Description of Access Management for the Cubis® MCA Balance

This description explains the comprehensive role and user management of Sartorius Cubis® MCA Premium laboratory balance with the QAPP extension [User management] and shows with application examples, how this extension can be configured and used.

Executive Summary

The Sartorius Cubis® MCA laboratory balance offers a modern and future-oriented user management that fulfills all requirements of 21 CFR Part 11 and EudraLex, Volume 4, Annex 11. In addition to the internal user management, which can be adapted to the company's security policy, the integration of an external LDAP-based user management is also possible.

1 Access management

A logged-in user is required in order to use the scale. Each user is linked to a role. With its rights, the role determines which functions are enabled for the logged-in user. With the initial installation, four predefined users with the corresponding roles are created, which can be used for the first operation. Through the QAPP extension [User management], further users and roles with rights can be created, as well as certain rules for the login can be set.

2 Default user

During initial commissioning or after a reset to factory settings, four users are automatically created in the selected language after running the setup wizard.
These predefined users have fixed roles, and hence also fixed rights for accessing the balance.
To gain full access to the device functions, you must log in as [Administrator].

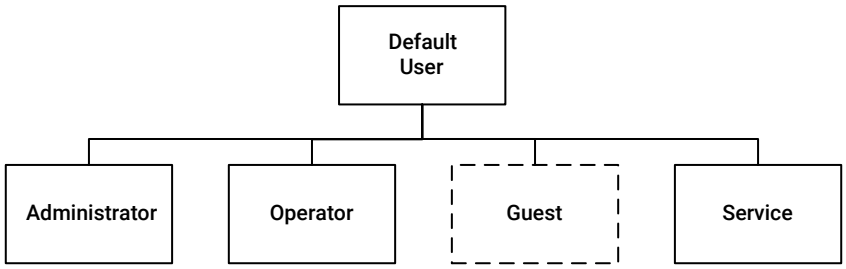

Figure 1: Predefined users

The predefined users cannot be deleted, but their respective settings can be modified. The guest is set to inactive ex-factory.
No password is set as default for administrator, user and guest. The service requires a special service password that has to be regenerated with every login using a service tool.

2.1 Settings of the predefined users

The administrator can customize the settings of the predefined users. The username, the user description, the language on the balance, the color for the user field and the login process can be modified. The role is defined as fixed for each user. Except for the administrator and the service, the users can be set as active or inactive. An example for editing a user can be found here.

2.2 Predefined roles and rights

The roles defined ex-factory cannot be deleted; pre-set rights for accessing the balance are set in the roles.

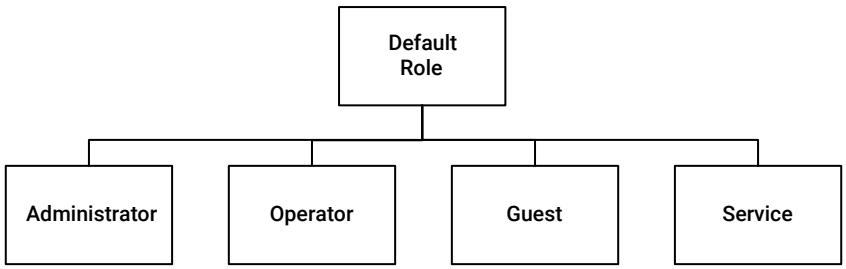

Figure 2: Predefined roles

These rights are assigned permanently to the predefined roles:

- The [Administrator] role has all the rights to guarantee full access. The balance can be set up according to the requirements using this role. This role has the rights for task management (create, edit, delete tasks), access to all points of the setup menu (change settings), user management (change users) and access to the QAPP Center.
- The [Operator] role can only execute the tasks.

- The [Guest] role has only rights to execute the assigned tasks.

2.3 Rules for login

The user login can be set to require password entry or not. The password must consist of at least one character. No further rules are activated ex-factory.

