Description of Network, Ethernet and Wi-Fi (WLAN) for the Cubis® MCA Balance

This document describes how to connect the balance to a network via Ethernet and Wi-Fi (WLAN). Examples are given to illustrate how to set up and use the balance in practice.

Executive Summary

The Cubis® MCA Premium laboratory balance offers comprehensive and flexible connectivity options for integrating the balance into laboratory IT. A large number of standardized IT protocols, such as REST web service, SMB or LDAP, are available via Ethernet and Wi-Fi, enabling direct integration without the use of additional middleware. In addition, the Cubis® can be remotely controlled over the network using a web browser and audit trail and other status information can be viewed.

1 Network connection Ethernet and Wi-Fi

A Cubis® MCA balance can be connected to a TCP/IP-based network using a cable via the Ethernet connection (RJ45 socket) and wireless via a Wi-Fi USB adapter (WLAN stick).

The transmission rates of the network connection are 10 Mbit/sec (10BASE-T, Ethernet) and 100 Mbit/sec (100BASE-TX Fast Ethernet).

The Ethernet connection is made with a connection cable, CAT 5 or higher, twisted in pairs, shielded, 1:1, UTP/STP, plug RJ45; e.g., patch cable CAT 5 depending upon the use (straight/cross-over).

For a wireless connection, Cubis® MCA supports the most common Wi-Fi USB adapters (WLAN sticks) which are offered in the market.

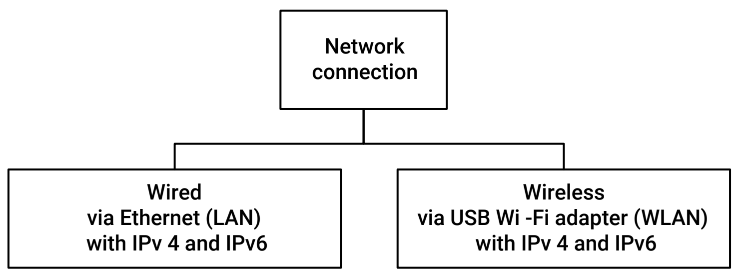

Figure 1: Network connection

The Cubis® MCA balance can have an IPv4 and an IPv6 address each on Ethernet and Wi-Fi respectively i.e., up to 4 addresses.

Via the network connections Ethernet (LAN) and Wi-Fi (WLAN), the Cubis® MCA balance simultaneously offers several network services.

1.1 General settings

The host name of the balance, ex-factory, is composed of the designation of the series and the last 3 bytes of the MAC address e.g., [cubis-1a477e]. The host name can be selected freely, but must be unique in a network.

1.2 Ethernet (LAN)

For the Ethernet connection of the balance, the IPv4 as well as IPv6 protocols can be used. It can be set separately for each protocol, whether the IP address is to be obtained automatically or whether the balance is given a fixed IP address. The respective protocol can also be disabled completely.

In the overview of settings for Ethernet, the status displays whether a connection to the network is established. Moreover, the unique MAC address of the balance is also shown here e.g., [00:30:D6:1F:77:569].

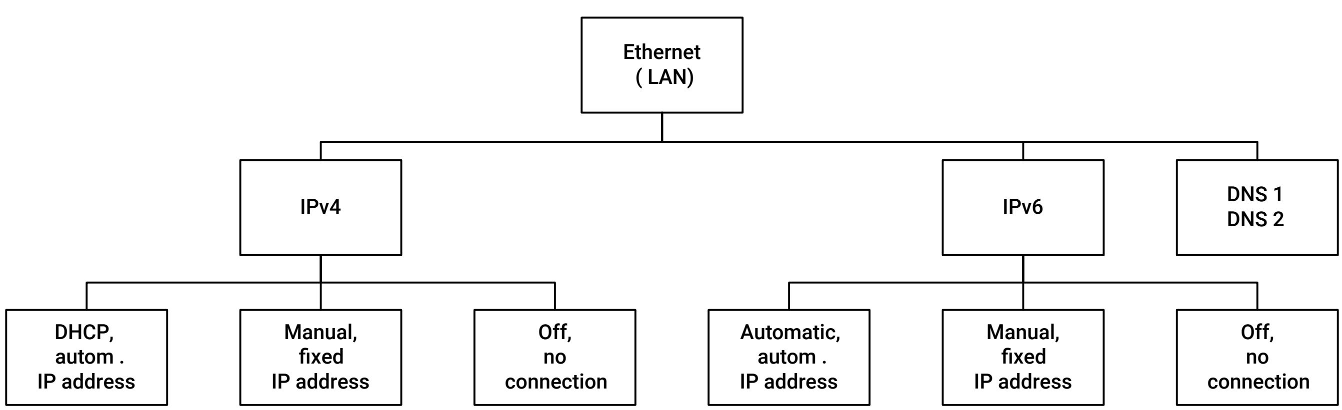

Figure 2: Ethernet with IPv4/IPv6

For operation with a fixed IP address, in addition to the IP address, depending on the protocol, the subnet mask and the gateway must also be entered manually for IPv4, or the prefix length and the gateway for IPv6. It is optional to enter the gateway and necessary only when a connection to the Internet is needed.

