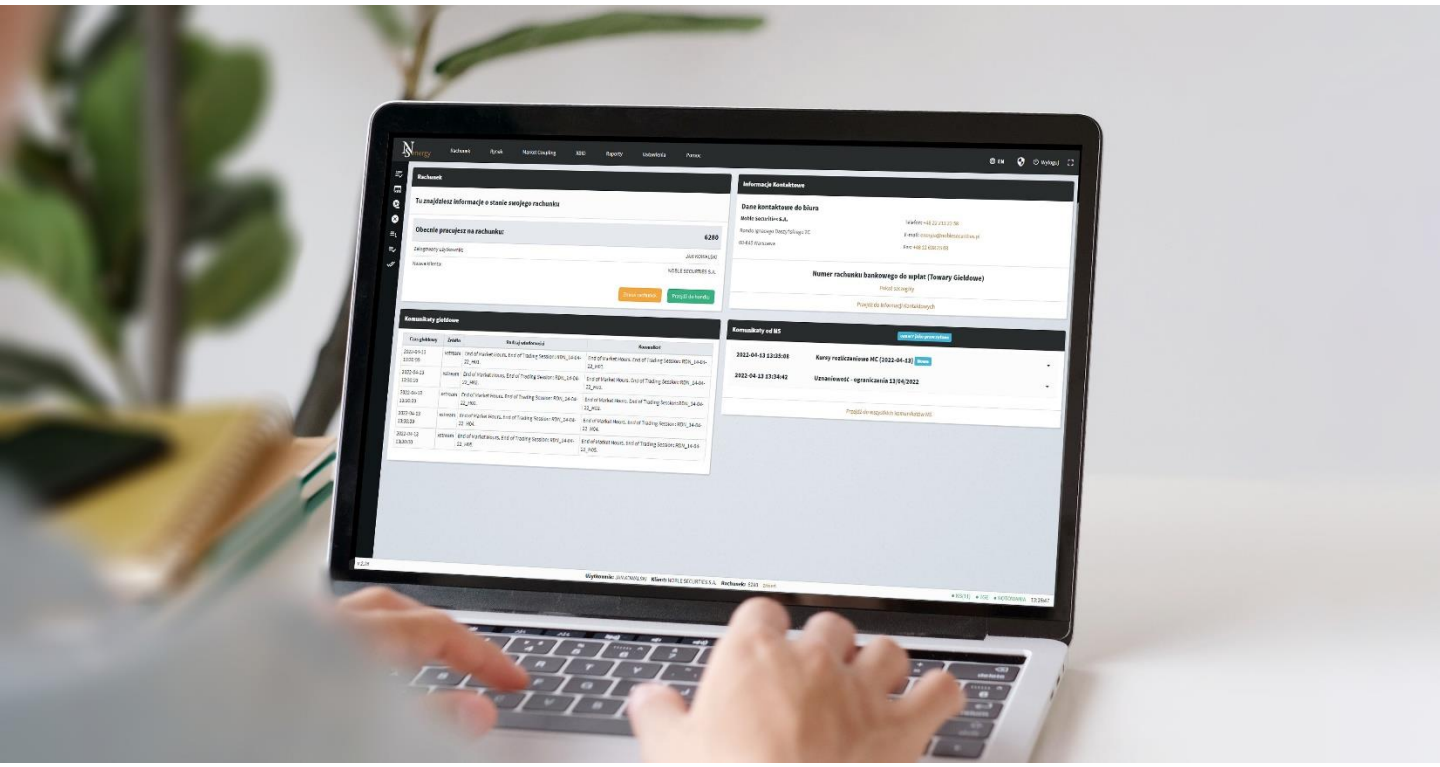
NOBLE SECURITIES
DOM MAKLERSKI



# Login method
# - two-factor authentication

Manual for Users
of NSenergy 2.0 application

In order to enhance safety with regard to the use of the application for transactions to be concluded on the Polish Power Exchange via NSenergy 2.0 (**"Application"**), Noble Securities S.A. (**"NS"**) has introduced an additional login security measure for the Application in the form of authentication codes. A authentication in the Application is carried out by means of two-factor authentication (2FA) when authorised entities (**"Users"**) log in, whereby a login and password set by the User is entered, followed by the entry of an authentication code send via SMS or email.

