

## Multi-factor authentication & Password policy

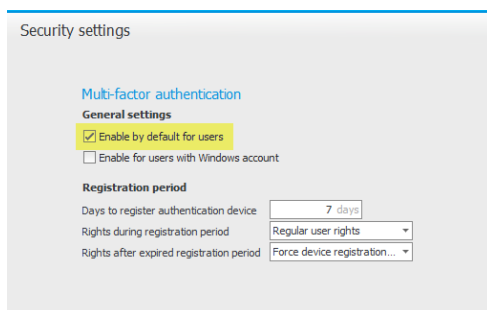
We have implemented a multi-factor authentication (MFA) feature where administrators can activate additional security measurements for users based on settings in the *Security settings* procedure.

MFA is currently supported in the Monitor G5 **desktop client** and **web client**.

### Security settings

Enable by default for users.

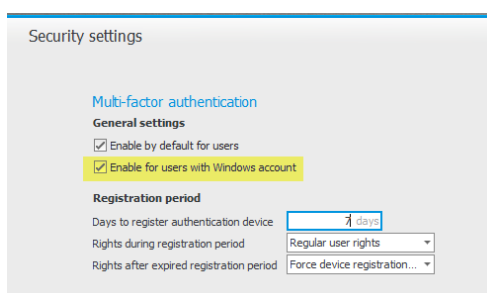
MFA can be activated in the *Security settings* procedure under General registers, by checking **Enable by default for users**. Enabling this setting will activate MFA in the desktop client and the web client, with the settings set under *Registration period*.



The screenshot shows the 'Security settings' window with the 'Multi-factor authentication' section expanded to 'General settings'. The checkbox 'Enable by default for users' is checked and highlighted in yellow. The checkbox 'Enable for users with Windows account' is unchecked. Under the 'Registration period' section, 'Days to register authentication device' is set to 7 days, 'Rights during registration period' is set to 'Regular user rights', and 'Rights after expired registration period' is set to 'Force device registration...'. The 'Force device registration...' option is highlighted in yellow.

Enable for users with Windows account

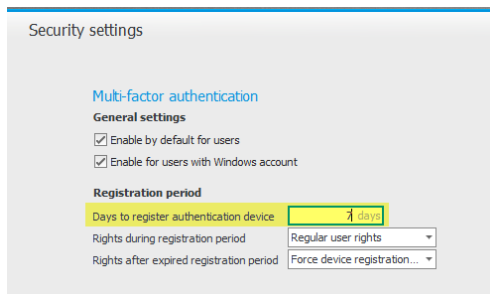
Additionally, checking **Enable for users with Windows account** ensures that MFA is activated for users that has a connected Windows account (i.e., an AD account).



The screenshot shows the 'Security settings' window with the 'Multi-factor authentication' section expanded to 'General settings'. Both checkboxes 'Enable by default for users' and 'Enable for users with Windows account' are checked and highlighted in yellow. Under the 'Registration period' section, 'Days to register authentication device' is set to 1 day, 'Rights during registration period' is set to 'Regular user rights', and 'Rights after expired registration period' is set to 'Force device registration...'. The 'Force device registration...' option is highlighted in yellow.

Days to register authentication device

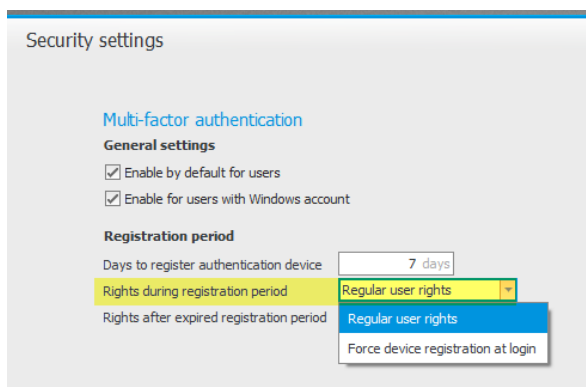
The setting **Days to register authentication device** under *Registration period* specifies how many days a user is allowed to set up MFA. An administrator will specify how rights should be applied to users *during* and *after* the registration period through the **Rights during registration period** and **Rights after registration period** settings covered in the next part.