All information necessary for this can be provided by the network administrator responsible for the company network.

1.2.1 IPv4 protocol

The IP address for the protocol IPv4 (4*8 bit = 32 bit) consists of 4 decimal numbers between 0 and 255, which are separated by a dot e.g., [123.4.56.123]. This format applies for the entry of the fixed IP address, the subnet mark and the gateway.

1.2.2 IPv6 protocol

The IP address for the protocol IPv6 (8*16 bit = 128 bit) consists of 8 alphanumeric hexadecimal numbers between 0 and FFFF, which are separated by a colon e.g., [ecb1:d583:6341:baf76:0:0:0:1].

The first 4 blocks (64 bit) constitute the prefix and the last 4 blocks the interface identifier. The IPv4 network mask and IPv4 network address are replaced by the prefix length and prefix in IPv6. The prefix length specifies the number of bits which constitute the prefix. Typical prefix length is 64. The prefix replaces the subnet mask in case of IPv6.

1.2.3 DNS 1 and DNS 2

In IP-based network systems, the DNS (Domain Name System) helps in responding to the queries of name resolution. A network can have several DNS servers, the Cubis® MCA supports the entry of two servers.

The IP address or the server name can be entered for each DNS server.

In case of DHCP, the DNS server is provided automatically by the DHCP server. In addition, in this case, DNS1 and DNS2 are added to the DNS server list.

1.3 Wi-Fi (WLAN)

A Wi-Fi USB adapter (WLAN stick) can be connected to the MCA balance; several adapters of this type are not supported.

In the overview of settings for Wi-Fi (WLAN), it is displayed via the status, whether a corresponding Wi-Fi USB adapter is attached and is connected to the network.

<u>Status display</u>

- No device available - No Wi-Fi USB adapter connected.
- Disconnected - No connection to the Wi-Fi network e.g., not logged in with Wi-Fi SSID and password.
- Ready - Connection established with the Wi-Fi network.
- Online - Connection established with the Wi-Fi network and the Internet.

If a connection has been made, then the unique MAC address of the Wi-Fi USB adapter is also shown here e.g., 34:C9:F0:89:6F:D6.

In Annexure, the section: Compatible Wi-Fi sticks.

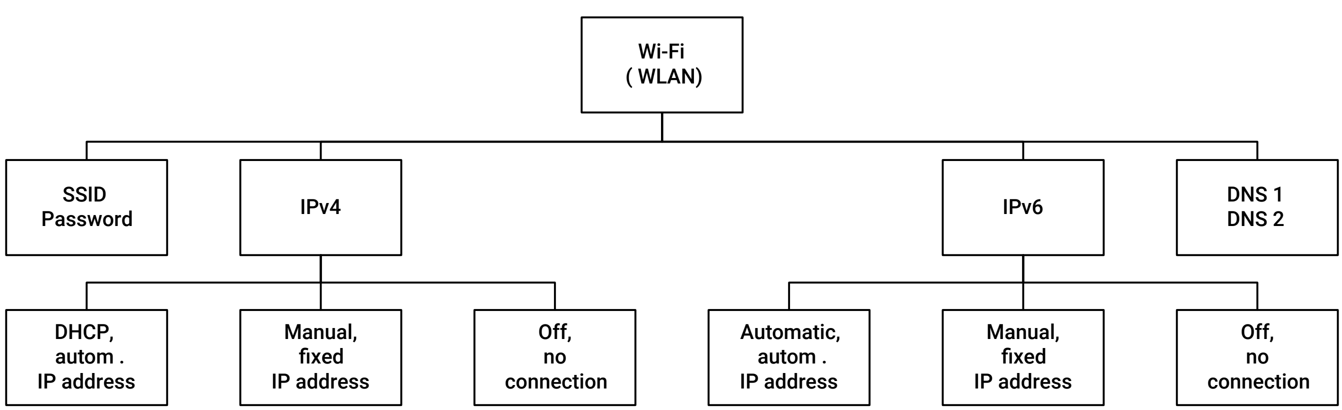

Figure 3: Wi-Fi with IPv4/IPv6

For operation with a fixed IP address, in addition to the IP address, depending on the protocol, the subnet mask and the gateway must also be entered manually for IPv4, or the prefix length and the gateway for IPv6. It is optional to enter the gateway and necessary only when a connection to the Internet is needed.

All information necessary for this can be provided by the network administrator responsible for the company network.

1.3.1 Wi-Fi SSID and Password

For connecting to a Wi-Fi network, the Wi-Fi SSID (the unique Wi-Fi network name) and the Wi-Fi password (the Wi-Fi network key) must be entered.

For authentication, the MCA balance supports the standards WEP, WPA-PSK and WPA2-PSK and hence also the PSK method for encryption.

1.3.2 IPv4/IPv6 protocol and DNS 1/2

For the protocol IPv4 and IPv6 as well as for DNS 1 and DNS 2, the same description applies to Wi-Fi (WLAN) as in case of Ethernet (LAN).

2 Network services

Via the network the Cubis® MCA balance offers several services simultaneously, a serial communication with different protocols, connectors for connecting to network mass storage devices and printers, a website and web service for the remote access, as well as the connection to an NTP server for synchronizing date and time.