## Default configuration of how the access code is delivered to the User

**Note!**

The initial way of logging in does not change and the login and password for the application account must be entered (Fig. 1).

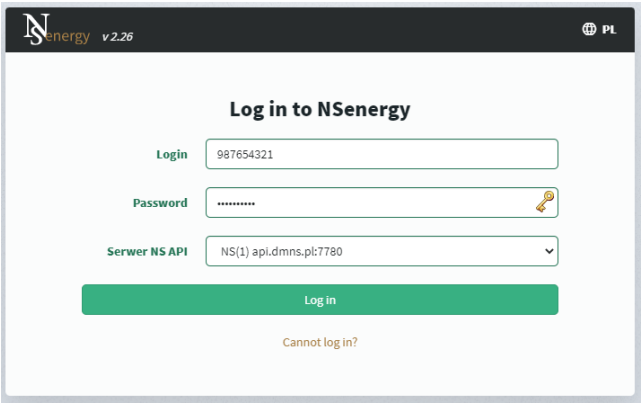



*Fig. 1. Login screen*

When logging in, after the two-factor authentication (2FA) service has been activated, the system will display a request for setting the method of sending the authentication code for the User (Fig. 2). Such a message will appear only once.

**NOTE!!!** It is important to have access to a mailbox and/or a mobile phone. The email code and/or SMS code will be sent at the Customer's details provided to the NS contact. In the event that the details have changed and the User has not informed NS of this, you will not be able to log in to the Application and NS will need to be contacted to update the contact details.

## Choice of method of access code delivery

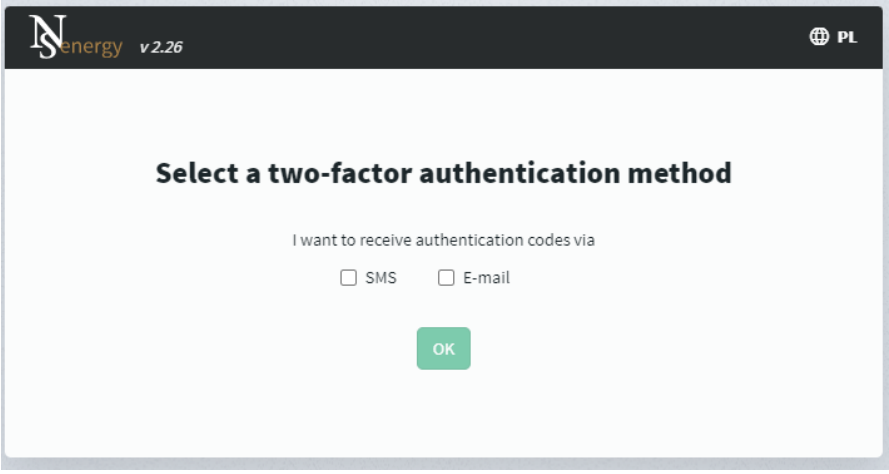



*Fig. 2. Choice of method of access code delivery*

You can set:

- code sent to an e-mail address (Fig. 3),
- code sent by SMS (Fig. 4),

or, for security reasons, both (Fig. 5).

At least one method of authentication must be selected for the second step. The method of receiving the code could be changed after logging in to the Application in SETTINGS (The description follows below).

