How to Configure

Strong Passwords

VC-MDx Recorder

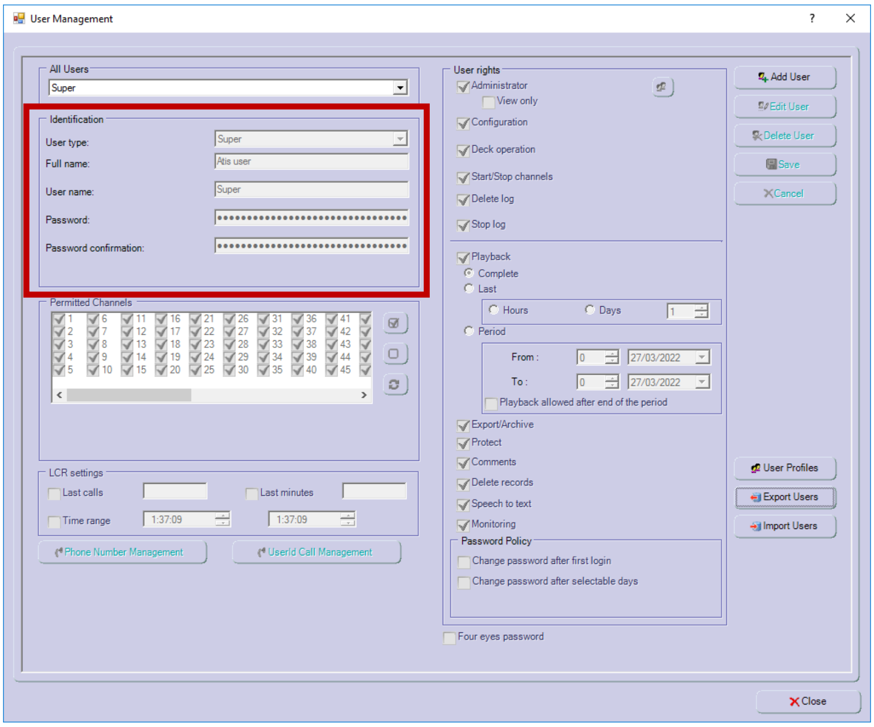
Date: **23.08.2022**

VC-MDx Password Configuration

This description refers to the document ***"Leaflet_MDX_Password_Management_ENG.pdf"***

1. Unique usernames with user identification

⇒ Open Settings/ User Management



User Management

All Users: Super

Identification
User type: Super
Full name: Atis user
User name: Super
Password: ••••••••••••••••••••••••••••••••
Password confirmation: ••••••••••••••••••••••••••••••••

Permitted Channels
☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15 ☑ 16 ☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21 ☑ 22 ☑ 23 ☑ 24 ☑ 25 ☑ 26 ☑ 27 ☑ 28 ☑ 29 ☑ 30 ☑ 31 ☑ 32 ☑ 33 ☑ 34 ☑ 35 ☑ 36 ☑ 37 ☑ 38 ☑ 39 ☑ 40 ☑ 41 ☑ 42 ☑ 43 ☑ 44 ☑ 45

LCR settings
□ Last calls □ Last minutes
□ Time range 1:37:09 1:37:09

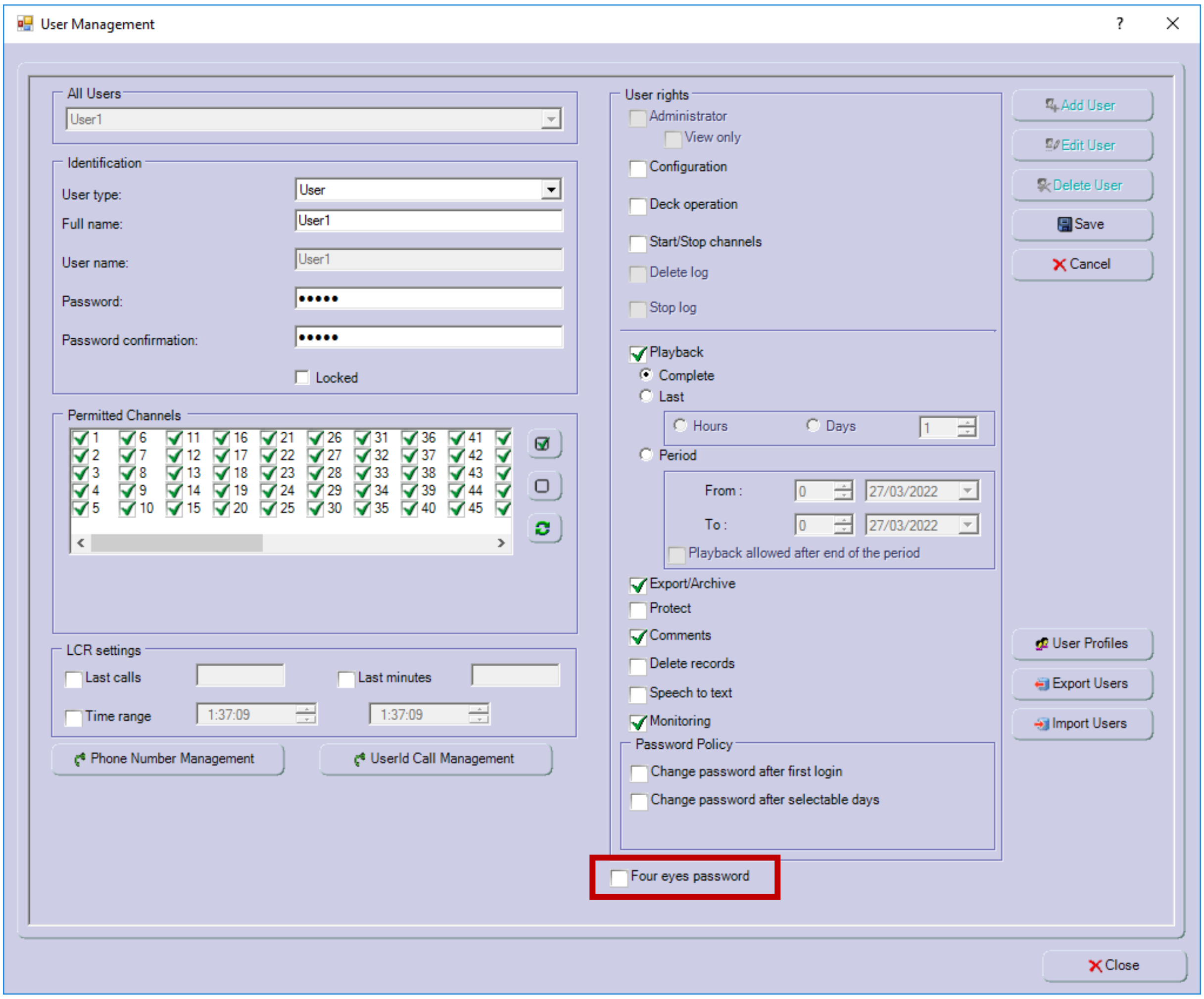
User rights
☑ Administrator
□ View only
☑ Configuration
☑ Deck operation
☑ Start/Stop channels
☑ Delete log
☑ Stop log
☑ Playback
● Complete
○ Last
○ Hours ○ Days 1
○ Period
From : 0 27/03/2022
To : 0 27/03/2022
□ Playback allowed after end of the period
☑ Export/Archive
☑ Protect
☑ Comments
☑ Delete records
☑ Speech to text
☑ Monitoring

