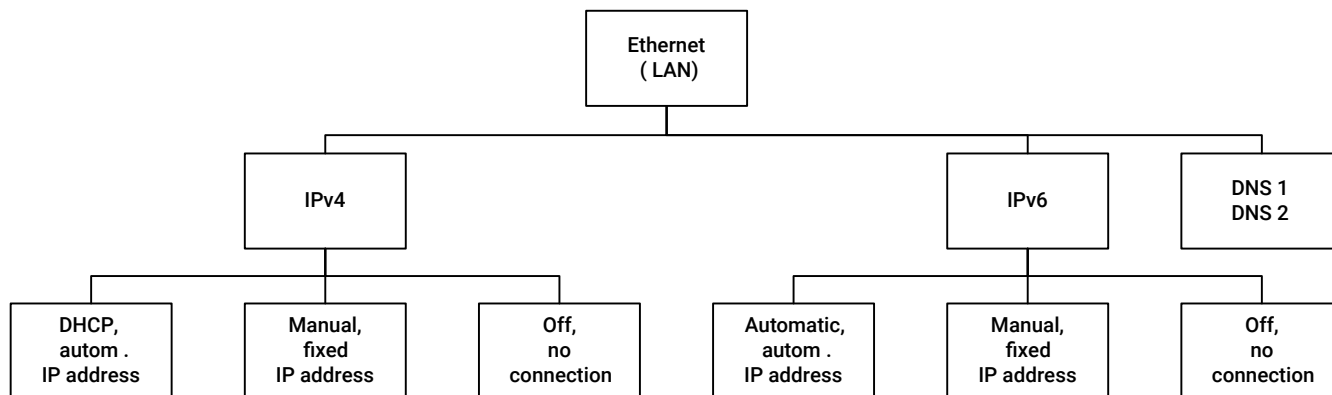


Figura 2: Ethernet con IPv4/IPv6

Per il funzionamento con un indirizzo IP fisso, oltre all'indirizzo IP, a seconda del protocollo, devono essere inseriti manualmente anche la subnet mask e il gateway per IPv4, o la lunghezza del prefisso e il gateway per IPv6.

L'inserimento del gateway è facoltativo e necessario solo quando è necessaria una connessione a Internet.

Tutte le informazioni necessarie per questo possono essere fornite dall'amministratore di rete responsabile della rete aziendale.

1.2.1 Protocollo IPv4

L'indirizzo IP per il protocollo IPv4 (4*8 bit = 32 bit) consiste in 4 numeri decimali tra 0 e 255, separati da un punto, per esempio, [123.4.56.123]. Questo formato si applica per l'inserimento dell'indirizzo IP fisso, il marchio di sottorete e il gateway.

1.2.2 Protocollo IPv6

L'indirizzo IP per il protocollo IPv6 (8*16 bit = 128 bit) consiste in 8 numeri alfanumerici esadecimali tra 0 e FFFF, che sono separati da una virgola, per esempio, [ecb1:d583:6341:baf76:0:0:0:1].

I primi 4 blocchi (64 bit) costituiscono il prefisso e gli ultimi 4 blocchi l'identificatore di interfaccia. La maschera di rete IPv4 e l'indirizzo di rete IPv4 sono sostituiti dalla lunghezza del prefisso e dal prefisso in IPv6. La lunghezza del prefisso specifica il numero di bit che costituiscono il prefisso. La lunghezza tipica del prefisso è 64. Il prefisso sostituisce la subnet mask nel caso di IPv6.

1.2.3 DNS 1 e DNS 2

Nei sistemi di rete basati su IP, il DNS (Domain Name System) aiuta a rispondere alle richieste di risoluzione dei nomi. Una rete può avere diversi server DNS, il Cubis® MCA supporta l'ingresso di due server.

L'indirizzo IP o il nome del server possono essere inseriti per ogni server DNS.

In caso di DHCP, il server DNS è fornito automaticamente dal server DHCP. Inoltre, in questo caso, DNS1 e DNS2 sono aggiunti alla lista dei server DNS.

1.3 Wi-Fi (WLAN)

Un adattatore USB Wi-Fi (WLAN stick) può essere collegato alla bilancia MCA; diversi adattatori di questo tipo non sono supportati.

Nella panoramica delle impostazioni per il Wi-Fi (WLAN), viene visualizzato tramite lo stato, se un adattatore USB Wi-Fi corrispondente è collegato ed è connesso alla rete.

Visualizzazione dello stato

- Nessun dispositivo disponibile - Nessun adattatore USB Wi-Fi collegato.
- Disconnesso - Nessuna connessione alla rete Wi-Fi, ad esempio, non ha effettuato l'accesso con SSID Wi-Fi e password.
- Pronto - Connessione stabilita con la rete Wi-Fi.
- Online - Connessione stabilita con la rete Wi-Fi e Internet.

Se è stata stabilita una connessione, l'indirizzo MAC univoco dell'adattatore Wi-Fi USB è mostrato anche qui, ad esempio 34:C9:F0:89:6F:D6.

In allegato, la sezione: Bastoni Wi-Fi compatibili.

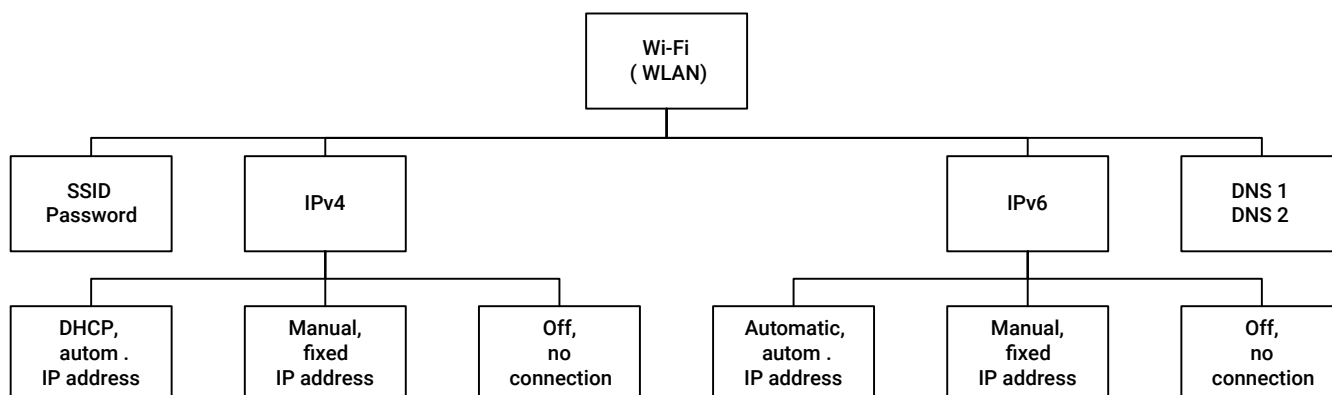


Figura 3: Wi-Fi con IPv4/IPv6

Per il funzionamento con un indirizzo IP fisso, oltre all'indirizzo IP, a seconda del protocollo, devono essere inseriti manualmente anche la subnet mask e il gateway per IPv4, o la lunghezza del prefisso e il gateway per IPv6. L'inserimento del gateway è facoltativo e necessario solo quando è necessaria una connessione a Internet.