2.4 Automatic login

In the device settings, an automatic login for the user [Administrator] or [Operator] can be set for the startup-up behavior of the balance. If no password is set for these users, the balance immediately logs on the set user and displays the main menu or starts the last used or a specific task. The behavior for this can be set up accordingly in the task start settings.

Even if user management is activated, it is not intended to automatically log in other newly created users in order to ensure CFR21 Part 11 compatibility. Instead, it should be possible for devices without user management to start automatically.

3 QAPP extension [User management]

Using the [User management] QAPP extension, further users can be created, modified and deleted. The added access management enables the creation, editing and deletion of further roles. Moreover, rules can also be set for login and logout as well as rules for local passwords. For using the network passwords, it is necessary to do the settings for the LDAP server.

The QAPP [User management] must be activated via the QAPP Center under the package [Pharma]. It can be used free of charge for 30 days before a license has to be acquired.

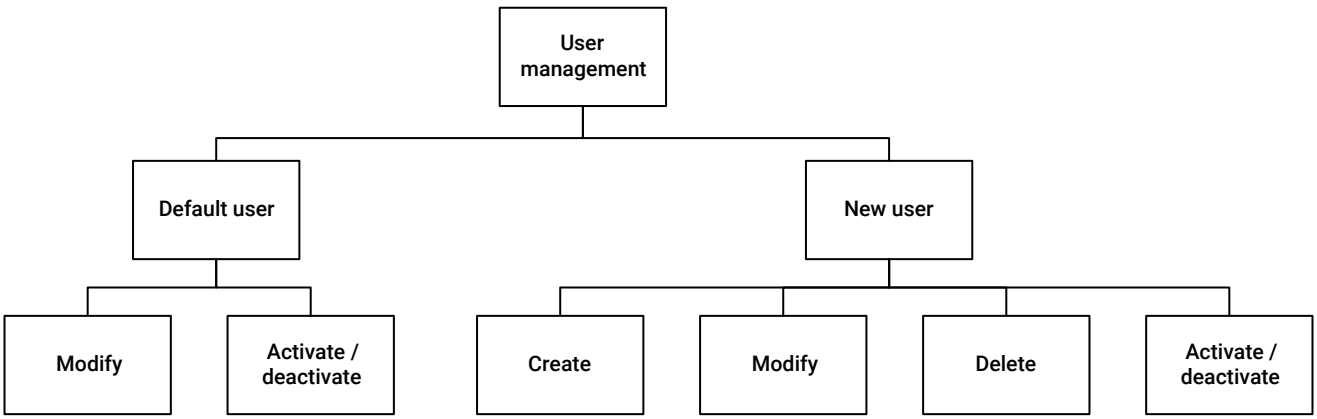

Figure 3: User management

3.1 User settings

Newly created users can be modified or deleted as well as set as active or inactive. All settings for these created users are accessible.

A display name and a login name must be assigned for each user. In addition, another user description can be entered. The user must be assigned one of the predefined or a newly created role with the rights contained therein. Furthermore, the language for operation and logging can be set individually for each user. For individual differentiation it is possible to select a color value for the user field. For the password it must be defined whether a local password on this scale, a network password or no password is required for the login.

The process of creating a user or a role can be streamlined using the duplicate function. When duplicating a user or role, it is essential to assign a unique name to the new entity. In practice, a template inactive user can be created, from whom all settings are then transferred to the new user.

See also chapter: Example for creating local user.

3.2 Access management

With the QAPP extension [User administration], functions for creating, editing and deleting roles and users are activated in the menu. In addition, menu items are provided for the management of logon and logoff rules, local

password rules and the configuration of an LDAP server.

