Descrizione della gestione degli utenti per la bilancia Cubis® MCA

Questa descrizione spiega il ruolo completo e la gestione degli utenti della bilancia da laboratorio Sartorius Cubis® MCA Premium con l'estensione QAPP [Gestione utenti] e mostra con esempi di applicazione come questa estensione può essere configurata e utilizzata.

Riassunto esecutivo

La bilancia da laboratorio Sartorius Cubis® MCA offre una gestione degli utenti moderna e orientata al futuro che soddisfa tutti i requisiti del 21 CFR Parte 11 e di EudraLex, Volume 4, Allegato 11. Oltre alla gestione interna degli utenti, che può essere adattata alla politica di sicurezza dell'azienda, è possibile anche l'integrazione di una gestione esterna degli utenti basata su LDAP.

1 Gestione degli accessi

Per utilizzare la bilancia è necessario un utente loggato. Ogni utente è collegato a un ruolo i cui diritti memorizzati determinano quali funzioni sono abilitate per l'utente loggato. Con l'installazione iniziale, vengono creati quattro utenti predefiniti con i ruoli corrispondenti, che possono essere utilizzati per la prima operazione. Attraverso l'estensione QAPP [Gestione utenti], possono essere creati altri utenti e ruoli con diritti, così come possono essere impostate alcune regole per il login.

2 Utente predefinito

Durante la prima messa in funzione o dopo un ripristino delle impostazioni di fabbrica, questi utenti vengono creati automaticamente nella lingua selezionata dopo aver eseguito la procedura guidata di configurazione.
Questi utenti predefiniti hanno ruoli fissi e quindi anche diritti fissi per l'accesso alla bilancia.
Il login deve essere fatto come [Amministratore] per ottenere l'accesso completo alla bilancia.

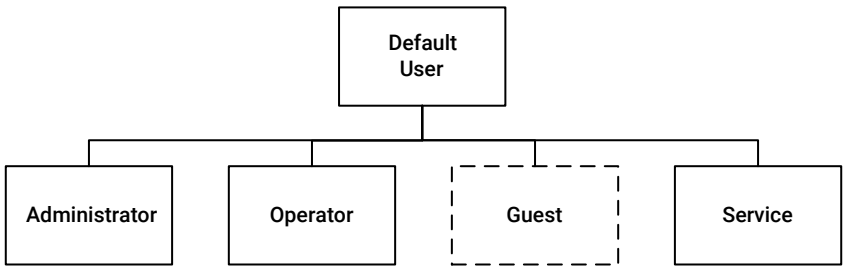

Figura 1: Utenti predefiniti

Gli utenti predefiniti non possono essere cancellati, ma le loro rispettive impostazioni possono essere modificate.
L'ospite è impostato in fabbrica come inattivo.
Nessuna password è impostata come predefinita per amministratore, utente e ospite. Il servizio richiede una speciale password di servizio, che deve essere rigenerata ad ogni login utilizzando uno strumento.

2.1 Impostazioni degli utenti predefiniti

L'amministratore può personalizzare le impostazioni degli utenti predefiniti. Il nome utente, la descrizione dell'utente, la lingua del saldo, il colore del campo utente e il processo di login possono essere modificati. Il ruolo è definito come fisso per ogni utente. Tranne l'amministratore stesso, gli utenti possono essere impostati come attivi o inattivi. Un esempio per modificare un utente può essere trovato qui.

2.2 Ruoli e diritti predefiniti

I ruoli definiti ex-fabbrica non possono essere cancellati; i diritti fissi di accesso alla bilancia sono impostati nei ruoli.

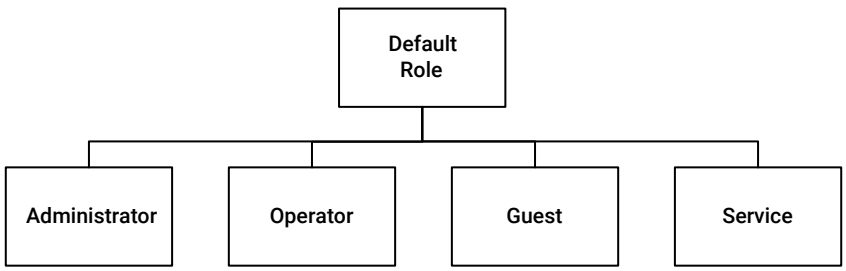

Figura 2: ruoli predefiniti

Questi diritti sono assegnati in modo permanente ai ruoli predefiniti:

- Il ruolo [Amministratore] ha tutti i diritti per garantire un accesso completo. Il bilancio può essere impostato secondo le esigenze utilizzando questo ruolo. Questo ruolo ha i diritti per la gestione dei compiti (creare, edit, cancellare i compiti), l'accesso a tutti i punti del menu di configurazione (cambiare le impostazioni), la gestione

degli utenti (cambiare gli utenti) e l'accesso al Centro QAPP.

- Il ruolo [Utente] può solo eseguire i compiti.
- Il ruolo [Guest] ha solo i diritti di eseguire i compiti assegnati.

2.3 Regole per il login

Il login utente può essere impostato per richiedere o meno l'inserimento di una password. La password deve consistere di almeno un carattere. Non ci sono altre regole attivate in fabbrica.

