Descripción de la red, Ethernet y Wi-Fi (WLAN) para la balanza MCA Cubis®

Este documento describe cómo conectar la balanza a una red a través de Ethernet y Wi-Fi (WLAN). Se dan ejemplos para ilustrar cómo configurar y utilizar la balanza en la práctica.

Resumen ejecutivo

La balanza de laboratorio Cubis® MCA Premium ofrece opciones de conectividad completas y flexibles para integrar la balanza en la TI del laboratorio. Un gran número de protocolos de TI estandarizados, como el servicio web REST, SMB o LDAP, están disponibles a través de Ethernet y Wi-Fi, lo que permite la integración directa sin el uso de middleware adicional. Además, la Cubis® puede controlarse de forma remota a través de la red mediante un navegador web y se puede consultar el registro de auditoría y otra información de estado.

1 Conexión de red Ethernet y Wi-Fi 4
1.1 Ajustes generales 4
1.2 Ethernet (LAN) 4
1.2.1 Protocolo IPv4 5
1.2.2 Protocolo IPv6 5
1.2.3 DNS 1 y DNS 2 5
1.3 Wi-Fi (WLAN) 5
1.3.1 SSID y contraseña del Wi-Fi 6
1.3.2 Protocolo IPv4/IPv6 y DNS 1/2 6
2 Servicios de red 6
2.1 Comunicación en serie 6
2.1.1 Protocolo del OSE 6
2.1.2 Protocolo xBPI 7
2.1.3 Protocolo SICS 7
2.1.4 QAPP directo 7
2.2 Conectores de red 7
2.2.1 YDP30-NET 7
2.2.2 Impresora de red 7
2.2.3 FTP / FTPS 8
2.2.4 Protocolo SMB 8
2.3 Página web 8
2.3.1 Servicios web 8
2.4 Servidor NTP para la fecha y la hora 8
2.5 Certificados 8
2.5.1 Obligaciones del operador 8
2.5.2 Restablecer certificados 9
2.5.3 Instalar o actualizar certificados 9
2.5.3.1 Certificados de cliente 9
2.5.3.2 Certificados CA 9
2.5.3.3 Tipos de archivos de certificado 9
2.5.4 Tipos de certificados 10
2.5.4.1 Certificados CA 10
2.5.4.2 Autoridades de certificación desconocidas 10
2.5.4.3 Certificados de dispositivos 10
2.5.4.4 Certificados Wifi 11
2.5.4.5 Certificados LDAPS 11
2.5.5 Conexiones de red seguras con SSL/TLS 11
2.5.5.1 Autoridades de certificación desconocidas 11
3 Ejemplos de aplicación 11
3.1 Informe de la configuración del menú en el servidor de archivos de Windows 11
3.1.1 Configuración 12
3.1.2 Aplicación 12
3.1.3 Solución de problemas 12

3.2 Actualizar el Centro QAPP del servidor FTP 13
3.2.1 Configuración 13
3.2.2 Aplicación 13
3.2.3 Solución de problemas 13
3.3 Ver las entradas del registro de auditoría a través del navegador web 14
3.3.1 Configuración 14
3.3.2 Aplicación 14
3.3.3 Solución de problemas 15
3.4 Sincronizar la fecha y la hora con el servidor NTP 15
3.4.1 Configuración 15
3.4.2 Solución de problemas 15
4 Anexo 16
4.1 Bastones Wi-Fi compatibles 16
5. Abreviaturas 17

1 Conexión de red Ethernet y Wi-Fi

Una balanza Cubis® MCA puede conectarse a una red basada en TCP/IP mediante un cable a través de la conexión Ethernet (toma RJ45) y de forma inalámbrica a través de un adaptador USB Wi-Fi (WLAN stick).

Las velocidades de transmisión de la conexión de red son de 10 Mbit/seg (10BASE-T, Ethernet) y 100 Mbit/seg (100BASE-TX Fast Ethernet).

La conexión Ethernet se realiza con un cable de conexión, CAT 5 o superior, trenzado en pares, apantallado, 1:1, UTP/STP, enchufe RJ45; por ejemplo, cable de conexión CAT 5 según el uso (recto/transversal).

Para una conexión inalámbrica, Cubis® MCA es compatible con los adaptadores USB Wi-Fi más comunes (memorias WLAN) que se ofrecen en el mercado.

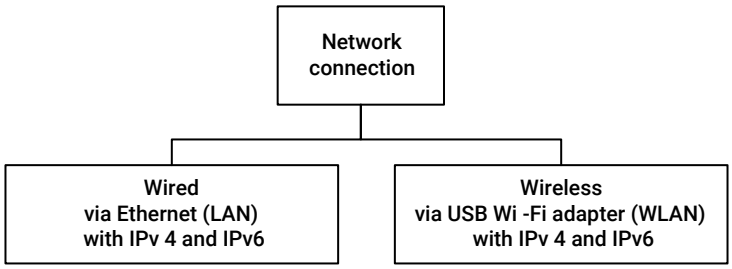

Figura 1: Conexión a la red

La balanza Cubis® MCA puede tener una dirección IPv4 y otra IPv6 en Ethernet y Wi-Fi respectivamente, es decir, hasta 4 direcciones.

A través de las conexiones de red Ethernet (LAN) y Wi-Fi (WLAN), la balanza Cubis® MCA ofrece simultáneamente varios servicios de red.

1.1 Ajustes generales

El nombre de host de la balanza, ex fábrica, se compone de la designación de la serie y de los 3 últimos bytes de la dirección MAC, por ejemplo, [cubis-1a477e]. El nombre de host puede seleccionarse libremente, pero debe ser único en una red.

1.2 Ethernet (LAN)

Para la conexión Ethernet de la balanza, se pueden utilizar los protocolos IPv4 así como IPv6. Se puede establecer por separado para cada protocolo, si la dirección IP debe obtenerse automáticamente o si la balanza recibe una dirección IP fija. También se puede desactivar completamente el protocolo correspondiente.

En el resumen de los ajustes para Ethernet, el estado muestra si se ha establecido una conexión con la red. Además, aquí también se muestra la dirección MAC única de la balanza, por ejemplo, [00:30:D6:1F:77:569].