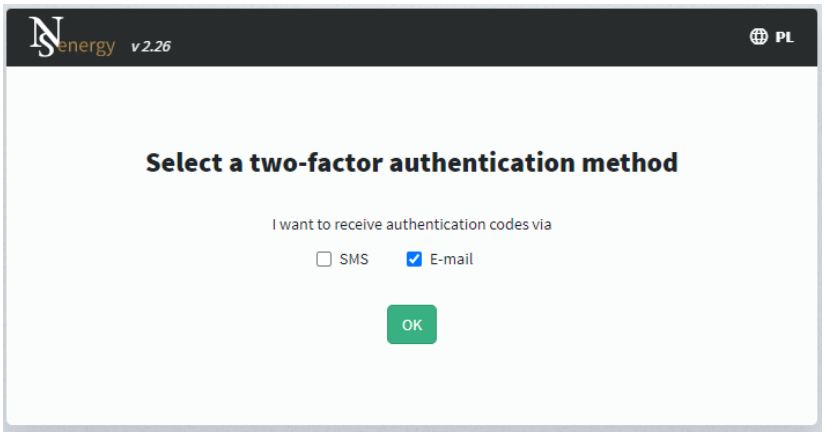



*Fig. 3. Choice of method of access code delivery to an e-mail address*

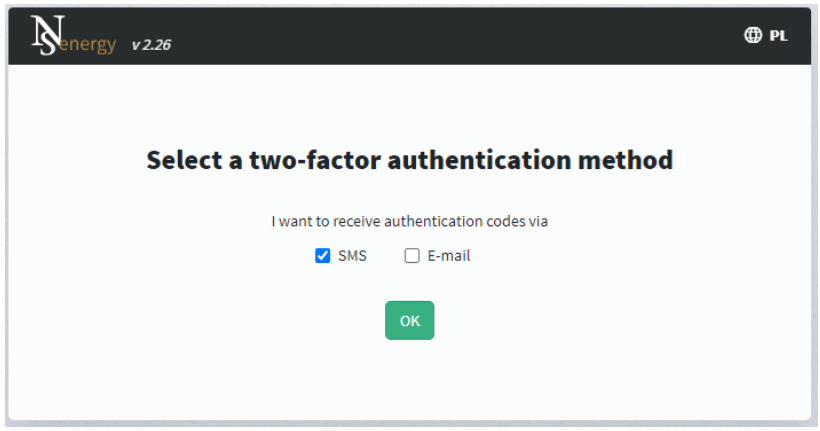



*Fig. 4. Choice of method of access code delivery by SMS*

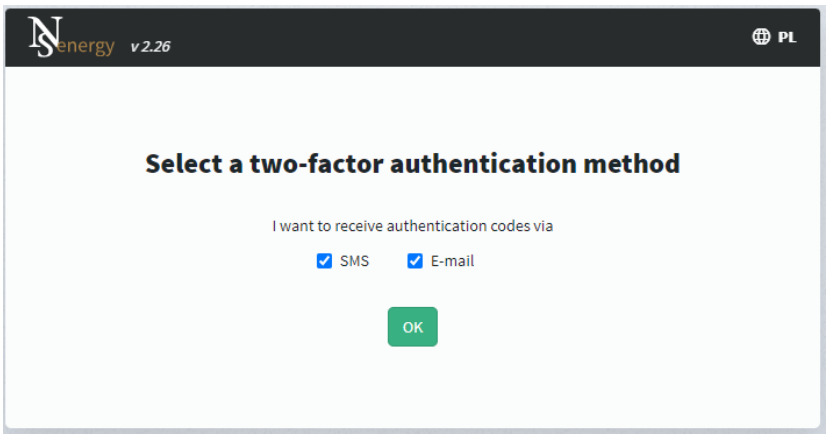



*Fig. 5. Choice of method of access code delivery to an e-mail address and by SMS*

### Adding the User's device as a stored (trusted) device

Once the code delivery method has been selected and approved, a prompt will be displayed, a question whether the User wants to add the current device (for instance computer, tablet or other device) as a trusted device (Fig.6). Adding a device to the trusted ones allows you to skip the otherwise mandatory authorisation of logging into the Application each time with authentication codes. If the User does not wish to remember the device, select the One-Time Access button, in which case the User will proceed to entering the one-time codes.

