



มหาวิทยาลัยมหิดล
วิทยาเขตแพะดะ



คู่มือขั้นตอนการใช้งาน 2-Factor Authentication สำหรับ VPN



📍 กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล

☎ โทรศัพท์ 02-849-6022

🌐 <https://muit.mahidol.ac.th/>



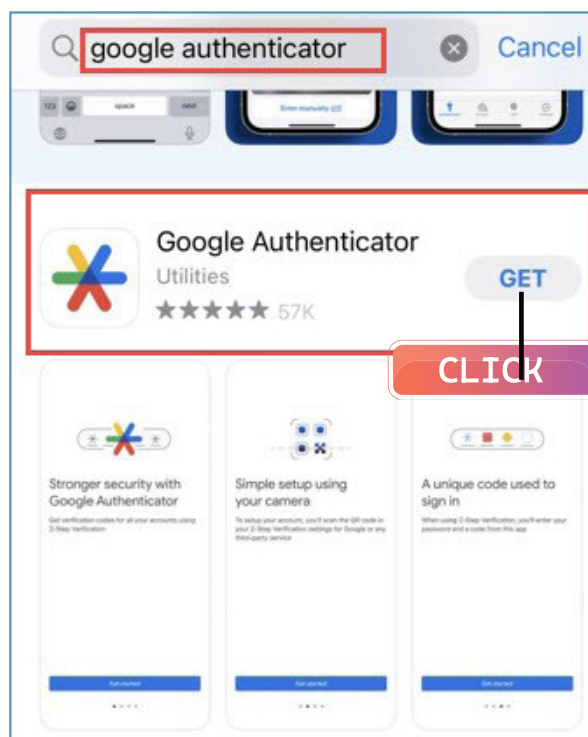
ขั้นตอนการใช้งาน 2-Factor Authentication สำหรับ VPN

ก่อนเริ่มใช้งาน 2-Factor Authentication (2FA) จำเป็นต้องดาวน์โหลดและติดตั้งแอปพลิเคชัน Authenticator ไว้บนอุปกรณ์สมาร์ตโฟนที่ต้องการทำการยืนยันตัวตนแบบ 2 ขั้นตอน ซึ่งจะมีให้เลือกใช้ได้หลาย Application เช่น Authy, Google Authenticator, Microsoft Authenticator, ฯลฯ โดยในคู่มือนี้จะยกตัวอย่างการใช้งานจากแอป Google Authenticator



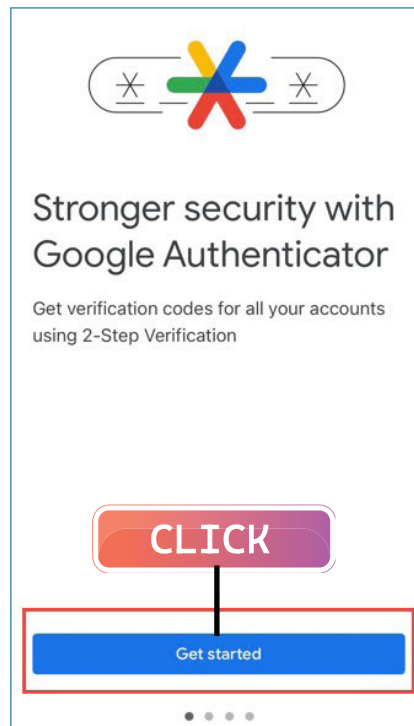
วิธีการติดตั้งแอปพลิเคชัน และตั้งค่า VPN สำหรับใช้งาน 2-Factor Authentication

1. ทำการติดตั้ง Application “Google Authenticator” จาก App Store (Iphone) หรือ Google Play Store (Android) บนอุปกรณ์สื่อสาร โทรศัพท์มือถือ หรือ Tablet