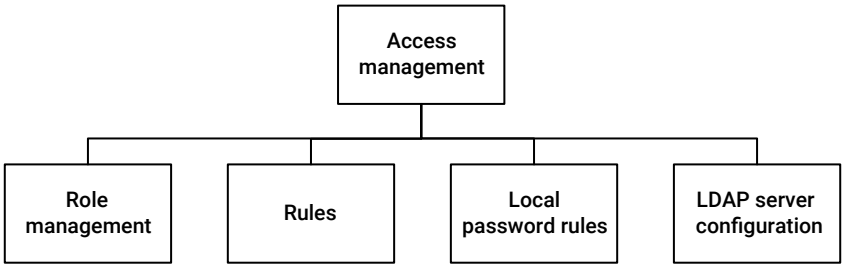

Figure 4: Access management

3.2.1 Role management

Newly created roles can be changed and deleted. Each role is uniquely identified on the device via a role name. For a more detailed description, a role description can also be stored. Different role rights are linked to each role. The roles can be assigned to newly created users and tasks. For the roles that are predefined ex works, the fixed rights are retained and these roles cannot be deleted.

See also chapter: Example for creating new role.

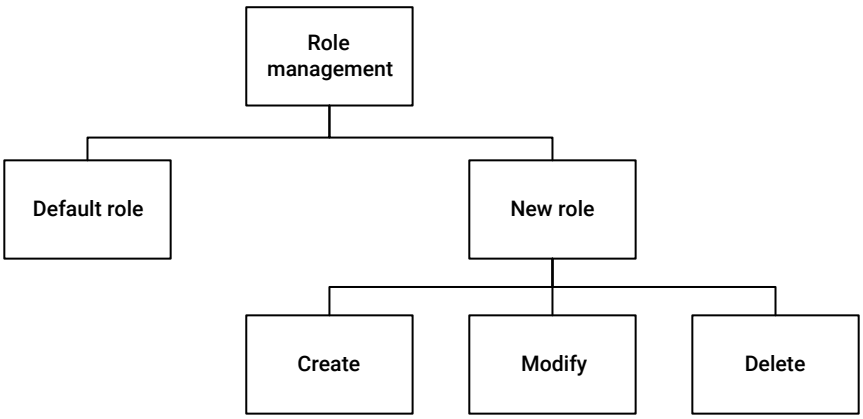

Figure 5: Role management

3.2.2 Role rights

The device allows individual access to device functions by assigning rights. The rights are described in detail below. The rights can be extended by firmware updates.

The default roles Administrator and Service automatically have all available rights. Neither role can be changed, so access to the entire system is always possible. If restricted rights are required, new roles must be created.

The following rights are available in the system:

- User management: Access to the management for creating, modifying or deleting device users. Needs also right to access settings menu.
- Task management: Access to the management for creating, changing or deleting tasks. Access is from the main menu and settings menu.
- Access device settings: General access to the settings menu. Partly required to gain access to underlying menu structures.
- Access QAPP Center: Access to the QAPP Center. From there, the QAPP Center can be updated, QAPP descriptions can be viewed and QAPPs can be licensed. Access is via the task management.
- Access audit trail: Read access to the audit trail and export of the data. This must be licensed by the corresponding extension.
- Access Data storage device: Access to read the data storage device and export data.
- Execute tasks:
- Access profile management:Access to weighing and print profiles

- Access device management: Access to the device settings like time configuration, device ids, device cleaning and display settings. Needs also right to access settings menu.
- Role management: Access to the management for creating, modifying or deleting device roles. Needs also right to access settings menu.
- Access management: Access to the “Access management” settings menu (prerequisite for role and user management, LDAP settings and password rules)
- LDAP/S settings: Access to the LDAP or LDAPS settings such as server configuration, assigned user roles and groups and the creation of new users
- Management of time-controlled actions: Access to the administration for creating, changing or deleting time-controlled actions, such as automatic device backup, export of device data, etc.
- Access connections: Access to the “Connections” menu
- Redirect failed data transfers: Allows sending generated files with pending transfers to different connectors
- Delete failed data transfers: Allows deleting generated files with pending transfers to different connectors
- Access firmware update: Allows to update firmware on non-secured balances
- Access QAPP installation: Allows installation of QAPPs
- Access backup and restore:
- Access export and import:
- Access reset to factory settings: Allows to reset device to factory defaults
- Unlock device: Unlock a device locked by another user
- Remote view: Show device display on device website
- Remote view and control: Control access to device on device website
- Manage jobs: View and delete jobs on device website
- Show calibration reports: Access to show calibration reports
- Show last reports: Access to show last reports on device website
- Access USB storage: Allow global read / write access on USB storages

3.3 Rules for login and logout

An automatic logout of the logged-in user can be set after a specific period of non-use of the balance.