**NOTE!!!** Do not store the device if you log in to the Application from a device which belongs to someone else, has not been provided by your employer for your exclusive use or, in particular, if it is a publicly accessible device.

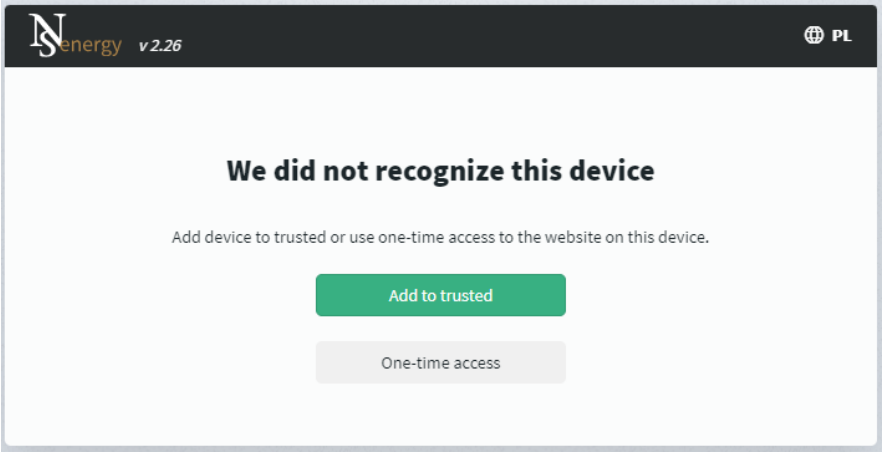



*Fig. 6. Message about storing the current device*

After expressing the wish to add the current device as trusted, the system will display a window (Fig. 7) in which you can enter a name for the saved device (Fig. 8).

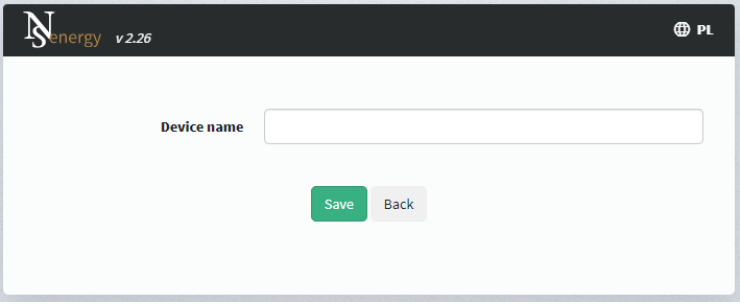



*Fig.7. Entering a name for the device*

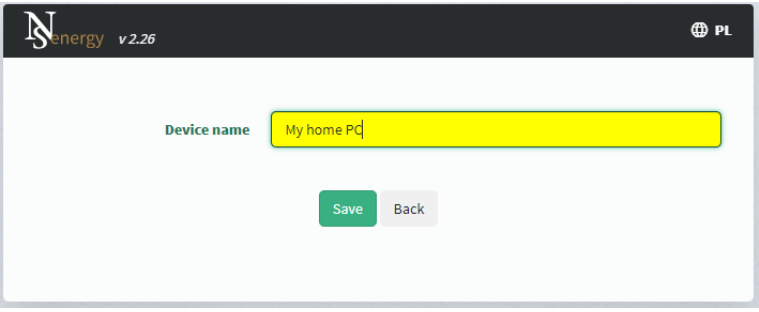



*Fig.8. Example of a name of device of your choice*

The user can opt out of remembering the device by selecting the Back button.

## Entering authentication codes

After selecting the code delivery method and optionally adding the device to trusted, the User will receive unique access codes to be entered to complete the login process (Fig. 9).