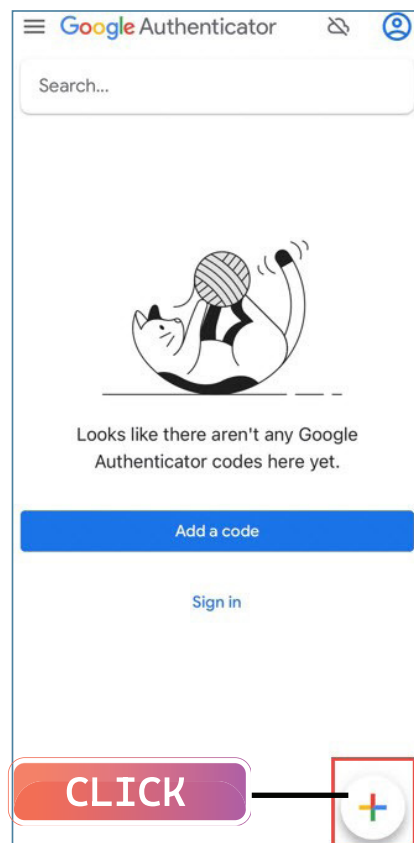
ภาพประกอบที่ 1 การติดตั้ง Application “Google Authenticator”

2. ทำการเปิด **Application Google Authenticator** เพื่อเริ่มต้นใช้งานตามรูปที่2



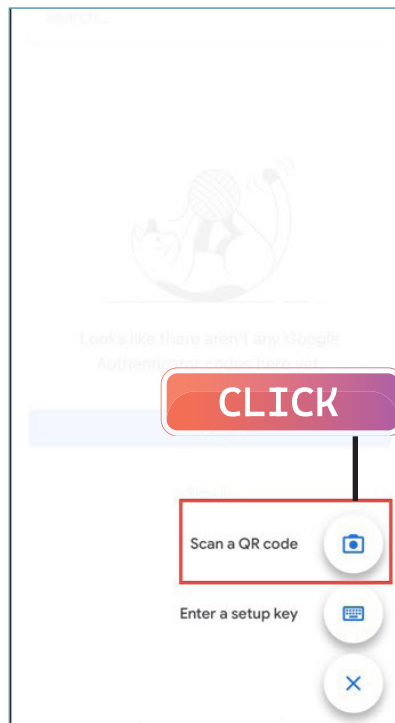
ภาพประกอบที่ 2 เปิด Application Google Authenticator