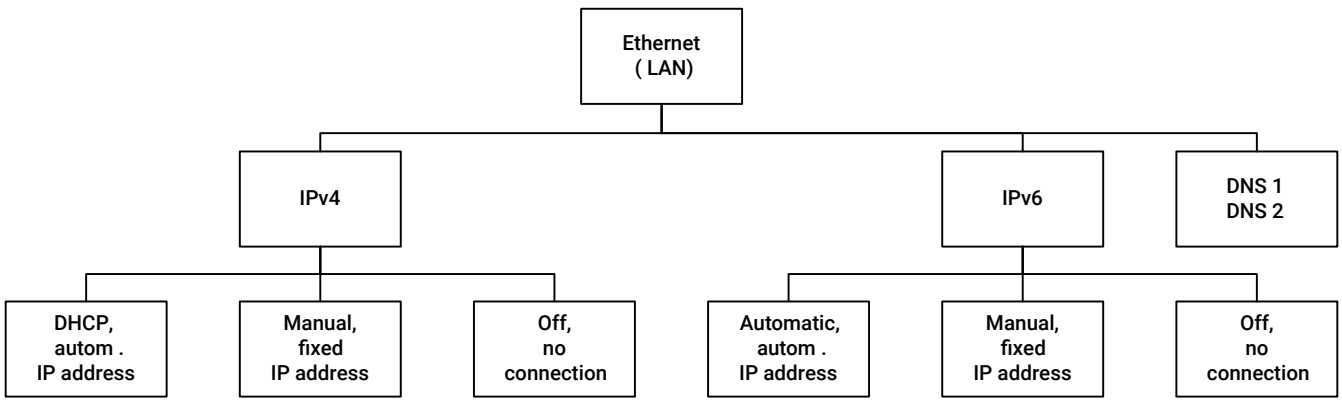

Figura 2: Ethernet con IPv4/IPv6

Para el funcionamiento con una dirección IP fija, además de la dirección IP, dependiendo del protocolo, también hay que introducir manualmente la máscara de subred y la pasarela para IPv4, o la longitud del prefijo y la pasarela para

IPv6. La introducción de la puerta de enlace es opcional y sólo es necesaria cuando se necesita una conexión a Internet.

Toda la información necesaria para ello puede ser proporcionada por el administrador de red responsable de la red de la empresa.

1.2.1 Protocolo IPv4

La dirección IP para el protocolo IPv4 (4*8 bits = 32 bits) consta de 4 números decimales entre 0 y 255, que se separan con un punto, por ejemplo, [123.4.56.123]. Este formato se aplica para la introducción de la dirección IP fija, la marca de subred y la pasarela.

1.2.2 Protocolo IPv6

La dirección IP para el protocolo IPv6 (8*16 bits = 128 bits) consta de 8 números hexadecimales alfanuméricos entre 0 y FFFF, que se separan con dos puntos, por ejemplo, [ecb1:d583:6341:baf76:0:0:0:1].

Los primeros 4 bloques (64 bits) constituyen el prefijo y los últimos 4 bloques el identificador de interfaz. La máscara de red IPv4 y la dirección de red IPv4 se sustituyen por la longitud del prefijo y el prefijo en IPv6. La longitud del prefijo especifica el número de bits que constituyen el prefijo. La longitud típica del prefijo es de 64. El prefijo sustituye a la máscara de subred en el caso de IPv6.

1.2.3 DNS 1 y DNS 2

En los sistemas de red basados en IP, el DNS (Domain Name System) ayuda a responder a las consultas de resolución de nombres. Una red puede tener varios servidores DNS, el Cubis® MCA soporta la entrada de dos servidores.

Se puede introducir la dirección IP o el nombre del servidor para cada servidor DNS.

En el caso de DHCP, el servidor DNS es proporcionado automáticamente por el servidor DHCP. Además, en este caso, DNS1 y DNS2 se añaden a la lista de servidores DNS.

1.3 Wi-Fi (WLAN)

Se puede conectar un adaptador USB Wi-Fi (WLAN stick) a la balanza MCA; varios adaptadores de este tipo no son compatibles.

En la vista general de los ajustes para Wi-Fi (WLAN), se muestra a través del estado, si un adaptador USB Wi-Fi correspondiente está conectado y está conectado a la red.

Muestra de estado

- No hay ningún dispositivo disponible - No hay ningún adaptador USB Wi-Fi conectado.
- Desconectado - No hay conexión con la red Wi-Fi, por ejemplo, no se ha iniciado la sesión con el SSID y la contraseña del Wi-Fi.
- Listo - Conexión establecida con la red Wi-Fi.
- En línea - Conexión establecida con la red Wi-Fi e Internet.

Si se ha establecido una conexión, también se muestra aquí la dirección MAC única del adaptador USB Wi-Fi, por ejemplo, 34:C9:F0:89:6F:D6.

En el anexo, el apartado: Bastones Wi-Fi compatibles.

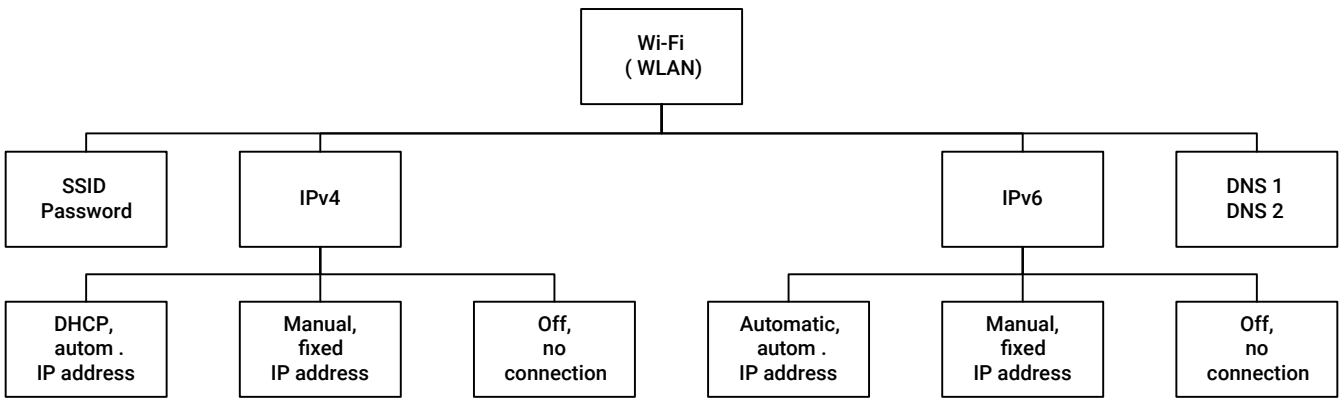

Figura 3: Wi-Fi con IPv4/IPv6

Para el funcionamiento con una dirección IP fija, además de la dirección IP, dependiendo del protocolo, también hay que introducir manualmente la máscara de subred y la pasarela para IPv4, o la longitud del prefijo y la pasarela para IPv6. La introducción de la puerta de enlace es opcional y sólo es necesaria cuando se necesita una conexión a Internet.

Toda la información necesaria para ello puede ser proporcionada por el administrador de red responsable de la red de la empresa.

1.3.1 SSID y contraseña del Wi-Fi

Para conectarse a una red Wi-Fi, hay que introducir el SSID Wi-Fi (el nombre único de la red Wi-Fi) y la contraseña Wi-Fi (la clave de la red Wi-Fi).

Para la autenticación, la balanza MCA admite los estándares WEP, WPA-PSK y WPA2-PSK y, por tanto, también el método PSK para el cifrado.

1.3.2 Protocolo IPv4/IPv6 y DNS 1/2

Para el protocolo IPv4 e IPv6, así como para DNS 1 y DNS 2, se aplica la misma descripción para Wi-Fi (WLAN) que en el caso de Ethernet (LAN).