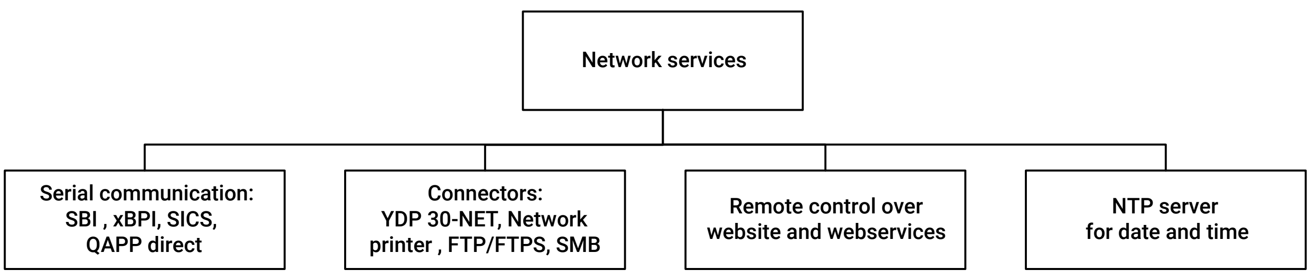

Figure 4: Network services

2.1 Serial communication

Using the network connection, it is possible to use the serial communication protocols SBI, xBPI, SICS, miniSICS, which can be operated regardless of the active task and its use. This client/server connection requires settings for a joint TCP port.

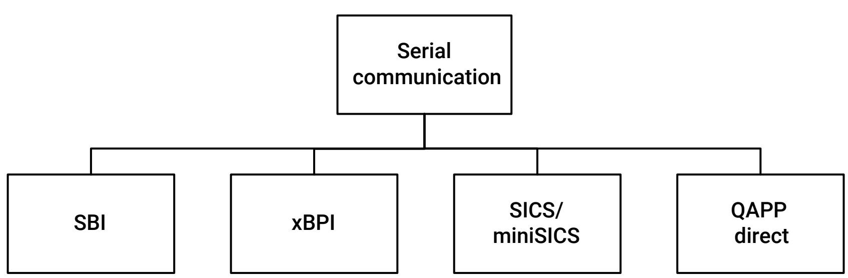

Figure 5: Serial communication via network

2.1.1 SBI protocol

This simple, ASCII-based protocol can control the basic functions of the balance using ESC commands. The output of display values can be individually requested via an ESC command, or automatically with each new weighing result in the display sequence cycle, or automatically after specific time intervals. It is possible to choose whether the output is provided with a stable display value only, or also without the display value being stable. The output format can be selected with or without identifier (header).

The SBI commands and output formats are given in a separate interface description.

2.1.2 xBPI protocol

This binary protocol offers an extended scope of commands. It can be used to control numerous balance functions.

There is a separate interface description of the possible xBPI commands.

2.1.3 SICS protocol
The SICS (Standard Interface Command Set) protocol establishes a compatibility with the MT-SICS protocol of Mettler and enables sending of commands to the balance for the basic functions. However, it should be noted that there are differences owing to the different hardware/software platforms.

The SICS and the miniSICS commands implemented in the balance are given in a separate interface description.

2.1.4 QAPP direct
Only the special QAPPs, which are started by a task, can use the interface for their purposes of input and output. The possibilities of input and output via the interface are described in the respective special QAPP.

2.2 Network connectors
In Cubis® MCA, the connectors establish the connection to the network servers which are to be used as mass storage devices or as printers.

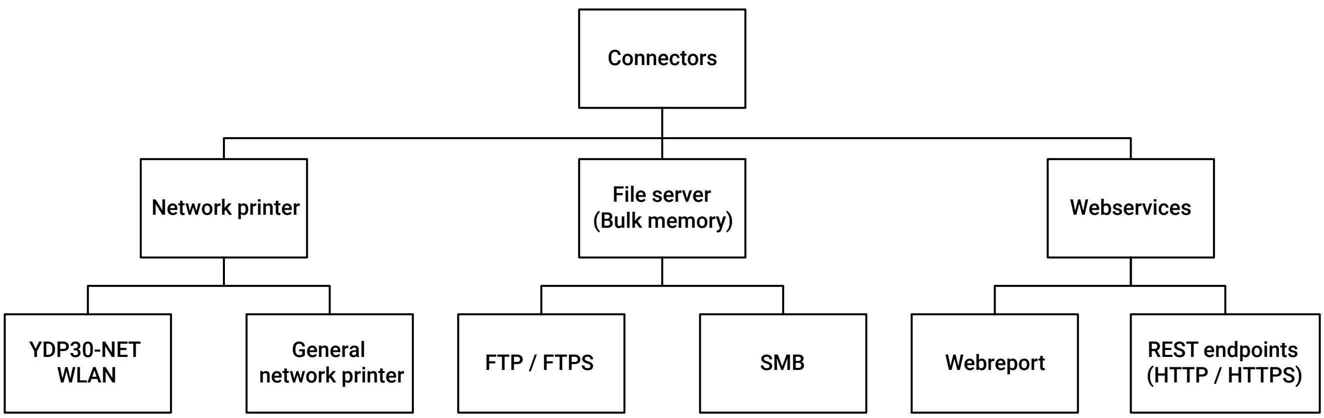

Figure 6: Network connectors

The YDP30-NET network printer can be connected by WLAN or as a general network printer with an independent Wi-Fi network or corporate network using DHCP.