3. กดเครื่องหมาย “+” เพื่อทำการเพิ่มการยืนยันตัวตน สำหรับ VPN ตามรูปที่3



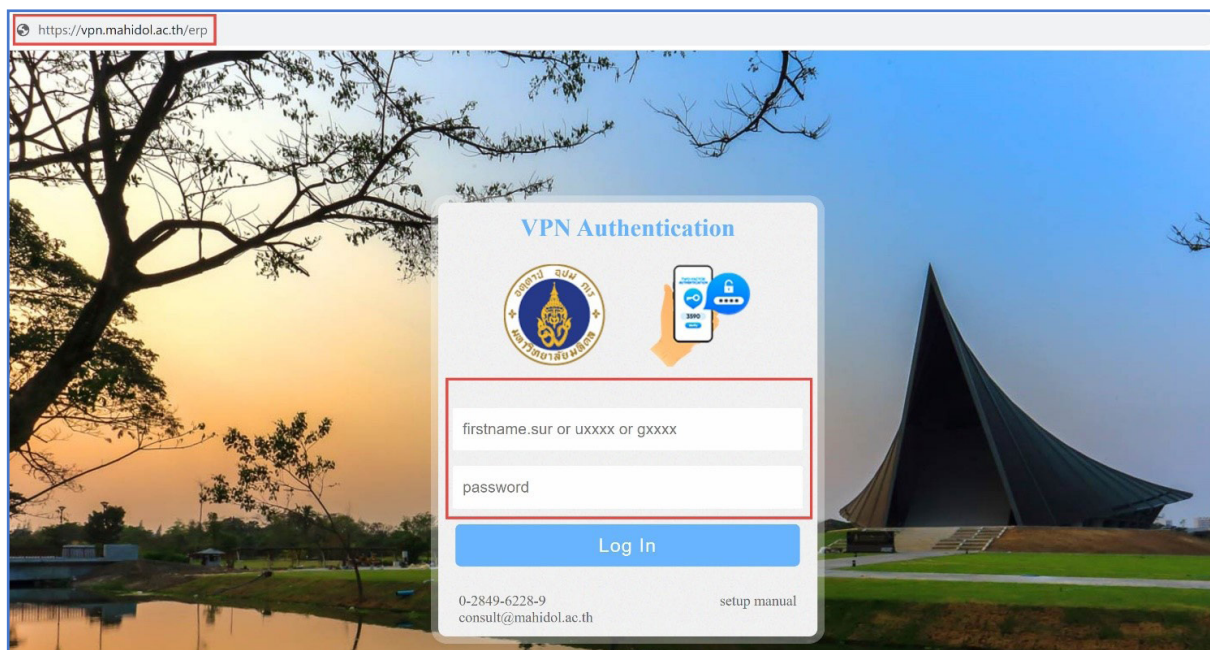
ภาพประกอบที่ 3 เพิ่มการยืนยันตัวตน

4. กดปุ่ม **“Scan QR Code”** เพื่อเริ่มทำการ scan QR Code เพื่อเพิ่มการยืนยันตัวตนสำหรับ VPN ตามรูปที่ 4



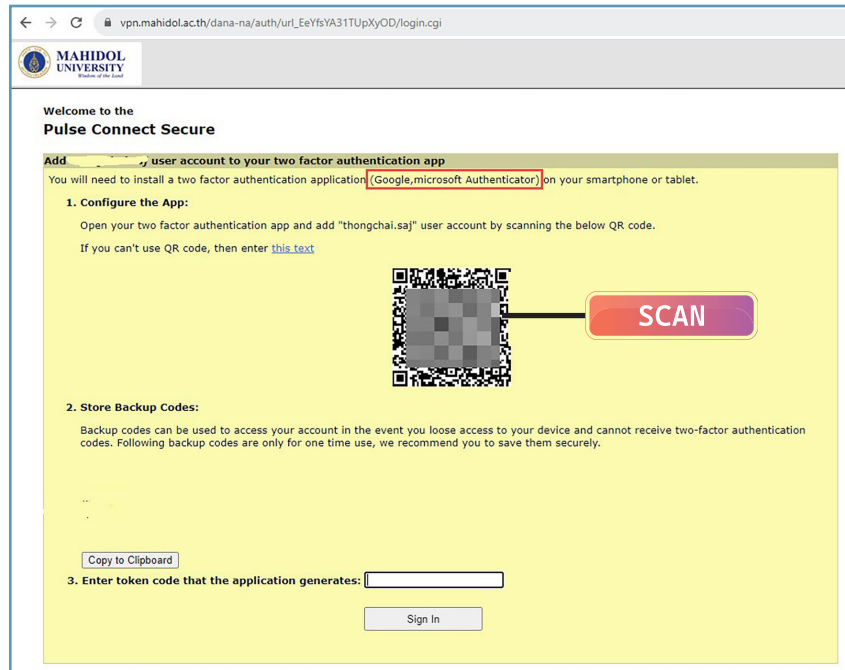
ภาพประกอบที่ 4 เพิ่มการยืนยันตัวตนสำหรับ VPN

5. ทำการเข้าใช้งาน VPN บนเครื่องคอมพิวเตอร์ ด้วย Web Browser (เช่น Google Chrome) โดยเข้าไปที่ **“<https://vpn.mahidol.ac.th/erp>”** แล้วทำการ Sign In เข้าสู่ระบบด้วย **Username** และ **Password** ของมหาวิทยาลัย ดังรูปที่ 5



