

Колибри ERP – двуфакторна автентикация

В Колибри ERP е имплементирана двуфакторна автентикация (2FA) чрез еднократни времеви пароли (Time based One Time Password).

На потребителите, за които е включена двуфакторна автентикация, след успешна автентикация с име и парола се изисква и допълнителна автентикация (второ ниво) с код, който се генерира от автентикаращо приложение, като например Authenticator, Authy, FreeOTP.

Успешната автентикация към системата се осъществява само след правилно въведен авторизационен код.

Авторизационните кодове са динамични и се генерират на всеки 30 секунди. Тоест всеки код е валиден само за 30 секунди.

Настройка на двуфакторна автентикация (2FA)

Включването на 2FA се извършва от администратор след отбелязване в данните за потребителя „Изискване за двуфакторна автентикация“.

ПОТРЕБИТЕЛИ

Списък	Редактиране	Групи	Номерации	Действия	Документи	Полета	Складове	Цени	Маркери	Сметки
--------	-------------	-------	-----------	----------	-----------	--------	----------	------	---------	--------

Основни данни за потребителя

Име (Login)	<input type="text"/>	Статус	Активен (1)
Парола	<input type="password"/>	Повтори парола	<input type="password"/>
Пълно име (bg)	<input type="text"/>	Инициали (bg)	<input type="text"/>
(en)	<input type="text"/>	(en)	<input type="text"/>

[Системни параметри](#)

Контрол на достъпа	Допълнителни данни	Имейл настройки	Копиране	Профили
--------------------	--------------------	-----------------	----------	---------

Контрол на достъпа

<input checked="" type="checkbox"/> Валиден потребител	Вид	Потребител
<input checked="" type="checkbox"/> Интерактивен	<input type="checkbox"/> Web services	

Двуфакторна автентикация

<input checked="" type="checkbox"/> Изисква се временна парола (TOTP)
<input type="checkbox"/> Установена проверка с временна парола

Ключ

Завършването на процеса по установяване на 2FA става с процеса на първоначално автентикиране към системата.

Първоначална двуфакторна автентикация

След включване на изискването за двуфакторна автентикация на потребителя всяка следваща автентикация ще изисква въвеждането на еднократната временна парола.

При първоначалното установяване на 2FA от потребителя трябва да се инсталира ключът за криптиране в избраното приложение за автентикация (например Google Authenticator, Authy или FreeOTP). Приложението обичайно се инсталира на мобилно устройство – Smart Phone.

1. Инсталиране на мобилно устройство на подходящ автентикатор (Google Authenticator, Authy или FreeOTP). В примерите ще бъде разгледано приложението FreeOTP.
2. Инсталиране на ключа за криптиране, генериран от Колибри ERP, в приложението за автентикация, става чрез сканиране на QR кода (или в редки случаи ръчно въвеждане на ключа).
3. Въвеждане на кода за автентикация генериран от приложението в Колибри ERP.

Стъпките при първоначална двуфакторна автентикация са илюстрирани с екранни снимки по-долу.