For login with password, a maximum number of failed attempts can be entered. The behavior after this number of failed attempts is either [no action], [login delay for re-login] or [deactivation of user account] can be set on the scale.

A deactivated user account must first be released again by a user with the user management right.

3.4 Local password rules

Rules can be specified for the local password of the user on this balance. In this way, the necessary use of characters (upper/lower case letters, numbers, special characters) in the password and the minimum length of the password can be defined. Moreover, the validity period of the password as well as the reuse of the password can also be configured.

See also chapter: Example for setting local password rules.

3.5 Network password (via LDAP)

If the [Network password] selection is set in the user settings for the password, then upon a login with this user the balance must be present in a network with LDAP server and the user must already be configured in the network. Thus, the rules defined in the network apply to the network password.

3.5.1 Settings of LDAP server

The device supports the logon of users via the "Lightweight Directory Access Protocol" (LDAP). Connecting to an LDAP directory server is useful if your users and groups are stored in a corporate directory. If the service is available

at the location where the balance is used (e.g. Microsoft Active Directory), users can also log on to the balance with their user data after successful setup.

The settings for the LDAP must be stored on the device. The exact details of the LDAP server can be obtained from the respective IT department responsible for the company network.

The LDAP configurations must be entered in the distinguished name (DN) form e.g. "uid=user,ou=People,ou=mycompany,c=en". Special characters must be expressed in an escape sequence. The full distinguished name of an entry can be copied directly from the corresponding LDAP management tool on some LDAP servers. This simplifies the entry.

Explanation of the acronyms:

- CN = [Common Name]
  The name by which the user is normally known e.g., First name.Surname.
- DN = [Distinguished Name]
  The unique designation of a user. This is the directory path which leads directly to the user in the server. The DN contains the CN for the case that there are several users with the CN name.
- OU = [Organizational Unit]
  A part of the DN i.e., the directory name, under which a user can be found. OU is used mostly for the department name or the location.
- DC = [Domain Component]
  The root of the LDAP tree i.e., the name of the root directory. Frequently, this is the company domain ([DC=Company name, DC=com])
- "UID = [Universal Identifier]
  Does not have any special meaning for LDAP; in some systems the username is present here, in which case one must enter [uid=%u] in the search filter."

Note: The notation in upper and lower case letters of the acronym (CN, DN, DC, OU, UID or cn, dn, dc, ou, uid) is irrelevant. However, the correct notation of the values coming after these is important.

The device supports some of the regular parameters for Microsoft Active Directory. If this directory schema is selected, some configurations are determined from the default attributes. Furthermore, it can be used to determine and assign roles from LDAP groups.

The necessary parameters are divided into:

- Connection and type of the LDAP server
- Data of the manager for reading the user data (read only)
- Specification of the user location
- Default setting for the initial login of a user

The individual parameters are described below with their significance for the configuration:

3.5.1.1 Server name

The server name specifies the host name or the IP address of the LDAP server. Currently, the current version supports the protocol LDAP protocol with its port 389. LDAPS is currently not supported.

- Syntax: [protocol]://[IP or host]:[port]
- Example: ldap://servername.domain.com:389 or ldap://172.16.244.99:389

3.5.1.2 Directory schema

The directory schema defines how entries are used in Active Directory (AD). The parameters change depending on the AD provider. The device provides a predefined built-in connector for the Microsoft LDAP directory servers. All other providers must be adapted via a generic configuration.