Password Policy
□ Change password after first login
□ Change password after selectable days

□ Four eyes password

2. Setting 4 eyes password principle. Two users must enter separate passwords in order to release the user account

⇒ Open Settings/ User Management



All Users: User1

User type: User
Full name: User1
User name: User1
Password: •••••
Password confirmation: •••••
□ Locked

☑ 1 ☑ 6 ☑ 11 ☑ 16 ☑ 21 ☑ 26 ☑ 31 ☑ 36 ☑ 41 ☑
☑ 2 ☑ 7 ☑ 12 ☑ 17 ☑ 22 ☑ 27 ☑ 32 ☑ 37 ☑ 42 ☑
☑ 3 ☑ 8 ☑ 13 ☑ 18 ☑ 23 ☑ 28 ☑ 33 ☑ 38 ☑ 43 ☑
☑ 4 ☑ 9 ☑ 14 ☑ 19 ☑ 24 ☑ 29 ☑ 34 ☑ 39 ☑ 44 ☑
☑ 5 ☑ 10 ☑ 15 ☑ 20 ☑ 25 ☑ 30 ☑ 35 ☑ 40 ☑ 45 ☑

□ Last calls □ Last minutes
□ Time range 1:37:09 1:37:09

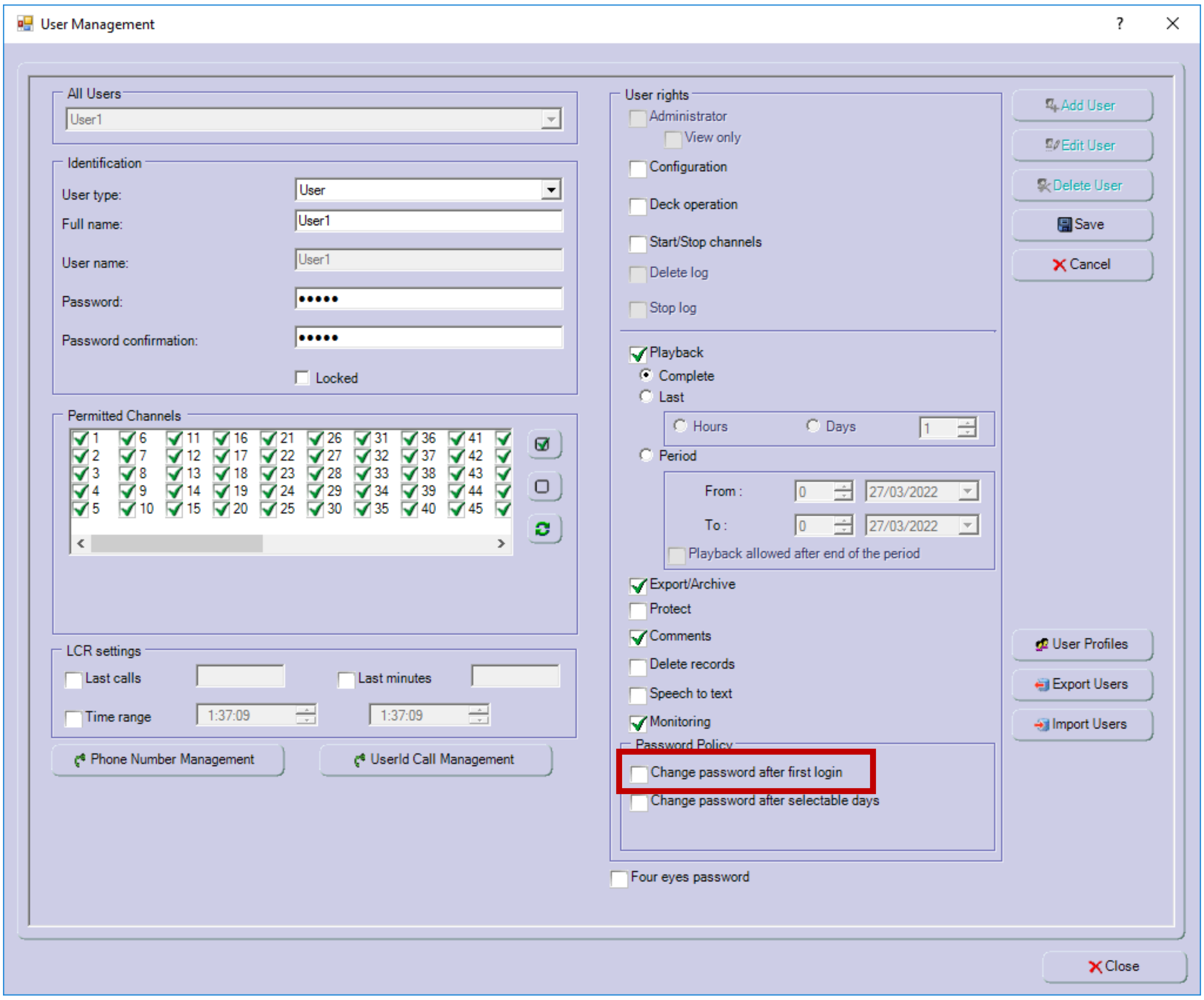
□ Administrator
□ View only
□ Configuration
□ Deck operation
□ Start/Stop channels
□ Delete log
□ Stop log
☑ Playback
● Complete
○ Last
○ Hours ○ Days 1
○ Period
From : 0 27/03/2022
To : 0 27/03/2022
□ Playback allowed after end of the period
☑ Export/Archive
□ Protect
☑ Comments
□ Delete records
□ Speech to text
☑ Monitoring