Tutte le informazioni necessarie per questo possono essere fornite dall'amministratore di rete responsabile della rete aziendale.

1.3.1 SSID e password Wi-Fi

Per la connessione a una rete Wi-Fi, è necessario inserire l'SSID Wi-Fi (il nome unico della rete Wi-Fi) e la password Wi-Fi (la chiave della rete Wi-Fi).

Per l'autenticazione, la bilancia MCA supporta gli standard WEP, WPA-PSK e WPA2-PSK e quindi anche il metodo PSK per la crittografia.

1.3.2 Protocollo IPv4/IPv6 e DNS 1/2

Per il protocollo IPv4 e IPv6 così come per DNS 1 e DNS 2, la stessa descrizione si applica al Wi-Fi (WLAN) come nel caso di Ethernet (LAN).

2 Servizi di rete

Attraverso la rete la bilancia Cubis® MCA offre diversi servizi simultaneamente, una comunicazione seriale con diversi protocolli, connettori per la connessione a dispositivi di memoria di massa e stampanti di rete, un sito web e servizio web per l'accesso remoto, così come la connessione a un server NTP per sincronizzare data e ora.

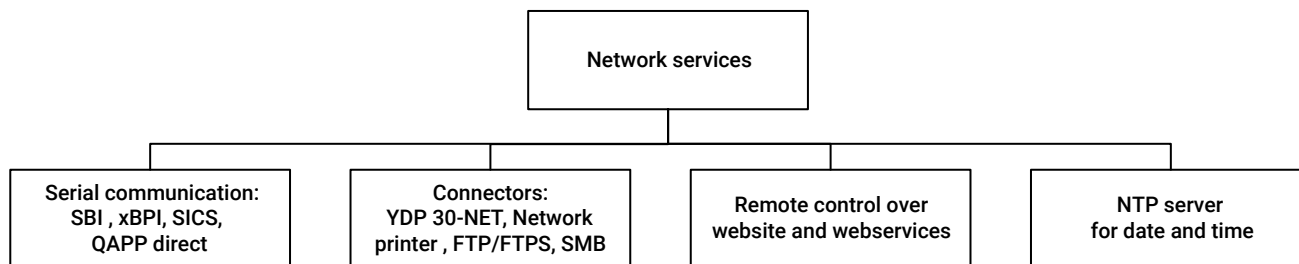


Figura 4: Servizi di rete

2.1 Comunicazione seriale

Utilizzando la connessione di rete, è possibile utilizzare i protocolli di comunicazione seriale SBI, xBPI, SICS, miniSICS, che possono essere utilizzati indipendentemente dal compito attivo e dal suo utilizzo. Questa connessione client/server richiede impostazioni per una porta TCP comune.

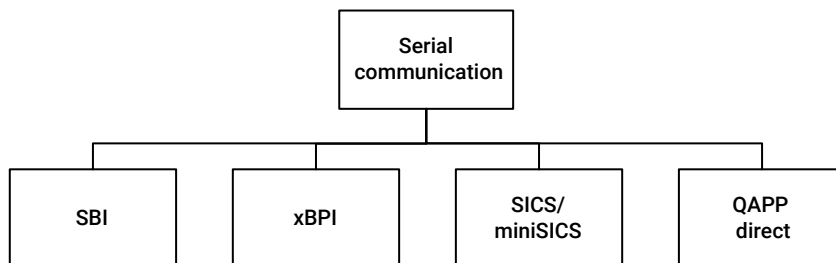


Figura 5: comunicazione seriale via rete

2.1.1 Protocollo SBI

Questo semplice protocollo basato su ASCII può controllare le funzioni di base della bilancia utilizzando i comandi ESC. L'uscita dei valori di visualizzazione può essere richiesta individualmente tramite un comando ESC, o automaticamente con ogni nuovo risultato di pesata nel ciclo della sequenza di visualizzazione, o automaticamente dopo determinati intervalli di tempo. È possibile scegliere se l'uscita viene fornita solo con un valore di visualizzazione stabile o anche senza che il valore di visualizzazione sia stabile. Il formato di uscita può essere selezionato con o senza identificatore (intestazione).

I comandi SBI e i formati di output sono dati in una descrizione separata dell'interfaccia.

2.1.2 protocollo xBPI

Questo protocollo binario offre una gamma estesa di comandi. Può essere usato per controllare numerose funzioni della bilancia.

C'è una descrizione separata dell'interfaccia dei possibili comandi xBPI.

2.1.3 Protocollo SICS

Il protocollo SICS (Standard Interface Command Set) stabilisce una compatibilità con il protocollo MT-SICS di Mettler e permette di inviare comandi alla bilancia per le funzioni di base. Tuttavia, va notato che ci sono differenze dovute alle diverse piattaforme hardware/software.

I comandi SICS e miniSICS implementati nella bilancia sono dati in una descrizione separata dell'interfaccia.

2.1.4 QAPP diretto

Solo le QAPP speciali, che sono avviate da un compito, possono usare l'interfaccia per i loro scopi di input e output. Le possibilità di input e output tramite l'interfaccia sono descritte nella rispettiva QAPP speciale.

2.2 Connettori di rete

In Cubis® MCA, i connettori stabiliscono la connessione ai server di rete che devono essere utilizzati come dispositivi di archiviazione di massa o come stampanti.