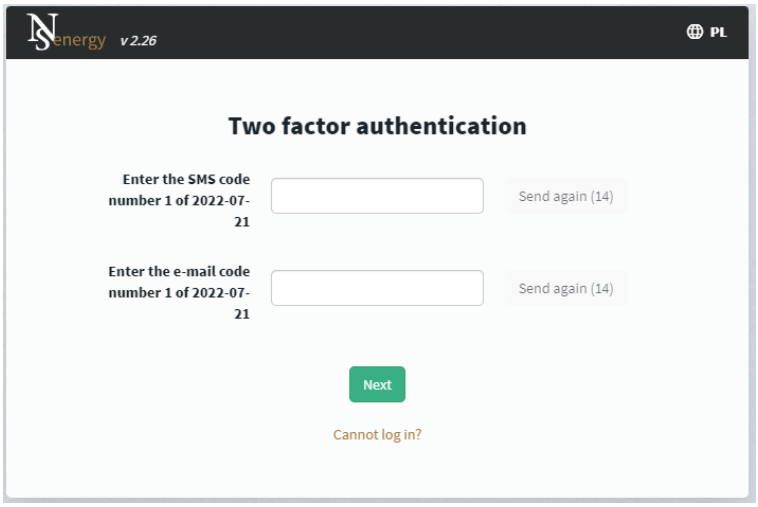



*Fig. 9. Screen for entering authentication code*

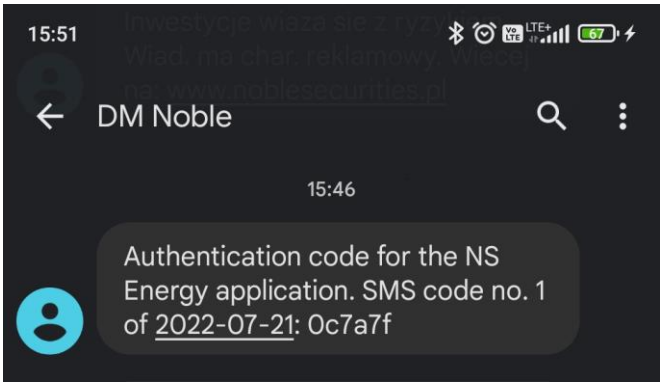



*Fig. 10. Example of SMS code*

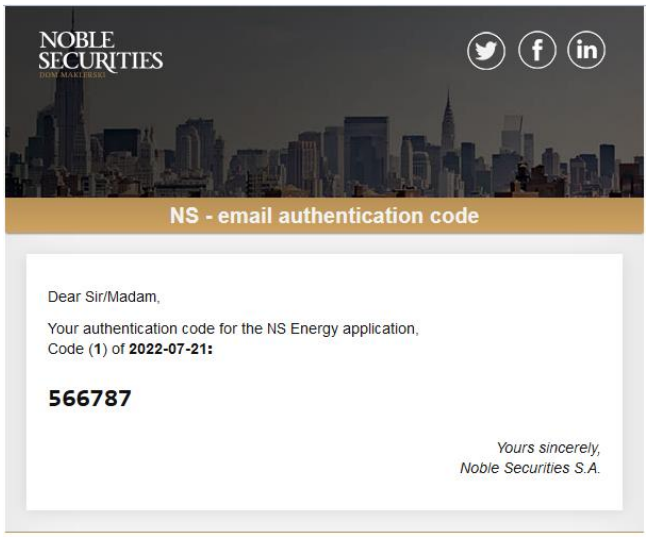



*Fig. 11. Example of code in an e-mail message*

**NOTE!!!** If the access code does not arrive within 60 seconds, the access code must be generated again by using the SEND AGAIN button. A maximum of 3 authentication codes can be generated during one login. Failure to receive a code may be due to outdated data submitted to NS. If you do not receive a code, please contact NS.