□ Change password after first login
□ Change password after selectable days

□ Four eyes password

3. Standard passwords (default settings) must be changed

⇒ Open Settings/ User Management



User Management

All Users: User1

Identification
User type: User
Full name: User1
User name: User1
Password: •••••
Password confirmation: •••••
□ Locked

Permitted Channels: ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15 ☑ 16 ☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21 ☑ 22 ☑ 23 ☑ 24 ☑ 25 ☑ 26 ☑ 27 ☑ 28 ☑ 29 ☑ 30 ☑ 31 ☑ 32 ☑ 33 ☑ 34 ☑ 35 ☑ 36 ☑ 37 ☑ 38 ☑ 39 ☑ 40 ☑ 41 ☑ 42 ☑ 43 ☑ 44 ☑ 45

LCR settings
□ Last calls
□ Last minutes
□ Time range 1:37:09 1:37:09

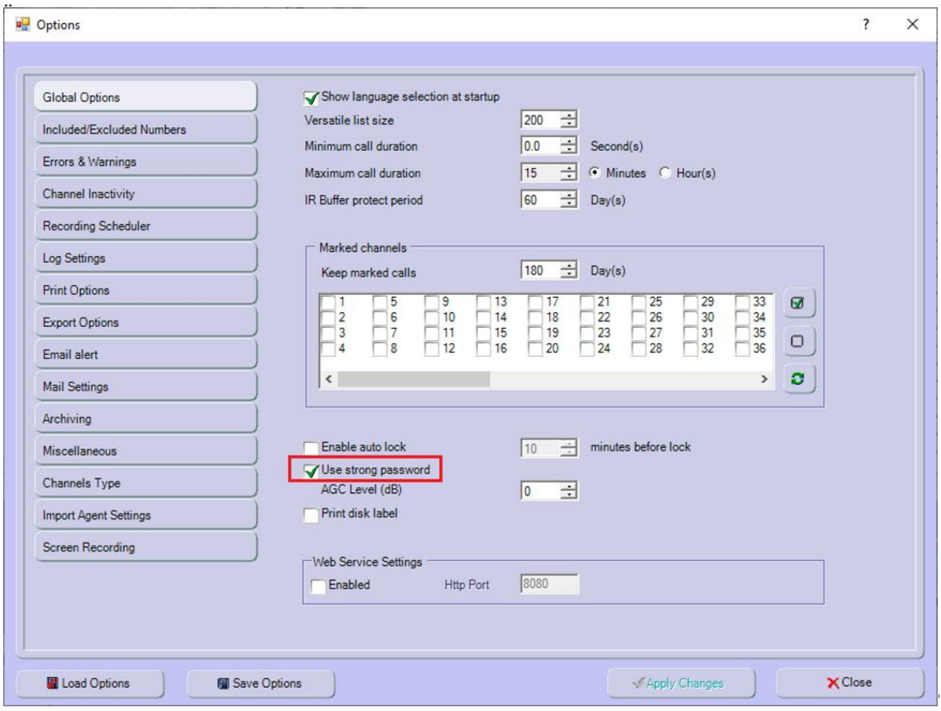
User rights
□ Administrator
□ View only
□ Configuration
□ Deck operation
□ Start/Stop channels
□ Delete log
□ Stop log
☑ Playback
● Complete
○ Last
○ Hours ○ Days 1
○ Period
From : 0 27/03/2022
To : 0 27/03/2022
□ Playback allowed after end of the period
☑ Export/Archive
□ Protect
☑ Comments
□ Delete records
□ Speech to text
☑ Monitoring

Password Policy
□ Change password after first login
□ Change password after selectable days

□ Four eyes password

4. Use of at least 8 characters with a combination of characters, special characters and numbers

⇒ Open Options/ Select Global Options



☑ Show language selection at startup

Versatile list size 200

Minimum call duration 0.0 Second(s)

Maximum call duration 15 ● Minutes ○ Hour(s)

IR Buffer protect period 60 Day(s)

Marked channels

Keep marked calls 180 Day(s)