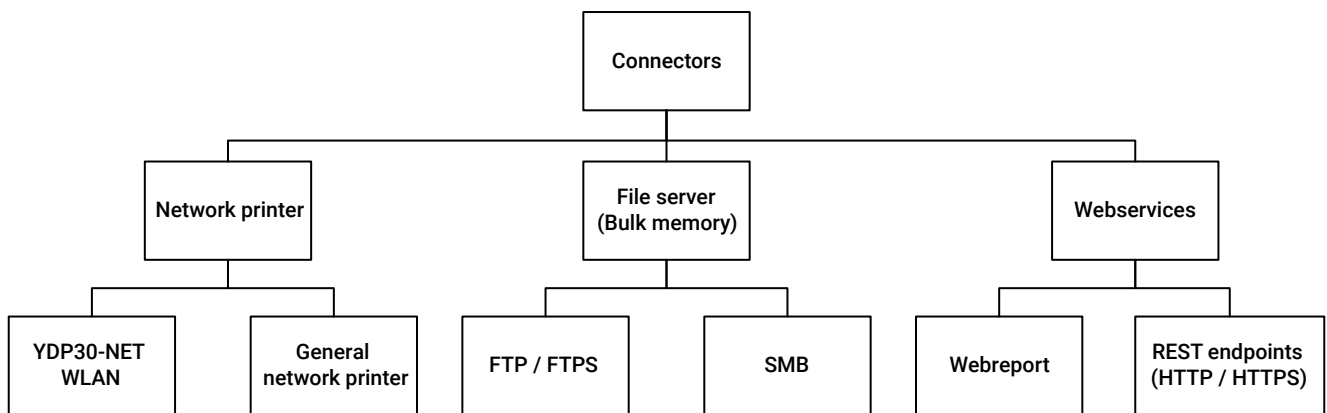


Figura 6: Connettori di rete

La stampante di rete YDP30-NET può essere collegata tramite WLAN o come stampante di rete generale con una rete Wi-Fi indipendente o una rete aziendale utilizzando DHCP.

Per la connessione a un dispositivo di memoria di massa, come il file server di Windows, FTP/FTPS o STARLIMS, è necessaria un'estensione speciale QAPP, che deve essere attivata tramite il Centro QAPP sotto [Connettività].

2.2.1 YDP30-NET

Questo connettore è destinato a collegare una stampante YDP30-NET con un cavo (LAN) o una connessione wireless (WLAN). Un connettore richiede un nome di connettore, un indirizzo IP o un nome host da inserire sulla stampante, nonché un numero di porta concordato tra la stampante e la bilancia.

La connessione wireless della stampante YDP30-NET è descritta in istruzioni separate.

2.2.2 Stampante di rete

Il connettore della stampante di rete permette, per esempio, le connessioni a una stampante A4 in una rete Wi-Fi indipendente con componenti Wi-Fi standard, o in una rete aziendale per DHCP con metodi di autenticazione standard. La stampante di rete deve supportare IPP (Internet Printing Protocol).

Un connettore richiede un nome di connettore, un indirizzo IP o un nome di host da inserire sulla stampante, così come il protocollo di trasferimento.

La descrizione separata [Print concept] descrive la configurazione e l'applicazione di una stampante di rete con un esempio di applicazione.

2.2.3 FTP / FTPS

Il File Transfer Protocol (FTP) è un protocollo di rete standard per il trasferimento di file tra un client e un server in una rete di computer.

La bilancia è il client FTP e può memorizzare file su un server FTP o recuperare file da un server FTP utilizzando il protocollo. Nel caso di FTPS, la connessione è anche criptata; i certificati necessari per questo sono descritti separatamente.

Per la connessione a un server FTP/FTPS, si deve creare un connettore con un nome unico, l'indirizzo IP e il numero di porta del server di rete, se necessario, una sotto-directory sul server e il nome utente e la password.

Nota: con diversi connettori sull'equilibrio verso lo stesso server, ma con diverse sotto-directory, la memorizzazione dei dati può essere facilmente strutturata in base all'argomento (backup, report, ...).

2.2.4 Protocollo SMB

Il connettore file server di Windows utilizza il protocollo di rete SMB. Questo protocollo facilita l'accesso alle unità di rete rilasciate dei computer Windows o Linux per memorizzare o recuperare i file di dati nelle directory di destinazione selezionate.

2.3 Sito web

Il sito web della bilancia MCA può essere visualizzato semplicemente tramite l'indirizzo IP della bilancia con un browser web. La pagina [My Cubis] (home page) mostra gli ID dei dispositivi impostati, le informazioni generali sui dispositivi della bilancia e le informazioni sul servizio.

Usando la pagina [Funzionamento a distanza], a seconda delle impostazioni del menu, è possibile visualizzare [Solo visualizzazione] o [Visualizzazione e controllo remoto] del bilancio MCA tramite il browser.

La pagina [Screenshot] crea un file PNG del display corrente, che può essere salvato.

Se l'estensione QAPP [Audit trail] è stata attivata nel Centro QAPP nel pacchetto [Pharma], allora viene visualizzato anche il sito web [Audit trail]. Le voci dell'audit trail possono essere filtrate, ordinate ed esportate secondo gli argomenti.

L'accesso al sito web può essere disattivato completamente tramite il menu e quindi anche il controllo remoto tramite il servizio web REST.

2.3.1 Webservices

Il funzionamento remoto delle funzioni sottostanti della bilancia MCA può anche essere fatto tramite un servizio web REST.

C'è una descrizione separata dei servizi web REST disponibili dell'equilibrio MCA.

2.4 Server NTP per data e ora

Cubis® MCA offre la possibilità di sincronizzare la data e l'ora con un server NTP. Per fare questo, la connessione con il server può essere attivata e l'indirizzo IP del server può essere inserito nelle impostazioni del dispositivo di MCA sotto Data/Ora e Configurazione NTP.

2.5 Certificati

Il bilanciamento Cubis® MCA supporta l'uso di certificati per un'integrazione affidabile nell'infrastruttura IT locale. L'MCA può elaborare i certificati di agenzie di certificazione di fiducia (CA), al fine di identificare i server di fiducia. L'MCA fornisce anche i propri certificati di dispositivi da scaricare. Questi certificati di dispositivo sono importati nel browser per l'accesso remoto sicuro al sito web del dispositivo.

C'è una descrizione separata sul tema dei [Certificati].