For connecting to a mass storage device, such as Windows file server, FTP/FTPS or STARLIMS, a special QAPP extension is necessary, which must be activated via the QAPP Center under [Connectivity].

2.2.1 YDP30-NET
This connector is intended for connecting a YDP30-NET printer with a cable (LAN) or a wireless connection (WLAN). A connector requires a connector name, an IP address, or a host name to be entered on the printer, as well as an agreed port number between printer and balance.

The wireless connection of the YDP30-NET printer is described in separate instructions.

2.2.2 Network printer
The network printer connector allows, for example, connections to an A4 printer in an independent Wi-Fi network with standard Wi-Fi components, or in a corporate network per DHCP with standard authentication methods. The network printer must support IPP (Internet Printing Protocol).

A connector requires a connector name, an IP address, or a host name to be entered on the printer, as well as the transfer protocol.

The separate description [Print concept] describes the setup and application of a network printer with an application example.

2.2.3 FTP / FTPS
The File Transfer Protocol (FTP) is a standard network protocol for transferring computer files between a client and a server in a computer network.

The balance is the FTP client and can store files on an FTP server or retrieve files from an FTP server using the protocol. In case of FTPS, the connection is also encrypted; the certificates necessary for this are described separately.

For connecting to an FTP/FTPS server, a connector must be created with a unique name, IP address and port number of the network server, if needed, a sub-directory on the server and the username and password.

Note: With several connectors on the balance to the same server, but with different sub-directories, the storage of data can be easily structured according to the topic (backup, report, ...).

2.2.4 SMB protocol

The Windows file server connector uses the SMB network protocol. This protocol facilitates access to the released network drives of Windows or Linux computers in order to store or retrieve data files in the selected target directories.

2.3 Website

The website of the MCA balance can be displayed simply via the IP address of the balance with a web browser. The [My Cubis] page (home page) displays the set device IDs, general device information of the balance and information about the service.

Using the [Remote operation] page, depending upon the settings in the menu, either [View only] or [View and remote control] of the MCA balance can be displayed via the browser.

The [Screenshot] page creates a PNG file of the current display, which can be saved.

If the [Audit trail] QAPP extension has been activated in the QAPP Center in the package [Pharma], then the [Audit trail] website is also displayed. The entries in the audit trail can be filtered, sorted and exported according to the topics.

The access to the website can be deactivated completely via the menu and hence also the remote control via the REST web service.

2.3.1 Webservices

The remote operation of the underlying functions of the MCA balance can also be done via a REST web service.

There is a separate description of the available REST web services of the MCA balance.

2.4 NTP server for date and time

Cubis® MCA offers the possibility of synchronizing the date and time with an NTP server. To do this, the connection with the server can be activated and the IP address of the server can be entered in the device settings of MCA under Date/Time and NTP Configuration.

2.5 Certificates

The Cubis® MCA balance supports the use of certificates for a trustworthy integration in the local IT infrastructure. The MCA can process the certificates of trusted certification agencies (CA), in order to identify trusted servers. The MCA also provides its own device certificates for download. These device certificates are primarily used for secure communication and authentication (e.g. FTPS, HTTPS, Webservices).

Root certificates have a limited period of validity and must be renewed at regular intervals. The expiry of a root certificate has no effect on the core functions or data of the balance itself. The balance displays a warning a few weeks before the expiry date.

Device certificates are based on the X.509 standard and use public-key cryptography, in which a key pair consisting of a public and private key is used. This key pair enables encrypted data transmission, verification of digital signatures and reliable identity authentication. Depending on how the private key is created and stored, it may be necessary to decrypt it with a passphrase before use.

2.5.1 Operator obligations

Sartorius Cubis MCA balances are delivered with pre-installed device certificates that have a limited validity.
Operators have the option of renewing the originally installed certificates and importing their own certificates.
The operator is responsible for managing and updating the certificates and ensuring their validity. In order to avoid possible security warnings or restrictions on secure connections, it is important that the validity of the certificates is checked regularly and renewed if necessary.

Updating the certificate has no effect on the weighing function or on integration into the local IT infrastructure. It is therefore not necessary to requalify or revalidate the devices when updating the certificates.

2.5.2 Reset certificates

If a warning about the certificate expiry is displayed after resetting the certificate, please update the certificate as described in the section Updating certificates

1. Provide the certificate files so that they can be accessed via a connector on the device, for example on a USB

memory device and the USB connector
2. Navigate to settings from home menu
3. Navigate to Connections menu into Certificates
4. Select System Certificates and Device Certificates
5. Select “Trash” icon to renew certificates and confirm the message “Reset certificates” with “Yes”
6. Check that new certificate “Sartorius Factory Authority” is available. This certificate will expire in 2043.
7. If “Sartorius Factory Authority” is visible on the list, the update was successful, and an Audit Trail entry is generated.

If a warning about the certificate expiry is displayed after resetting the certificate, please update the certificate as described in the section Updating certificates

2.5.3 Install or update certificates

To install or update a certificate, follow these instructions.