□ Enable auto lock 10 minutes before lock

☑ Use strong password

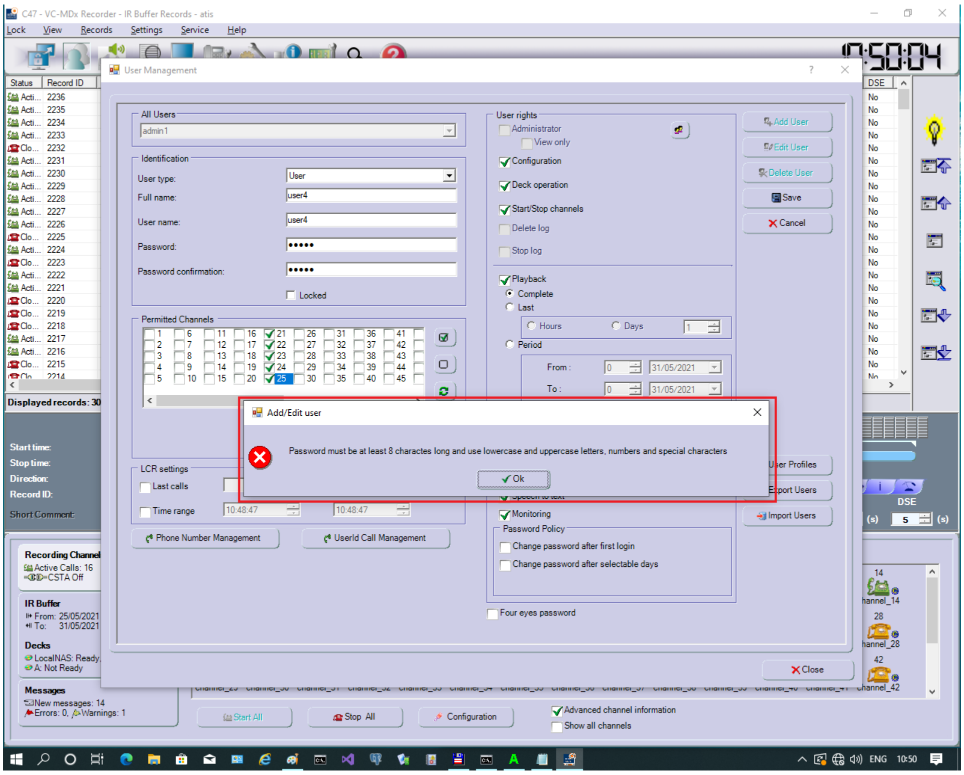
AGC Level (dB) 0

□ Print disk label

Web Service Settings

□ Enabled Http Port 8080

In case of “Use strong password” is checked and a password is set, which does not correspond to the strong password criteria, a warning message will be displayed :



Add/Edit user

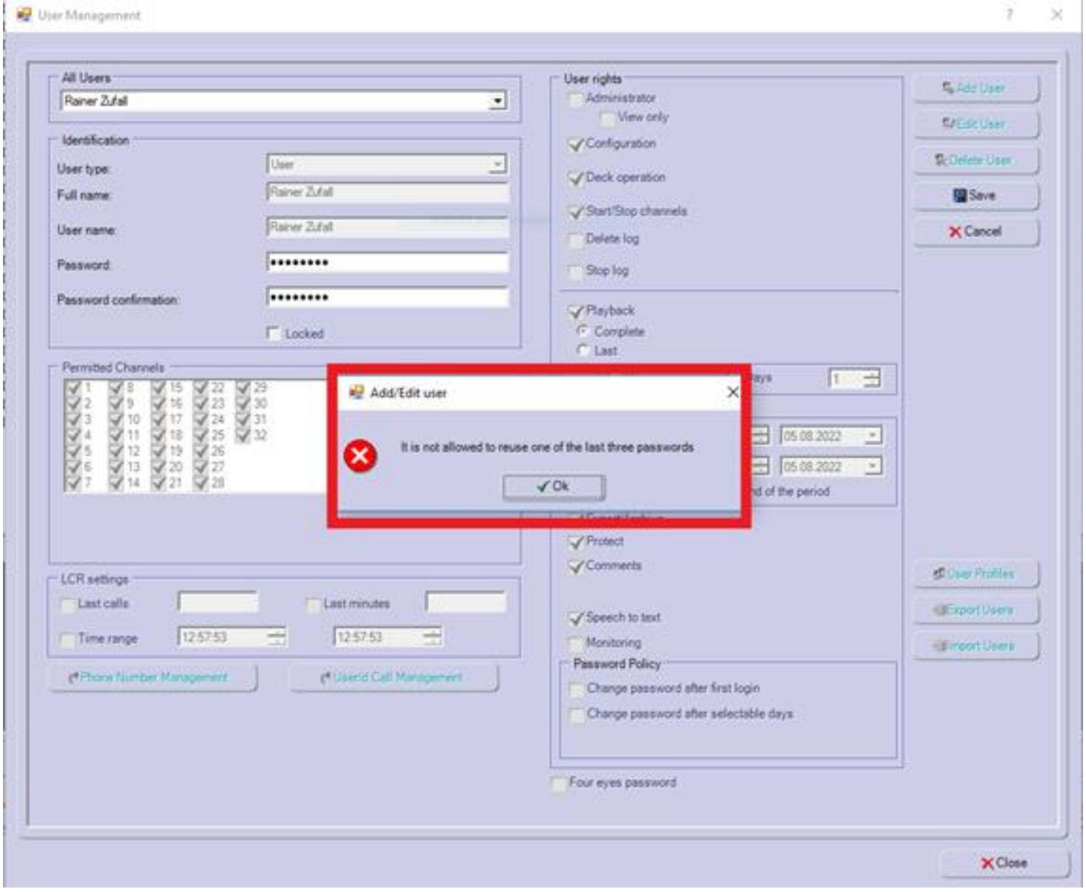
Password must be at least 8 charactes long and use lowercase and uppercase letters, numbers and special characters