I certificati dei dispositivi si basano sullo standard X.509 e utilizzano la crittografia a chiave pubblica, in cui viene utilizzata una coppia di chiavi composta da una chiave pubblica e una privata. Questa coppia di chiavi consente la trasmissione criptata dei dati, la verifica delle firme digitali e l'autenticazione affidabile dell'identità. A seconda di come viene creata e conservata la chiave privata, può essere necessario decifrarla con una passphrase prima di utilizzarla.

2.5.1 Obblighi dell'operatore

Le bilance Sartorius Cubis MCA vengono fornite con certificati del dispositivo preinstallati che hanno una validità limitata. Gli operatori hanno la possibilità di rinnovare i certificati originariamente installati e di importare i propri certificati.

L'operatore è responsabile della gestione e dell'aggiornamento dei certificati e della loro validità. Per evitare possibili avvisi di sicurezza o restrizioni sulle connessioni sicure, è importante controllare regolarmente la validità dei certificati e rinnovarli se necessario.

L'aggiornamento del certificato non ha alcun effetto sulla funzione di pesatura o sull'integrazione nell'infrastruttura

IT locale. Non è quindi necessario riqualificare o riconvalidare i dispositivi quando si aggiornano i certificati.

2.5.2 Azzeramento dei certificati

Se dopo la reimpostazione del certificato viene visualizzato un avviso sulla scadenza del certificato, aggiornare il certificato come descritto nella sezione Aggiornamento dei certificati.

1. Fornire i file di certificato in modo che sia possibile accedervi tramite un connettore sul dispositivo, ad esempio su un dispositivo di memoria USB e sul connettore USB.
2. Andare alle impostazioni dal menu iniziale
3. Nel menu Connessioni, passare al sottomenu Certificati.
4. Selezionare i certificati di sistema e poi i certificati del dispositivo
5. Selezionare l'icona "Cestino" per rinnovare i certificati e confermare il messaggio "Reimposta certificati" con "Sì".
6. Verificare che sia disponibile il nuovo certificato "Sartorius Factory Authority". Questo certificato scadrà nel 2043.
7. Se "Sartorius Factory Authority" è visibile nell'elenco, l'aggiornamento è riuscito e viene generata una voce dell'Audit Trail.

Se dopo la reimpostazione del certificato viene visualizzato un avviso sulla scadenza del certificato, aggiornare il certificato come descritto nella sezione Aggiornamento dei certificati.

2.5.3 Installare o aggiornare i certificati

Per installare o aggiornare un certificato, seguire queste istruzioni.

2.5.3.1 Certificati del cliente

1. Fornire i file di certificato in modo che sia possibile accedervi tramite un connettore sul dispositivo, ad esempio su un dispositivo di memoria USB e sul connettore USB.
2. Andare alle impostazioni dal menu iniziale
3. Passare al menu Connessioni e selezionare Certificati
4. Navigare nel menu corrispondente per il quale si vuole installare un certificato. La differenziazione e la spiegazione dei certificati si trovano nel capitolo Tipi di certificati.
5. Premere il pulsante [IMPORT] e selezionare il connettore corrispondente tramite il quale è possibile accedere ai file di certificato da installare.
6. Selezionare [Certificato] e selezionare il file del certificato con la chiave pubblica dall'elenco dei file disponibili tramite il connettore. Sono supportati i seguenti formati: .pem e .crt.
7. Selezionare [Chiave privata] e selezionare il file del certificato con la chiave privata dall'elenco dei file disponibili tramite il connettore. Sono supportati i seguenti formati: .key
8. Selezionare [Password chiave privata] e inserire la password della chiave privata.
9. Confermare l'importazione. I file vengono trasferiti al sistema dopo l'esito positivo della verifica.

2.5.3.2 Certificati CA

1. Rendere disponibili i file di certificato in modo che sia possibile accedervi tramite un connettore sul dispositivo, ad esempio su un dispositivo di memoria USB e sul connettore USB.
2. Passare alle impostazioni dal menu principale
3. Nel menu Connessioni, passare al sottomenu Certificati.
4. Navigare nel menu corrispondente per il quale si vuole installare un certificato. La differenziazione e la spiegazione dei certificati si trovano nel capitolo Tipi di certificati.
5. Premere il pulsante [IMPORT] e selezionare il connettore corrispondente tramite il quale è possibile accedere ai file di certificato da installare.
6. Selezionare il file del certificato dall'elenco dei file disponibili tramite il connettore. Sono supportati i seguenti formati: .pem e .crt.

2.5.3.3 Tipi di file di certificato

Un breve abbecedario sulla PKI: le chiavi si dividono in due parti, una chiave pubblica e una chiave privata. La chiave pubblica può essere distribuita pubblicamente e ampiamente e può essere utilizzata per verificare, ma non replicare, le informazioni generate con la chiave privata. La chiave privata deve essere mantenuta segreta.

- I file .key sono generalmente la chiave privata utilizzata dal server per crittografare e impacchettare i dati per la verifica da parte dei client.
- I file .pem sono generalmente la chiave pubblica, utilizzata dal client per verificare e decifrare i dati inviati dai server. I file PEM possono anche essere chiavi private codificate.
- I file .p12 contengono entrambe le metà della chiave, in modo che gli amministratori possano gestire facilmente le metà delle chiavi.

- I file .cert o .crt sono i certificati firmati con una chiave pubblica, informazioni sul proprietario della chiave e la firma digitale dell'autorità di certificazione che ha emesso il certificato. Ciò consente di classificare un sistema come affidabile da parte di terzi.
- Nei file .cer, i certificati sono solitamente in formato binario o Base64. Pertanto, differiscono dai file .crt in termini di codifica.

2.5.4 Tipi di certificati

Per una connessione sicura ai servizi di rete, la bilancia richiede diversi certificati che possono essere caricati sulla bilancia. Si distingue tra i seguenti certificati:

- Certificati CA (autorità di certificazione fidate)
- Certificato del dispositivo
- Certificato di autenticazione WiFi
- CertificatoLDAPS

2.5.4.1 Certificati CA

Un certificato CA (Certificate Authority Certificate) è un certificato digitale emesso da un'autorità affidabile, la cosiddetta Certificate Authority (CA). Il suo scopo è quello di confermare l'autenticità e l'affidabilità di un partner o di un servizio di comunicazione. Quando due dispositivi o programmi comunicano tra loro in rete, un certificato CA consente a entrambe le parti di assicurarsi di essere effettivamente collegate al partner di comunicazione desiderato e non a un malintenzionato che si spaccia per lui.