**After logging in, the User can verify when the previous login to the system took place. On the main page of the Application in the account information under the customer name (Fig. 12) and in the bar at the bottom of the Application (Fig. 13).**

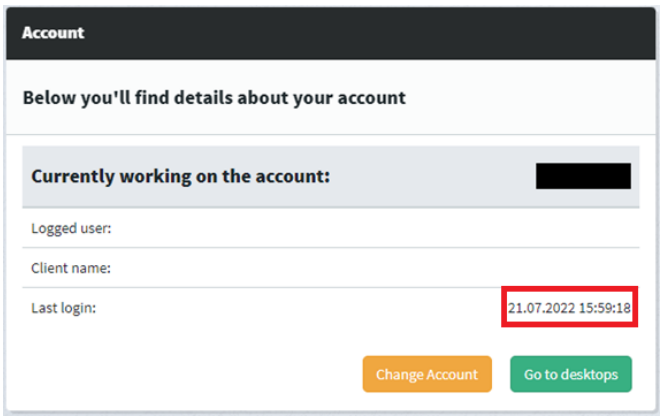



*Fig. 12. Last login*

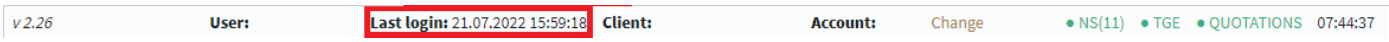



*Fig. 13. Last login*

**Configuration of the way codes are delivered and management of stored devices**

In order to change the method of receiving codes, go to the settings, which are visible after logging into the Application. From the menu, select Settings -> Two-Factor Authentication (Fig. 14).

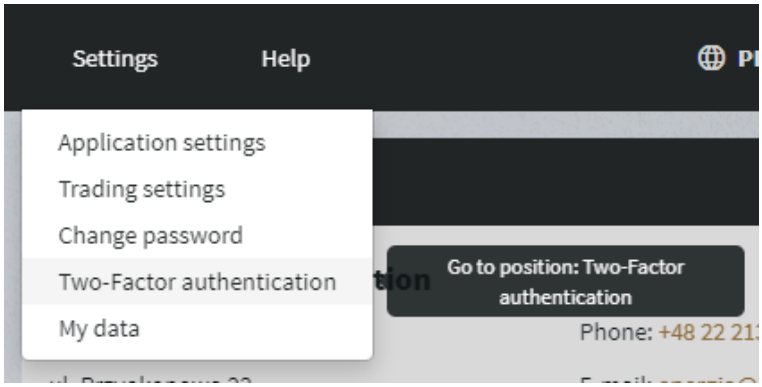



*Fig. 14. SETTINGS icon*

After navigating to the two-factor authentication settings, the 'two-factor authentication' window will be displayed (Fig. 15).