### Rights during registration period

The rights include:

- **Regular user rights** – Ensures that users will have access to procedures even if they skip the device registration.
- **Force device registration at login** – Makes users unable to skip the registration process and they will be forced to register a device at login.

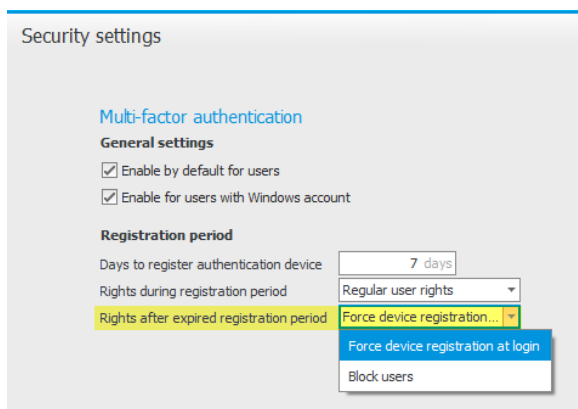


### Rights after expired registration period

The rights include:

- **Force device registration at login** – Forces users to register a device.
- **Block users** – Prevents users from signing in.

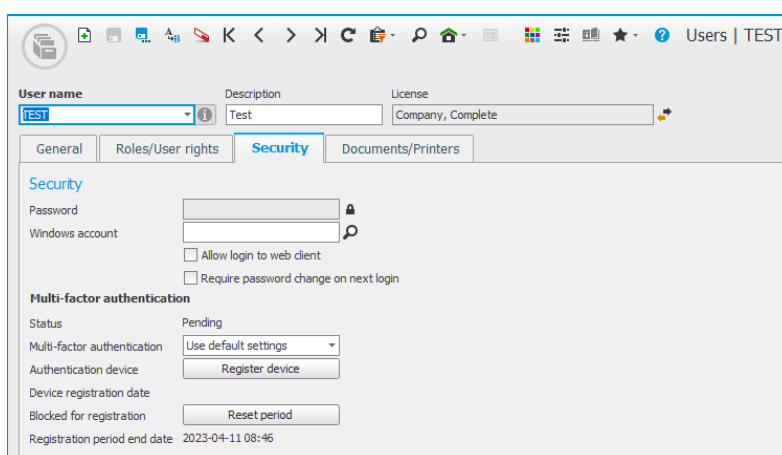
**Note:** If the registration period expires for a user and the **Block users** has been selected, the user will be required to contact a system administrator to unlock the account.



## Users procedure

On the Security tab in the *Users* procedure, administrators can change how the MFA is set up on a per user basis:

- **Status** – Contains the status of the MFA. The status will be displayed as either *Pending*, *Enabled* or *Disabled*, depending on how MFA has been set up on a specific user.
- **Multi-factor authentication** – Contains settings on how MFA should be applied to a specific user according to the options in the list. When **Use default settings** has been selected, settings in the *Security settings* procedure will be applied by default to users. Selecting **On** activates MFA while selecting **Off** disables the feature. Changing these options can be useful when an administrator for example wants to enable or disable MFA on individual users only.
- **Authentication device** – Can be used to register or remove a device from a user.
- **Device registration date** – Contains the date of when a device was registered to a user.
- **Blocked for registration** – Can be used to manually unblock users who has exceeded the limit of the registration period by allowing an extended registration period. This setting is dependent on the setting **Days to register authentication device**, which can be set in the *Security settings* procedure.
- **Registration period end date** – Contains the date of when the registration period ends.