✓ Ok

5. No reuse of passwords, at least for 3 previously used passwords

⇒ Open Settings/ User Management

It is impossible to reuse one of the 3 lats used passwords. If the Administrator intends to reuse one of the 3 last used passwords, the below message will appear:



User Management

All Users: Rainer Zufall

Identification
User type: User
Full name: Rainer Zufall
User name: Rainer Zufall
Password: •••••••••
Password confirmation: •••••••••
□ Locked

Permitted Channels: ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15 ☑ 16 ☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21 ☑ 22 ☑ 23 ☑ 24 ☑ 25 ☑ 26 ☑ 27 ☑ 28 ☑ 29 ☑ 30 ☑ 31 ☑ 32

LCR settings
□ Last calls □ Last minutes
□ Time range 12:57:53 12:57:53

User rights
□ Administrator
□ View only
☑ Configuration
☑ Deck operation
☑ Start/Stop channels
□ Delete log
□ Stop log
☑ Playback
● Complete
○ Last
05.08.2022
05.08.2022
☑ Protect
☑ Comments
☑ Speech to text
□ Monitoring

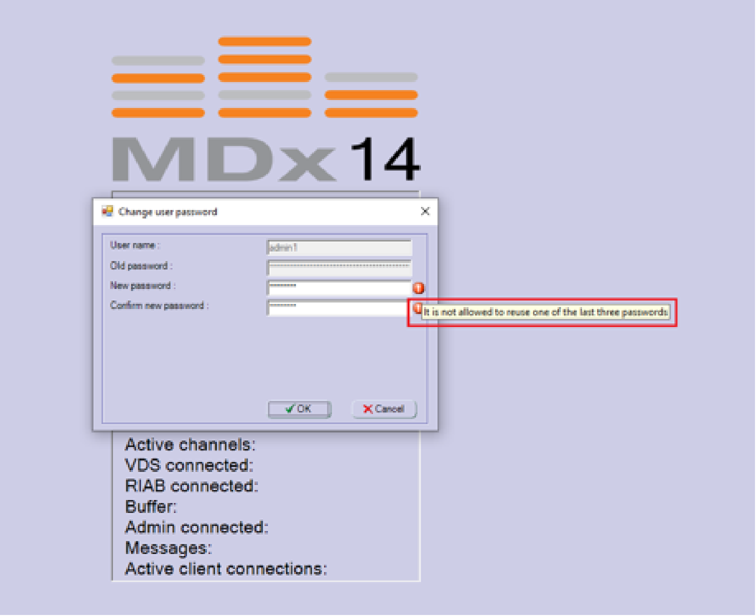
Password Policy
□ Change password after first login
□ Change password after selectable days

□ Four eyes password

Add/Edit user

It is not allowed to reuse one of the last three passwords

Or if an user tries to change his password



Change user password

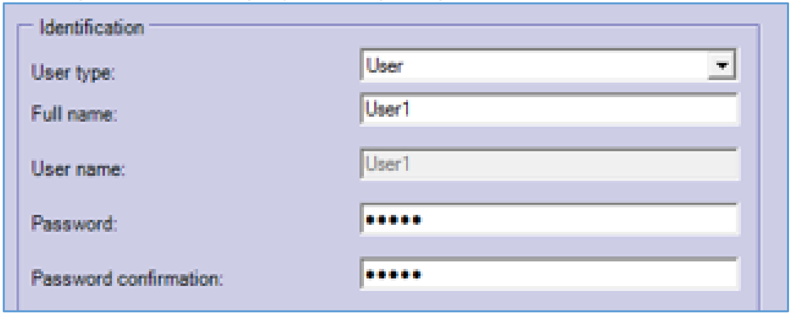
User name : admin1
Old password :
New password : ********
Confirm new password : ********

It is not allowed to reuse one of the last three passwords

Active channels:
VDS connected:
RIAB connected:
Buffer:
Admin connected:
Messages:
Active client connections:

6. No ability to view or print passwords

It is impossible to display nor to print passwords



Identification

User type: User

Full name: User1

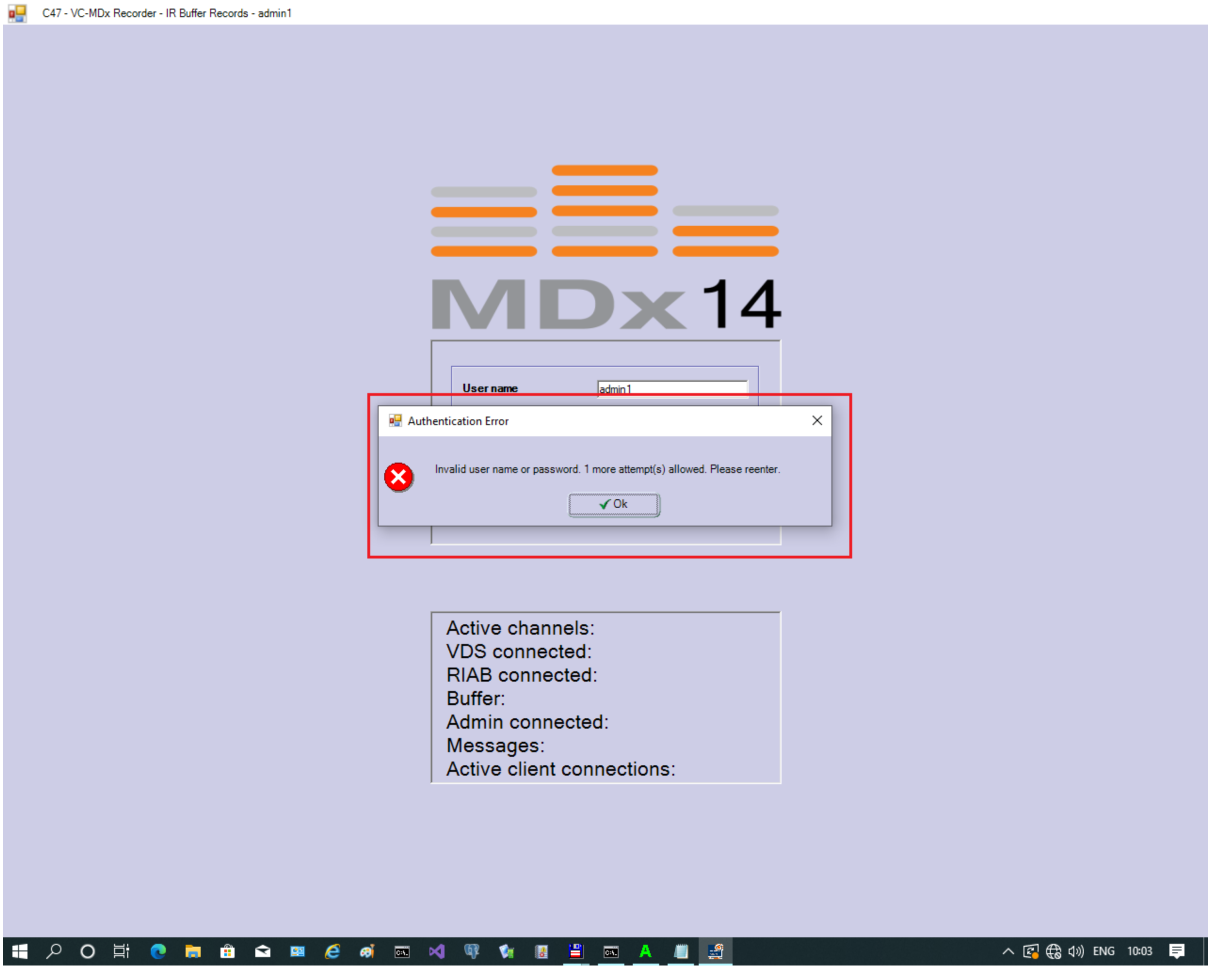
User name: User1

Password: •••••

Password confirmation: •••••

7. Account locked after incorrect password entry after a preset number of incorrect attempts

After a predefined number of failed login attempts (3 for User type, 2 for Administrator type, none for Super user type), the following message is displayed



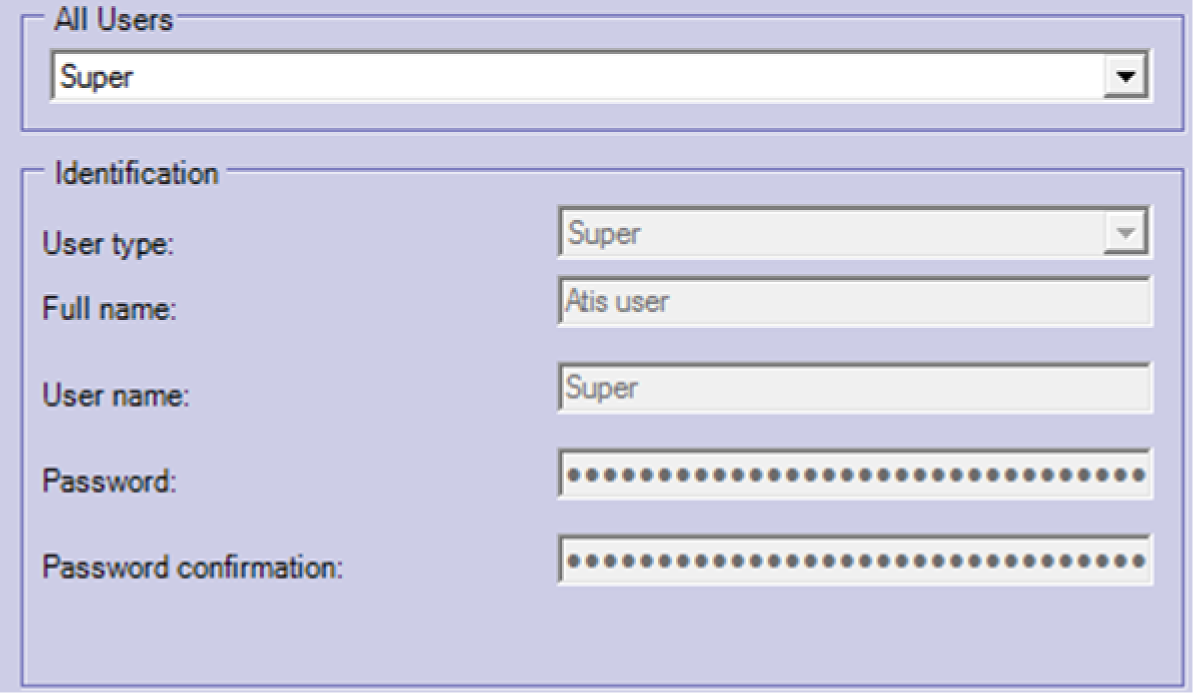
Invalid user name or password. 1 more attempt(s) allowed. Please reenter.

Active channels:
VDS connected:
RIAB connected:
Buffer:
Admin connected:
Messages:
Active client connections:

8. Encrypted storage of passwords using SHA2 algorithm

In former versiuons the VC-MDx applications used Data Encryption Standard (DES) algorithm.

Since SW version 14.x.x.x. teh VC-MDx applications is using the SHA256 hash algorithm to store the passwords of the users. For this reason, the values of the fields containing passwords of the "users" table of the "vcexdatabase" will be automatically converted from the DES encryption password value to the value obtained by SHA256 algorithm applied to the password.