2.4 Accesso automatico

Nelle impostazioni del dispositivo è possibile impostare un login automatico per l'utente [Administrator] o [Operator] per il comportamento all'avvio della bilancia. Se non è impostata alcuna password per questi utenti, la bilancia accede immediatamente all'utente impostato e visualizza il menu principale o avvia l'ultimo task utilizzato o un task specifico. Il comportamento per questo può essere impostato di conseguenza nelle impostazioni di avvio dell'attività.

Anche se la gestione degli utenti è attivata, non è prevista la registrazione automatica di altri utenti appena creati, al fine di garantire la compatibilità con la CFR21 Part 11. Dovrebbe invece essere possibile avviare automaticamente i dispositivi senza gestione degli utenti.

3 Estensione del QAPP [Gestione degli utenti]

Utilizzando l'estensione QAPP [Gestione utenti] è possibile creare, modificare e cancellare altri utenti. La gestione degli accessi aggiunta permette la creazione, la modifica e la cancellazione di ulteriori ruoli. Inoltre, possono essere impostate regole per il login e il logout, nonché regole per le password locali. Per utilizzare le password di rete, è necessario fare le impostazioni per il server LDAP.

Il QAPP [Gestione utenti] deve essere attivato tramite il Centro QAPP sotto il pacchetto [Pharma]. Può essere utilizzato gratuitamente per 30 giorni prima di dover acquistare una licenza.

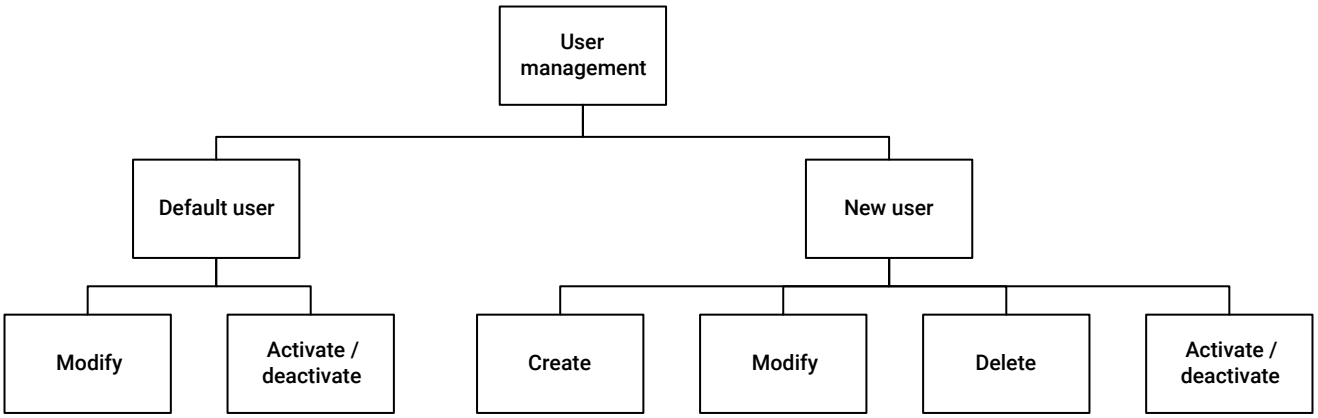

Figura 3: Gestione degli utenti

3.1 Impostazioni utente

Gli utenti appena creati possono essere modificati o cancellati e impostati come attivi o inattivi. Tutte le impostazioni di questi utenti creati sono accessibili.

Un nome di visualizzazione e un nome di accesso devono essere assegnati per ogni utente. Inoltre, può essere inserita un'altra descrizione dell'utente. All'utente deve essere assegnato uno dei ruoli predefiniti o un ruolo appena creato con i diritti contenuti in esso. Inoltre, la lingua per il funzionamento e la registrazione può essere impostata individualmente per ogni utente. Per la differenziazione individuale è possibile selezionare un valore di colore per il campo utente. Per la password deve essere definito se per il login è richiesta una password locale su questa scala, una password di rete o nessuna password.

Il processo di creazione di un utente o di un ruolo può essere semplificato utilizzando la funzione di duplicazione. Quando si duplica un utente o un ruolo, è essenziale assegnare un nome unico alla nuova entità. In pratica, è possibile creare un modello di utente inattivo, da cui trasferire tutte le impostazioni al nuovo utente.

Vedere anche il capitolo: Esempio per creare un utente locale.

3.2 Gestione degli accessi

Il QAPP [Gestione utenti] aggiunge nel menu le impostazioni per la gestione dei ruoli, le regole per il login e il logout e la password locale così come le impostazioni per un server LDAP, se si usano password di rete.

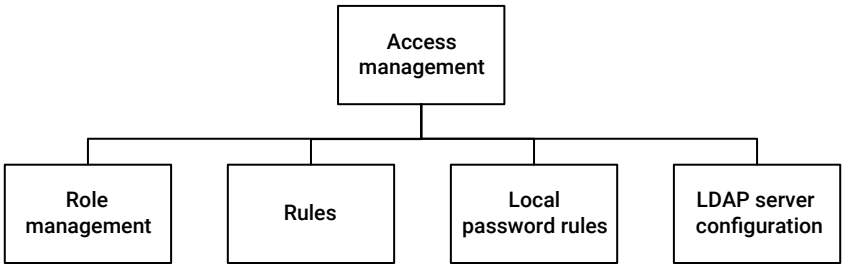

Figura 4: Gestione degli accessi

3.2.1 Gestione dei ruoli

I ruoli appena creati possono essere modificati e cancellati. Ogni ruolo è identificato in modo univoco sul dispositivo tramite un nome di ruolo. Per una descrizione più dettagliata, può essere memorizzata anche una descrizione del ruolo. Ad ogni ruolo sono collegati diversi diritti di ruolo. I ruoli possono essere assegnati a nuovi utenti e compiti creati. Per i ruoli che sono predefiniti ex works, i diritti fissi sono mantenuti e questi ruoli non possono essere cancellati.