- Microsoft Active Directory
  The configuration uses the sAMAccountName parameter to identify the user name. With this configuration, the user's data is updated each time the user logs in (i.e., the first and subsequent times) based on the user's data

in LDAP. This includes username, display name, assigned role if applicable. However, for role assignment, only the following applies:
- Only direct groups (i.e. no nested groups) are synchronized from LDAP.
- Only roles that are already configured and present on the device are assigned. I.e. each role needs a connection to a group in LDAP.

- Generic
  In the generic configuration, the parameters for the login must be explicitly stored. For this purpose, it must be known under which parameter the login name is stored in LDAP. This depends on the existing LDAP configuration. If the parameters for the display name are also stored, the display name of the user is also updated when logging in. With the generic scheme it is not possible to get the role assignment from a group of the LDAP.

3.5.1.3 Manager DN (Distinguished name)
The unique designation, the directory path of the user account [Manager] on the LDAP server. This user should have a read permission in the LDAP server, in order to be able to search for other users. This is mostly a virtual user, whose password is not changed constantly. In case of a login query (login), the [Manager] searches for the user, who wishes to log on to the LDAP server. For managers with [First name.Surname].

- Example: DN=Surname /, First name, OU=Resources, OU=User, OU=GO-Goettingen, OU=Region Europe, DC=Company name, DC=com

3.5.1.4 Manager password
The password of the user account [Manager], in order to be able to log on to the server for the search request.

3.5.1.5 User OU
The place, the directory on the LDAP server, starting from which the user is to be searched. Do not use the root directory here, as otherwise the search for a user can take very long in large companies and can thus cause timeouts.

- Example: OU=GO-Goettingen, OU=Region-Europe, DC=Company name, DC=com

3.5.1.6 Role assignment
Dynamic assignment of roles is possible only if the Microsoft Active Directory schema is selected. This function enables the option of role assignments. The description of how to configure assignments can be found here.

- LDAP group: searches the user's LDAP memberships for one of the configured group role mappings. If a mapping is found, the user is given that role for the session.
- Local user: Assign the user the role that is already stored for the user on the device.

3.5.1.7 Search filter (generic only)
The filter specifies which LDAP parameter should be used as the login name. This is often 'sAMAccountName' for a Microsoft Active Directory. Other directory services use 'uId'. Depending on the service or company specification, the parameter can be different. Basically, anything that is stored in LDAP and is suitable as an identifier is possible as a login name, e.g. e-mail, etc.

The filter must be entered in the form: <property>=%u. %u is replaced by the login name on the device.

- Example: sAMAccountName=%u
  Notice: Always pay attention to upper/lower case letters when using the filter.

3.5.1.8 LDAP attribute for display name
The display name attribute designates the attribute name in your LDAP system under which the display name is stored. This option is changeable only for the generic configuration. In case of Microsoft Active Directory configuration the attribute 'displayName' is used.

3.5.1.9 Auto create user
When set to [Off], the user must already exist on the balance with the same name as in the network, in order to log on to the network. During login, only those users are displayed in the selection that are present on the balance.

If the selection is set to [On] for this point and the user is not yet available on the balance, then during login it is possible to enter the username as saved in the network. Upon a successful log on to the network, this user is then

automatically created in the balance with the specified values for language and role.

3.5.1.10 Default role
The role to be used for automatically created users is set with this default setting.

3.5.1.11 Default language
The language can be set as default for this point for the case that the automatic creation of users on the balance is enabled.

3.5.1.12 Detailed logging
Since every IT infrastructure is different, the device offers the option of logging individual steps during the LDAP connection in more detail. However, this function should only be activated for checking and test purposes so that data from the LDAP is not logged unintentionally. Select [Yes] to activate logging. Passwords are not output. Follow the service instructions to view the logs.

3.5.2 Role assignment via LDAP
Based on an assignment of users to different LDAP groups, an assignment of roles can be made on the device. For this purpose, the names of the group as well as the assignment of the respective group must be defined on the device. This function is currently only available for the Microsoft Active Directory schema.