2 Servicios de red

A través de la red, la balanza Cubis® MCA ofrece varios servicios simultáneamente, una comunicación serie con diferentes protocolos, conectores para la conexión a dispositivos de almacenamiento masivo en red e impresoras, un sitio web y servicio web para el acceso remoto, así como la conexión a un servidor NTP para la sincronización de fecha y hora.

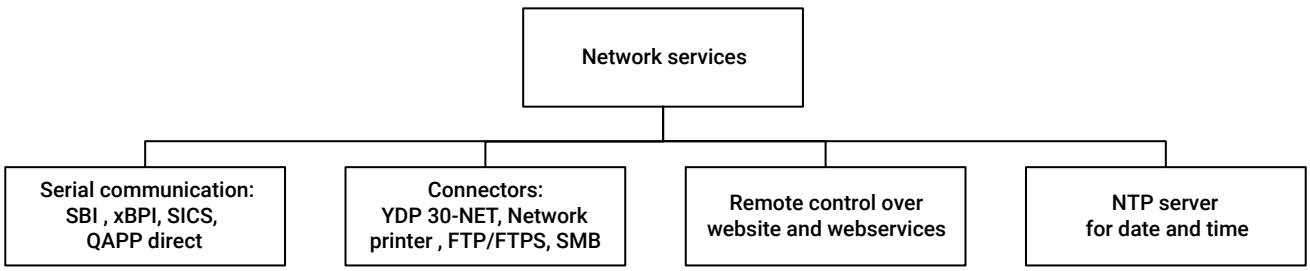

Figura 4: Servicios de red

2.1 Comunicación en serie

Utilizando la conexión de red, es posible utilizar los protocolos de comunicación en serie SBI, xBPI, SICS, miniSICS, que pueden funcionar independientemente de la tarea activa y de su uso. Esta conexión cliente/servidor requiere la configuración de un puerto TCP conjunto.

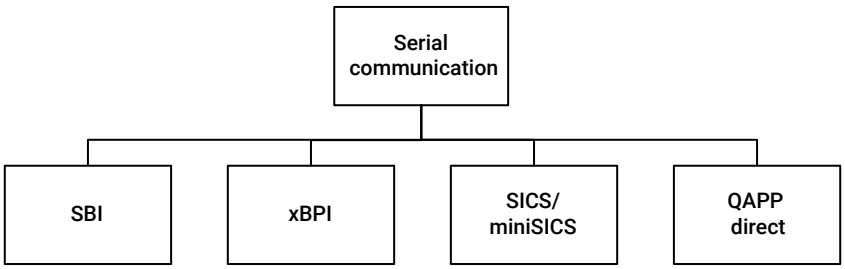

Figura 5: Comunicación en serie a través de la red

2.1.1 Protocolo del OSE

Este sencillo protocolo, basado en ASCII, permite controlar las funciones básicas de la balanza mediante comandos ESC. La salida de los valores de visualización puede solicitarse individualmente a través de un comando ESC, o automáticamente con cada nuevo resultado de pesaje en el ciclo de la secuencia de visualización, o automáticamente después de intervalos de tiempo específicos. Es posible elegir si la salida se proporciona con un valor de visualización estable solamente, o también sin que el valor de visualización sea estable. El formato de

salida puede seleccionarse con o sin identificador (cabecera).

Los comandos SBI y los formatos de salida se dan en una descripción de la interfaz por separado.

2.1.2 Protocolo xBPI
Este protocolo binario ofrece una amplia gama de comandos. Puede utilizarse para controlar numerosas funciones de la balanza.

Hay una descripción separada de la interfaz de los posibles comandos xBPI.

2.1.3 Protocolo SICS
El protocolo SICS (Standard Interface Command Set) establece una compatibilidad con el protocolo MT-SICS de Mettler y permite el envío de comandos a la balanza para las funciones básicas. Sin embargo, hay que tener en cuenta que existen diferencias debido a las diferentes plataformas de hardware/software.

Los comandos SICS y miniSICS implementados en la balanza se dan en una descripción de interfaz separada.

2.1.4 QAPP directo
Sólo los QAPP especiales, que son iniciados por una tarea, pueden utilizar la interfaz para sus fines de entrada y salida. Las posibilidades de entrada y salida a través de la interfaz se describen en el QAPP especial correspondiente.

2.2 Conectores de red
En Cubis® MCA, los conectores establecen la conexión con los servidores de red que se van a utilizar como dispositivos de almacenamiento masivo o como impresoras.

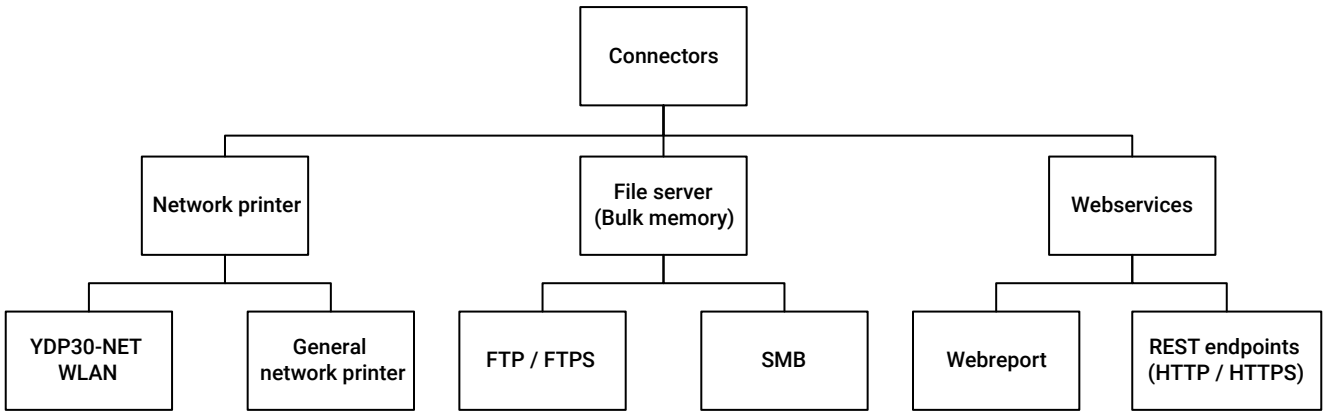

Figura 6: Conectores de red

La impresora de red YDP30-NET puede conectarse por WLAN o como impresora de red general con una red Wi-Fi independiente o una red corporativa mediante DHCP.

Para conectarse a un dispositivo de almacenamiento masivo, como un servidor de archivos de Windows, FTP/FTPS o STARLIMS, es necesaria una extensión especial de QAPP, que debe activarse a través del Centro de QAPP en [Conectividad].