Vedere anche il capitolo: Esempio per creare un nuovo ruolo.

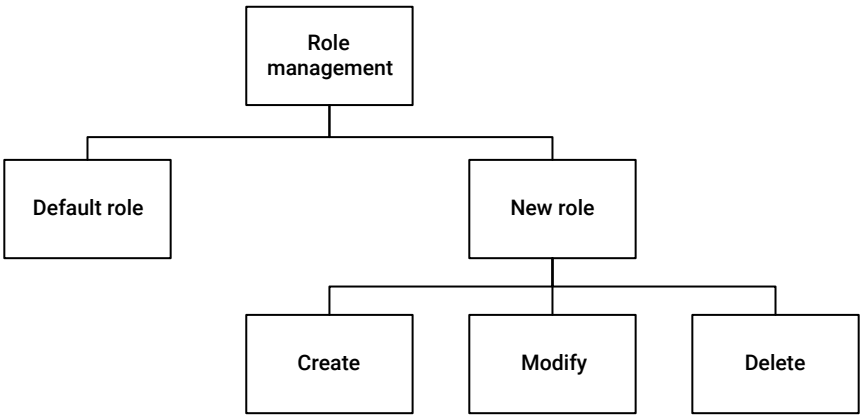

Figura 5: Gestione dei ruoli

3.2.2 Diritti di ruolo

Il dispositivo consente l'accesso individuale alle funzioni del dispositivo mediante l'assegnazione di diritti. I diritti sono descritti in dettaglio di seguito. I diritti possono essere estesi mediante aggiornamenti del firmware.

I ruoli predefiniti Amministratore e Servizio dispongono automaticamente di tutti i diritti disponibili. Nessuno dei due ruoli può essere modificato, quindi l'accesso all'intero sistema è sempre possibile. Se sono necessari diritti limitati, è necessario creare nuovi ruoli.

Nel sistema sono disponibili i seguenti diritti:

- Gestione degli utenti: Accesso alla gestione per creare, modificare o eliminare gli utenti del dispositivo. Richiede anche il diritto di accedere al menu delle impostazioni.
- Gestione attività: Accesso alla gestione per la creazione, la modifica o l'eliminazione delle attività. L'accesso avviene dal menu principale e dal menu delle impostazioni.
- Accesso alle impostazioni del dispositivo: Accesso generale al menu delle impostazioni. Richiesto in parte per accedere alle strutture di menu sottostanti.
- Accesso al Centro QAPP: Accesso al Centro QAPP. Da qui è possibile aggiornare il QAPP Center, visualizzare le descrizioni dei QAPP e concedere le licenze per i QAPP. L'accesso avviene tramite la gestione delle attività.

- Accesso audit trail: Accesso in lettura all'audit trail ed esportazione dei dati. La licenza deve essere concessa dall'estensione corrispondente.
- Accesso all’archivio dati:
- Esecuzione di attività:
- Gestione dei profili di accesso: Accesso ai profili di pesatura e stampa
- Accesso a impostazioni dell’apparecchio:
- Gestione dei ruoli: Accesso alla gestione per la creazione, la modifica o l'eliminazione dei ruoli del dispositivo. Richiede anche il diritto di accedere al menu delle impostazioni.
- Gestione degli accessi: Accesso al menu delle impostazioni "Gestione degli accessi" (prerequisito per la gestione dei ruoli e degli utenti, le impostazioni LDAP e le regole per le password).
- ImpostazioniLDAP/S: Accesso alle impostazioni LDAP o LDAPS, come la configurazione del server, i ruoli e i gruppi assegnati agli utenti e la creazione di nuovi utenti.
- Gestione delle azioni temporizzate: Accesso all'amministrazione per la creazione, la modifica o l'eliminazione di azioni temporizzate, come il backup automatico del dispositivo, l'esportazione dei dati del dispositivo, ecc.
- Accesso alle connessioni: Accesso al menu "Connessioni".
- Reindirizzare trasferimenti file falliti:
- Eliminare i trasferimenti di dati non riusciti: Permette di eliminare i file generati con trasferimenti in sospeso verso connettori diversi.
- Accesso all'aggiornamento del firmware: Consente di aggiornare il firmware sulle bilance non protette.
- Accesso a aggiornamento del firmware:
- Accesso a backup e ripristino:
- Accesso all'esportazione e all'importazione: Accesso alla gestione delle impostazioni del dispositivo per l'esportazione o l'importazione.
- Ripristino delle impostazioni di fabbrica: Consente di ripristinare il dispositivo alle impostazioni di fabbrica.
- Sblocca dispositivo: Consente di sbloccare il dispositivo che è stato bloccato da un altro utente.
- Visualizzazione remota: Mostra la visualizzazione del dispositivo sul sito web del dispositivo
- Visione e controllo da remoto: Controllo dell'accesso al dispositivo sul sito web del dispositivo stesso.
- Gestire gli ordini: Visualizzare ed eliminare gli ordini sul sito web del dispositivo.
- Mostra rapporti di calibrazione: Accesso alla visualizzazione dei rapporti di calibrazione.
- Mostra ultimi rapporti: Accesso alla visualizzazione degli ultimi rapporti sul sito web del dispositivo.
- Accesso alla memoria USB: Consente l'accesso globale in lettura/scrittura alle memorie USB.