The order of the groups determines the search order. The first matching group name, which is stored as attribute 'MemberOf' in the respective user, is found, the set role is assigned at each logon. The order can be changed by using the up and down arrows next to each group assignment entry.

To automatically assign roles to the user, do the following:

1. Make sure that the desired users have already been assigned to appropriate groups in your LDAP. The scale checks during a login if only the group name (Common Name) is linked to the user. The full path to the group is not evaluated.
2. In the LDAP settings menu, set the directory scheme to "Microsoft Active Directory" and the role assignment to "LDAP Group". This will unlock the role assignment option in the top menu bar. Open the menu.
3. The + creates a new mapping. Enter the same name for the group name as it is found in LDAP. Pay attention to upper and lower case.
   The role can be selected from a drop-down list. It contains all roles that are available on the system.
   Acknowledge the selection with the confirm button. Repeat this step until all desired roles are associated with a group.
4. When all entries have been created, finally set the prioritization. If a user is included in more than one group, the prioritization determines which role should be used preferentially. The groups are searched from top to bottom. You can move the prioritization with the arrow keys. Wrong groups can be removed with the delete button.

4 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. Corresponding user rights are needed for setting up the QAPP extension, users, roles, rights and rules.

The [User management] QAPP extension must be activated for all application examples, except for the first one.

4.1 Example for editing user settings
In this example, the Administrator user should get a specific color in the user field and the login should be done with a local password.

4.1.1 Setting up
1. Edit the settings of the specified user e.g., [Administrator].
   a. Open the [Settings] menu.
   b. Navigate to [Access Management] -> [User management] -> [Administrator], the current settings are displayed.
   c. Activate the editing of the settings using the [Edit] button.
   d. Select the [User color profile] menu item and set the color, for instance, [Red] for the user field.
   e. Select the [Login method] menu item and set the selection to [Local password].
   f. The [OK] button applies your settings and displays these as overview.
   g. Exit the menu and log out from the main menu by using the [User logout] button.

2. With the [Administrator] selection and the [User login] button, the system now asks for to enter a password for the login.
   a. Press the [New password] button and enter your desired password.
   b. After confirmation, your password must be entered again for security reasons.
      If the password entered both the times is identical, then you get the confirmation that your password has been changed successfully.

Note: Keep your Administrator password safe; if lost, it can be deleted only through the Sartorius Service.

4.1.2 Application

For logging on to the balance e.g., after power-on or after a user change through logout, you must enter your password as user [Administrator].

4.1.3 Troubleshooting

Password:

1. The password must consist of at least one character.
2. While entering, pay attention to capital and small letters.

4.2 Example for creating local user

This example describes the setup and application of a local user along with the available roles. The user should get a local password.

4.2.1 Setting up

Configuration steps:

1. Activate the [User management] 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 [User management] 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. Configure a local user, for instance, [My local user].
   a. Log in as [Administrator] with the necessary rights, if not yet done.
   b. Open the [Settings] menu.
   c. Navigate to [User management] and activate the creation of a new user with the [+] button.
   d. Enter a display name, a login name and optionally a user description, such as [My local user] as display name, [local.user] as login name and as description [Local user with password].
   e. Open the selection of the role and select the [User] menu item.
   f. Select [Language] to select the text guidance on the balance required by the user.
   g. Open the [Login method] selection and set the [Local password] menu item.
   h. The [OK] button applies your settings and displays these as overview.
   i. Using the buttons, it is now possible for you to [Deactivate]/[Activate] this user, to set the [Password], to [Delete] the user or to [Edit] the settings.
   j. Exit the menu and log out from the main menu by using the [User logout] button.

4.2.2 Application

After selecting the new user e.g., [My local user], and the [User login] button, the entry of a password is demanded each time this user logs in.

User steps:

1. If no password was assigned while creating the user, the first entry of the password is done now.
   a. Press the [New password] button and enter your desired password.
   b. After confirmation, your password must be entered again for security reasons.
      If the password entered both the times is identical, then you get the confirmation that your password has been changed successfully.

