



# **Two Factor Authentication (2FA)**

## **User's Manual**



## 1 Introduction

This manual provides a practical guidance for setting up and using the Two Factor Authentication (2FA) method to login into TERMINAL application, available on the AEGIS platform.

## 2 What is a 2FA

Two Factor Authentication also known as 2FA, is a security method in which a user needs to present two independent pieces of evidence to the authentication mechanism to gain the access to the application. To be granted with the access, both pieces (factors) needs to be successfully recognized as (a) something only the user knows and (b) something only the user has. The most popular factors used in electronic authentication is password (factor a) and code generated on the user's phone (factor b).

To be able to use 2FA the user needs to use a third-party authenticator – specialized application that is installed on the user's phone and generates frequently changing code used in the authorization process.

## 3 Getting the authenticator

Authenticator is an application that generates authorization codes needed to get the access to the protected application. The authenticator should be installed on the phone to which only the user has access (personal phone or company phone used exclusively by the user).

---

*NOTE: If your phone is lost, contact TERMINAL administrator immediately.*

---

There is a number of third party authenticators available for both Android and IOS (Apple) phones that may be downloaded from the Google Play Store or from the Apple App Store. The most popular are Authenticator by Google, Microsoft Authenticator, Twilio Authy or 2FAS<sup>1</sup>. The Agency strongly recommend use of Google Authenticator or Microsoft Authenticator.

Before going to the next step of the procedure, you need to install one of these applications on the phone.

---

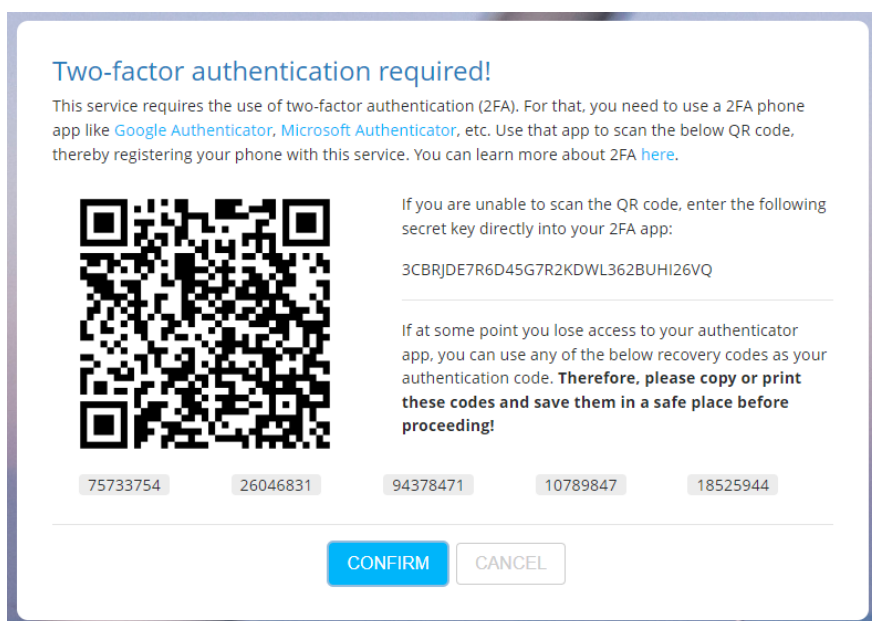
<sup>1</sup> Links to applications are included in the Section 6; you can use your own authenticator application if it supports QR Codes, however the Agency cannot guarantee proper cooperation of other applications with the TERMINAL 2FA



## 4 Enabling 2FA for the access to the TERMINAL


For the security reasons, the 2FA method is required for every user accessing the TERMINAL application. If you are logging to TERMINAL for the first time after the 2FA was introduced, you need to initialize your authenticator.

After a user logs in on the AEGIS platform with the user name (email) and password, and after accessing the TERMINAL, instead of going directly to the application, the authenticator initialization window will be presented (see Figure 1)



**Two-factor authentication required!**

This service requires the use of two-factor authentication (2FA). For that, you need to use a 2FA phone app like [Google Authenticator](#), [Microsoft Authenticator](#), etc. Use that app to scan the below QR code, thereby registering your phone with this service. You can learn more about 2FA [here](#).