3.3 Regole per il login e il logout

Un logout automatico dell'utente loggato può essere impostato dopo un periodo specifico di non utilizzo della bilancia.

Per il login con password, può essere inserito un numero massimo di tentativi falliti. Il comportamento dopo questo numero di tentativi falliti è [nessuna azione], [ritardo di login per il re-login] o [disattivazione dell'account utente] può essere impostato sulla scala.

Un account utente disattivato deve prima essere rilasciato nuovamente da un utente con il diritto di gestione degli utenti.

3.4 Regole locali per le password

Si possono specificare delle regole per la password locale dell'utente su questa bilancia. In questo modo, l'uso necessario di caratteri (lettere maiuscole/minuscole, numeri, caratteri speciali) nella password e la lunghezza minima della password possono essere definiti. Inoltre, il periodo di validità della password così come il riutilizzo della password possono essere configurati.

Vedi anche il capitolo: Esempio per impostare le regole locali per le password.

3.5 Password di rete (via LDAP)

Se la selezione [Password di rete] è impostata nelle impostazioni utente per la password, allora al momento del login con questo utente la bilancia deve essere presente in una rete con server LDAP e l'utente deve essere già configurato nella rete. Quindi, le regole definite nella rete si applicano alla password di rete.

3.5.1 Impostazioni del server LDAP

Il dispositivo supporta il logon degli utenti tramite il "Lightweight Directory Access Protocol" (LDAP). Se il servizio è disponibile nel luogo in cui viene utilizzata la bilancia (ad es. Microsoft Active Directory), gli utenti possono anche accedere alla bilancia con i loro dati utente dopo un'impostazione riuscita.

Le impostazioni per l'LDAP devono essere memorizzate sul dispositivo. I dettagli esatti del server LDAP possono essere ottenuti dal rispettivo dipartimento IT responsabile della rete aziendale.

Le configurazioni LDAP devono essere inserite nella forma di nome distinto (DN), ad esempio "uid=user,ou=People,ou=mycompany,c=en". I caratteri speciali devono essere espressi con una sequenza di escape. Il nome distinto completo di una voce può essere copiato direttamente dallo strumento di gestione LDAP corrispondente su alcuni server LDAP. Questo semplifica la voce.

Spiegazione degli acronimi:

- CN = [Nome comune]
  Il nome con cui l'utente è normalmente conosciuto, ad esempio, Nome.Cognome.
- DN = [Distinguished Name]
  La designazione unica di un utente. Questo è il percorso della directory che porta direttamente all'utente nel server. Il DN contiene il CN nel caso in cui ci siano più utenti con lo stesso nome CN.
- OU = [Unità Organizzativa]
  Una parte del DN, cioè il nome della directory, sotto la quale un utente può essere trovato. OU è usato soprattutto per il nome del dipartimento o la località.
- DC = [componente del dominio]
  La radice dell'albero LDAP, cioè il nome della directory principale. Spesso, questo è il dominio aziendale ([DC=Nome della società, DC=com])
- "UID = [Universal Identifier]
  Non ha alcun significato speciale per LDAP; in alcuni sistemi il nome utente è presente qui, nel qual caso si deve inserire [uid=%u] nel filtro di ricerca."

Nota: la notazione in lettere maiuscole e minuscole della sigla (CN, DN, DC, OU, UID o cn, dn, dc, ou, uid) è irrilevante. Tuttavia, la corretta notazione dei valori che vengono dopo questi è importante.

Il dispositivo supporta alcuni dei parametri regolari per Microsoft Active Directory. Se questo schema di directory è selezionato, alcune configurazioni sono determinate dagli attributi predefiniti. Inoltre, può essere usato per determinare e assegnare ruoli da gruppi LDAP.

I parametri necessari sono divisi in:

- Connessione e tipo di server LDAP
- Dati del gestore per leggere i dati dell'utente (sola lettura)
- Specificazione della posizione dell'utente
- Impostazione predefinita per il login iniziale di un utente

I singoli parametri sono descritti di seguito con il loro significato per la configurazione:

3.5.1.1 Nome del server

Il nome del server specifica il nome host o l'indirizzo IP del server LDAP. Attualmente, la versione corrente supporta il protocollo LDAP con la sua porta 389. LDAPS non è attualmente supportato.

- Sintassi: [protocollo]://[IP o host]:[porta]
- Esempio: ldap://servername.domain.com:389 o ldap://172.16.244.99:389

3.5.1.2 Schema di directory

Lo schema della directory definisce come le voci sono utilizzate in Active Directory (AD). I parametri cambiano a seconda del provider AD. Il dispositivo fornisce un connettore predefinito integrato per i server di directory Microsoft LDAP. Tutti gli altri provider devono essere adattati tramite una configurazione generica.