Note: Keep your password safe; if lost, it must then be deleted by the [Administrator] user.

4.2.3 Troubleshooting

Password:

1. The password must consist of at least one character.
2. While entering, pay attention to capital and small letters.

4.3 Example for creating new role

In this example, a new role is to be created with the right of task management and access to the Setup menu.

4.3.1 Setting up

Configuration steps:

1. Activate the [User management] 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 [User management] 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. Configure a new role e.g., [My role task and menu].
   a. Log in as [Administrator] with the necessary rights, if not yet done.
   b. Open the [Settings] menu.
   c. Navigate to [Access management] -> [Role management].
   d. Use the [+] button to activate the creation of a new role.
   e. Enter a role name and, optionally, a role description e.g., [My role task and menu] and as description [Role with task and menu rights].
   f. Open the selection of role rights and select [Task management] and [Access settings menu].
   g. The [OK] button applies your settings and displays an overview of the roles.
3. You can now assign this role to a user via the user management.

4.4 Example for setting local password rules

This example describes the modification of the local password rules so that the rule applies to all users and their passwords that it must have a length of at least 8 characters and must contain capital/small letters and numbers.

4.4.1 Setting up

Configuration steps:

1. Activate the [User management] 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 [User management] 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. Configure the password rules according to the desired requirements.
   a. Log in as [Administrator] with the necessary rights, if not yet done.
   b. Open the [Settings] menu.
   c. Navigate to [Access management] -> [Local password rules].
   d. Open the [Password length (characters)] selection and select the necessary characters to be used in the password, [Lower-case letters], [Uper-case letters] and [Numbers].
   e. Enter the necessary minimum length e.g., 8 characters via the [Password minimum length] menu item.
   f. The [Password validity period] and [Prevent password reuse] selection items remain [Off] in this example.
   g. Exit the menu and log out from the main menu by using the [User logout] button.

4.4.2 Application

For logging on to the balance e.g., after power-on or after a user change through logout, you must now, as the user, fulfill the set password rules with a local password.

User steps:

1. Upon selection of a user e.g., [My local user] and the [User login] button, you may now possibly get the message that the password rules are not fulfilled for your password.

a. Press the [New password] button and enter your desired password.
b. After confirmation, your password must be entered again for security reasons. If the password entered both the times is identical, then you get the confirmation that your password has been changed successfully.

Note: Keep your password safe; if lost, it must then be deleted by the Administrator user.

4.4.3 Troubleshooting

Password:

1. The password must consist of upper/lower case letters and numbers.
2. The password must have a length of at least 8 characters.
3. While entering, pay attention to capital and small letters.

4.5 Example for creating network user

In this example, a new user is to be created, whose login data username and password are fetched from an LDAP server in the network. The user is given a role available in the balance.

4.5.1 Setting up

Configuration steps:

1. The following items are the prerequisite for configuring a network user.
   a. The [User management] QAPP extension is activated on the balance.
   b. The balance is connected to the network and an LDAP server is present there.
   c. The settings for this LDAP server have been configured in the balance.
   d. The user is configured in the network.
2. Configure a network user, for instance, [My network user].
   a. Log in as [Administrator] with the necessary rights, if not yet done.
   b. Open the [Settings] menu.
   c. Navigate to [User management] and activate the creation of a new user with the [+] button.
   d. Enter the login name in exactly the same way as configured in the network e.g., [First name.Surname]. Additionally the input of the display name is necessary e.g. [Surname].
   e. Optionally, you can also enter a user description e.g., [Network user].
   f. Open the selection of the role and select the [User] menu item.
   g. Select [Language] to select the text guidance on the balance required by the user.
   h. Using the [User color profile] menu item, you can set the desired color for the user field.
   i. Open the [Login process] selection and set the [LDAP] menu item for network login.
   j. The [OK] button applies your settings and displays these as overview.
   k. Using the buttons, it is now possible for you to [Deactivate]/[Activate] this user, to [Delete] the user or to [Edit] the settings.
   l. Exit the menu and log out from the main menu by using the [User logout] button.