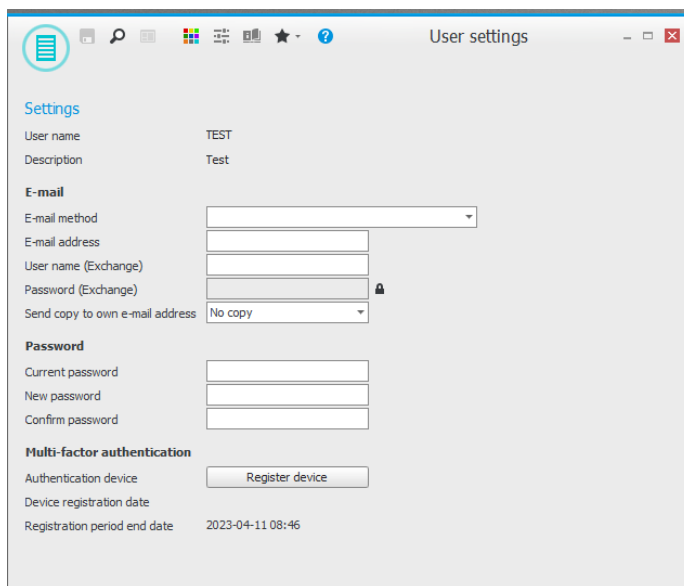
The screenshot shows the 'Users' procedure in the Monitor ERP System, specifically the 'Security' tab for a user named 'TEST'. The user's description is 'Test' and the license is 'Company, Complete'. The 'Security' tab is active, showing various settings:

- General:** Password, Windows account, and checkboxes for 'Allow login to web client' and 'Require password change on next login'.
- Multi-factor authentication:** Status is 'Pending', Multi-factor authentication is set to 'Use default settings', and there is a 'Register device' button.
- Blocked for registration:** There is a 'Reset period' button.
- Registration period end date:** 2023-04-11 08:46.

## User settings

When signed into the client, users can access *User settings* and set up MFA. *User settings* contains similar settings as found on the Security tab in the *Users* procedure:

- **Authentication device** – Can be used to register a device when MFA has been enabled by a system administrator.
- **Device registration date** – Contains the date of when a device was registered to the user.
- **Registration period end date** – Contains the date of when the registration period ends for the user.



**Settings**

User name: TEST  
Description: Test

**E-mail**

E-mail method: [dropdown]  
E-mail address: [text]  
User name (Exchange): [text]  
Password (Exchange): [text]   
Send copy to own e-mail address: No copy [dropdown]

**Password**

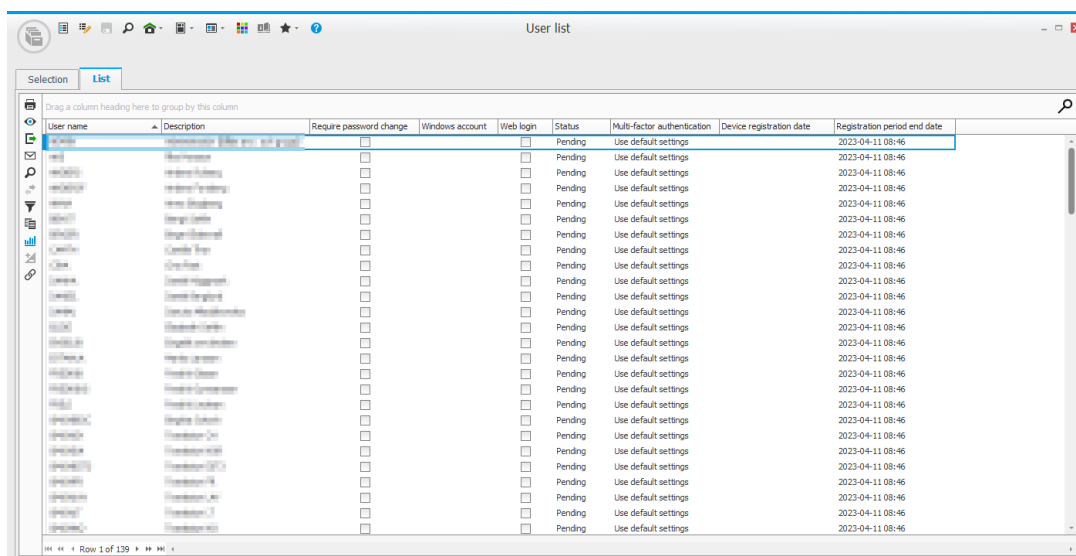
Current password: [text]  
New password: [text]  
Confirm password: [text]

**Multi-factor authentication**

Authentication device: [Register device button]  
Device registration date: 2023-04-11 08:46  
Registration period end date: 2023-04-11 08:46

## User list – Security

The *User list* procedure contains the *Security* list type where settings for MFA can be listed and administered as preferred.