- Microsoft Active Directory
  La configurazione usa il parametro sAMAccountName per identificare il nome utente. Con questa configurazione, i dati dell'utente vengono aggiornati ogni volta che l'utente accede (cioè la prima volta e quelle successive) in base ai dati dell'utente in LDAP. Questo include nome utente, nome visualizzato, ruolo assegnato, se applicabile. Tuttavia, per l'assegnazione dei ruoli, vale solo quanto segue:
  - Solo i gruppi diretti (cioè nessun gruppo annidato) sono sincronizzati da LDAP.
  - Solo i ruoli che sono già configurati e presenti sul dispositivo sono assegnati. Cioè ogni ruolo ha bisogno di una connessione a un gruppo in LDAP.
- Generico
  Nella configurazione generica, i parametri per il login devono essere memorizzati esplicitamente. A tal fine, deve essere noto sotto quale parametro il nome del login è memorizzato in LDAP. Questo dipende dalla configurazione LDAP esistente. Se i parametri per il nome di visualizzazione sono anche memorizzati, il nome di visualizzazione dell'utente è anche aggiornato quando si effettua il login. Con lo schema generico non è possibile ottenere l'assegnazione del ruolo da un gruppo del LDAP.

3.5.1.3 Manager DN (Distinguished name)

La designazione unica, il percorso della directory dell'account utente [Manager] sul server LDAP. Questo utente deve avere un permesso di lettura nel server LDAP, per poter cercare altri utenti. Questo è per lo più un utente virtuale, la cui password non viene cambiata costantemente. In caso di una richiesta di accesso (login), il [Manager] cerca l'utente che vuole accedere al server LDAP. Per i manager con [Nome.Cognome].

- Esempio: DN=Cognome /, Nome, OU=Risorse, OU=Utente, OU=GO-Goettingen, OU=Regione Europa, DC=Nome azienda, DC=com

3.5.1.4 Password del gestore

La password dell'account utente [Manager], per poter accedere al server per la richiesta di ricerca.

3.5.1.5 Utente OU

Il luogo, la directory sul server LDAP, a partire dalla quale l'utente deve essere cercato. Non usare qui la directory principale, perché altrimenti la ricerca di un utente può durare molto a lungo nelle grandi aziende e può quindi causare timeout.

- Esempio: OU=GO-Goettingen, OU=Regione-Europa, DC=Nome della società, DC=com

3.5.1.6 Assegnazione del ruolo

L'assegnazione dinamica dei ruoli è possibile solo se è selezionato lo schema Microsoft Active Directory. Questa funzione abilita l'opzione di assegnazione dei ruoli. La descrizione di come configurare le assegnazioni può essere trovata qui.

- GruppoLDAP: cerca tra le appartenenze LDAP dell'utente una delle mappature di ruolo di gruppo configurate. Se viene trovata una mappatura, all'utente viene dato quel ruolo per la sessione.
- Utente locale: Assegna all'utente il ruolo che è già memorizzato per l'utente sul dispositivo.

3.5.1.7 Filtro di ricerca (solo generico)

Il filtro specifica quale parametro LDAP dovrebbe essere usato come nome di login. Questo è spesso 'sAMAccountName' per una Microsoft Active Directory. Altri servizi di directory usano 'uId'. A seconda del servizio o delle specifiche aziendali, il parametro può essere diverso. Fondamentalmente, tutto ciò che è memorizzato in LDAP ed è adatto come identificatore è possibile come nome di login, ad esempio e-mail, ecc.

Il filtro deve essere inserito nella forma: <property>=%u. %u è sostituito dal nome di login del dispositivo.

- Esempio: sAMAccountName=%u
  Attenzione: Fate sempre attenzione alle lettere maiuscole/minuscole quando usate il filtro.

3.5.1.8 Attributo LDAP per il nome visualizzato

L'attributo display name designa il nome dell'attributo nel tuo sistema LDAP sotto il quale il display name è memorizzato. Questa opzione è modificabile solo per la configurazione generica. In caso di configurazione Microsoft Active Directory viene utilizzato l'attributo 'displayName'.

3.5.1.9 Crea automaticamente l'utente

Quando è impostato su [Off], l'utente deve già esistere sulla bilancia con lo stesso nome della rete, per poter accedere alla rete. Durante il login, nella selezione vengono visualizzati solo gli utenti presenti sulla bilancia.

Se la selezione è impostata su [On] per questo punto e l'utente non è ancora disponibile sulla bilancia, allora durante il login è possibile inserire il nome utente come salvato nella rete. Dopo un login riuscito alla rete, questo utente viene creato automaticamente nella bilancia con i valori specificati per la lingua e il ruolo.

3.5.1.10 Ruolo predefinito

Il ruolo da utilizzare per gli utenti creati automaticamente è impostato con questa impostazione predefinita.

3.5.1.11 Lingua predefinita

La lingua può essere impostata come predefinita per questo punto nel caso in cui la creazione automatica di utenti sulla bilancia sia abilitata.

3.5.1.12 Registrazione dettagliata

Poiché ogni infrastruttura IT è diversa, il dispositivo offre la possibilità di registrare più dettagliatamente i singoli passi durante la connessione LDAP. Tuttavia, questa funzione dovrebbe essere attivata solo per scopi di controllo e test, in modo che i dati da LDAP non vengano registrati involontariamente. Selezionare [Sì] per attivare la registrazione. Le password non vengono emesse. Seguire le istruzioni del servizio per visualizzare i log.

3.5.2 Assegnazione di ruoli tramite LDAP

Sulla base di un'assegnazione degli utenti a diversi gruppi LDAP, un'assegnazione di ruoli può essere fatta sul dispositivo. A tal fine, i nomi del gruppo così come l'assegnazione del rispettivo gruppo devono essere definiti sul dispositivo. Questa funzione è attualmente disponibile solo per lo schema Microsoft Active Directory.

