

Pepita Group Zrt. – Password Management Admin Policy

1. Introduction to the Two-Factor Authentication (2FA) System

1.1 Purpose of Introducing 2FA

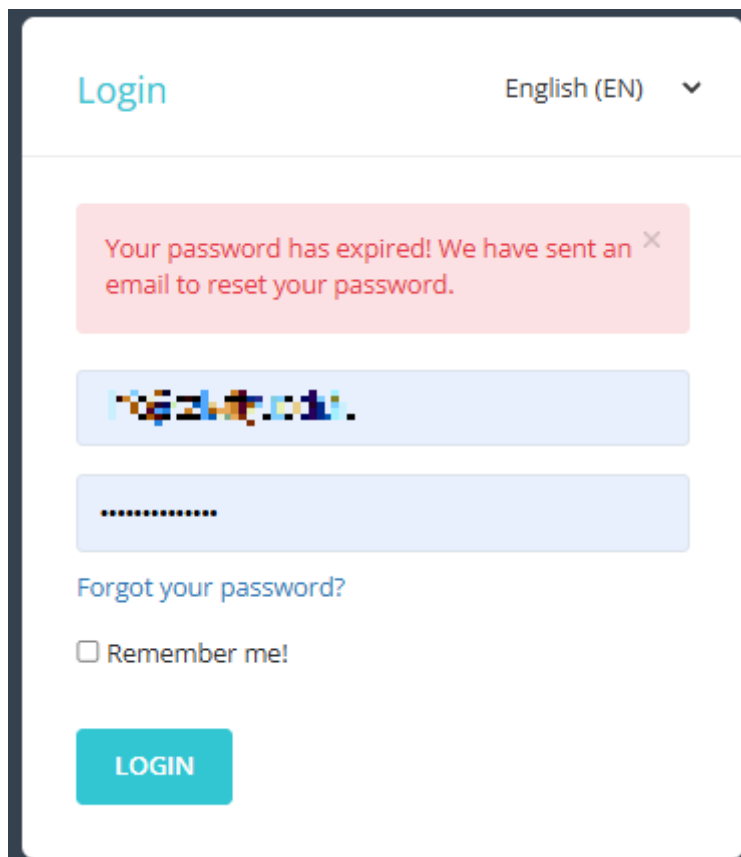
To enhance system security, two-factor authentication (2FA) is being introduced. Its purpose is to ensure that access to user accounts is protected not only by a password but also by a second layer of authentication.

1.2 Password Validity and Change

Currently used passwords will remain valid until May 15, 2026. After this date, the system will no longer accept old passwords, making password changes mandatory. Password changes can also be completed optionally before the deadline.

1.3 Handling Expired Passwords

If a password has expired, the user will receive an error message upon login indicating that a new password must be set. In this case, the system will provide guidance on how to change the password.



The screenshot shows a login interface with the following elements:

- Top left: "Login" text in blue.
- Top right: "English (EN)" with a dropdown arrow.
- Center: A red error message box with a close icon (X) that reads: "Your password has expired! We have sent an email to reset your password."
- Below the error: A blue input field containing a blurred password.
- Below that: A blue input field with a masked password (dots).
- Below the masked password: A blue link that says "Forgot your password?".
- Below the link: A checkbox labeled "Remember me!".
- At the bottom: A blue "LOGIN" button.

1.4 Password Requirements in the New System

New passwords must meet the following security requirements:

- Must be at least 12 characters long
- Must not exceed 64 characters
- Must include both lowercase and uppercase letters

- Must include at least one number
- Must include at least one symbol (e.g., #, \$, @, _)
- Must not contain the same character repeated three times consecutively
- Must not contain the local part of the user's email address
- Must not be the same as any of the last 5 previously used passwords

1.5 Password Validity with 2FA Enabled

If the user enables two-factor authentication (2FA), the password validity period will be extended to 1 year.

2. Enabling Two-Factor Authentication (2FA)

To ensure a higher level of security, we recommend that our partners enable two-factor authentication.

2.1 Accessing 2FA Activation

After logging in, navigate to the Users menu in the sidebar, then select the Two-Factor Authentication tab.

Click the "Enable Two-Factor Authentication" button to begin activation.


TWO-FACTOR AUTHENTICATION (2FA)

Status:
Disabled


Two-factor authentication (2FA) increases your account security by adding an additional security step to your login process.


One-Time Password (OTP) Allowed:
Disabled

One-time password (OTP) allows you to receive login codes via email instead of using 2FA.

 **What is the email code?**


This is an alternative login method. If you cannot use the authenticator app, you can receive the login code via email. This is especially useful if you do not have your phone with you.

 **Enable OTP**

 **What happens when you enable it?**

When you click the enable button, you will receive a QR code that you need to scan with an authenticator app. After that, you will need a 6-digit code from the app every time you log in.

Available apps: Google Authenticator, Microsoft Authenticator, Authy or any other TOTP-compatible authenticator app.

 **Enable Two-Factor Authentication**

2.2 Redirect to Activation Interface

After clicking the button, the system will automatically redirect you to the activation interface where the 2FA setup can be completed.

TWO-FACTOR AUTHENTICATION

Step 1

Install a compatible app on your mobile, such as **Google Authenticator**.