All Users

Super

Identification

User type: Super

Full name: Atis user

User name: Super

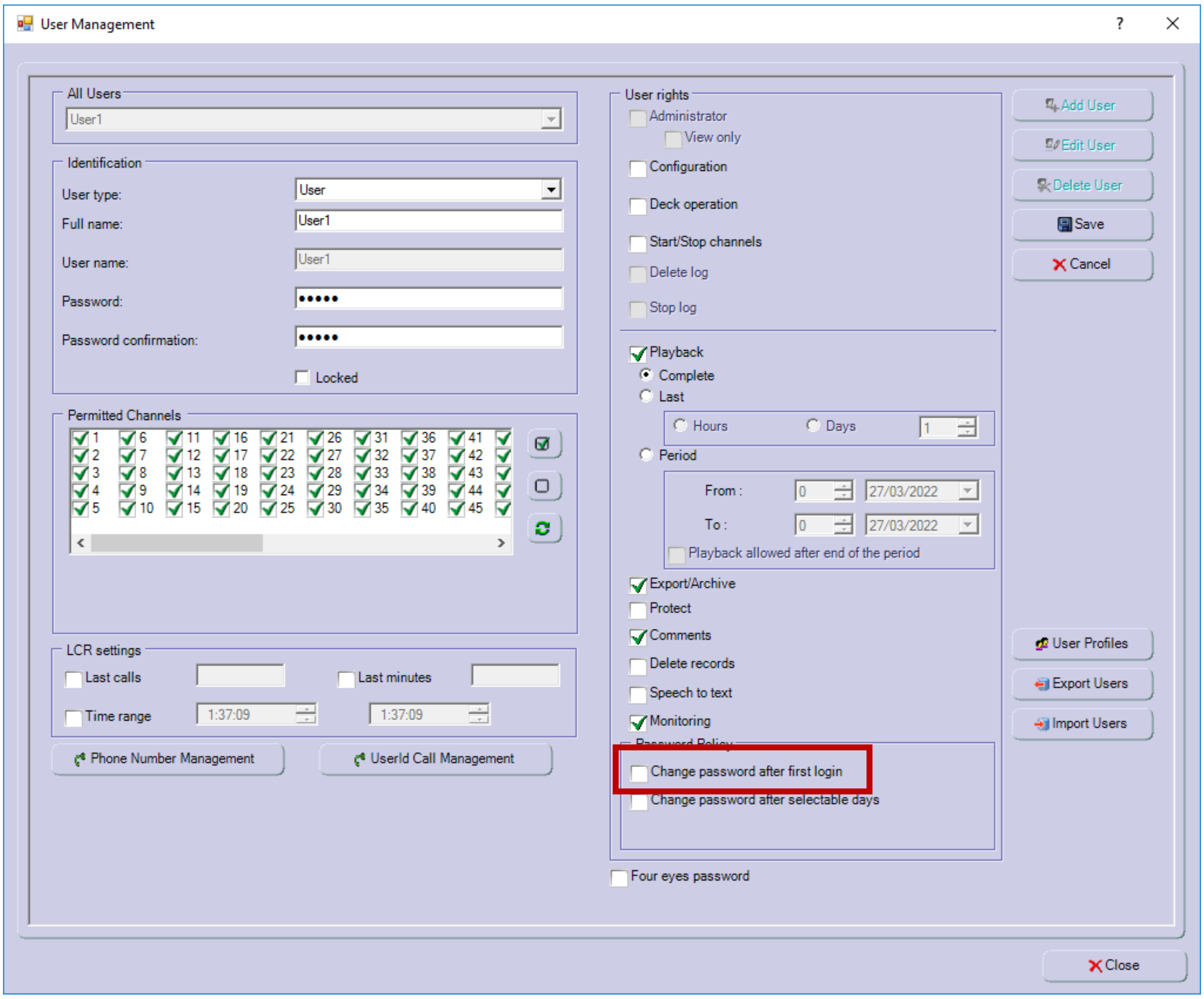
Password: ••••••••••••••••••••••••••••••••

Password confirmation: ••••••••••••••••••••••••••••••••

9. Automatic request to change the password after the first login

⇒ Open Settings/ User Management

Activate checkbox to enable this function



User Management

All Users: User1

Identification
- User type: User
- Full name: User1
- User name: User1
- Password: •••••
- Password confirmation: •••••
- □ Locked

Permitted Channels: ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15 ☑ 16 ☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21 ☑ 22 ☑ 23 ☑ 24 ☑ 25 ☑ 26 ☑ 27 ☑ 28 ☑ 29 ☑ 30 ☑ 31 ☑ 32 ☑ 33 ☑ 34 ☑ 35 ☑ 36 ☑ 37 ☑ 38 ☑ 39 ☑ 40 ☑ 41 ☑ 42 ☑ 43 ☑ 44 ☑ 45