L'ordine dei gruppi determina l'ordine di ricerca. Il primo nome di gruppo corrispondente, che è memorizzato come attributo 'MemberOf' nel rispettivo utente, viene trovato, il ruolo impostato viene assegnato ad ogni logon. L'ordine può essere cambiato usando le frecce su e giù accanto ad ogni voce di assegnazione del gruppo.

Per assegnare automaticamente i ruoli all'utente, fate come segue:

1. Assicurati che gli utenti desiderati siano già stati assegnati ai gruppi corrispondenti nel tuo LDAP. Quando un utente si collega, la bilancia controlla se solo il nome del gruppo (Common Name) è collegato all'utente. Il percorso completo del gruppo non viene valutato.
2. Nel menu delle impostazioni LDAP, imposta lo schema della directory su "Microsoft Active Directory" e l'assegnazione dei ruoli su "Gruppo LDAP". Questo abiliterà l'opzione di assegnazione dei ruoli nella barra del menu in alto. Aprire il menu.
3. Il + crea un nuovo incarico. Inserisci per il nome del gruppo la stessa denominazione che si trova nell'LDAP. Fate attenzione alle maiuscole e alle minuscole.
   Il ruolo può essere selezionato da un elenco a discesa. Contiene tutti i ruoli che sono disponibili nel sistema. Conferma la selezione con il pulsante conferma. Ripeti questo passo fino a quando tutti i ruoli desiderati sono collegati a un gruppo.
4. Quando tutte le voci sono state create, impostate finalmente la priorità. Se un utente è incluso in più di un gruppo, la priorità determina quale ruolo deve essere usato preferibilmente. I gruppi vengono cercati dall'alto verso il basso. Puoi spostare la priorità con i tasti freccia. I gruppi errati possono essere rimossi con il simbolo di cancellazione.

4 Esempi di applicazioni

Gli esempi di applicazione si riferiscono alla versione MCA dal pacchetto 09-03-04.01.xx in poi, insieme alle opzioni di impostazione e alle funzionalità che contiene. I diritti utente corrispondenti sono necessari per impostare l'estensione QAPP, gli utenti, i ruoli, i diritti e le regole.

L'estensione QAPP [Gestione utenti] deve essere attivata per tutti gli esempi di applicazione, tranne il primo.

4.1 Esempio di modifica delle impostazioni dell'utente

In questo esempio, l'utente Amministratore dovrebbe avere un colore specifico nel campo utente e il login dovrebbe essere fatto con una password locale.

4.1.1 Impostazione

1. Modifica le impostazioni dell'utente specificato, ad esempio, [Administrator].
   a. EXAMPLE_CHANGE_USER_SET_CONF_STEP_1_A
   b. EXAMPLE_CHANGE_USER_SET_CONF_STEP_1_B
   c. EXAMPLE_CHANGE_USER_SET_CONF_STEP_1_C
   d. EXAMPLE_CHANGE_USER_SET_CONF_STEP_1_D
   e. EXAMPLE_CHANGE_USER_SET_CONF_STEP_1_E
   f. EXAMPLE_CHANGE_USER_SET_CONF_STEP_1_F
   g. EXAMPLE_CHANGE_USER_SET_CONF_STEP_1_G
2. Con la selezione [Administrator] e il pulsante [User login], il sistema chiede ora di inserire una password per il login.
   a. EXAMPLE_CHANGE_USER_SET_CONF_STEP_2_A
   b. EXAMPLE_CHANGE_USER_SET_CONF_STEP_2_B

Nota: Tieni al sicuro la tua password di amministratore; se persa, può essere cancellata solo attraverso il Servizio Sartorius.

4.1.2 Applicazione

Per accedere alla bilancia, ad esempio, dopo l'accensione o dopo un cambio di utente tramite logout, dovete inserire la vostra password come utente [Administrator].

4.1.3 Risoluzione dei problemi

Password:

1. La password deve essere composta da almeno un carattere.
2. Durante l'inserimento, fate attenzione alle lettere maiuscole e minuscole.

4.2 Esempio di creazione di un utente locale

Questo esempio descrive la configurazione e l'applicazione di un utente locale insieme ai ruoli disponibili. L'utente dovrebbe avere una password locale.

4.2.1 Impostazione

Fasi di configurazione:

1. Attivare l'estensione QAPP [Gestione utenti], se non ancora fatto.
   a. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_1_A
   b. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_1_B
   c. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_1_C
   d. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_1_D
2. Configura un utente locale, per esempio, [Il mio utente locale].
   a. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_2_A
   b. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_2_B
   c. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_2_C
   d. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_2_D
   e. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_2_E
   f. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_2_F
   g. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_2_G
   h. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_2_H
   i. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_2_I
   j. EXAMPLE_CREATE_LOCAL_USER_CONF_STEP_2_J

4.2.2 Applicazione

Dopo aver selezionato il nuovo utente, ad esempio, [My local user], e il pulsante [User login], l'inserimento di una password è richiesto ogni volta che questo utente accede.

Passi dell'utente:

1. Se non è stata assegnata alcuna password durante la creazione dell'utente, il primo inserimento della password viene fatto ora.
   a. EXAMPLE_CREATE_LOCAL_USER_APPL_STEP_1_A
   b. EXAMPLE_CREATE_LOCAL_USER_APPL_STEP_1_B

Nota: tieni la tua password al sicuro; se la perdi, deve essere cancellata dall'utente [Administrator].