Автентикация с еднократна времева парола

QR код



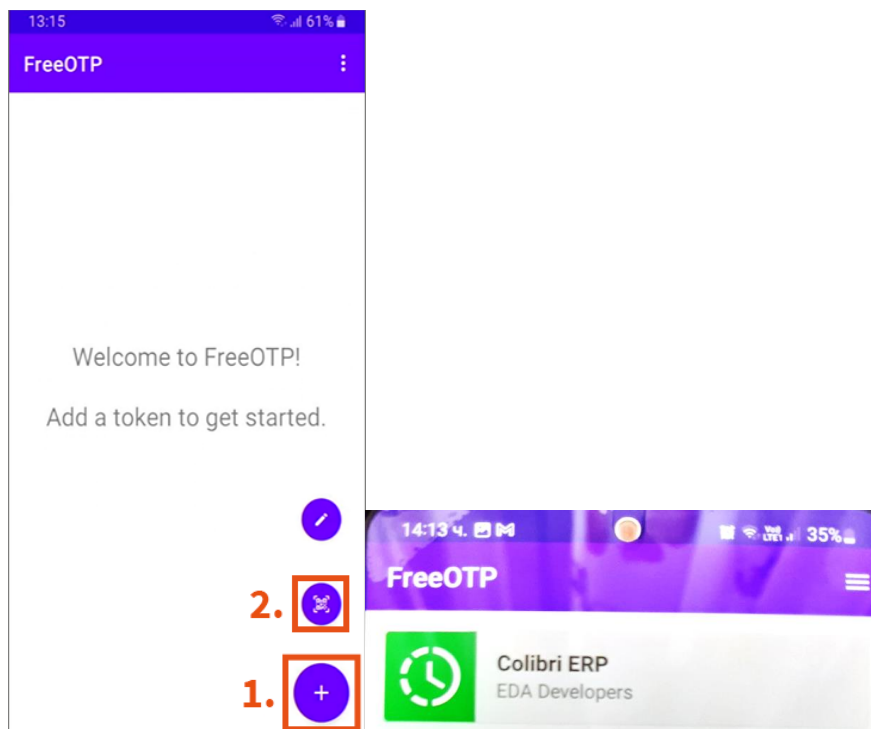
Ключ

Период (секунди)

Въведете код

Вход

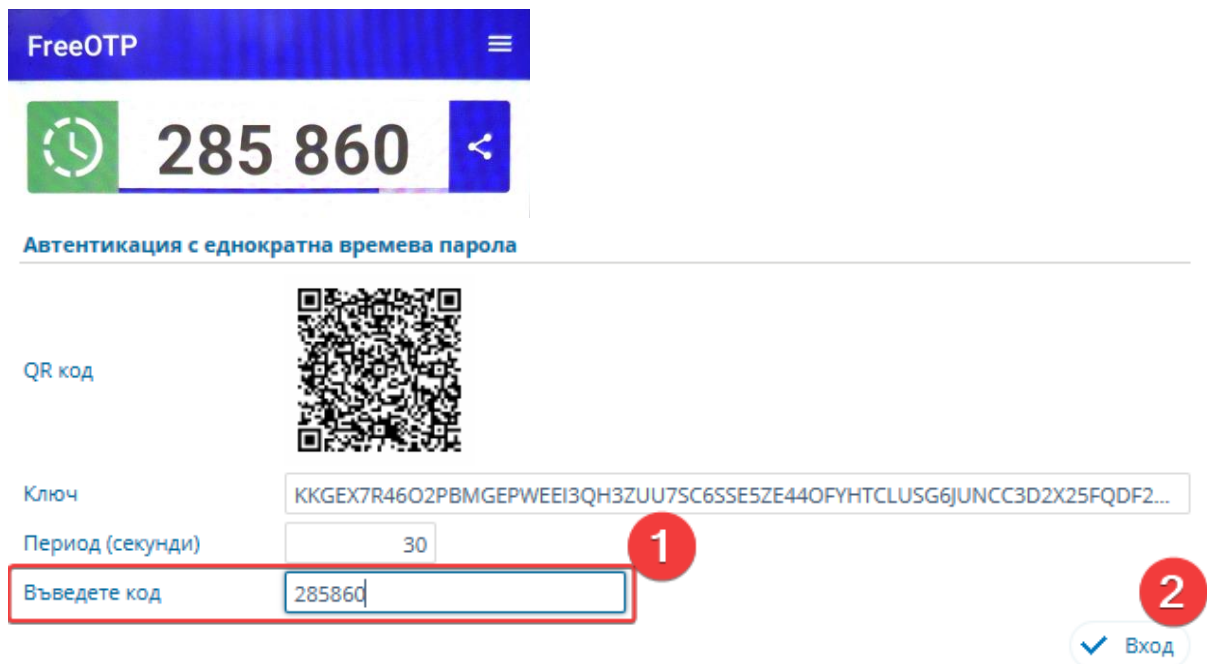
Фигура 1 Първоначална автентикация и екран с информация за инсталиране на ключа в приложението за автентикация.