If you are unable to scan the QR code, enter the following secret key directly into your 2FA app:

3CBRJDE7R6D45G7R2KDWL362BUHI26VQ

If at some point you lose access to your authenticator app, you can use any of the below recovery codes as your authentication code. **Therefore, please copy or print these codes and save them in a safe place before proceeding!**

75733754   26046831   94378471   10789847   18525944

Figure 1. Authenticator initialization window

**IMPORTANT! Write and save in a secure place five 8-digit codes displayed in the lower part of the window. These codes will help you to restore the access to the application if your authenticator application is lost. You can use each code only once (this means you can login to the system only five times without the authenticator). In such a case, consult Section 6 of this manual. DO NOT SHARE THESE CODES WITH ANYONE!**



Using the authenticator application, you need to add the TERMINAL account to the authenticator. The method of adding a new account differs from one authenticator to another. Examples below presents the process with the Google Authenticator. Please consult manuals of your application to add an account.

To add an account to the authenticator you need to click on (+) sign in the application<sup>2</sup>. The authenticator shall permit adding an account either with QR Code or manually. If you select adding by QR Code, the authenticator will open a camera view, which needs to be pointed on the QR Code displayed on the screen (cf. Figure 1). When the code will be decoded, the account will be added automatically to the application. If the QR Code cannot be decoded by the authenticator or you have selected manual procedure, than the authenticator presents a text field where the key shall be provided. The key is visible on the right side of the QR Code (a string of 32 alphanumeric characters).

---

*NOTE: You cannot use more than one authenticator to access the same account. If you need to change the authenticator, read Section 6 of this manual.*

---

If the account has been added correctly, click on 'CONFIRM' button.

---

*NOTE: All accounts added to the authenticator shall display 'EU ACER' label along with the account name. If not, please contact AEGIS administrator.*

---

The TERMINAL application will verify and register the authenticator presenting the windows as on Figure 2.

---

<sup>2</sup> It could be also a button 'add account', 'pair a service' or similar

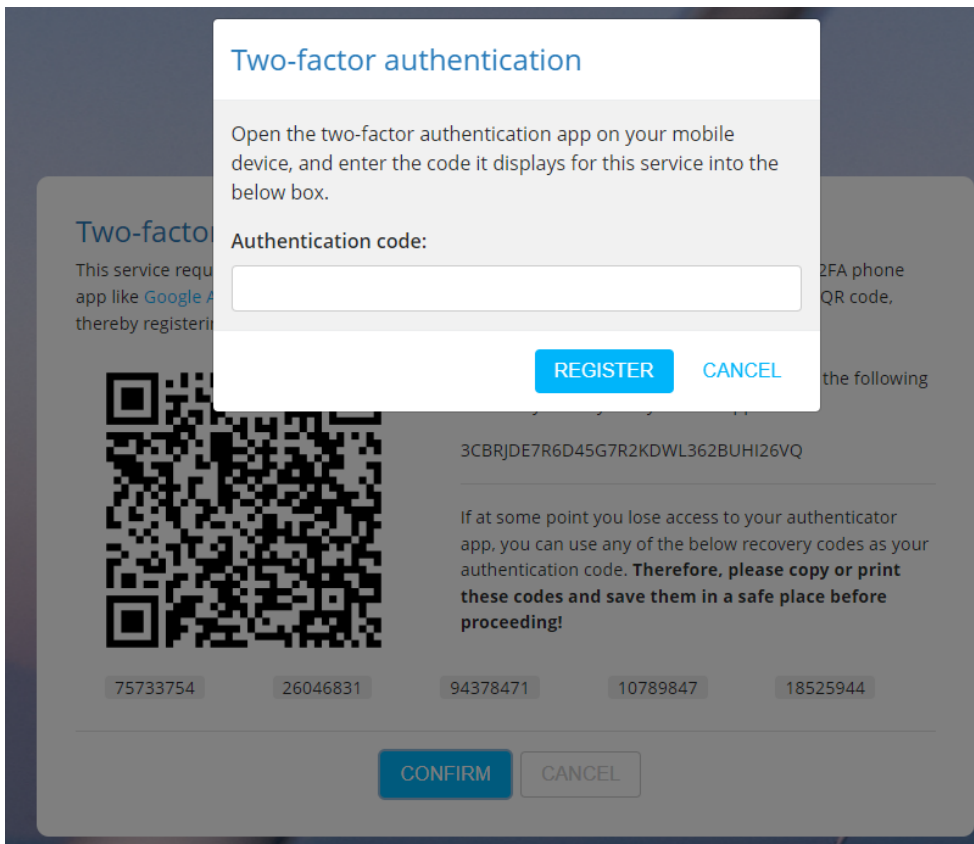


Figure 2. Authenticator registration window

In the 'Authentication code' field, enter a code that is at this moment displayed at the authenticator on your phone.