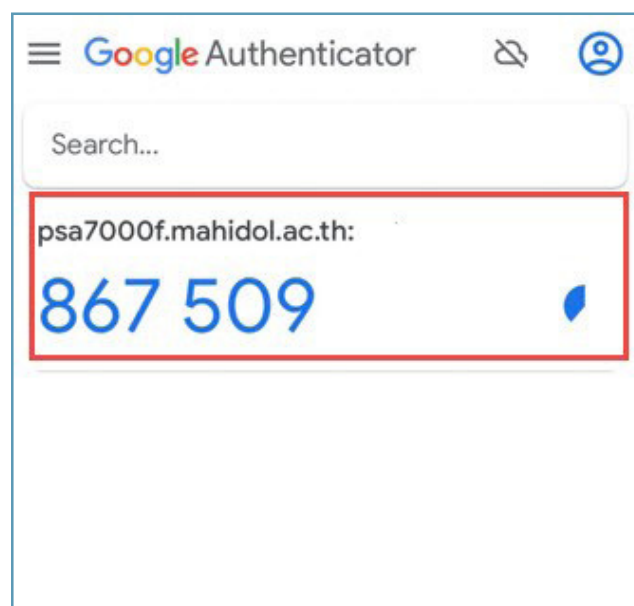
ภาพประกอบที่ 5 ไปที่ <https://vpn.mahidol.ac.th/erp> แล้ว Sign in

6. เมื่อทำการ Sign in สำเร็จ ระบบจะแสดงหน้าเว็บสำหรับลงทะเบียนเพื่อทำการเปิดใช้งาน 2-Factor Authentication ด้วย Application Authenticator โดยจะแสดง QR Code สำหรับ scan ด้วย Application Authenticator เพื่อทำการเปิดใช้งานตามรูปที่ 6



ภาพประกอบที่ 6 หน้าจอแสดง QR Code สำหรับ scan

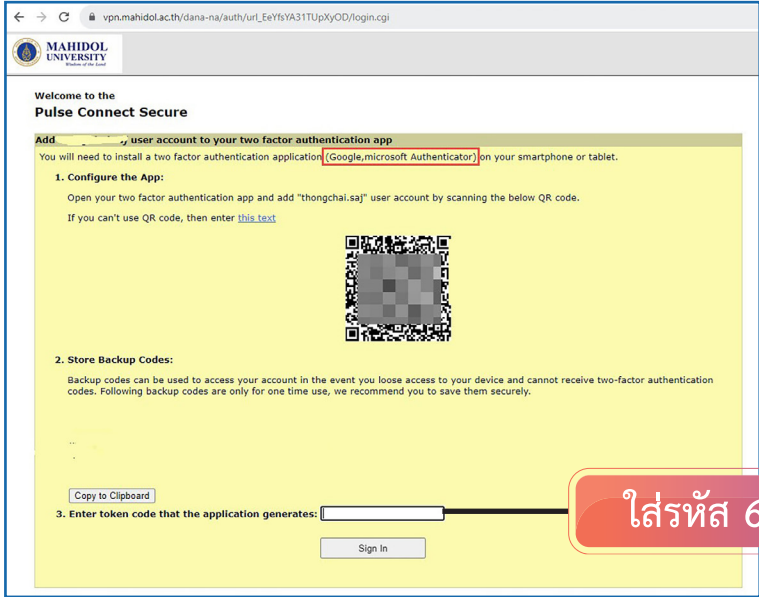
7. ทำการ Scan QR Code โดยใช้ Application Google Authenticator จากอุปกรณ์สื่อสารที่ได้ทำการติดตั้งไว้ เมื่อ Scan สำเร็จ จะขึ้นรหัสตัวเลข 6 หลัก ซึ่งรหัสนี้จะเปลี่ยนใหม่ทุก 30 วินาที (ขึ้นอยู่กับ Application Authenticator ที่ใช้) ตามรูปที่ 7



ภาพประกอบที่ 7 ตัวอย่างหน้าจอแสดงรหัสตัวเลข 6 หลัก

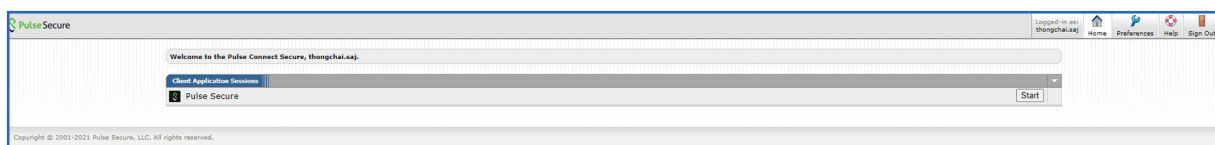


8. นำรหัส 6 หลักที่ได้จาก Application Authenticator มากรอกในหน้าเว็บไซต์บน
เครื่องคอมพิวเตอร์ (ตามขั้นตอนที่ 3) ตามรูปที่ 8 จากนั้นกด Sign In 