2.2.1 YDP30-NET
Este conector está pensado para conectar una impresora YDP30-NET con un cable (LAN) o una conexión inalámbrica (WLAN). Un conector requiere que se introduzca un nombre de conector, una dirección IP o un nombre de host en la impresora, así como un número de puerto acordado entre la impresora y la balanza.

La conexión inalámbrica de la impresora YDP30-NET se describe en unas instrucciones aparte.

2.2.2 Impresora de red
El conector de impresora de red permite, por ejemplo, la conexión a una impresora A4 en una red Wi-Fi independiente con componentes Wi-Fi estándar, o en una red corporativa por DHCP con métodos de autenticación estándar. La impresora de red debe ser compatible con IPP (Internet Printing Protocol).

Un conector requiere que se introduzca un nombre de conector, una dirección IP o un nombre de host en la impresora, así como el protocolo de transferencia.

La descripción separada [Concepto de impresión] describe la configuración y aplicación de una impresora de red

con un ejemplo de aplicación.

2.2.3 FTP / FTPS

El Protocolo de Transferencia de Archivos (FTP) es un protocolo de red estándar para transferir archivos informáticos entre un cliente y un servidor en una red informática.

La balanza es el cliente FTP y puede almacenar archivos en un servidor FTP o recuperar archivos de un servidor FTP utilizando el protocolo. En el caso de FTPS, la conexión también está cifrada; los certificados necesarios para ello se describen por separado.

Para conectarse a un servidor FTP/FTPS, hay que crear un conector con un nombre único, la dirección IP y el número de puerto del servidor de red, si es necesario, un subdirectorio en el servidor y el nombre de usuario y la contraseña.

Nota: Con varios conectores de la balanza al mismo servidor, pero con diferentes subdirectorios, el almacenamiento de datos puede estructurarse fácilmente según el tema (copia de seguridad, informe, ...).

2.2.4 Protocolo SMB

El conector del servidor de archivos de Windows utiliza el protocolo de red SMB. Este protocolo facilita el acceso a las unidades de red liberadas de los ordenadores Windows o Linux para almacenar o recuperar archivos de datos en los directorios de destino seleccionados.

2.3 Página web

La página web de la balanza MCA puede visualizarse simplemente a través de la dirección IP de la balanza con un navegador web. En la página [My Cubis] (página de inicio) se muestran los identificadores de dispositivo establecidos, la información general del dispositivo de la balanza y la información sobre el servicio.

Utilizando la página de [Operación remota], dependiendo de la configuración del menú, se puede mostrar [Sólo vista] o [Vista y control remoto] de la balanza MCA a través del navegador.

La página [Captura de pantalla] crea un archivo PNG de la pantalla actual, que puede guardarse.

Si se ha activado la extensión QAPP [Audit trail] en el Centro QAPP del paquete [Pharma], también se muestra la página web [Audit trail]. Las entradas del registro de auditoría pueden filtrarse, clasificarse y exportarse según los temas.

El acceso a la página web se puede desactivar completamente a través del menú y, por tanto, también el control remoto a través del servicio web REST.

2.3.1 Servicios web

La operación remota de las funciones subyacentes de la balanza MCA también puede realizarse a través de un servicio web REST.

Hay una descripción separada de los servicios web REST disponibles de la balanza MCA.

2.4 Servidor NTP para la fecha y la hora

Cubis® MCA ofrece la posibilidad de sincronizar la fecha y la hora con un servidor NTP. Para ello, se puede activar la conexión con el servidor e introducir la dirección IP del mismo en los ajustes del dispositivo de MCA en Configuración de fecha/hora y NTP.

2.5 Certificados

La balanza MCA de Cubis® admite el uso de certificados para una integración de confianza en la infraestructura informática local. La MCA puede procesar los certificados de agencias de certificación (CA) de confianza, para identificar servidores de confianza. La MCA también proporciona sus propios certificados de dispositivo para su descarga. Estos certificados de dispositivo se importan en los navegadores para el acceso remoto seguro al sitio web del dispositivo.

Hay una descripción separada sobre el tema de los [Certificados].

Los certificados de dispositivo se basan en la norma X.509 y utilizan criptografía de clave pública, en la que se emplea un par de claves formado por una clave pública y otra privada. Este par de claves permite la transmisión cifrada de datos, la verificación de firmas digitales y la autenticación fiable de identidades. Dependiendo de cómo se cree y almacene la clave privada, puede ser necesario descifrarla con una frase de contraseña antes de utilizarla.

2.5.1 Obligaciones del operador

Las balanzas Cubis MCA de Sartorius se entregan con certificados de dispositivo preinstalados que tienen una

validez limitada. Los operadores tienen la opción de renovar los certificados instalados originalmente e importar sus propios certificados.
El operador es responsable de gestionar y actualizar los certificados y garantizar su validez. Para evitar posibles advertencias de seguridad o restricciones en las conexiones seguras, es importante comprobar periódicamente la validez de los certificados y renovarlos si es necesario.

La actualización del certificado no afecta a la función de pesaje ni a la integración en la infraestructura informática local. Por lo tanto, no es necesario recalificar o revalidar los dispositivos al actualizar los certificados.

2.5.2 Restablecer certificados

Si aparece una advertencia sobre la caducidad del certificado después de restablecerlo, actualícelo como se describe en la sección Actualización de certificados.

1. Proporcionar los archivos de certificado de forma que se pueda acceder a ellos a través de un conector del dispositivo, por ejemplo, en un dispositivo de memoria USB y el conector USB.
2. Ir a la configuración desde el menú de inicio
3. Vaya al menú Conexiones en Certificados
4. Seleccione Certificados de sistema y Certificados de dispositivo
5. Seleccione el icono "Papelera" para renovar los certificados y confirme el mensaje "Restablecer certificados" con "Sí".
6. Compruebe que el nuevo certificado "Sartorius Factory Authority" está disponible. Este certificado caducará en 2043.
7. Si "Sartorius Factory Authority" aparece en la lista, la actualización se ha realizado correctamente y se genera una entrada en el registro de auditoría.

Si aparece una advertencia sobre la caducidad del certificado después de restablecerlo, actualícelo como se describe en la sección Actualización de certificados.

2.5.3 Instalar o actualizar certificados

Para instalar o actualizar un certificado, siga estas instrucciones.

2.5.3.1 Certificados de cliente

1. Proporcionar los archivos de certificado de forma que se pueda acceder a ellos a través de un conector del dispositivo, por ejemplo, en un dispositivo de memoria USB y el conector USB.
2. Ir a la configuración desde el menú de inicio
3. Vaya al menú Conexiones en Certificados
4. Navegue hasta el menú correspondiente para el que se desea instalar un certificado. La diferenciación y explicación de los certificados se encuentra en el capítulo Tipos de certificados.
5. Pulse el botón [IMPORTAR] y seleccione el conector correspondiente a través del cual se puede acceder a los archivos de certificado que se van a instalar.
6. Seleccione [Certificado] y seleccione el archivo de certificado con la clave pública de la lista de archivos disponibles a través del conector. Se admiten los siguientes formatos: .pem y .crt.
7. Seleccione [Clave privada] y seleccione el archivo de certificado con la clave privada de la lista de archivos disponibles a través del conector. Se admiten los siguientes formatos: .key
8. Seleccione [Contraseña de clave privada] e introduzca la contraseña de la clave privada.
9. Confirme la importación. Los archivos se transfieren al sistema tras una verificación correcta.