---

*NOTE: Codes are presented and valid only through a short time frame (typically 15-20 seconds). After the time elapses, a new code is generated. The time remaining is typically displayed in some graphical form on the authenticator. If you use a code that invalidates in few seconds, you may not provide the code in a due time – in such case wait for the generation of a new code.*

---

After you provide the code, click on 'REGISTER' button. The authenticator initialization is over and you will be moved to the login authorization window (see next Section).

---

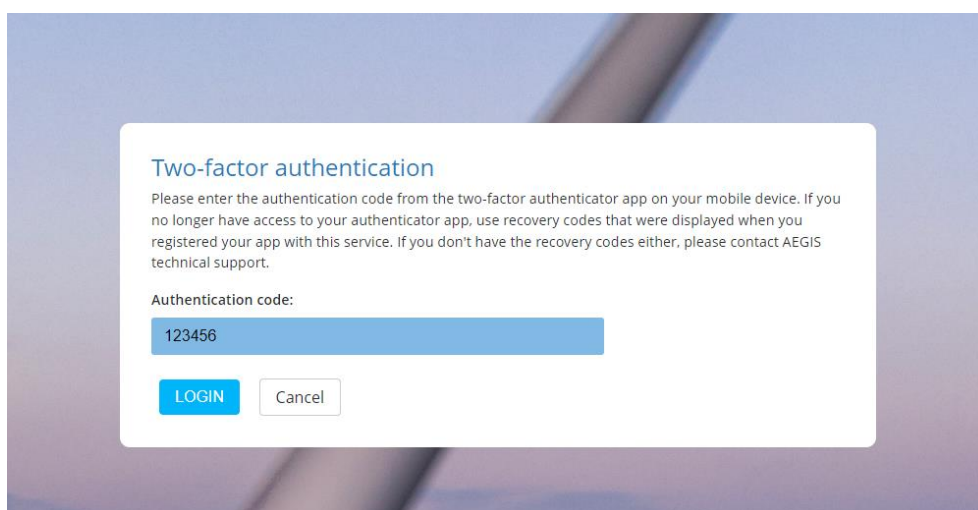
*IMPORTANT: After successful initialization of the authenticator, the login authentication window is presented immediately. You cannot use the same code to login as you used for authenticator initialization! Please wait for another code to be generated.*

---



## 5 Logging with 2FA to the TERMINAL

If your authenticator has been initialized or you are accessing the TERMINAL once again after entering your username and password on AEGIS main page, after clicking on the TERMINAL tile, the following window will be presented (see Figure 3).



**Two-factor authentication**

Please enter the authentication code from the two-factor authenticator app on your mobile device. If you no longer have access to your authenticator app, use recovery codes that were displayed when you registered your app with this service. If you don't have the recovery codes either, please contact AEGIS technical support.

Authentication code:

123456

**LOGIN** Cancel

*Figure 3. Login authentication by 2FA*

Open your authenticator on your phone and provide the code generated in the 'Authentication code' field. Then click on LOGIN button. If the authentication was successful, you will be redirected to the TERMINAL application.

---

*NOTE: You can use only one authenticator for your account. If you wish to change the authenticator or remove it, please consult Section 6.*

---

## 6 Removing/resetting authenticator

You can reset your authenticator registration in any moment. In particular, this procedure should be executed when:

- You lost your phone and authenticator application;
- You wish to change the authenticator application.





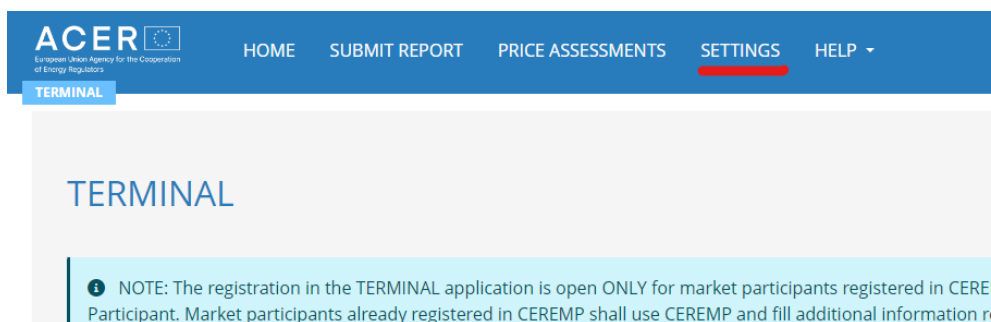
In the first case, you can login to the TERMINAL using one of five recovery codes that were presented during authentication registration (see Section 4). In the second case, please login using your current authenticator.