Se un certificato CA è classificato come affidabile, il dispositivo accetta automaticamente tutti i certificati da esso derivati. In questo modo si crea una cosiddetta catena di certificati che può essere tracciata dal certificato della CA principale fino al rispettivo certificato del dispositivo.

2.5.4.2 Autorità di certificazione sconosciute

Il dispositivo offre anche la possibilità di fidarsi dei certificati che non sono stati emessi da un'autorità di certificazione nota. Se questa opzione è attivata, il dispositivo accetta tali certificati senza verificarne la validità tramite una catena di certificati. Ciò può essere utile in ambienti di test o di sviluppo, ma rappresenta un rischio per la sicurezza nell'uso produttivo, poiché l'autenticità e l'affidabilità dei certificati utilizzati non sono garantite. Questa opzione può essere attivata in Certificati, Certificati di sistema, [Fidati di autorità di certificazione sconosciute].

2.5.4.3 Certificati del dispositivo

I certificati dei dispositivi conferiscono a un dispositivo un'identità unica che gli consente di autenticarsi presso i sistemi connessi. Ciò garantisce che solo i dispositivi autorizzati possano accedere ai dati e che la comunicazione tra i dispositivi sia protetta. Questi certificati si basano sugli standard X.509 e sono generati da certificati a chiave pubblica (Public Key Infrastructure, PKI). Ciò consente ai dispositivi di identificare altri dispositivi e server affidabili.

In der Regel wird ein Gerätezertifikat von der internen Zertifizierungsstelle (CA) einer Organisation ausgestellt. Lo Zertifikat viene siglato con lo Schlüssel privato dello Stammzertifikat (CA-Zertifikat) dell'Organizzazione, che è la base per la firma di altri Zertifikat.

La sicurezza dei dispositivi è responsabilità dell'operatore e non è un servizio fornito dal produttore Sartorius. È quindi importante proteggere il dispositivo con il proprio certificato non appena arriva alla propria organizzazione. I dispositivi vengono consegnati franco fabbrica con un certificato standard di Sartorius.

I certificati dei dispositivi devono essere creati internamente al sistema e alla rete, il che richiede una CA privata. Esistono due approcci:

1. Creare una CA privata con strumenti quali OpenSSL o Microsoft CA.
2. Assumere un fornitore di PKI gestite (mPKI) per gestire le vostre esigenze di autenticazione e crittografia.

2.5.4.4 Certificati Wifi

Un certificato WiFi è un certificato digitale utilizzato per l'autenticazione e la crittografia sicure in una rete wireless (WLAN). In genere, tali certificati sono utilizzati come parte di WPA2-Enterprise o WPA3-Enterprise, in cui viene utilizzato il metodo di autenticazione 802.1X (ad esempio EAP-TLS).

Con WPA2-Enterprise o WPA3-Enterprise, l'autenticazione viene solitamente effettuata tramite il cosiddetto server RADIUS, spesso collegato a un servizio di directory (LDAP/Active Directory). I certificati vengono utilizzati per

consentire ai client e ai server RADIUS di identificarsi reciprocamente in modo sicuro.

2.5.4.5 Certificati LDAPS

I server LDAP (Lightweight Directory Access Protocol) utilizzano i certificati per proteggere le comunicazioni con i client o altri servizi. I server LDAP sono spesso responsabili della gestione centrale degli utenti e dei diritti. Se la connessione non è sicura, i dati sensibili degli utenti (ad esempio, password, informazioni su gruppi o ruoli) possono essere intercettati o manipolati.

Poiché il server LDAP comunica tramite LDAPS (LDAP via SSL/TLS), la connessione è criptata. Inoltre, il client utilizza il certificato del server per verificare l'identità del server LDAP. Il certificato del server LDAPS deve quindi essere memorizzato sul dispositivo.

2.5.5 Connessioni di rete sicure con SSL/TLS

I protocolli di sicurezza come SSL (Secure Sockets Layer) e TLS (Transport Layer Security) sono utilizzati per trasferire dati in modo sicuro. Essi definiscono le modalità di utilizzo degli algoritmi di crittografia e di autenticazione per garantire una connessione sicura contro le intercettazioni e le manipolazioni.

SSL è una vecchia tecnologia di sicurezza standard che stabilisce una connessione crittografata tra un server e un client. Nel caso della bilancia (ad esempio Cubis MCA), può trattarsi di una comunicazione criptata con un browser web che accede al sito web del dispositivo. Nel frattempo, SSL è stato sostituito da TLS (Transport Layer Security) come tecnologia successiva. Tuttavia, poiché SSL è il termine più noto, TLS/SSL viene utilizzato in relazione ai certificati o alla protezione dei dati trasmessi, anche se TLS viene utilizzato solo in background. Attualmente la bilancia supporta TLS fino alla versione 1.3.

2.5.5.1 Autorità di certificazione sconosciute

Il dispositivo offre anche la possibilità di fidarsi dei certificati che non sono stati emessi da un'autorità di certificazione nota. Se questa opzione è attivata, il dispositivo accetta tali certificati senza verificarne la validità tramite una catena di certificati. Ciò può essere utile in ambienti di test o di sviluppo, ma rappresenta un rischio per la sicurezza nell'uso produttivo, poiché l'autenticità e l'affidabilità dei certificati utilizzati non sono garantite. Questa opzione può essere attivata in Certificati, Certificati di sistema, [Fidati di autorità di certificazione sconosciute].

3 Esempi di applicazioni

Gli esempi di applicazione si riferiscono alla versione MCA dal pacchetto 09-03-04.01.xx in poi, insieme alle opzioni di impostazione e alle funzionalità che contiene. Per configurare le connessioni di rete, i connettori e le interfacce sono necessari diritti utente appropriati.

Per la configurazione dell'interfaccia Ethernet e Wi-Fi, è richiesta una conoscenza di base delle reti basate su TCP/IP e delle tecnologie di rete in generale.

Il prerequisito per tutti gli esempi è una connessione della bilancia con una rete via Ethernet (LAN) o Wi-Fi (WLAN).

3.1 Segnalazione delle impostazioni dei menu sul file server di Windows

Questo esempio descrive la configurazione e l'uso della bilancia MCA in modo che un file di report con tutte le impostazioni della bilancia possa essere esportato dal menu [Settings] in formato PDF, tramite il connettore [Windows file server] usando il protocollo di rete SMB, nella directory di destinazione di un'unità di rete rilasciata.