2.5.3.1 Client certificates

1. Provide the certificate files so that they can be accessed via a connector on the device, for example on a USB memory device and the USB connector
2. Navigate to settings from home menu
3. Navigate to Connections menu into Certificates
4. Navigate to the corresponding menu for which a certificate is to be installed. The differentiation and explanation of the certificates can be found in the chapter Certificate types
5. Press the [IMPORT] button and select the corresponding connector via which the certificate files to be installed can be accessed.
6. Select [Certificate] and select the certificate file with the public key from the list of files available via the connector. The following formats are supported: .pem and .crt
7. Select [Private key] and select the certificate file with the private key from the list of files available via the connector. The following formats are supported: .key
8. Select [Private key password] and enter the password for the private key.
9. Confirm the import. The files are transferred to the system after successful verification.

2.5.3.2 CA certificates

1. Make the certificate files available so that they can be accessed via a connector on the device, for example on a USB memory device and the USB connector
2. Navigate to the settings from the main menu
3. In the Connections menu, navigate to the Certificates submenu
4. Navigate to the corresponding menu for which a certificate is to be installed. The differentiation and explanation of the certificates can be found in the chapter Certificate types
5. Press the [IMPORT] button and select the corresponding connector via which the certificate files to be installed can be accessed.
6. Select the certificate file from the list of files available via the connector. The following formats are supported: .pem and .crt

2.5.3.3 Certificate file types

A brief primer on PKI: Keys come in two halves, a public key and a private key. The public key can be distributed publicly and widely, and you can use it to verify, but not replicate, information generated using the private key. The private key must be kept secret.

- .key files are generally the private key used by the server to encrypt and package data for verification by the clients.
- .pem files are generally the public key, used by the client to verify and decrypt data sent by servers. PEM files could also be encoded private keys.
- .p12 files have both halves of the key embedded, so that administrators can easily manage halves of keys.
- .cert or .crt files are the signed certificates with a public key, information about the key owner and the digital signature of the certification authority that issued the certificate. This allows a system to be classified as trustworthy by a third party.
- In .cer files, the certificates are usually in binary or Base64 format. They therefore differ from .crt files in terms of their coding.

2.5.4 Certificate types

For a secure connection to network services, the balance requires different certificates that can be loaded onto the balance. A distinction is made between the following certificates:

- CA certificates (trusted certification authorities)
- Device certificate
- WiFi authentication certificate
- LDAPS certificate

2.5.4.1 CA certificates

A CA certificate (Certificate Authority Certificate) is a digital certificate issued by a trustworthy authority - the so-called Certificate Authority (CA). Its purpose is to confirm the authenticity and trustworthiness of a communication partner or service. When two devices or programs communicate with each other over a network, a CA certificate enables both sides to ensure that they are actually connected to the desired communication partner and not to an attacker who is impersonating them.

If a CA certificate is classified as trustworthy, the device automatically accepts all certificates derived from it. This creates a so-called certificate chain that can be traced back from the root CA certificate to the respective device certificate.

2.5.4.2 Unknown certification authorities

The device also offers the option of trusting certificates that have not been issued by a known certification authority. If this option is activated, the device accepts such certificates without checking their validity via a certificate chain. This can be useful in test or development environments, but poses a security risk in productive use, as the authenticity and trustworthiness of the certificates used is not guaranteed.
This option can be activated under Certificates, System certificates, [Trust unknown certification authorities].

2.5.4.3 Device certificates

Device certificates give a device a unique identity that enables it to authenticate itself to connected systems. This ensures that only authorized devices can access data and that communication between devices is protected. These certificates are based on X.509 standards and are generated by public key certificates (Public Key Infrastructure, PKI). This allows devices to identify other trusted devices and servers.

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

The security of the devices is the responsibility of the operator and is not a service provided by the manufacturer Sartorius. It is therefore important to secure the device with your own certificate as soon as it arrives at your organization. The devices are delivered ex works with a standard certificate from Sartorius.

Device certificates should be created internally in your system and network, which requires a private CA. There are two approaches:

1. Create your own private CA with tools such as OpenSSL or Microsoft CA.
2. Hire a managed PKI (mPKI) provider to handle your authentication and encryption needs.

2.5.4.4 Wifi certificates

A WiFi certificate is a digital certificate that is used for secure authentication and encryption in a wireless network (WLAN). Typically, such certificates are used as part of WPA2-Enterprise or WPA3-Enterprise, in which the 802.1X authentication method (e.g. EAP-TLS) is used.

With WPA2-Enterprise or WPA3-Enterprise, authentication is usually carried out via the so-called RADIUS server, which is often connected to a directory service (LDAP/Active Directory). Certificates are used so that clients and RADIUS servers can identify each other securely.

2.5.4.5 LDAPS certificates

LDAP servers (Lightweight Directory Access Protocol) use certificates to secure their communication with clients or other services. LDAP servers are often responsible for central user and rights management. If the connection is not secure, sensitive user data (e.g. passwords, group or role information) can be intercepted or manipulated.

As the LDAP server communicates via LDAPS (LDAP via SSL/TLS), the connection is encrypted. In addition, the client uses the server certificate to verify the identity of the LDAP server. The LDAPS server certificate must therefore be stored on the device.