Available apps:

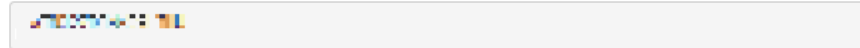
You can use any TOTP-compatible authenticator app, for example: Google Authenticator, Microsoft Authenticator, Authy, or any similar app.

Step 2

Scan the following QR code in the app:



Alternatively, enter the following secret key in the application



Step 3

Enter your 2FA code generated by your application

Submit

2.3 Required Application

An authenticator application is required for activation. For example, the Microsoft Authenticator app can be used, available for both Android and iOS devices.

2.4 Scanning QR Code and Entering Code

Scan the QR code displayed on the activation screen using the authenticator app.

After successful scanning, the app will generate a 6-digit security code.

Enter this code into the appropriate field and click "Submit" to finalize the activation of two-factor authentication.

2.5 Note on Interrupted 2FA Activation Process

If the 2FA activation process is interrupted for any reason, the process is not lost.

2.6 Restrictions and Recovery for 2FA

Once two-factor authentication has been enabled, it cannot be disabled. The system only allows deletion of the secret key used for 2FA.

⚠ What is the reset for?

If you have lost access to your authenticator app, or want to set it up on a new device, use this button. You will receive a new QR code that you need to scan in the app again.

 [Reset Two-Factor Authentication](#)



If the user loses access to the authenticator application (e.g., due to device change or app deletion), access recovery must be handled through customer support.

After resetting the secret key, customer support will allow the user to register a new device or reactivate two-factor authentication.

After logging out and logging back in, the user will have the opportunity to complete the activation process again by following the previously described steps.


TWO-FACTOR AUTHENTICATION ×

Step 1 Install a compatible app on your mobile, such as **Google Authenticator**.

Available apps:
You can use any TOTP-compatible authenticator app, for example: Google Authenticator, Microsoft Authenticator, Authy, or any similar app.

Step 2 Scan the following QR code in the app:



Alternatively, enter the following secret key in the application

Step 3 Enter your 2FA code generated by your application

3. Use of One-Time Password (OTP)

3.1 Enabling One-Time Password

The OTP function is available under the Two-Factor Authentication tab. It can be activated by selecting the appropriate option.

3.2 Requirement for OTP Usage

OTP can only be used together with two-factor authentication (2FA). It is not available as a standalone login method without 2FA enabled.

3.3 How OTP Works

OTP allows users to authenticate during login using a one-time code instead of an authenticator application.

3.4 Sending and Using the Code

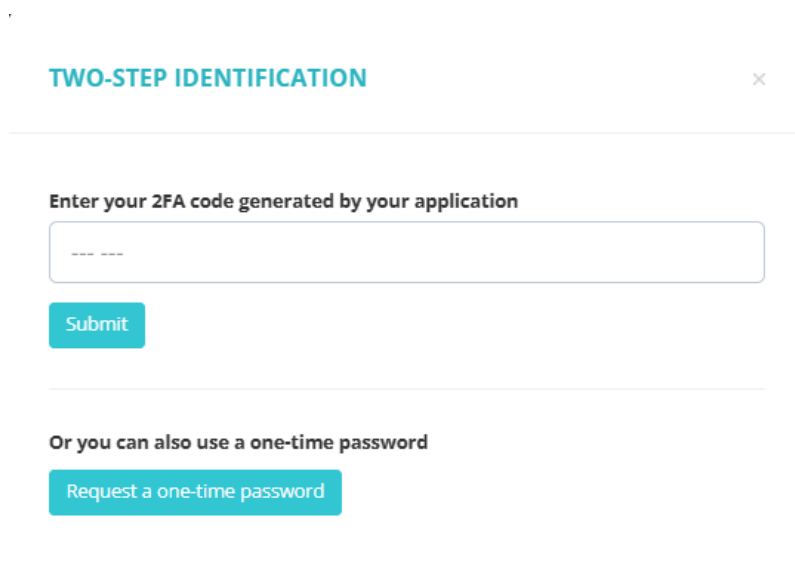
During login, the system sends a one-time security code to the user's registered email address. By entering the received code, the user can successfully log in to the system.

4. Logging into the Account Using 2FA

4.1 Initiating Login Process

After entering a valid username and password and clicking the "Login" button, an additional authentication panel will appear.

This panel contains a field for entering a 6-digit security code and a button labeled "Request One-Time Password."



The screenshot shows a modal window titled "TWO-STEP IDENTIFICATION" with a close button (x) in the top right corner. Below the title, there is a text prompt: "Enter your 2FA code generated by your application". Underneath this prompt is a text input field containing six dashes (----). Below the input field is a teal "Submit" button. A horizontal line separates this section from the next. Below the line, there is another text prompt: "Or you can also use a one-time password". Underneath this prompt is a teal button labeled "Request a one-time password".

4.2 Login with Authenticator Application

Enter the 6-digit code displayed in the authenticator application into the appropriate field. Click "Submit" to successfully log in if the code is correct.

Enter your 2FA code generated by your application

4.3 Login with One-Time Password (OTP)

Clicking the “Request One-Time Password” button will update the interface and display a new input field.

Enter the 6-digit code received via email into this field.

After entering the code, click “Submit” to complete login if the code is correct.

Or you can also use a one-time password

The code you received in the email:

4.4 Requesting a New One-Time Code

If a new code is needed (e.g., the previous one expired or was not received), click the “Request New Code” button to receive a new one-time password.