Фигура 2 Добавяне на ключ към FreeOTP чрез сканиране на QR код и визуализация след успешно инсталиране.

Инсталирането на ключа става чрез сканиране на QR кода визуализиран от Колибри ERP.

При успешна инсталация на ключа се визуализира в списъка с удостоверения и можете да получите кодове чрез избор (tap/click) на удостоверителя.



The screenshot shows the FreeOTP application interface. At the top, there is a blue header with 'FreeOTP' and a menu icon. Below the header, there is a green clock icon, a large display showing the number '285 860', and a back arrow icon. Underneath, the text 'Автентикация с еднократна времева парола' is displayed. The main area contains a QR code labeled 'QR код', a key labeled 'Ключ' with the value 'KKGEX7R46O2PBMGEPWEEI3QH3ZUU7SC6SSE5ZE44OFYHTCLUSG6JUNCC3D2X25FQDF2...', and a period labeled 'Период (секунди)' set to '30'. A red box highlights the 'Въведете код' input field containing '285860', with a red circle '1' next to it. To the right, there is a 'Вход' button with a checkmark and a red circle '2' next to it.

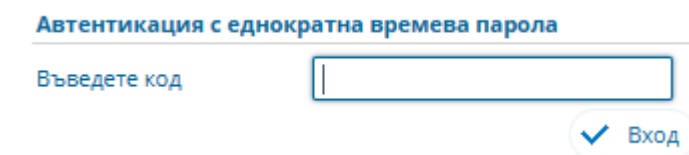
Фигура 3 Въвеждане на временния код за автентикация.

След успешна проверка на кода в Колибри ERP, автентикацията е успешна. В противен случай, системата изисква повторно въвеждане на код.

Важно: Имайте в предвид, че всеки код е валиден само за 30 секунди.

Двуфакторна автентикация след установяване на първоначалната

При успешно преминал процес на първоначална автентикация, за всяка следваща автентикация се изисква само временния код за достъп.



The screenshot shows the FreeOTP application interface after the initial setup. It features the text 'Автентикация с еднократна времева парола' and a 'Въведете код' input field. Below the input field is a 'Вход' button with a checkmark.

Фигура 4 Двуфакторна автентикация след установена първоначална.

Управление на двуфакторната автентикация от профила на потребителя

В зависимост от установената глобална настройка на системата, потребители сами могат да включват и изключват двуфакторната автентикация за своя акаунт, ако това е разрешено.

В профила на потребителя има нова секция „Двуфакторна автентикация“, в която потребителя може да извършва следното:

- Включва/изключва двуфакторната автентикация;
- Инсталира ключа за автентикация в приложението за автентикация;
- Генериране на нов ключ за автентикация.

Настройки
Профил

ПРОФИЛ


Профил | Документи | Имейл настройки

Потребител: Група:

Клон / обект:

Параметри | Съхранени настройки | Смяна на парола | **Двуфакторна автентикация** | Смяна на профил

Изисква се временна парола (TOTP)
 Установена проверка с временна парола

QR код: 

Ключ:

Период (секунди):

[Заяви нов ключ](#)

Фигура 5 Управление на двуфакторната автентикация от профила на потребителя.

Двуфакторна автентикация при работа с повече от една база данни

При включване на двуфакторната автентикация в една от базите данни, достъпни за потребителя, автоматично се включва във всички останали и се синхронизира при всяка промяна на ключа.

Изключването на двуфакторната автентикация може да се осъществи само чрез изключването последователно във всички бази данни достъпни от потребителя. В противен случай, тя автоматично ще се установява отново.