2.5.5 Secure network connections with SSL/TLS

Security protocols such as SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are used to transfer data securely. They define how encryption and authentication algorithms are to be used in order to ensure a connection that is secure against interception and manipulation.

SSL is an older standard security technology that establishes an encrypted connection between a server and a client. In the case of the balance (e.g. Cubis MCA), this can be encrypted communication with a web browser that accesses the device website. In the meantime, SSL has been replaced by TLS (Transport Layer Security) as the successor technology. However, as SSL is the better-known term, TLS/SSL is used in relation to certificates or securing transmitted data, even if only TLS is used in the background. The balance currently supports TLS up to version 1.3.

2.5.5.1 Unknown certification authorities

The device also offers the option of trusting certificates that have not been issued by a known certification authority. If this option is activated, the device accepts such certificates without checking their validity via a certificate chain. This can be useful in test or development environments, but poses a security risk in productive use, as the authenticity and trustworthiness of the certificates used is not guaranteed.
This option can be activated under Certificates, System certificates, [Trust unknown certification authorities].

3 Application Examples

The application examples relate to the MCA version from package 09-03-04.01.xx onwards, along with the settings options and functionalities it contains. Appropriate user rights are required for configuring the network connections, connectors, and interfaces.

For configuring the Ethernet and the Wi-Fi interface, basic knowledge of TCP/IP-based networks and network technologies in general is required.

The prerequisite for all examples is a connection of the balance with a network via Ethernet (LAN) or Wi-Fi (WLAN).

3.1 Report of menu settings on Windows file server

This example describes the configuration and use of the MCA balance so that a report file with all settings of the balance can be exported from the menu [Settings] in the PDF format, via the connector [Windows file server] using the SMB network protocol, to the target directory of a released network drive.

For transferring files via SMB protocol, a [Connection to Windows file server] QAPP extension from the [Connectivity] package is required. The extension can be used free of charge for 30 days, after which it must be licensed.

A released drive with SMB protocol in your network is a requirement for this application.

This application can, therefore, be used to centrally store the menu settings of all networked MCA balances.

3.1.1 Setting up

Configuration steps:

1. Activate the [Connection to Windows File Server] QAPP extension, if this has not yet been done.
   a. Open the [Task management] menu, followed by the [QAPP Center].
   b. Choose the [Connectivity] software package, and within it the [Connection to Windows File Server] QAPP. The description and version of the QAPP will be displayed.
   c. Use the [License] button to activate this QAPP; the order and license information will be displayed.
   d. If this QAPP was not ordered as [factory licensed], start the test version or enter the license code that you have purchased for this QAPP.

2. Set up a connector to a Windows file server e.g., [My SMB server for settings].
   a. Open the [Settings] menu.
   b. Navigate to [Connections] -> [Connectors] -> [SMB].
   c. Use the [+] button to activate the creation of a new connector.
   d. Assign a unique name to this connector.
   e. Enter the network path for Host and Share, making sure that you use the correct spelling [//Host name/Share

name].
 f. Also enter the name of a sub-directory on the server, in which to save the files.
 g. Enter the username and password for access to the authorized drive in your network. Pay attention to the correct notation here too, particularly, upper/lower case letters.

3.1.2 Application

User steps:

1. From the main menu, use the [Setup] button to open the menu for the settings of the balance.
2. Press the [Export] button in the navigation and toolbar.
3. A list of the connectors is displayed, via which the report file can be exported.
4. Select your created connector e.g., [My SMB server for settings]. The report file is created and exported to the SMB server via the connector.
5. You get the [Report sent] and [Process completed] messages as confirmation for a successful export. The report file in the PDF format, with the related check file, is now present in the server and can be viewed.
6. If the report file could not be exported, then this file is not lost, see Troubleshooting.

Note: The PDF file format is a platform-independent data format for documents. Print output in this format can be viewed on each computer. For each PDF output file, a matching test file containing the checksum (MD5 hash value) of the PDF data is created. When the file is transferred, this checksum is saved in the audit trail. Using an appropriate tool, this PDF file can be compared with the check file to ensure the integrity of the PDF data.

3.1.3 Troubleshooting

No report file exported to the directory of SMB file server.

1. Make sure that all the configuration steps mentioned above have been followed.
2. Check that the balance is connected to the network e.g., via an Ethernet cable. The IP address of the balance in the network must be displayed in the [Status center] under [Device information].
3. Check the network path in the connector and the correct spelling of Host and Share, as well as the username and password for access rights to the SMB file server.
4. Test the connection of the connectors with the SMB file server by activating the [Info] button in the overview of the set values. If all the settings are correct and the SMB file server is accessible, you will receive a message stating that the connector is available.
5. If not, then check that the SMB file server is present in the network and that a file can be saved there from your PC.
6. If there is an [Transfer failure] error message, then you can do the following with the export:
   a. Retry: Retry exporting the report file to the network server.
   b. Retry later: The export of the report file is repeated automatically. Outstanding transfers are displayed in the [Status center] under [Messages].
   c. Redirect: You can redirect the report file to another connector.
   d. Delete: The export of the report file is canceled and deleted.