2.5.3.2 Certificados CA

1. Hacer que los archivos de certificado estén disponibles para que se pueda acceder a ellos a través de un conector del dispositivo, por ejemplo, en un dispositivo de memoria USB y el conector USB.
2. Acceda a los ajustes desde el menú principal
3. En el menú Conexiones, vaya al submenú Certificados
4. Navegue hasta el menú correspondiente para el que se desea instalar un certificado. La diferenciación y explicación de los certificados se encuentra en el capítulo Tipos de certificados.
5. Pulse el botón [IMPORTAR] y seleccione el conector correspondiente a través del cual se puede acceder a los archivos de certificado que se van a instalar.
6. Seleccione el archivo de certificado de la lista de archivos disponibles a través del conector. Se admiten los siguientes formatos: .pem y .crt.

2.5.3.3 Tipos de archivos de certificado

Breve introducción a la PKI: las claves se dividen en dos partes, una pública y otra privada. La clave pública puede distribuirse pública y ampliamente, y puede utilizarse para verificar, pero no replicar, la información generada

utilizando la clave privada. La clave privada debe mantenerse en secreto.

- Los archivos .key son generalmente la clave privada utilizada por el servidor para cifrar y empaquetar datos para su verificación por parte de los clientes.
- Los archivos .pem son generalmente la clave pública, utilizada por el cliente para verificar y descifrar los datos enviados por los servidores. Los archivos PEM también podrían ser claves privadas codificadas.
- Los archivos .p12 tienen incrustadas las dos mitades de la clave, para que los administradores puedan gestionar fácilmente las mitades de las claves.
- Los archivos .cert o .crt son los certificados firmados con una clave pública, información sobre el propietario de la clave y la firma digital de la autoridad de certificación que emitió el certificado. Esto permite que un sistema sea clasificado como fiable por un tercero.
- En los archivos .cer, los certificados suelen estar en formato binario o Base64. Por lo tanto, difieren de los archivos .crt en cuanto a su codificación.

2.5.4 Tipos de certificados

Para una conexión segura a los servicios de red, la balanza necesita diferentes certificados que se pueden cargar en la balanza. Se distingue entre los siguientes certificados:

- Certificados CA (autoridades de certificación de confianza)
- Certificado de dispositivo
- Certificado de autenticación WiFi
- Certificado LDAPS

2.5.4.1 Certificados CA

Un certificado CA (Certificate Authority Certificate) es un certificado digital emitido por una autoridad de confianza, la denominada Autoridad de Certificación (CA). Su finalidad es confirmar la autenticidad y fiabilidad de un interlocutor o servicio de comunicación. Cuando dos dispositivos o programas se comunican entre sí a través de una red, un certificado CA permite a ambas partes asegurarse de que están realmente conectados con el interlocutor deseado y no con un atacante que se hace pasar por él.

Si un certificado de CA se clasifica como fiable, el dispositivo acepta automáticamente todos los certificados derivados de él. Esto crea una cadena de certificados que puede rastrearse desde el certificado de la CA raíz hasta el certificado del dispositivo correspondiente.

2.5.4.2 Autoridades de certificación desconocidas

El dispositivo también ofrece la opción de confiar en certificados que no han sido emitidos por una autoridad de certificación conocida. Si se activa esta opción, el dispositivo acepta dichos certificados sin comprobar su validez mediante una cadena de certificados. Esto puede ser útil en entornos de prueba o desarrollo, pero supone un riesgo para la seguridad en el uso productivo, ya que no se garantiza la autenticidad y fiabilidad de los certificados utilizados.
Esta opción se puede activar en Certificados, Certificados del sistema, [Confiar en autoridades de certificación desconocidas].

2.5.4.3 Certificados de dispositivos

Los certificados de dispositivo otorgan a éste una identidad única que le permite autenticarse ante los sistemas conectados. Esto garantiza que sólo los dispositivos autorizados puedan acceder a los datos y que la comunicación entre dispositivos esté protegida. Estos certificados se basan en las normas X.509 y son generados por certificados de clave pública (Public Key Infrastructure, PKI). Esto permite a los dispositivos identificar otros dispositivos y servidores de confianza.

En este Reglamento se establece un certificado de gestión del centro de certificación interno (CA) de una organización. El certificado se firmará con el sello privado del certificado de empresa (CA-Zertifikat) de la organización, que servirá de base para la firma de otros certificados.

La seguridad de los aparatos es responsabilidad del operador y no es un servicio proporcionado por el fabricante Sartorius. Por lo tanto, es importante asegurar el aparato con su propio certificado tan pronto como llegue a su organización. Los aparatos se entregan de fábrica con un certificado estándar de Sartorius.

Los certificados de dispositivo deben crearse internamente en su sistema y red, lo que requiere una CA privada. Existen dos enfoques:

1. Cree su propia CA privada con herramientas como OpenSSL o Microsoft CA.
2. Contrate a un proveedor de PKI gestionada (mPKI) para que se encargue de sus necesidades de autenticación y cifrado.

2.5.4.4 Certificados Wifi

Un certificado WiFi es un certificado digital que se utiliza para la autenticación y el cifrado seguros en una red inalámbrica (WLAN). Normalmente, estos certificados se utilizan como parte de WPA2-Enterprise o WPA3-Enterprise, en las que se utiliza el método de autenticación 802.1X (por ejemplo, EAP-TLS).

Con WPA2-Enterprise o WPA3-Enterprise, la autenticación suele realizarse a través del llamado servidor RADIUS, que suele estar conectado a un servicio de directorio (LDAP/Active Directory). Se utilizan certificados para que los clientes y los servidores RADIUS puedan identificarse entre sí de forma segura.

2.5.4.5 Certificados LDAPS

Los servidores LDAP (Lightweight Directory Access Protocol) utilizan certificados para proteger su comunicación con los clientes u otros servicios. Los servidores LDAP suelen encargarse de la gestión centralizada de usuarios y derechos. Si la conexión no es segura, los datos sensibles de los usuarios (por ejemplo, contraseñas, información sobre grupos o roles) pueden ser interceptados o manipulados.

Como el servidor LDAP se comunica a través de LDAPS (LDAP mediante SSL/TLS), la conexión está cifrada. Además, el cliente utiliza el certificado del servidor para verificar la identidad del servidor LDAP. Por lo tanto, el certificado del servidor LDAPS debe almacenarse en el dispositivo.

2.5.5 Conexiones de red seguras con SSL/TLS

Protocolos de seguridad como SSL (Secure Sockets Layer) y TLS (Transport Layer Security) se utilizan para transferir datos de forma segura. Definen cómo deben utilizarse los algoritmos de encriptación y autenticación para garantizar una conexión segura contra la interceptación y la manipulación.