User name	Description	Require password change	Windows account	Web login	Status	Multi-factor authentication	Device registration date	Registration period end date
TEST	TEST	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST1	TEST1	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST2	TEST2	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST3	TEST3	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST4	TEST4	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST5	TEST5	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST6	TEST6	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST7	TEST7	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST8	TEST8	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST9	TEST9	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST10	TEST10	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST11	TEST11	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST12	TEST12	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST13	TEST13	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST14	TEST14	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST15	TEST15	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST16	TEST16	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST17	TEST17	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST18	TEST18	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46
TEST19	TEST19	<input type="checkbox"/>		<input type="checkbox"/>	Pending	Use default settings	2023-04-11 08:46	2023-04-11 08:46

## Register device – Desktop client

Once the MFA has been activated in the *Security settings* procedure, users can register a device from the login prompt in the desktop client.

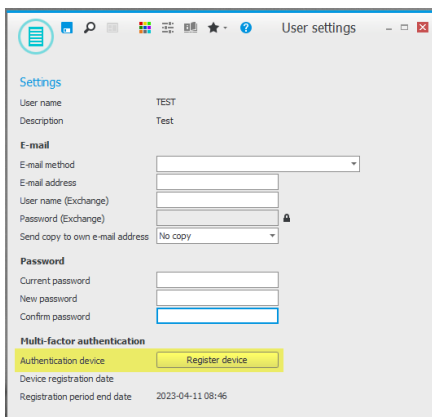
### Login prompt

After logging in, users will be presented with the MFA registration dialog where users can scan the QR-code in an authentication app and register a device.



### User settings

When signed in it is also possible to add the device in *User settings* by pressing the button and following the on-screen instructions.

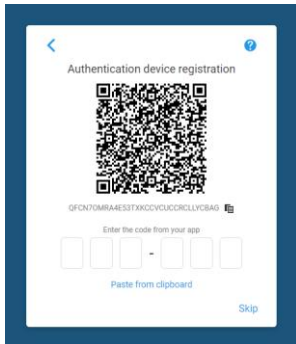


## Register device – Web client

Once the MFA has been activated in the *Security settings* procedure in the desktop client, user accounts eligible for web access can register a device in the web client.

### Login prompt

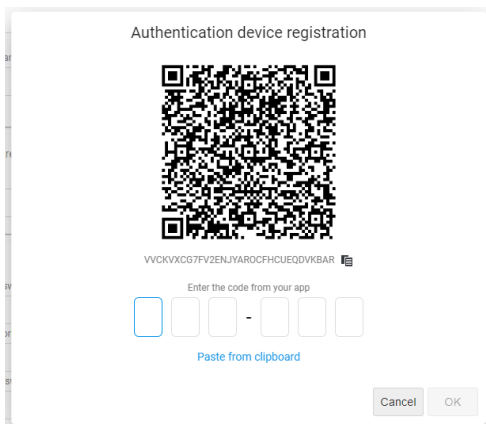
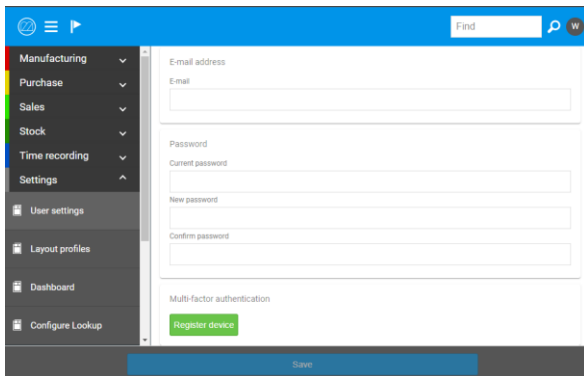
After logging in, users will be presented with the MFA registration dialog where users can scan the QR-code in an authentication app and register a device.