3.2 Update the QAPP Center of FTP server

This example describes the setup and application of the Cubis® MCA balance, in order to load the update for the QAPP Center of an FTP server.

For transferring files from an FTP network server, a [Connection to FTP/FTPS] QAPP extension from the [Connectivity] package is required. The extension can be used free of charge for 30 days, after which it must also be licensed.

Prerequisite for this application is an appropriately set up FTP server in your network.

For networked MCA balances, this application enables the update of the QAPP Center from a central source.

3.2.1 Setting up

Configuration steps:

1. Activate the [Connection to FTP/FTPS] QAPP extension, if this has not yet been done.
   a. Open the [Task management] menu, followed by the [QAPP Center].
   b. Select the [Connectivity] software package, and within it, the [Connection to FTP/FTPS] QAPP. The description and version of the QAPP will be displayed.
   c. Use the [License] button to activate this QAPP; the order and license information will be displayed.

   d. If this QAPP was not ordered as [factory licensed], start the test version or enter the license code that you have purchased for this QAPP.

2. Set up a connector to an FTP server e.g., [My FTP server for QAPP Center update].
   a. Open the [Settings] menu.
   b. Navigate to [Connections] -> [Connectors] -> [FTP].
   c. Use the [+] button to activate the creation of a new connector.
   d. Assign a unique name to this connector.
   e. Enter the IP address of the network server, ensuring that you spell it correctly
   f. A port number is required for the connection: the number 21 has been assigned. If required, you can enter a different port number.
   g. For updating the QAPP Center, you can also specify a sub-directory for the files stored in the server.
   h. Enter the username and password for accessing the FTP server. Pay attention to the correct notation here too, particularly, upper/lower case letters.

3.2.2 Application
User steps:

1. From the main menu, use the [Setup] button to open the menu for the settings of the balance.
2. Navigate to the [Device maintenance] -> [Install QAPP Center] menu item. A list of connectors is displayed, using which a package can be loaded for updating the QAPP Center.
3. Select your created connector e.g., [My FTP server for QAPP Center update]. The connection to the FTP server is established and a list of available packages for updating the QAPP Center is displayed.
4. Select the desired version of the QAPP Center and confirm the message for update.
5. The QAPP Center is now copied in the balance from the FTP server and updated. As confirmation, you get the updated version of the QAPP Center displayed.
6. See Troubleshooting, if the update could not be done.

3.2.3 Troubleshooting
Updating the QAPP Center not possible via the connector.

1. Make sure that all the configuration steps mentioned above have been followed.
2. Check that the balance is connected to the network e.g., via an Ethernet cable. The IP address of the balance in the network must be displayed in the [Status center] under [Device information].
3. Check the IP address and port number of the FTP server, as well as the username and password for access rights to the server in the connector.
4. Test the connection of the connectors with the FTP server by activating the [Info] button in the overview of the set values. If all the settings are correct and the FTP server is accessible, you will receive a message stating that the connector is available.
5. Check with your PC whether the specified sub-directory and as well as the file for updating the QAPP Center are present in the FTP server in the network.

3.3 View audit trail entries via web browser
This example describes the setup and use of the MCA balance so that entries in the audit trail of the balance can be viewed using the web browser.

The web browser [Chrome] is recommended for the remote operation of the MCA balance.

A secure connection of the balance with the browser via the HTTPS protocol requires certain device certificates.

For this, the MCA balance provides its own device certificates for download. These device certificates must be imported into the browser for the secure remote access to the device website. There is a separate description on the subject of [Certificates].

The complete scope of the audit trail can be used only after activating the [Audit trail] QAPP extension in the QAPP Center under [Pharma (QP1)].

A use of this application is, for instance, the central remote monitoring of settings in all the networked MCA balances.

3.3.1 Setting up
Configuration steps:

1. Activate the [Audit trail] QAPP extension, if not yet done.

   a. Open the [Task management] menu, followed by the [QAPP Center].
   b. Select the software package [Pharma] and QAPP [Audit trail] in it. The description and version of the QAPP will be displayed.
   c. Use the [License] button to activate this QAPP; the order and license information will be displayed.
   d. If this QAPP was not ordered as [factory licensed], start the test version or enter the license code that you have purchased for this QAPP.

2. Activate the website of the MCA balance, if not yet done.
   a. Open the [Settings] menu.
   b. Navigate to [Connections] -> [Website / web services].
   c. Set the [Website access] menu item to [Enabled, no authentication].

3. If necessary, activate the remote access to the website of the MCA balance.
   a. Open the [Settings] menu.
   b. Navigate to [Connections] -> [Website / web services].
   c. Under the [Remote access] menu item, select the [View and remote control] setting.

3.3.2 Application

User steps:

1. Start the web browser e.g., [Chrome] on your PC.
2. Enter the IP address of your balance, which is displayed in the [Status center] under [Device information].
3. If you have not yet imported the device certificates of the balance in the browser, you will see the [This is not a secure connection] message in the browser.
4. Using the [Advanced] button and the [Next...] link, you can now go to the IP address of the balance, which in this case is seen as unsafe or else you must first import the device certificates of your balance in your browser. There is a separate description on the subject of [Certificates].
5. Otherwise, the [My Cubis] page (home page) is now displayed in the browser.
6. Select the [Audit trail] page for the example.
7. You can now sort the list of entries according to ID, timestamp and user.
8. The list of entries can be displayed in ascending or descending order.
9. You can also set filters, in order to view only specific groups of entries.

