

การตั้งค่าการยืนยันตัวตนแบบสองขั้นตอน (2FA)

เพื่อช่วยรักษาความปลอดภัยของบัญชี การยืนยันตัวตนแบบสองขั้นตอน (2FA) จะต้องใช้เมื่อเข้าถึง Client Area

ครั้งแรกที่ผู้ใช้เข้าสู่ระบบหลังเปิดการใช้งาน 2FA ผู้ใช้จะได้รับคำแนะนำผ่านกระบวนการตั้งค่าครั้งเดียว เมื่อเสร็จสิ้น จะต้องใช้แอปยืนยันตัวตนของผู้ใช้เพื่อยืนยันตัวตนทุกครั้งที่จะเข้าสู่ระบบ

ก่อนเริ่ม

หากผู้ใช้ยังไม่มีแอปพลิเคชันยืนยันตัวตน โปรดทำการติดตั้งบนโทรศัพท์มือถือ

สามารถใช้แอปพลิเคชันยืนยันตัวตนที่เข้ากันได้กับ TOTP ทุกแอปพลิเคชัน

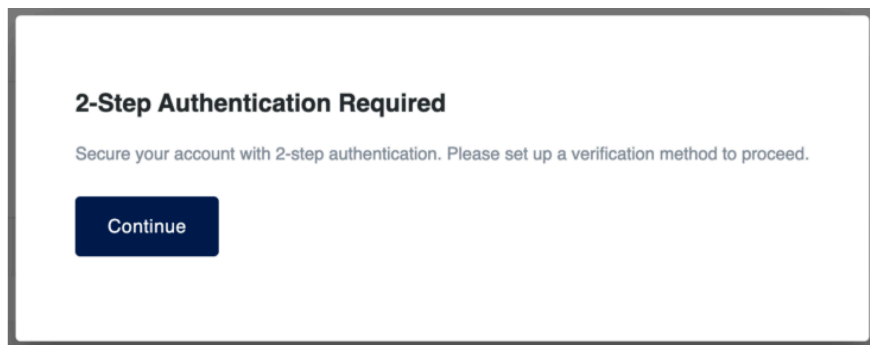
รวมถึง:

- Google Authenticator
- Microsoft Authenticator
- แอปพลิเคชันยืนยันตัวตนอื่นๆ ที่เข้ากันได้ ซึ่งมีให้ดาวน์โหลดฟรีจาก App Store หรือ Google Play

Step 1 - การเริ่มตั้งค่า

หลังจากเข้าสู่ client area ผู้ใช้จะเห็น **"2-step authentication required"**

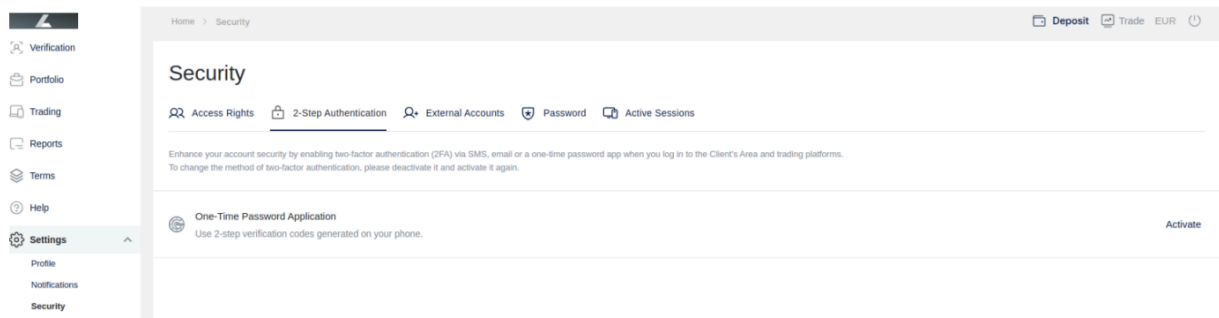
คลิก **ดำเนินการต่อ** เพื่อเริ่มต้นขั้นตอนการตั้งค่า



Step 2 - เปิดหน้าการเปิดใช้งาน

จะถูกนำไปที่: หน้าตั้งค่า → ความปลอดภัย → การยืนยันตัวตนแบบ 2 ขั้นตอน

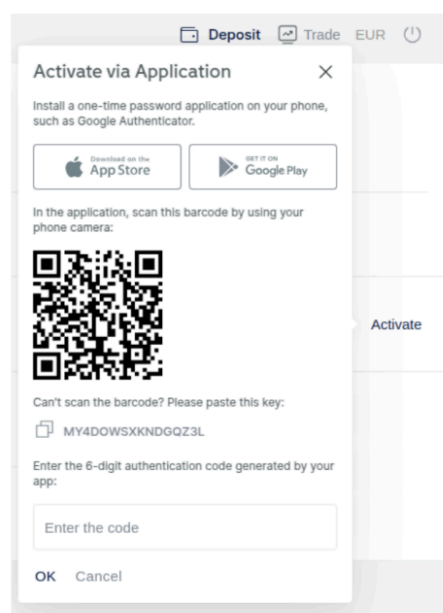
อยู่ถัดจาก **One-Time Password Application** คลิกที่ **Active** เพื่อเปิดใช้งาน



Step 3 - เชื่อมต่อแอปยืนยันตัวตน

ในแอป “**Activate via Application**”

1. เปิดแอปพลิเคชันยืนยันตัวตนบนโทรศัพท์มือถือ
2. สแกนคิวอาร์โค้ดที่แสดงบนหน้าจอ
3. ถ้าไม่สามารถสแกนได้ เลือกป้อนคีย์โค้ดตั้งค่า (หรือตัวเลือกที่คล้ายกัน) ในแอป และป้อนคีย์ตั้งค่าที่แสดงอยู่ใต้รหัส QR ด้านล่าง
4. แอปจะสร้างรหัสยืนยัน 6 หลัก ที่รีเฟรชทุก 30 วินาที
5. คีย์รหัสปัจจุบันใน**ช่องใส่รหัส** แล้วคลิก **OK**



ตั้งค่าเสร็จสิ้น

การยืนยันตัวตนแบบสองขั้นตอนเปิดใช้งานแล้ว

หลังจากนี้ ทุกครั้งที่เข้าสู่ client's area ผู้ใช้จะถูกขอให้ใส่รหัสผ่าน 6 หลัก ปัจจุบันจากแอปยืนยันตัว

ขั้นตอนการยืนยันเพิ่มเติมนี้ช่วยปกป้องบัญชีของผู้ใช้ โดยการตรวจสอบให้แน่ใจว่ามีเพียงผู้ใช้เท่านั้นที่สามารถเข้าถึงได้ แม้ว่าจะมีคนอื่นรู้รหัสผ่านก็ตาม