Per trasferire i file tramite il protocollo SMB, è necessaria un'estensione QAPP [Connection to Windows file server] dal pacchetto [Connectivity]. L'estensione può essere usata gratuitamente per 30 giorni, dopodiché deve essere licenziata.

Un'unità rilasciata con protocollo SMB nella vostra rete è un requisito per questa applicazione.

Questa applicazione può quindi essere utilizzata per memorizzare centralmente le impostazioni di menu di tutte le bilance MCA in rete.

3.1.1 Impostazione

Fasi di configurazione:

1. Attiva l'estensione QAPP [Connection to Windows File Server], se non è ancora stato fatto.
 - a. Apri il menu [Task management], seguito dal [QAPP Center].
 - b. Scegli il pacchetto software [Connectivity] e al suo interno il QAPP [Connection to Windows File Server].

Verranno visualizzate la descrizione e la versione del QAPP.

- c. Usa il pulsante [Licenza] per attivare questo QAPP; verranno visualizzate le informazioni sull'ordine e sulla licenza.
 - d. Se questo QAPP non è stato ordinato come [con licenza di fabbrica], avvia la versione di prova o inserisci il codice di licenza che hai acquistato per questo QAPP.
2. Impostare un connettore a un file server Windows, ad esempio, [Il mio server SMB per le impostazioni].
 - a. Aprire il menu [Settings].
 - b. Vai a [Connections] -> [Connectors] -> [SMB].
 - c. Usa il pulsante [+] per attivare la creazione di un nuovo connettore.
 - d. Assegna un nome unico a questo connettore.
 - e. Inserisci il percorso di rete per Host e Share, assicurandoti di usare l'ortografia corretta [//nome host/nome share].
 - f. Inserisci anche il nome di una sotto-directory sul server, in cui salvare i file.
 - g. Inserisci il nome utente e la password per l'accesso all'unità autorizzata nella tua rete. Fate attenzione alla notazione corretta anche qui, in particolare alle lettere maiuscole/minuscole.

3.1.2 Applicazione

Passi dell'utente:

1. Dal menu principale, utilizzare il pulsante [Setup] per aprire il menu per le impostazioni del bilanciamento.
2. Premete il tasto [Export] nella barra di navigazione e degli strumenti.
3. Viene visualizzata una lista dei connettori attraverso i quali il file di report può essere esportato.
4. Selezionare il connettore creato, ad esempio, [Il mio server SMB per le impostazioni]. Il file di report viene creato ed esportato al server SMB tramite il connettore.
5. Si ottengono i messaggi [Report inviato] e [Processo completato] come conferma del successo dell'esportazione. Il file di report in formato PDF, con il relativo file di controllo, è ora presente nel server e può essere visualizzato.
6. Se il file di report non può essere esportato, allora questo file non è perso, vedi Risoluzione dei problemi.

Nota: Il formato di file PDF è un formato dati indipendente dalla piattaforma per i documenti. L'output di stampa in questo formato può essere visualizzato su ogni computer. Per ogni file di output PDF, viene creato un file di prova corrispondente contenente il checksum (valore di hash MD5) dei dati PDF. Quando il file viene trasferito, questo checksum viene salvato nell'audit trail. Utilizzando uno strumento appropriato, questo file PDF può essere confrontato con il file di controllo per assicurare l'integrità dei dati PDF.

3.1.3 Risoluzione dei problemi

Nessun file di report esportato nella directory del file server SMB.

1. Assicuratevi che tutti i passi di configurazione menzionati sopra siano stati seguiti.
2. Controllare che la bilancia sia collegata alla rete, ad esempio tramite un cavo Ethernet. L'indirizzo IP della bilancia nella rete deve essere visualizzato nel [Status center] sotto [Device information].
3. Controlla il percorso di rete nel connettore e l'ortografia corretta di Host e Share, così come il nome utente e la password per i diritti di accesso al file server SMB.
4. Testate la connessione dei connettori con il file server SMB attivando il pulsante [Info] nella panoramica dei valori impostati. Se tutte le impostazioni sono corrette e il file server SMB è accessibile, riceverai un messaggio che indica che il connettore è disponibile.
5. In caso contrario, controllate che il file server SMB sia presente nella rete e che un file possa essere salvato lì dal vostro PC.
6. Se c'è un messaggio di errore [Transfer failure], allora potete fare quanto segue con l'esportazione:
 - a. Riprova: Riprova l'esportazione del file di report al server di rete.
 - b. Riprova più tardi: L'esportazione del file di report viene ripetuta automaticamente. I trasferimenti in sospeso vengono visualizzati nel [Centro di stato] sotto [Messaggi].
 - c. Redirect: puoi reindirizzare il file di report a un altro connettore.
 - d. Elimina: L'esportazione del file di report viene annullata e cancellata.

3.2 Aggiornare il centro QAPP del server FTP

Questo esempio descrive la configurazione e l'applicazione del bilanciamento Cubis® MCA, al fine di caricare l'aggiornamento per il Centro QAPP di un server FTP.

Per il trasferimento di file da un server di rete FTP, è necessaria un'estensione QAPP [Connection to FTP/FTPS] dal pacchetto [Connectivity]. L'estensione può essere usata gratuitamente per 30 giorni, dopodiché deve essere

concessa in licenza.

Il prerequisito per questa applicazione è un server FTP adeguatamente impostato nella vostra rete.

Per le bilance MCA in rete, questa applicazione permette l'aggiornamento del QAPP Center da una fonte centrale.