SSL es una tecnología de seguridad estándar más antigua que establece una conexión cifrada entre un servidor y un cliente. En el caso de la balanza (por ejemplo, Cubis MCA), puede tratarse de una comunicación cifrada con un navegador web que accede al sitio web del dispositivo. Entretanto, SSL ha sido sustituido por TLS (Transport Layer Security) como tecnología sucesora. Sin embargo, como SSL es el término más conocido, TLS/SSL se utiliza en relación con los certificados o la seguridad de los datos transmitidos, aunque sólo se utilice TLS en segundo plano. Actualmente, la balanza admite TLS hasta la versión 1.3.

2.5.5.1 Autoridades de certificación desconocidas

El dispositivo también ofrece la opción de confiar en certificados que no han sido emitidos por una autoridad de certificación conocida. Si se activa esta opción, el dispositivo acepta dichos certificados sin comprobar su validez mediante una cadena de certificados. Esto puede ser útil en entornos de prueba o desarrollo, pero supone un riesgo para la seguridad en el uso productivo, ya que no se garantiza la autenticidad y fiabilidad de los certificados utilizados.
Esta opción se puede activar en Certificados, Certificados del sistema, [Confiar en autoridades de certificación desconocidas].

3 Ejemplos de aplicación

Los ejemplos de aplicación se refieren a la versión de MCA a partir del paquete 09-03-04.01.xx, junto con las opciones de configuración y las funcionalidades que contiene. Para configurar las conexiones de red, los conectores y las interfaces se necesitan los derechos de usuario adecuados.

Para la configuración de la interfaz Ethernet y Wi-Fi, se requieren conocimientos básicos de las redes basadas en TCP/IP y de las tecnologías de red en general.

El requisito previo para todos los ejemplos es la conexión de la balanza con una red a través de Ethernet (LAN) o Wi-Fi (WLAN).

3.1 Informe de la configuración del menú en el servidor de archivos de Windows

Este ejemplo describe la configuración y el uso de la balanza MCA para poder exportar un archivo de informe con todos los ajustes de la balanza desde el menú [Ajustes] en formato PDF, a través del conector [Servidor de archivos

Windows] utilizando el protocolo de red SMB, al directorio de destino de una unidad de red liberada.

Para transferir archivos a través del protocolo SMB, se requiere una extensión QAPP [Conexión al servidor de archivos de Windows] del paquete [Conectividad]. La extensión puede utilizarse de forma gratuita durante 30 días, tras los cuales debe obtenerse una licencia.

Una unidad liberada con protocolo SMB en su red es un requisito para esta aplicación.

Por lo tanto, esta aplicación puede utilizarse para almacenar de forma centralizada los ajustes del menú de todas las balanzas MCA conectadas en red.

3.1.1 Configuración

Pasos de configuración:

1. Active la extensión QAPP [Conexión al servidor de archivos de Windows], si aún no lo ha hecho.
   a. Abra el menú [Gestión de tareas], seguido del [Centro QAPP].
   b. Elija el paquete de software [Conectividad] y, dentro de él, el QAPP [Conexión al servidor de archivos de Windows]. Se mostrará la descripción y la versión del QAPP.
   c. Utilice el botón [Licencia] para activar este QAPP; se mostrará la información sobre el pedido y la licencia.
   d. Si este QAPP no se pidió como [licencia de fábrica], inicie la versión de prueba o introduzca el código de licencia que ha adquirido para este QAPP.
2. Configure un conector a un servidor de archivos de Windows, por ejemplo, [Mi servidor SMB para la configuración].
   a. Abra el menú [Configuración].
   b. Vaya a [Conexiones] -> [Conectores] -> [SMB].
   c. Utilice el botón [+] para activar la creación de un nuevo conector.
   d. Asigna un nombre único a este conector.
   e. Introduzca la ruta de red para el host y el recurso compartido, asegurándose de utilizar la ortografía correcta [//Nombre del host/Nombre del recurso compartido].
   f. Introduzca también el nombre de un subdirectorio en el servidor, en el que guardar los archivos.
   g. Introduzca el nombre de usuario y la contraseña para acceder a la unidad autorizada en su red. Preste atención a la notación correcta aquí también, en particular, las letras mayúsculas / minúsculas.

3.1.2 Aplicación

Pasos del usuario:

1. Desde el menú principal, utilice el botón [Setup] para abrir el menú para los ajustes de la balanza.
2. Pulse el botón [Exportar] en la barra de navegación y de herramientas.
3. Se muestra una lista de los conectores, a través de los cuales se puede exportar el archivo de informe.
4. Seleccione el conector creado, por ejemplo, [Mi servidor SMB para la configuración]. El archivo de informe se crea y se exporta al servidor SMB a través del conector.
5. Obtendrá los mensajes [Informe enviado] y [Proceso finalizado] como confirmación de que la exportación se ha realizado correctamente. El archivo de informe en formato PDF, con el archivo de comprobación relacionado, está ahora presente en el servidor y se puede ver.
6. Si no se ha podido exportar el archivo del informe, este archivo no se ha perdido, consulte la sección de resolución de problemas.

Nota: El formato de archivo PDF es un formato de datos para documentos independiente de la plataforma. La salida de impresión en este formato puede verse en cada ordenador. Para cada archivo de salida PDF, se crea un archivo de prueba que contiene la suma de comprobación (valor hash MD5) de los datos PDF. Cuando se transfiere el archivo, esta suma de comprobación se guarda en el registro de auditoría. Utilizando una herramienta adecuada, este archivo PDF puede compararse con el archivo de comprobación para garantizar la integridad de los datos PDF.

3.1.3 Solución de problemas

No se ha exportado ningún archivo de informe al directorio del servidor de archivos SMB.

1. Asegúrese de que se han seguido todos los pasos de configuración mencionados anteriormente.
2. Compruebe que la balanza está conectada a la red, por ejemplo, mediante un cable Ethernet. La dirección IP de la balanza en la red debe aparecer en el [Centro de estado] en [Información del dispositivo].
3. Compruebe la ruta de red en el conector y la ortografía correcta de Host y Share, así como el nombre de usuario y la contraseña para los derechos de acceso al servidor de archivos SMB.
4. Pruebe la conexión de los conectores con el servidor de archivos SMB activando el botón [Info] en el resumen de

los valores establecidos. Si todos los ajustes son correctos y el servidor de archivos SMB es accesible, recibirá un mensaje indicando que el conector está disponible.
5. Si no es así, compruebe que el servidor de archivos SMB está presente en la red y que se puede guardar un archivo allí desde su PC.
6. Si aparece un mensaje de error [Fallo de transferencia], puede hacer lo siguiente con la exportación:
   a. Reintentar: Reintentar la exportación del archivo de informe al servidor de red.
   b. Vuelva a intentarlo más tarde: La exportación del archivo de informe se repite automáticamente. Las transferencias pendientes se muestran en el [Centro de estado] en [Mensajes].
   c. Redirigir: Puede redirigir el archivo del informe a otro conector.
   d. Borrar: La exportación del archivo de informe se cancela y se elimina.