3.3.3 Troubleshooting

The home page of the balance is not displayed in the browser.

1. Check that the balance is connected to the network e.g., via an Ethernet cable. The IP address of the balance in the network must be displayed in the [Status center] under [Device information].
2. Make sure that the [Website access] menu item is set to [Enabled].

The connection to the balance is displayed as [Unsecure] in the browser.

1. Import the device certificates of the balance in your browser. There is a separate description on the subject of [Certificates].

The [Audit trail] page cannot be selected on the home page of the balance.

1. Make sure that all the configuration steps mentioned above have been followed. In particular, the [Audit trail] QAPP extension has been activated and the license for this is still valid.

3.4 Synchronize date and time with NTP server

This example describes the setup and application of Cubis® MCA, in order to enable a synchronization of date and time of the balance with an NTP server.

The prerequisite for this use is the access to an NTP server in your company network or in the public network.

The time deviation between the balance and the NTP server is checked every 10 minutes. If the deviation is greater than 3 seconds, the time in the balance is then corrected and the change is entered in the audit trail.

This application enables an easy automatic update and synchronization of date and time on all the networked MCA balances.

3.4.1 Setting up

Configuration steps:

1. Set up an active NTP configuration.
   a. Open the [Settings] menu.
   b. Navigate to [Device settings] -> [Date and time] -> [NTP configuration].
   c. Activate the configuration of the NTP server settings using the [Edit] button.
   d. Set the [NTP operating status] menu item to [Enabled].
   e. Via the [Server IP] enter the address of the NTP server in the format IPv4 e.g., 192.53.103.108. (This is an NTP server of the Physical-Technical Federal Institute in Braunschweig, Germany.)
   f. Confirm the NTP configuration with the [OK] button.
   g. Test the connection to the NTP server by activating the [Info] button in the overview of the NTP configuration.

2. Set the correct time zone for your location.
   a. Open the [Settings] menu.
   b. Navigate to [Device settings] -> [Date and time] -> [Set date and time].
   c. Activate the settings for date and time using the [Edit] button.
   d. Set your location using the [Time zone] menu item, [UTC +/- time, place]. Thereafter, the time and date are displayed immediately matching with your local time.

Note: After setting the date, time and time zone, the MCA balance asks you to restart the system.

3.4.2 Troubleshooting

No connection possible to the NTP server.

1. Make sure that all the configuration steps mentioned above have been followed.
2. Check that the balance is connected to the network e.g., via an Ethernet cable. The IP address of the balance in the network must be displayed in the [Status center] under [Device information].
3. Check with your PC, whether you can access the IP address of the NTP server.

4 Appendix

4.1 Compatible Wi-Fi sticks

Cubis® MCA supports the most common Wi-Fi sticks (USB WLAN adapters) which are available in the market.

Keep in mind the following items when selecting a Wi-Fi stick:

1. Avoid Wi-Fi sticks without name. Always buy a known brand.
2. If possible, check the data sheet of the Wi-Fi stick to ensure that it contains one of the following supported chip sets.

Supported Wi-Fi chip sets are:

- 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. Abbreviations

DHCP	Dynamic Host Configuration Protocol	A communication protocol in computer technology. It allows for the allocation of the network configuration to clients by a server.
DNS	Domain Name System	System for resolution of computer names in IP addresses and vice versa.
FTP	File Transfer Protocol	A standard network protocol for the transfer of files between a client and a server within a network.
FTPS	FTP over TLS	A method for encrypting the File Transfer Protocol (FTP).
HTTPS	Hypertext Transfer Protocol Secure	A communications protocol with which the data can be transmitted as encrypted.
IPv4	Internet Protocol version 4	Internet protocol of version 4.
IPv6	Internet Protocol version 6	Internet protocol of version 6.
MAC address	Media Access Control address	Physical hardware address, unique identifier of the device in the network.
NTP	Network Time Protocol	A standard for synchronizing clocks in computer systems.
PNG	Portable Network Graphics	Portable network graphics, a raster graphics format with lossless data compression.
PSK	Pre-shared key	Encryption method in which the key must be known to both the participants before communication.
REST	Representational State Transfer	Programming paradigm for distributed systems, particularly for web services.
SMB	Server Message Block	A network protocol for file, print, and other server services in computer networks.
SSID	Service Set Identifier	Freely selectable network name e.g., for Wi-Fi.
URL	Uniform Resource Locator	Identification for Internet or web addresses.
UTC	Universal Time, Coordinated	World time, also Earth time or Universal time.
WEP	Wired Equivalent Privacy	Standard encryption protocols for WLAN.
Wi-Fi	Wireless Fidelity	Wireless network, synonym for WLAN.
WLAN	Wireless Local Area Network	Wireless, local network.
WPA	Wi-Fi Protected Access	Encryption methods for a wireless network. Successor of WEP.
WPA2	Wi-Fi Protected Access 2	Implementation of a security standard for radio networks. Successor of WPA.