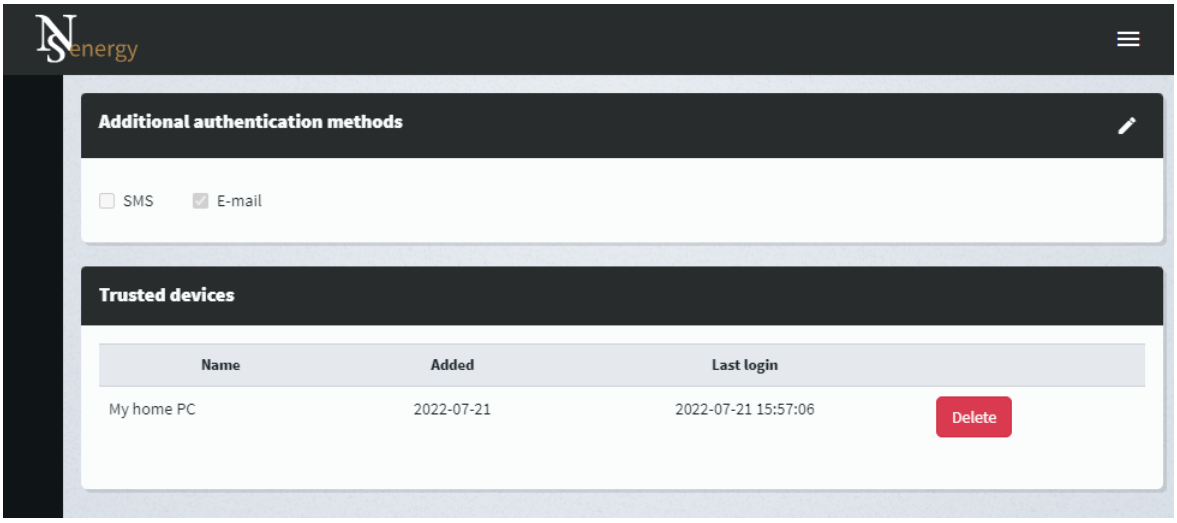



*Fig. 15. Window with settings for two-factor authentication*

To change the current method of receiving codes, click on the pencil icon in the top right corner. Change the method of receiving codes and save the settings by clicking on the floppy disk icon (Fig. 16).

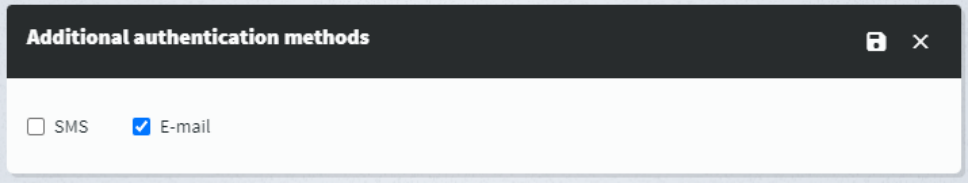



*Fig. 16. Section for selecting the authentication code delivery method*

Before saving the changes, confirm the selection with a unique access code sent with the previously selected authentication method (Fig. 17).

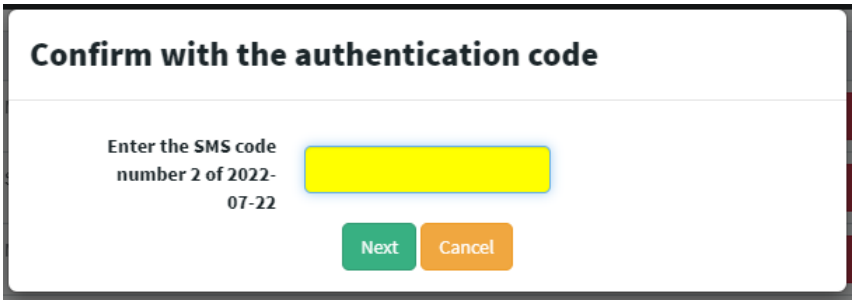



*Fig. 17. Confirmation with the authentication code*

Correctly entering the code will change the way of receiving further codes, which will be confirmed by a message (Fig. 18)

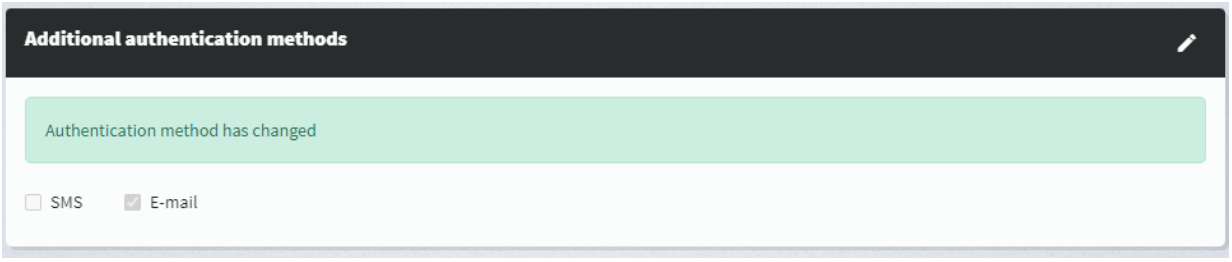



*Fig. 18. Confirmation of change in authentication method*

**NOTE!!!** The two-factor authentication may not be opted out of. The User must select at least one method to provide the code. If the User does not select any method, the settings will not be saved and the User will not be able to log in to the Application.