4.5.2 Application

User steps:

1. The following items are the prerequisite for the login of a network user e.g., [First name.Surname]:
   a. The balance is connected to the network and an LDAP server is present there.
   b. The settings for this LDAP server have been configured in the balance.
   c. The user [First name.Surname] is configured in the network.
   d. The user [First name.Surname] is created in the balance.
2. Upon selection of this network user e.g., [First name.Surname], and the [User login] button, the login is now done with the password stored in the network.
3. Enter the network password. After a successful login to the network, this user is activated with his settings and rights, as configured in the balance.

4.5.3 Troubleshooting

No connection to the LDAP server:

1. Check the connection of your balance with the network.
   Check whether an IP address of the balance is displayed in [Status center].
2. Check whether you can log on to your PC with the same username and password.
   Let your administrator check the settings for the LDAP server on the balance.

Password:

1. Enter your network password in the correct form.
   Pay attention to upper and lower case letters.

4.6 Example for Automatically creating network user

This example describes the automatic creation of a user in the balance, whose login is done via the balance with username and password on a LDAP server in the network. In the balance, the user gets the predefined language and role.

4.6.1 Setting up

Configuration steps:

1. The following items are the prerequisite for automatic configuration of a network user in the balance.
   a. The [User management] QAPP extension is activated on the balance.
   b. The balance is connected to the network and an LDAP server is present there.
   c. The settings for this LDAP server have been configured in the balance, particularly, the [Auto create user] menu item is set to [On] and the predefined settings for language and role are selected.
   d. The user is configured in the network.
2. In the login display, activate the field with the last used username.
   The list of users created in the balance is displayed.
3. For automatically creating a new network user, press the [+] button and confirm the message displayed with [Continue].
4. Enter the username as configured in the network.
5. Thereafter, enter the password as stored in the network.
6. After a successful login to the network, this user is created automatically in the balance, with the entered username and the predefined language as well as the predefined role.
7. The newly created user is displayed in the list of the users available in the balance and you can now select the user.

4.6.2 Application

User steps:

1. The following items are the prerequisite for the login of a network user e.g. [First name.Surname].
   a. The balance is connected to the network and an LDAP server is present there.
   b. The settings for this LDAP server have been configured in the balance.
   c. The user [First name.Surname] is configured in the network.
   d. The user [First name.Surname] is created in the balance.
2. Upon selection of this network user e.g., [First name.Surname], and the [User login] button, the login is now done with the password stored in the network
3. Enter the network password. After a successful login to the network, this user is activated with his settings and rights, as configured in the balance.

4.6.3 Troubleshooting

No connection to the LDAP server:

1. Check the connection of your balance with the network.
   Check whether an IP address of the balance is displayed in [Status center].
2. Check whether you can log on to your PC with the same username and password.
   Let your administrator check the settings for the LDAP server on the balance.

Password:

1. Enter your network password in the correct form.
   Pay attention to upper and lower case letters.

5. Abbreviations

CN	Common Name	The name by which the user is normally known in the network.
DC	Domain Component	Domain components, the root of the LDAP director, mostly the company domain.
DN	Distinguished Name	A unique object name in the LDAP directories, here the unique identifier of a user.
OU	Organisational Unit	Organizational unit, folder name, under which the user can be found e.g., the department.
UID	Universal Identifier	Universal identifier, no special meaning.
FDA	Food and Drug Administration	Food and Drug Administration of the United States.
LDAP	Lightweight Directory Access Protocol	Network protocol for query and modification of information of distributed directory services, based on the TCP/IP protocol.
LDAPS	LDAP over SSL/TLS	LDAP network protocol with encryption.
SSL	Secure Sockets Layer	Hybrid encryption protocol for safe data transfer in the Internet.
TLS	Transport Layer Security	Successor of SSL
21 CFR Part 11		Part 11 of Title 21 of the FDA regulation, regulates, among other things, electronic records and signatures.