### User settings

The *User settings* page contains a button where users can manually register a device, if they previously skipped the step of registering a device in the login prompt.

**Note:** The button will only become active if MFA has been enabled in the *Security settings* procedure in the desktop client.

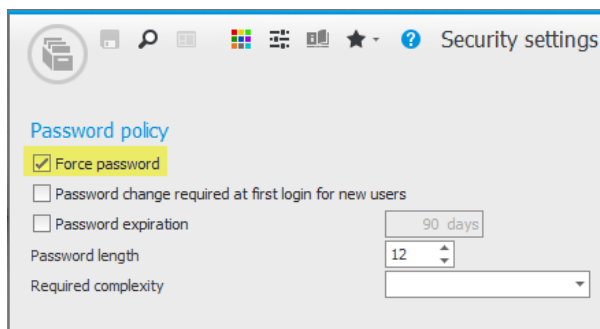


## Password policy

We have implemented a password policy feature where system administrators can set a password policy for all or specific users. The password policy can be used with or without MFA. The password policy restricts or adds additional conditions for password requirements, based on the following settings in the *Security settings* procedure.

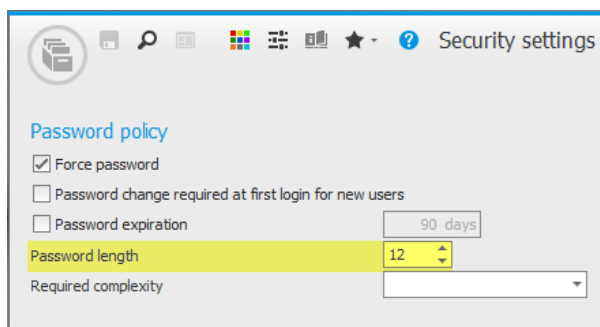
### Force password

The password policy can be activated by checking the **Force password** setting.



### Password length

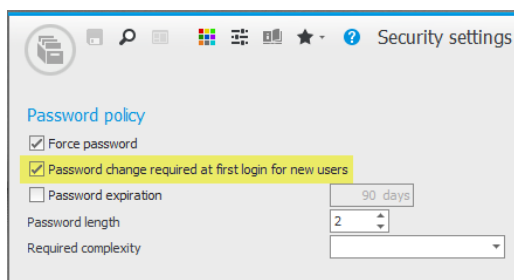
The **Password length** setting will be activated once **Force password** has been checked. By default, this is set to 12 characters – but system administrators can set a preferred password length.



### Password change required at first login for new users

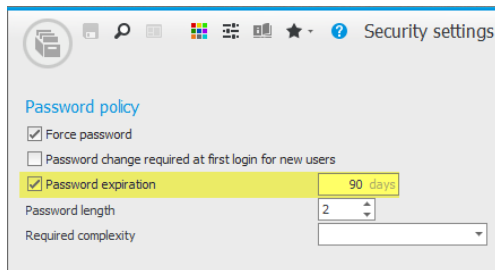
A password change can be activated on new users by default, by checking the setting **Password change required at first login for new users**.

**Note:** The setting only applies to new user accounts and the system administrator is required to add a temporary password that matches the password requirements on the new user. The user will then be asked to change the password upon the first login.



## Password expiration

A password expiration date can be set by checking the Password expiration setting. By default, this is set to 90 days – but system administrators can set a preferred password expiration. The setting applies to users with an existing password and counts the expiration based on the last time the user added or updated the password.



## Required complexity

A required password complexity can be set by checking one or combining several settings in the **Required complexity** setting:

- **CAPITAL/lower-case** – Requires users to include capital- and lower-case letters in the password.
- **Digits** – Requires users to include digits in the password.
- **Special characters** – Requires users to include special characters in the password.