3.2.1 Impostazione

Fasi di configurazione:

1. Attivare l'estensione QAPP [Connessione a FTP/FTPS], se questo non è stato ancora fatto.
 - a. Apri il menu [Task management], seguito dal [QAPP Center].
 - b. Seleziona il pacchetto software [Connectivity] e, al suo interno, la QAPP [Connection to FTP/FTPS]. Verranno visualizzate la descrizione e la versione del QAPP.
 - c. Usa il pulsante [Licenza] per attivare questo QAPP; verranno visualizzate le informazioni sull'ordine e sulla licenza.
 - d. Se questo QAPP non è stato ordinato come [con licenza di fabbrica], avvia la versione di prova o inserisci il codice di licenza che hai acquistato per questo QAPP.
2. Impostare un connettore a un server FTP, ad esempio, [Il mio server FTP per l'aggiornamento del Centro QAPP].
 - a. Aprite il menu [Settings].
 - b. Vai a [Connections] -> [Connectors] -> [FTP].
 - c. Usa il pulsante [+] per attivare la creazione di un nuovo connettore.
 - d. Assegna un nome unico a questo connettore.
 - e. Inserisci l'indirizzo IP del server di rete, assicurandoti di scriverlo correttamente
 - f. Un numero di porta è richiesto per la connessione: il numero 21 è stato assegnato. Se necessario, è possibile inserire un numero di porta diverso.
 - g. Per aggiornare il QAPP Center, puoi anche specificare una sotto-directory per i file memorizzati nel server.
 - h. Inserisci il nome utente e la password per accedere al server FTP. Fate attenzione alla notazione corretta anche qui, in particolare alle lettere maiuscole/minuscole.

3.2.2 Applicazione

Passi dell'utente:

1. Dal menu principale, usare il pulsante [Setup] per aprire il menu per le impostazioni del bilanciamento.
2. Passare alla voce di menu [Device maintenance] -> [Install QAPP Center]. Viene visualizzato un elenco di connettori con i quali è possibile caricare un pacchetto per l'aggiornamento del QAPP Center.
3. Selezionare il connettore creato, ad esempio [Il mio server FTP per l'aggiornamento del QAPP Center]. Viene stabilita la connessione al server FTP e viene visualizzato un elenco di pacchetti disponibili per l'aggiornamento del QAPP Center.
4. Selezionare la versione desiderata del Centro QAPP e confermare il messaggio di aggiornamento.
5. Il QAPP Center viene ora copiato nel saldo dal server FTP e aggiornato. Come conferma, viene visualizzata la versione aggiornata del Centro QAPP.
6. Vedi Risoluzione dei problemi, se l'aggiornamento non può essere fatto.

3.2.3 Risoluzione dei problemi

L'aggiornamento del centro QAPP non è possibile tramite il connettore.

1. Assicuratevi che tutti i passi di configurazione menzionati sopra siano stati seguiti.
2. Controllare che la bilancia sia collegata alla rete, ad esempio tramite un cavo Ethernet. L'indirizzo IP della bilancia nella rete deve essere visualizzato nel [Status center] sotto [Device information].
3. Controlla l'indirizzo IP e il numero di porta del server FTP, così come il nome utente e la password per i diritti di accesso al server nel connettore.
4. Testate la connessione dei connettori con il server FTP attivando il pulsante [Info] nella panoramica dei valori impostati. Se tutte le impostazioni sono corrette e il server FTP è accessibile, riceverai un messaggio che indica che il connettore è disponibile.
5. Controllate con il vostro PC se la sotto-directory specificata e il file per l'aggiornamento del QAPP Center sono presenti nel server FTP nella rete.

3.3 Visualizza le voci della traccia di controllo tramite browser web

Questo esempio descrive l'impostazione e l'uso della bilancia MCA in modo che le voci nella traccia di controllo della bilancia possano essere visualizzate utilizzando il browser web.

Il browser web [Chrome] è raccomandato per il funzionamento remoto della bilancia MCA.

Una connessione sicura della bilancia con il browser attraverso il protocollo HTTPS richiede determinati certificati del dispositivo.

Per questo, l'equilibrio MCA fornisce i propri certificati del dispositivo per il download. Questi certificati del dispositivo devono essere importati nel browser per l'accesso remoto sicuro al sito web del dispositivo. C'è una descrizione separata sul tema [Certificati].

L'ambito completo della pista di controllo può essere utilizzato solo dopo aver attivato l'estensione QAPP [pista di controllo] nel Centro QAPP sotto [Pharma (QP1)].

Un uso di questa applicazione è, per esempio, il monitoraggio remoto centrale delle impostazioni in tutte le bilance MCA in rete.

3.3.1 Impostazione

Fasi di configurazione:

1. Attivare l'estensione QAPP [Audit trail], se non ancora fatto.
 - a. Apri il menu [Task management], seguito dal [QAPP Center].
 - b. Seleziona il pacchetto software [Pharma] e il QAPP [Audit trail] in esso. Verranno visualizzate la descrizione e la versione del QAPP.
 - c. Usa il pulsante [Licenza] per attivare questo QAPP; verranno visualizzate le informazioni sull'ordine e sulla licenza.
 - d. Se questo QAPP non è stato ordinato come [con licenza di fabbrica], avvia la versione di prova o inserisci il codice di licenza che hai acquistato per questo QAPP.
2. Attivare il sito web del bilancio MCA, se non ancora fatto.
 - a. Aprite il menu [Settings].
 - b. Vai a [Connections] -> [Website / web services].
 - c. Impostare la voce di menu [Accesso al sito web] su [Abilitato, nessuna autenticazione].
3. Se necessario, attivare l'accesso remoto al sito web del saldo MCA.
 - a. Aprite il menu [Settings].
 - b. Vai a [Connections] -> [Website / web services].
 - c. Sotto la voce di menu [Accesso remoto], selezionate l'impostazione [Vista e controllo remoto].

3.3.2 Applicazione

Passi dell'utente:

1. Avviare il browser web, ad esempio, [Chrome] sul tuo PC.
2. Inserisci l'indirizzo IP della tua bilancia, che viene visualizzato in [Status center] sotto [Device information].
3. Se non hai ancora importato i certificati del dispositivo della bilancia nel browser, vedrai il messaggio [Questa non è una connessione sicura] nel browser.
4. Utilizzando il pulsante [Advanced] e il link [Next...], si può ora andare all'indirizzo IP della bilancia, che in questo caso è visto come non sicuro, oppure si devono prima importare i certificati del dispositivo della bilancia nel browser. C'è una descrizione separata sull'argomento [Certificati].
5. Altrimenti, la pagina [My Cubis] (home page) viene visualizzata nel browser.
6. Seleziona la pagina [Audit trail] per l'esempio.
7. Ora è possibile ordinare l'elenco delle voci in base a ID, timestamp e utente.
8. L'elenco delle voci può essere visualizzato in ordine crescente o decrescente.
9. Puoi anche impostare dei filtri, per visualizzare solo gruppi specifici di voci.

3.3.3 Risoluzione dei problemi

La pagina iniziale della bilancia non viene visualizzata nel browser.