3.2 Actualizar el Centro QAPP del servidor FTP

Este ejemplo describe la configuración y aplicación de la balanza Cubis® MCA, para cargar la actualización del Centro QAPP de un servidor FTP.

Para transferir archivos desde un servidor de red FTP, se necesita una extensión QAPP [Conexión a FTP/FTPS] del paquete [Conectividad]. La extensión se puede utilizar de forma gratuita durante 30 días, tras los cuales también se debe obtener una licencia.

El requisito previo para esta aplicación es un servidor FTP debidamente configurado en su red.

Para las balanzas MCA en red, esta aplicación permite la actualización del Centro QAPP desde una fuente central.

3.2.1 Configuración

Pasos de configuración:

1. Active la extensión QAPP [Conexión a FTP/FTPS], si aún no lo ha hecho.
   a. Abra el menú [Gestión de tareas], seguido del [Centro QAPP].
   b. Seleccione el paquete de software [Conectividad] y, dentro de él, el QAPP [Conexión a FTP/FTPS]. Se mostrará la descripción y la versión del QAPP.
   c. Utilice el botón [Licencia] para activar este QAPP; se mostrará la información sobre el pedido y la licencia.
   d. Si este QAPP no se pidió como [licencia de fábrica], inicie la versión de prueba o introduzca el código de licencia que ha adquirido para este QAPP.
2. Configure un conector a un servidor FTP, por ejemplo, [Mi servidor FTP para la actualización del Centro QAPP].
   a. Abra el menú [Configuración].
   b. Vaya a [Conexiones] -> [Conectores] -> [FTP].
   c. Utilice el botón [+] para activar la creación de un nuevo conector.
   d. Asigna un nombre único a este conector.
   e. Introduzca la dirección IP del servidor de red, asegurándose de escribirla correctamente
   f. Se requiere un número de puerto para la conexión: se ha asignado el número 21. Si es necesario, puede introducir un número de puerto diferente.
   g. Para actualizar el Centro QAPP, también puede especificar un subdirectorio para los archivos almacenados en el servidor.
   h. Introduzca el nombre de usuario y la contraseña para acceder al servidor FTP. Preste atención a la notación correcta aquí también, en particular, las letras mayúsculas / minúsculas.

3.2.2 Aplicación

Pasos del usuario:

1. Desde el menú principal, utilice el botón [Setup] para abrir el menú para los ajustes de la balanza.
2. Vaya al menú [Mantenimiento de dispositivos] -> [Instalar el Centro QAPP]. Se muestra una lista de conectores con los que se puede cargar un paquete para actualizar el Centro QAPP.
3. Seleccione el conector creado, por ejemplo, [Mi servidor FTP para la actualización del Centro QAPP]. Se establece la conexión con el servidor FTP y se muestra una lista de paquetes disponibles para actualizar el Centro QAPP.
4. Seleccione la versión deseada del Centro QAPP y confirme el mensaje de actualización.
5. El Centro QAPP se copia ahora en la balanza desde el servidor FTP y se actualiza. Como confirmación, se muestra la versión actualizada del Centro QAPP.
6. Consulte la sección de resolución de problemas, si la actualización no pudo realizarse.

3.2.3 Solución de problemas

La actualización del Centro QAPP no es posible a través del conector.

1. Asegúrese de que se han seguido todos los pasos de configuración mencionados anteriormente.
2. Compruebe que la balanza está conectada a la red, por ejemplo, mediante un cable Ethernet. La dirección IP de la balanza en la red debe aparecer en el [Centro de estado] en [Información del dispositivo].
3. Compruebe la dirección IP y el número de puerto del servidor FTP, así como el nombre de usuario y la contraseña para los derechos de acceso al servidor en el conector.
4. Pruebe la conexión de los conectores con el servidor FTP activando el botón [Info] en el resumen de los valores configurados. Si todos los ajustes son correctos y el servidor FTP es accesible, recibirá un mensaje indicando que el conector está disponible.
5. Compruebe con su PC si el sub-directorio especificado y así como el archivo para la actualización del Centro QAPP están presentes en el servidor FTP en la red.

3.3 Ver las entradas del registro de auditoría a través del navegador web

Este ejemplo describe la configuración y el uso de la balanza MCA para que las entradas en el registro de auditoría de la balanza puedan ser vistas usando el navegador web.

Se recomienda el navegador web [Chrome] para el funcionamiento remoto de la balanza MCA.

La conexión segura de la balanza con el navegador a través del protocolo HTTPS requiere ciertos certificados del dispositivo.

Para ello, la balanza MCA proporciona sus propios certificados de dispositivo para su descarga. Estos certificados de dispositivo deben ser importados en el navegador para el acceso remoto seguro a la página web del dispositivo. Hay una descripción separada sobre el tema de [Certificados].

El alcance completo de la pista de auditoría sólo se puede utilizar después de activar la extensión QAPP [Pista de auditoría] en el Centro QAPP bajo [Pharma (QP1)].

Un uso de esta aplicación es, por ejemplo, la supervisión centralizada a distancia de los ajustes en todas las balanzas MCA en red.

3.3.1 Configuración

Pasos de configuración:

1. Active la extensión [Audit trail] QAPP, si aún no lo ha hecho.
   a. Abra el menú [Gestión de tareas], seguido del [Centro QAPP].
   b. Seleccione el paquete de software [Pharma] y el QAPP [Audit trail] en él. Se mostrará la descripción y la versión del QAPP.
   c. Utilice el botón [Licencia] para activar este QAPP; se mostrará la información sobre el pedido y la licencia.
   d. Si este QAPP no se pidió como [licencia de fábrica], inicie la versión de prueba o introduzca el código de licencia que ha adquirido para este QAPP.
2. Activar la página web del saldo de la CRM, si aún no lo ha hecho.
   a. Abra el menú [Configuración].
   b. Vaya a [Conexiones] -> [Sitio web / servicios web].
   c. Establezca la opción de menú [Acceso al sitio web] en [Activado, sin autenticación].
3. Si es necesario, active el acceso remoto a la página web de la balanza MCA.
   a. Abra el menú [Configuración].
   b. Vaya a [Conexiones] -> [Sitio web / servicios web].
   c. En la opción de menú [Acceso remoto], seleccione el ajuste [Vista y control remoto].

3.3.2 Aplicación

Pasos del usuario:

1. Inicie el navegador web, por ejemplo, [Chrome] en su PC.
2. Introduzca la dirección IP de su balanza, que se muestra en el [Centro de estado] en [Información del dispositivo].
3. Si aún no ha importado los certificados de dispositivo de la balanza en el navegador, verá el mensaje [Esta no es una conexión segura] en el navegador.
4. Con el botón [Avanzado] y el enlace [Siguiente...], ahora puede ir a la dirección IP de la balanza, que en este caso se ve como insegura o bien debe importar primero los certificados del dispositivo de su balanza en su navegador. Hay una descripción separada sobre el tema de [Certificados].
5. De lo contrario, la página [Mi Cubis] (página de inicio) se muestra ahora en el navegador.
6. Seleccione la página [Audit trail] para el ejemplo.