In the section on memorised devices, a list of the devices that have been stored appears (Fig. 17). A maximum of 5 devices can be stored. To add another device the previously added one must be deleted (DELETE button next to the device).

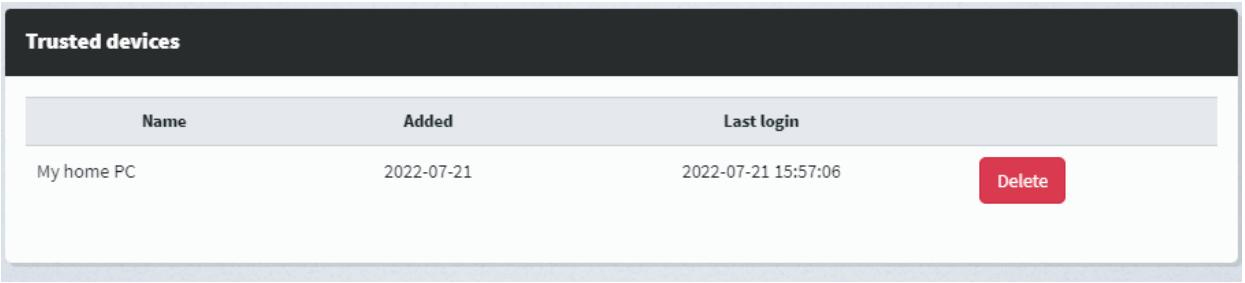



*Fig. 19. List of trusted devices*

In the list above, each device has a unique name (given by the User), the date of adding and the date of the last login from that device.

### Password change

The method of changing the password to the Application has not changed, however, it will be additionally required to approve this change with a one-time authentication code (Fig. 20).

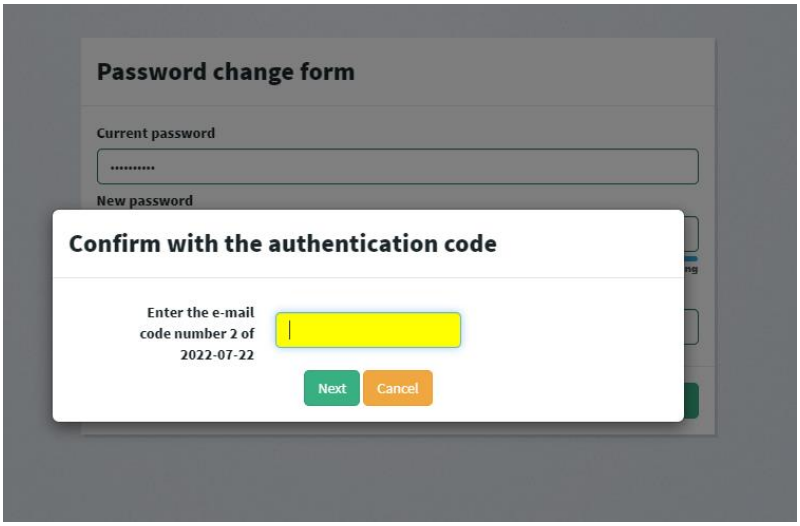



*Fig. 20. Confirmation of the password change with the use of the authentication code*

NOBLE SECURITIES
DOM MAKLERSKI

## Do you have any questions? Contact us:


www.noblesecurities.pl

energia@noblesecurities.pl

+48 22 213 22 58



Noble Securities S.A. Prosta 67, 00-838 Warsaw +48 22 244 13 03 Fax: +48 12 411 17 66 entered in the Register of Businesses of the National Court Register kept by the District Court for the Capital City of Warsaw. Warsaw in Warsaw, 13th Commercial Division, under KRS number: 0000018651 REGON (Business Register Number): 350647408, NIP (Tax Identification Number): 676 01 08 427 Share capital of PLN 3,494,747 fully paid-up.