4.2.3 Risoluzione dei problemi

Password:

1. La password deve essere composta da almeno un carattere.

2. Durante l'inserimento, fate attenzione alle lettere maiuscole e minuscole.

4.3 Esempio di creazione di un nuovo ruolo

In questo esempio, un nuovo ruolo deve essere creato con il diritto di gestione dei compiti e l'accesso al menu Setup.

4.3.1 Impostazione

Fasi di configurazione:

1. Attivare l'estensione QAPP [Gestione utenti], se non ancora fatto.
   a. EXAMPLE_CREATE_NEW_ROLE_CONF_STEP_1_A
   b. EXAMPLE_CREATE_NEW_ROLE_CONF_STEP_1_B
   c. EXAMPLE_CREATE_NEW_ROLE_CONF_STEP_1_C
   d. EXAMPLE_CREATE_NEW_ROLE_CONF_STEP_1_D

2. Configura un nuovo ruolo, ad esempio, [Il mio ruolo attività e menu].
   a. EXAMPLE_CREATE_NEW_ROLE_CONF_STEP_2_A
   b. EXAMPLE_CREATE_NEW_ROLE_CONF_STEP_2_B
   c. EXAMPLE_CREATE_NEW_ROLE_CONF_STEP_2_C
   d. EXAMPLE_CREATE_NEW_ROLE_CONF_STEP_2_D
   e. EXAMPLE_CREATE_NEW_ROLE_CONF_STEP_2_E
   f. EXAMPLE_CREATE_NEW_ROLE_CONF_STEP_2_F
   g. EXAMPLE_CREATE_NEW_ROLE_CONF_STEP_2_G

3. Ora puoi assegnare questo ruolo a un utente tramite la gestione degli utenti.

4.4 Esempio per l'impostazione di regole di password locali

Questo esempio descrive la modifica delle regole per le password locali in modo che la regola si applichi a tutti gli utenti e alle loro password che devono avere una lunghezza di almeno 8 caratteri e devono contenere lettere maiuscole/piccole e numeri.

4.4.1 Impostazione

Fasi di configurazione:

1. Attivare l'estensione QAPP [Gestione utenti], se non ancora fatto.
   a. EXAMPLE_SET_LOCAL_PASSW_RULES_CONF_STEP_1_A
   b. EXAMPLE_SET_LOCAL_PASSW_RULES_CONF_STEP_1_B
   c. EXAMPLE_SET_LOCAL_PASSW_RULES_CONF_STEP_1_C
   d. EXAMPLE_SET_LOCAL_PASSW_RULES_CONF_STEP_1_D

2. Configurare le regole della password secondo i requisiti desiderati.
   a. EXAMPLE_SET_LOCAL_PASSW_RULES_CONF_STEP_2_A
   b. EXAMPLE_SET_LOCAL_PASSW_RULES_CONF_STEP_2_B
   c. EXAMPLE_SET_LOCAL_PASSW_RULES_CONF_STEP_2_C
   d. EXAMPLE_SET_LOCAL_PASSW_RULES_CONF_STEP_2_D
   e. EXAMPLE_SET_LOCAL_PASSW_RULES_CONF_STEP_2_E
   f. EXAMPLE_SET_LOCAL_PASSW_RULES_CONF_STEP_2_F
   g. EXAMPLE_SET_LOCAL_PASSW_RULES_CONF_STEP_2_G

4.4.2 Applicazione

Per accedere alla bilancia, ad esempio, dopo l'accensione o dopo un cambio di utente attraverso il logout, dovete ora, come utente, soddisfare le regole di password impostate con una password locale.

Passi dell'utente:

1. Dopo aver selezionato un utente, ad esempio, [Il mio utente locale] e il pulsante [Login utente], è possibile che venga visualizzato il messaggio che le regole della password non sono soddisfatte per la tua password.
   a. EXAMPLE_SET_LOCAL_PASSW_RULES_APPL_STEP_1_A
   b. EXAMPLE_SET_LOCAL_PASSW_RULES_APPL_STEP_1_B

Nota: tieni la tua password al sicuro; se la perdi, deve essere cancellata dall'utente amministratore.

4.4.3 Risoluzione dei problemi

Password:

1. La password deve essere composta da lettere maiuscole/minuscole e numeri.
2. La password deve avere una lunghezza di almeno 8 caratteri.
3. Durante l'inserimento, fate attenzione alle lettere maiuscole e minuscole.

4.5 Esempio di creazione di un utente di rete

In questo esempio, un nuovo utente deve essere creato, i cui dati di login, nome utente e password, sono recuperati da un server LDAP nella rete. All'utente viene dato un ruolo disponibile nel bilancio.

4.5.1 Impostazione

Fasi di configurazione:

1. I seguenti elementi sono il prerequisito per la configurazione di un utente di rete.
   a. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_1_A
   b. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_1_B
   c. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_1_C
   d. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_1_D
2. Configura un utente di rete, per esempio, [Il mio utente di rete].
   a. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_2_A
   b. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_2_B
   c. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_2_C
   d. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_2_D
   e. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_2_E
   f. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_2_F
   g. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_2_G
   h. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_2_H
   i. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_2_I
   j. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_2_J
   k. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_2_K
   l. EXAMPLE_CREATE_NETWORK_USER_CONF_STEP_2_L

4.5.2 Applicazione

Passi dell'utente:

1. I seguenti elementi sono il prerequisito per il login di un utente di rete, ad esempio, [Nome.Cognome]:
   a. EXAMPLE_CREATE_NETWORK_USER_APPL_STEP_1_A
   b. EXAMPLE_CREATE_NETWORK_USER_APPL_STEP_1_B
   c. EXAMPLE_CREATE_NETWORK_USER_APPL_STEP_1_C
   d. EXAMPLE_CREATE_NETWORK_USER_APPL_STEP_1_D
2. Dopo la selezione di questo utente di rete, ad esempio, [Nome.Cognome], e il pulsante [Login utente], il login è ora fatto con la password memorizzata nella rete.
3. Inserire la password di rete. Dopo un login di successo alla rete, questo utente viene attivato con le sue impostazioni e diritti, come configurato nel bilancio.