---

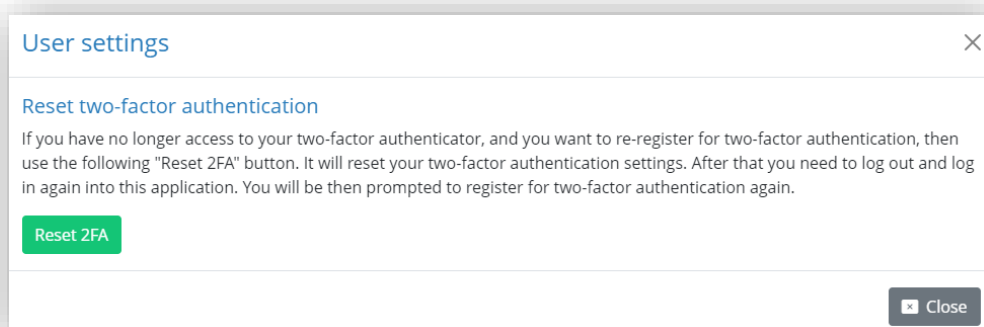
***IMPORTANT: If you lost recovery codes or you used all of them, please contact AEGIS administrator. Please note, that for security reasons, you may be required to confirm your identity.***

---

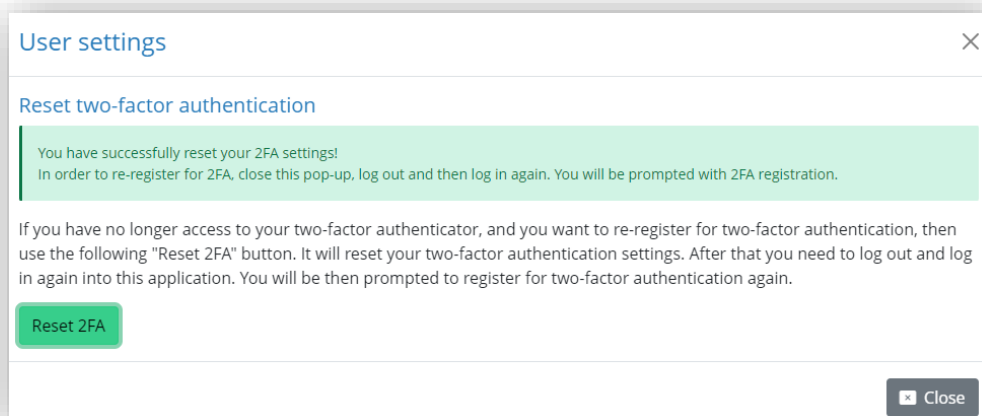
Once logged in, select SETTINGS from the menu (see Figure 4). The reset window will be displayed (Figure 5). When you press 'RESET 2FA' button the registration of your authenticator will be removed. You will be informed about success of this operation by notification as presented in Figure 6.



*Figure 4. Settings option for 2FA authenticator reset*



*Figure 5. Authenticator reset window*



*Figure 6. Message when the authenticator registration has been removed successfully*

If you are changing the authenticator, please remove also the account related to TERMINAL in the old authenticator. Removal of the association depends on the authenticator application, in most cases it is an option denoted with trash bin icon or 'Delete' button while editing account details in the authenticator application.

In case of any problems with the procedure, please contact AEGIS administrators.

## 7 Additional information

All questions related to the 2FA used for the access to the TERMINAL application shall be submitted to [aegis.admin@acer.europa.eu](mailto:aegis.admin@acer.europa.eu)

### **Authenticator applications:**

Google Authenticator (IOS)

<https://apps.apple.com/us/app/google-authenticator/id388497605>

Google Authenticator (Android)

<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2>

Microsoft Authenticator (IOS)

<https://apps.apple.com/us/app/microsoft-authenticator/id983156458>

Microsoft Authenticator (Android)

<https://play.google.com/store/apps/details?id=com.azure.authenticator>



