

NEMO – NOMINATION AND ENERGY MANAGEMENT ONLINE

SETTING UP YOUR TWO FACTOR AUTHENTICATION (2FA)

Version: 1.0.0
Status: ISSUED
Issue Date: 12.10.2017

HOW TO SET UP TWO FACTOR AUTHENTICATION

If your account has been set up as a **customer administrator**, you will be required to have extra security on your account. This is because you are able to create accounts for your organisation. This will involve what we call a soft token (a one-time password), that will be generated by your mobile phone / tablet. This soft token will become the second factor, used in addition to your password.

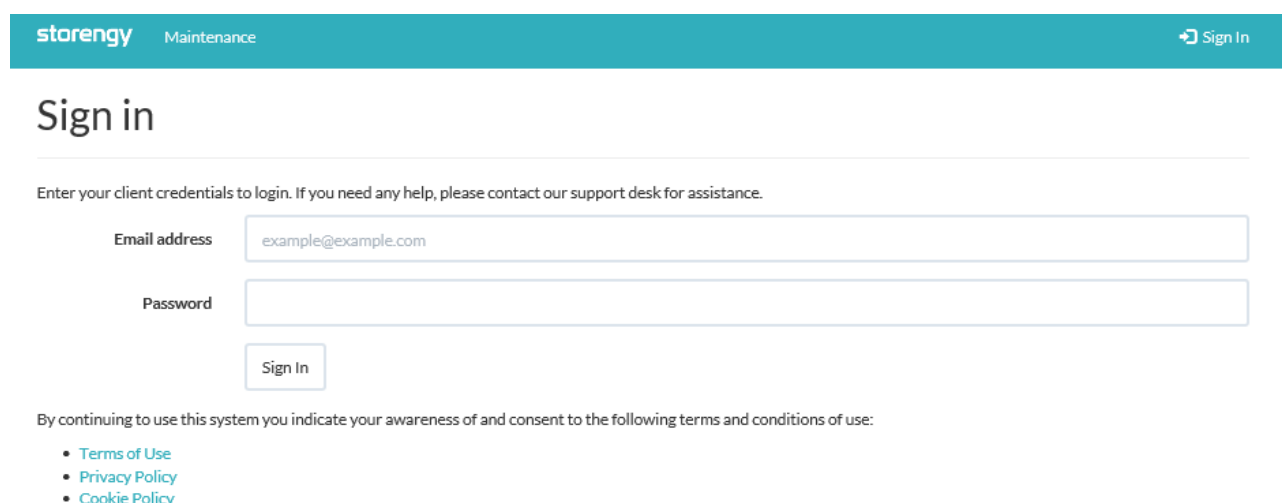
1. DOWNLOAD AN AUTHENTICATOR APPLICATION

For iPhone and Android phones or tablets, you may want to download Google Authenticator, which is a free app. For a Windows phone, the Windows store has options such as the Windows Authenticator.

Once you have downloaded the application you are ready to set up your two factor authentication.

2. CONFIGURE THE AUTHENTICATOR APP TO BE LINKED TO NEMO

From Your PC / Laptop, access the NEMO site and type in your first login details:



The screenshot shows the NEMO Sign in page. At the top, there is a teal header with the 'storengy' logo on the left, 'Maintenance' in the center, and a 'Sign In' button on the right. Below the header, the page title 'Sign in' is displayed. A horizontal line separates the title from the main content. Below the line, there is a prompt: 'Enter your client credentials to login. If you need any help, please contact our support desk for assistance.' This is followed by two input fields: 'Email address' with the placeholder text 'example@example.com' and 'Password'. Below the password field is a 'Sign In' button. At the bottom of the form, there is a line of text: 'By continuing to use this system you indicate your awareness of and consent to the following terms and conditions of use:' followed by three bullet points: 'Terms of Use', 'Privacy Policy', and 'Cookie Policy'.

You will then be prompted with this screen:

Two-factor authentication

Your role requires you enable two factor authentication to ensure your account is secure. Please setup two factor authentication now.

Download Google Authenticator

Whilst you can use any authenticator app that supports TOTP, we recommend Google Authenticator:



Scan the barcode

Open the authenticator app and choose the "Scan a barcode" option:



Alternatively if you have problems scanning the barcode you can also enter the key manually:

73EN3JTQGQY63JZB

Enter a verification code

When you're asked for a verification code, get it from the authenticator app. Enter the 6-digit code that you see in the app below - the code changes frequently, so no need to memorize it.

Code

Save

Now, open your phone's Authenticator Application. Click on the "+" sign to add a new entry, and select **Scan barcode**.

Point your phone at the screen and scan the QR code. The entry will be automatically added in your authenticator app.

Two-Factor Authentication

1. Scan this barcode with your Google Authenticator app:


5TBQQKASYGATBAQV407SYYIBB4EQU5U5
2. **Print out this page** and store the barcode in a safe place. Otherwise, there will be no way to regain access to your account if you lose your phone.
3. Type in the pin to confirm:

ENABLE TWO-FACTOR AUTH

Type the code which appears against the Storengy entry from the Authenticator app, into the browser, as shown below – please note that your code will differ:

Scan the barcode

Open the authenticator app and choose the "Scan a barcode" option:



Alternatively if you have problems scanning the barcode you can also enter the key manually:

73EN3JTQGQY63JZB

Enter a verification code

When you're asked for a verification code, get it from the authenticator app. Enter the 6-digit code that you see in the app below - the code changes

Code X

Click on **“Save”** and this should take you to the Home screen.

You will be required to use the second factor each time you log on, as well as your password.

Please, note, that we strongly recommend that you do not save your password in the browser. Instead, please consider a password solution, such as OnePass, or KeyPass.

3. WHAT HAPPENS IF MY TOKEN IS LOST?

Sometimes, it is possible to lose the 2FA association, for example when you change phones. If this happens, please ring the Commercial team for a soft token reset, or email commercial@storengy.co.uk.

If you have concerns that your account(s) have been compromised, please email it.security@storengy.co.uk immediately.