1. Controllare che la bilancia sia collegata alla rete, ad esempio tramite un cavo Ethernet. L'indirizzo IP della bilancia nella rete deve essere visualizzato nel [Status center] sotto [Device information].
2. Assicuratevi che la voce di menu [Website access] sia impostata su [Enabled].

La connessione alla bilancia viene visualizzata come [Unsecure] nel browser.

1. Importa i certificati del dispositivo della bilancia nel tuo browser. C'è una descrizione separata sul tema [Certificati].

La pagina [Audit trail] non può essere selezionata sulla pagina iniziale della bilancia.

1. Assicuratevi che tutti i passi di configurazione menzionati sopra siano stati seguiti. In particolare, l'estensione QAPP [Audit trail] è stata attivata e la relativa licenza è ancora valida.

3.4 Sincronizzare data e ora con il server NTP

Questo esempio descrive la configurazione e l'applicazione di Cubis® MCA, per permettere una sincronizzazione della data e dell'ora della bilancia con un server NTP.

Il prerequisito per questo uso è l'accesso a un server NTP nella vostra rete aziendale o nella rete pubblica.

La deviazione temporale tra la bilancia e il server NTP viene controllata ogni 10 minuti. Se la deviazione è superiore a 3 secondi, l'ora nella bilancia viene corretta e la modifica viene inserita nella traccia di controllo.

Questa applicazione permette un facile aggiornamento automatico e la sincronizzazione di data e ora su tutte le bilance MCA in rete.

3.4.1 Impostazione

Fasi di configurazione:

1. Impostare una configurazione NTP attiva.
 - a. Aprite il menu [Settings].
 - b. Passare a [Impostazioni dispositivo] -> [Data e ora] -> [Configurazione NTP].
 - c. Attivare la configurazione delle impostazioni del server NTP usando il pulsante [Edit].
 - d. Impostare la voce di menu [NTP operating status] su [Enabled].
 - e. Attraverso il [Server IP] inserite l'indirizzo del server NTP nel formato IPv4, ad esempio 192.53.103.108. (Questo è un server NTP dell'Istituto Federale Fisico-Tecnico di Braunschweig, Germania).
 - f. Confermate la configurazione NTP con il pulsante [OK].
 - g. Testate la connessione al server NTP attivando il pulsante [Info] nella panoramica della configurazione NTP.
2. Imposta il fuso orario corretto per la tua posizione.
 - a. Aprite il menu [Settings].
 - b. Passare a [Impostazioni dispositivo] -> [Data e ora] -> [Imposta data e ora].
 - c. Attivare le impostazioni di data e ora con il pulsante [Modifica].
 - d. Impostare la propria posizione utilizzando la voce di menu [Time zone], [UTC +/- time, place]. In seguito, l'ora e la data vengono visualizzate immediatamente corrispondenti alla vostra ora locale.

Nota: Dopo aver impostato la data, l'ora e il fuso orario, la bilancia MCA chiede di riavviare il sistema.

3.4.2 Risoluzione dei problemi

Nessuna connessione possibile al server NTP.

1. Assicuratevi che tutti i passi di configurazione menzionati sopra siano stati seguiti.
2. Controllare che la bilancia sia collegata alla rete, ad esempio tramite un cavo Ethernet. L'indirizzo IP della bilancia nella rete deve essere visualizzato nel [Status center] sotto [Device information].
3. Controllate con il vostro PC se potete accedere all'indirizzo IP del server NTP.

4 Appendice

4.1 Bastoni Wi-Fi compatibili

Cubis® MCA supporta le più comuni chiavette Wi-Fi (adattatori USB WLAN) che sono disponibili sul mercato.

Tenete a mente i seguenti elementi quando scegliete una chiavetta Wi-Fi:

1. Evitare i bastoni Wi-Fi senza nome. Comprate sempre una marca conosciuta.
2. Se possibile, controllate la scheda tecnica della chiavetta Wi-Fi per assicurarvi che contenga uno dei seguenti chip set supportati.

I set di chip Wi-Fi supportati sono:

- 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. Abbreviazioni

DHCP	Dynamic Host Configuration Protocol	Un protocollo di comunicazione nella tecnologia informatica. Permette l'assegnazione della configurazione di rete ai client da parte di un server.
DNS	Domain Name System	Sistema per la risoluzione dei nomi dei computer in indirizzi IP e viceversa.
FTP	File Transfer Protocol	Un protocollo di rete standard per il trasferimento di file tra un client e un server all'interno di una rete.
FTPS	FTP over TLS	Un metodo per criptare il File Transfer Protocol (FTP).
HTTPS	Hypertext Transfer Protocol Secure	Un protocollo di comunicazione con il quale i dati possono essere trasmessi come criptati.
IPv4	Internet Protocol version 4	Protocollo Internet della versione 4.
IPv6	Internet Protocol version 6	Protocollo Internet della versione 6.
MAC address	Media Access Control address	Indirizzo hardware fisico, identificatore unico del dispositivo nella rete.
NTP	Network Time Protocol	Uno standard per sincronizzare gli orologi nei sistemi informatici.
PNG	Portable Network Graphics	Grafica di rete portatile, un formato grafico raster con compressione dei dati senza perdita.
PSK	Pre-shared key	Metodo di crittografia in cui la chiave deve essere conosciuta da entrambi i partecipanti prima della comunicazione.
REST	Representational State Transfer	Paradigma di programmazione per sistemi distribuiti, in particolare per i servizi web.
SMB	Server Message Block	Un protocollo di rete per file, stampa e altri servizi di server nelle reti di computer.
SSID	Service Set Identifier	Nome della rete liberamente selezionabile, ad esempio, per il Wi-Fi.
URL	Uniform Resource Locator	Identificazione per Internet o indirizzi web.
UTC	Universal Time, Coordinated	Ora mondiale, anche ora terrestre o tempo universale.
WEP	Wired Equivalent Privacy	Protocolli di crittografia standard per WLAN.
Wi-Fi	Wireless Fidelity	Rete senza fili, sinonimo di WLAN.
WLAN	Wireless Local Area Network	Senza fili, rete locale.
WPA	Wi-Fi Protected Access	Metodi di crittografia per una rete senza fili. Successore di WEP.
WPA2	Wi-Fi Protected Access 2	Implementazione di uno standard di sicurezza per le reti radio. Successore del WPA.