7. Ahora puede ordenar la lista de entradas según el ID, la marca de tiempo y el usuario.
8. La lista de entradas puede mostrarse en orden ascendente o descendente.
9. También puede establecer filtros para ver sólo grupos específicos de entradas.

3.3.3 Solución de problemas

La página de inicio de la balanza no se muestra en el navegador.

1. Compruebe que la balanza está conectada a la red, por ejemplo, mediante un cable Ethernet. La dirección IP de la balanza en la red debe aparecer en el [Centro de estado] en [Información del dispositivo].
2. Asegúrese de que la opción de menú [Acceso a la página web] está ajustada a [Activado].

La conexión a la balanza se muestra como [No segura] en el navegador.

1. Importe los certificados del dispositivo de la balanza en su navegador. Hay una descripción separada sobre el tema de [Certificados].

La página [Audit trail] no se puede seleccionar en la página de inicio de la balanza.

1. Asegúrese de que se han seguido todos los pasos de configuración mencionados anteriormente. En particular, se ha activado la extensión [Audit trail] QAPP y la licencia para ello sigue siendo válida.

3.4 Sincronizar la fecha y la hora con el servidor NTP

Este ejemplo describe la configuración y la aplicación de Cubis® MCA, para permitir una sincronización de la fecha y la hora de la balanza con un servidor NTP.

El requisito previo para este uso es el acceso a un servidor NTP en la red de su empresa o en la red pública.

La desviación de tiempo entre la balanza y el servidor NTP se comprueba cada 10 minutos. Si la desviación es superior a 3 segundos, la hora de la balanza se corrige y el cambio se introduce en el registro de auditoría.

Esta aplicación permite una fácil actualización y sincronización automática de la fecha y la hora en todas las balanzas MCA en red.

3.4.1 Configuración

Pasos de configuración:

1. Establezca una configuración NTP activa.
   a. Abra el menú [Configuración].
   b. Acceda a [Configuración del dispositivo] -> [Fecha y hora] -> [Configuración NTP].
   c. Active la configuración de los ajustes del servidor NTP mediante el botón [Editar].
   d. Establezca el elemento de menú [Estado de funcionamiento de NTP] en [Activado].
   e. A través de la [IP del servidor] introduzca la dirección del servidor NTP en el formato IPv4, por ejemplo, 192.53.103.108. (Se trata de un servidor NTP del Instituto Federal Físico-Técnico de Braunschweig, Alemania).
   f. Confirme la configuración NTP con el botón [OK].
   g. Pruebe la conexión con el servidor NTP activando el botón [Info] en la vista general de la configuración NTP.
2. Establezca la zona horaria correcta para su ubicación.
   a. Abra el menú [Configuración].
   b. Acceda a [Ajustes del dispositivo] -> [Fecha y hora] -> [Ajustar fecha y hora].
   c. Active la configuración de la fecha y la hora con el botón [Editar].
   d. Establezca su ubicación mediante la opción de menú [Zona horaria], [UTC +/- hora, lugar]. A partir de entonces, la hora y la fecha se muestran inmediatamente coincidiendo con su hora local.

Nota: Después de ajustar la fecha, la hora y la zona horaria, la balanza MCA le pide que reinicie el sistema.

3.4.2 Solución de problemas

No es posible la conexión con el servidor NTP.

1. Asegúrese de que se han seguido todos los pasos de configuración mencionados anteriormente.
2. Compruebe que la balanza está conectada a la red, por ejemplo, mediante un cable Ethernet. La dirección IP de la balanza en la red debe aparecer en el [Centro de estado] en [Información del dispositivo].
3. Compruebe con su PC si puede acceder a la dirección IP del servidor NTP.

4 Anexo

4.1 Bastones Wi-Fi compatibles

Cubis® MCA es compatible con las memorias Wi-Fi más comunes (adaptadores WLAN USB) disponibles en el mercado.

Ten en cuenta los siguientes elementos a la hora de seleccionar un stick Wi-Fi:

1. Evite las barras de Wi-Fi sin nombre. Compre siempre una marca conocida.
2. Si es posible, compruebe la hoja de datos del stick Wi-Fi para asegurarse de que contiene uno de los siguientes conjuntos de chips compatibles.

Los conjuntos de chips Wi-Fi compatibles son:

- 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. Abreviaturas

DHCP	Dynamic Host Configuration Protocol	Protocolo de comunicación en tecnología informática. Permite la asignación de la configuración de la red a los clientes por parte de un servidor.
DNS	Domain Name System	Sistema de resolución de nombres de ordenadores en direcciones IP y viceversa.
FTP	File Transfer Protocol	Protocolo de red estándar para la transferencia de archivos entre un cliente y un servidor dentro de una red.
FTPS	FTP over TLS	Un método para encriptar el Protocolo de Transferencia de Archivos (FTP).
HTTPS	Hypertext Transfer Protocol Secure	Un protocolo de comunicaciones con el que los datos pueden transmitirse de forma encriptada.
IPv4	Internet Protocol version 4	Protocolo de Internet de la versión 4.
IPv6	Internet Protocol version 6	Protocolo de Internet de la versión 6.
MAC address	Media Access Control address	Dirección física del hardware, identificador único del dispositivo en la red.
NTP	Network Time Protocol	Una norma para sincronizar los relojes en los sistemas informáticos.
PNG	Portable Network Graphics	Gráficos de red portátiles, un formato de gráficos de trama con compresión de datos sin pérdidas.
PSK	Pre-shared key	Método de encriptación en el que la clave debe ser conocida por ambos participantes antes de la comunicación.
REST	Representational State Transfer	Paradigma de programación para sistemas distribuidos, especialmente para servicios web.
SMB	Server Message Block	Protocolo de red para los servicios de archivo, impresión y otros servicios de servidor en las redes informáticas.
SSID	Service Set Identifier	Nombre de la red de libre elección, por ejemplo, para el Wi-Fi.
URL	Uniform Resource Locator	Identificación para las direcciones de Internet o de la web.
UTC	Universal Time, Coordinated	La hora mundial, también la hora de la Tierra o la hora universal.
WEP	Wired Equivalent Privacy	Protocolos de encriptación estándar para WLAN.
Wi-Fi	Wireless Fidelity	Red inalámbrica, sinónimo de WLAN.
WLAN	Wireless Local Area Network	Inalámbrico, red local.
WPA	Wi-Fi Protected Access	Métodos de encriptación para una red inalámbrica. Sucesor de WEP.
WPA2	Wi-Fi Protected Access 2	Implementación de un estándar de seguridad para redes de radio. Sucesor de WPA.