4.5.3 Risoluzione dei problemi

Nessuna connessione al server LDAP:

1. Controllare la connessione della bilancia alla rete.
   Controllare se un indirizzo IP della bilancia viene visualizzato in [Status center].
2. Controlla se puoi accedere al tuo PC con lo stesso nome utente e password.
   Fai controllare al tuo amministratore le impostazioni del server LDAP sulla bilancia.

Password:

1. Inserisci la tua password di rete nella forma corretta.
   Fate attenzione alle lettere maiuscole e minuscole.

4.6 Esempio di creazione automatica di un utente di rete

Questo esempio descrive la creazione automatica di un utente nella bilancia, il cui login viene fatto tramite la bilancia con nome utente e password su un server LDAP nella rete. Nella bilancia, l'utente ottiene la lingua e il ruolo predefiniti.

4.6.1 Impostazione

Fasi di configurazione:

1. I seguenti elementi sono il prerequisito per la configurazione automatica di un utente di rete nella bilancia.
   a. EXAMPLE_AUTOM_CREATE_NETWORK_USER_CONF_STEP_1_A
   b. EXAMPLE_AUTOM_CREATE_NETWORK_USER_CONF_STEP_1_B
   c. EXAMPLE_AUTOM_CREATE_NETWORK_USER_CONF_STEP_1_C
   d. EXAMPLE_AUTOM_CREATE_NETWORK_USER_CONF_STEP_1_D
2. Nel display di login, attiva il campo con l'ultimo nome utente utilizzato.
   Viene visualizzato l'elenco degli utenti creati nel saldo.
3. Per creare automaticamente un nuovo utente di rete, premere il pulsante [+] e confermare il messaggio inviato con [Continua].
4. Inserisci il nome utente come configurato nella rete.
5. In seguito, inserite la password come memorizzata nella rete.
6. Dopo un login di successo alla rete, questo utente viene creato automaticamente nella bilancia, con il nome utente inserito e la lingua predefinita così come il ruolo predefinito.
7. L'utente appena creato viene visualizzato nella lista degli utenti disponibili nella bilancia e puoi ora selezionarlo.

4.6.2 Applicazione

Passi dell'utente:

1. I seguenti elementi sono il prerequisito per il login di un utente di rete, ad esempio [Nome.Cognome].
   a. EXAMPLE_AUTOM_CREATE_NETWORK_USER_APPL_STEP_1_A
   b. EXAMPLE_AUTOM_CREATE_NETWORK_USER_APPL_STEP_1_B
   c. EXAMPLE_AUTOM_CREATE_NETWORK_USER_APPL_STEP_1_C
   d. EXAMPLE_AUTOM_CREATE_NETWORK_USER_APPL_STEP_1_D
2. Dopo la selezione di questo utente di rete, ad esempio, [Nome.Cognome], e il pulsante [Login utente], il login è ora fatto con la password memorizzata nella rete
3. Inserire la password di rete. Dopo un login di successo alla rete, questo utente viene attivato con le sue impostazioni e diritti, come configurato nel bilancio.

4.6.3 Risoluzione dei problemi

Nessuna connessione al server LDAP:

1. Controllare la connessione della bilancia alla rete.
   Controllare se un indirizzo IP della bilancia viene visualizzato in [Status center].
2. Controlla se puoi accedere al tuo PC con lo stesso nome utente e password.
   Fai controllare al tuo amministratore le impostazioni del server LDAP sulla bilancia.

Password:

1. Inserisci la tua password di rete nella forma corretta.
   Fate attenzione alle lettere maiuscole e minuscole.

5. Abbreviazioni

CN	Common Name	Il nome con cui l'utente è normalmente conosciuto nella rete.
DC	Domain Component	Componenti del dominio, la radice del direttore LDAP, per lo più il dominio aziendale.
DN	Distinguished Name	Un nome di oggetto unico nelle directory LDAP, qui l'identificatore unico di un utente.
OU	Organisational Unit	Unità organizzativa, nome della cartella, sotto la quale l'utente può essere trovato, per esempio, il dipartimento.
UID	Universal Identifier	Identificatore universale, nessun significato speciale.
FDA	Food and Drug Administration	Food and Drug Administration degli Stati Uniti.
LDAP	Lightweight Directory Access Protocol	Protocollo di rete per l'interrogazione e la modifica delle informazioni dei servizi di directory distribuiti, basato sul protocollo TCP/IP.
LDAPS	LDAP over SSL/TLS	Protocollo di rete LDAP con crittografia.
SSL	Secure Sockets Layer	Protocollo ibrido di crittografia per il trasferimento sicuro dei dati in Internet.
TLS	Transport Layer Security	Successore di SSL
21 CFR Part 11		La parte 11 del titolo 21 del regolamento della FDA regola, tra l'altro, le registrazioni e le firme elettroniche.