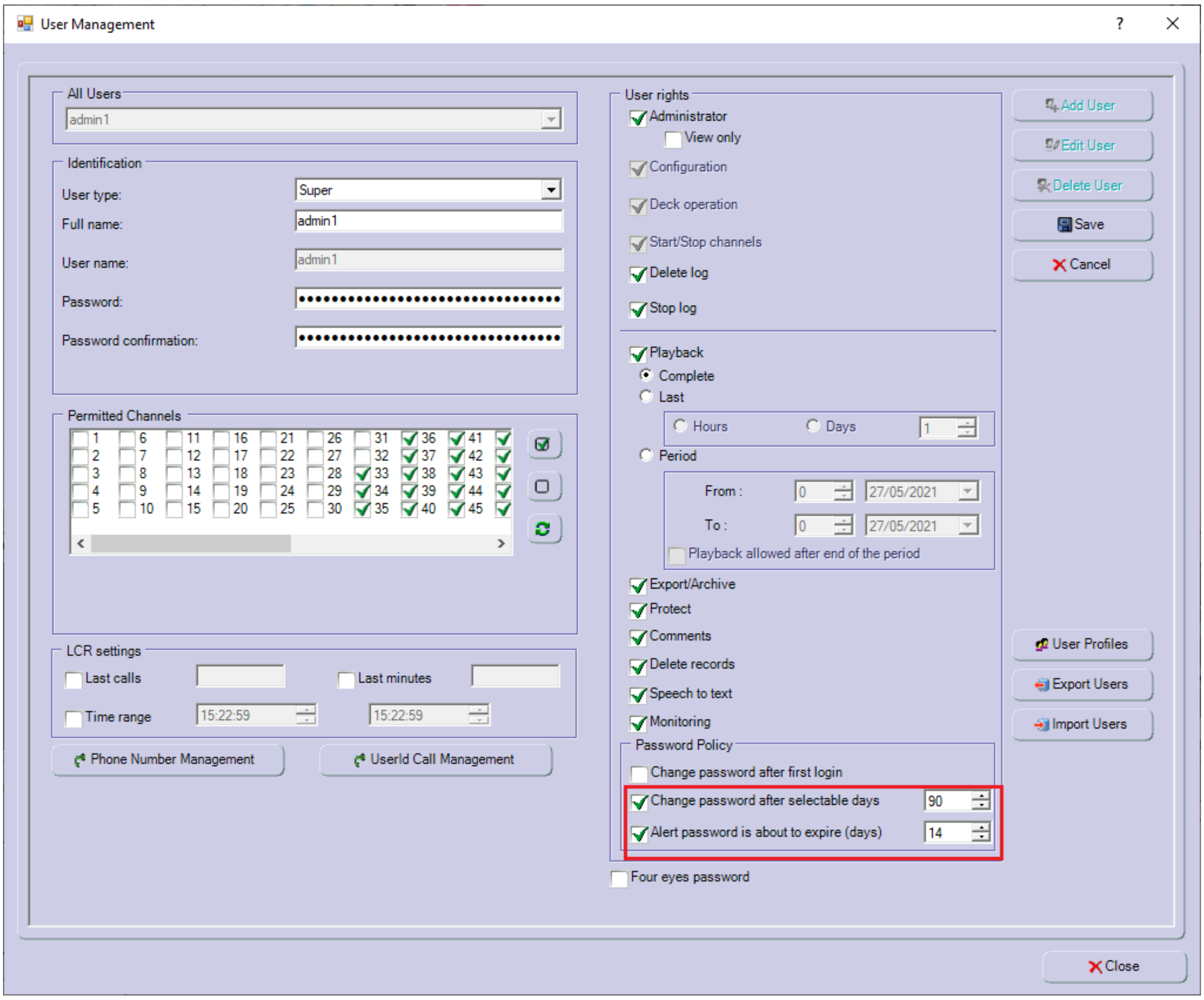
LCR settings
- □ Last calls
- □ Last minutes
- □ Time range 1:37:09 1:37:09

User rights
- □ Administrator
- □ View only
- □ Configuration
- □ Deck operation
- □ Start/Stop channels
- □ Delete log
- □ Stop log
- ☑ Playback
  - ● Complete
  - ○ Last (○ Hours ○ Days 1)
  - ○ Period (From : 0 27/03/2022; To : 0 27/03/2022)
  - □ Playback allowed after end of the period
- ☑ Export/Archive
- □ Protect
- ☑ Comments
- □ Delete records
- □ Speech to text
- ☑ Monitoring

Password Policy
- □ Change password after first login
- □ Change password after selectable days

□ Four eyes password

10. **The password expires after an adjustable time (factory setting 90 days) and prompt to change the password with an adjustable interval (factory setting 14 days)**
⇒ Open Settings/ User Management



User Management

All Users: admin1

Identification
User type: Super
Full name: admin1
User name: admin1
Password: ••••••••••••••••••••••••••••••••
Password confirmation: ••••••••••••••••••••••••••••••••

Permitted Channels
□ 1 □ 2 □ 3 □ 4 □ 5
□ 6 □ 7 □ 8 □ 9 □ 10
□ 11 □ 12 □ 13 □ 14 □ 15
□ 16 □ 17 □ 18 □ 19 □ 20
□ 21 □ 22 □ 23 □ 24 □ 25
□ 26 □ 27 □ 28 □ 29 □ 30
□ 31 □ 32 ☑ 33 ☑ 34 ☑ 35
☑ 36 ☑ 37 ☑ 38 ☑ 39 ☑ 40
☑ 41 ☑ 42 ☑ 43 ☑ 44 ☑ 45
☑ ☑ ☑ ☑ ☑

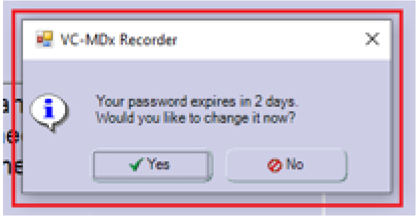
LCR settings
□ Last calls
□ Last minutes
□ Time range 15:22:59 15:22:59

User rights
☑ Administrator
□ View only
☑ Configuration
☑ Deck operation
☑ Start/Stop channels
☑ Delete log
☑ Stop log
☑ Playback
● Complete
○ Last
○ Hours ○ Days 1
○ Period
From : 0 27/05/2021
To : 0 27/05/2021
□ Playback allowed after end of the period
☑ Export/Archive
☑ Protect
☑ Comments
☑ Delete records
☑ Speech to text
☑ Monitoring

Password Policy
□ Change password after first login
☑ Change password after selectable days 90
☑ Alert password is about to expire (days) 14
□ Four eyes password

The password expiration is selectable for time period (days).

If the function *"Strong password"* (see chapter) is enabled, an additional checkbox *"Alert password is about to expire"* will appear. If this *"Alert password is about to expire"* is checked, a warning message may appear:



VC-MDx Recorder

Your password expires in 2 days.
Would you like to change it now?

*** End of Document ***