ภาพประกอบที่ 8 กรอกรหัส 6 หลักในหน้าเว็บไซต์ <https://vpn.mahidol.ac.th/erp>

9. เมื่อลงทะเบียนสำเร็จระบบจะแสดงหน้าจอตามรูปที่ 9 เสร็จสิ้นกระบวนการลงเบียนใช้งาน 2-Factor Authentication สามารถทำการปิดหน้าเวป หรือ Sign Out ออกจากระบบได้



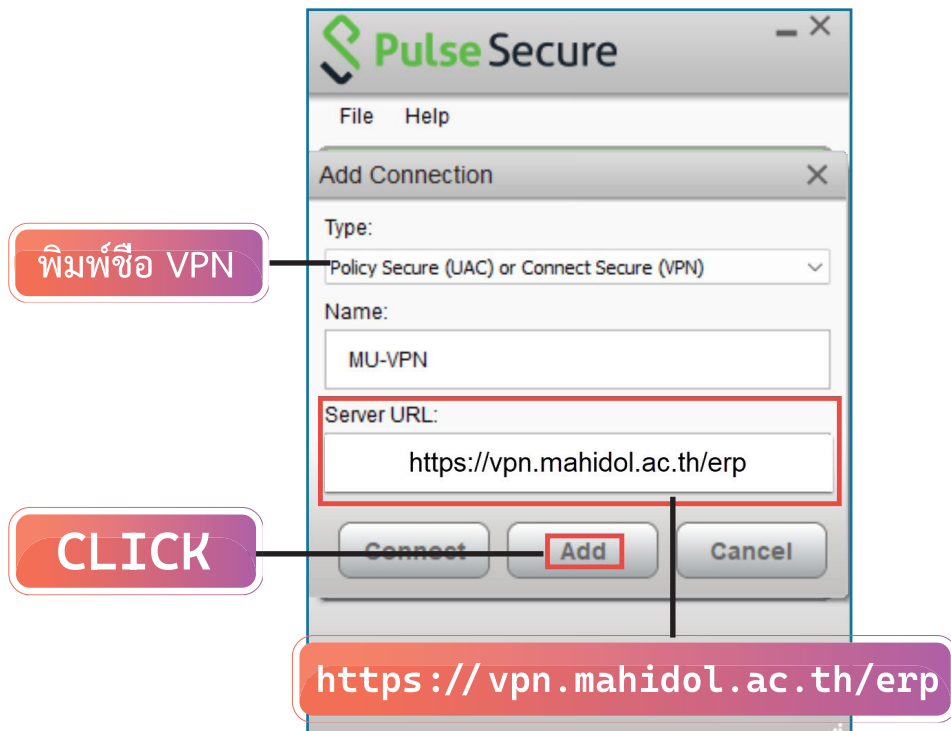
ภาพประกอบที่ 9 หน้าจอเมื่อลงเบียนใช้งาน 2-Factor Authentication สำเร็จ



ขั้นตอนการเข้าใช้งาน VPN ผ่าน Application Pulse Secure IIUU 2-Factor Authentication

1. ทำการเพิ่ม VPN Connection โดยระบุข้อมูลดังนี้ (ตามรูปที่ 10)

- **Name** : ตั้งค่าชื่อในการเชื่อมต่อ ได้ตามต้องการ (ตามตัวอย่างใช้ MU-VPN)
- **Server URL** : ระบุ <https://vpn.mahidol.ac.th/erp>



ภาพประกอบที่ 10 การเพิ่ม VPN Connection

2. เข้าใช้งาน VPN โดยการกรอก **Username** และ **Password** จากนั้นกด Connect ตามรูปที่ 11



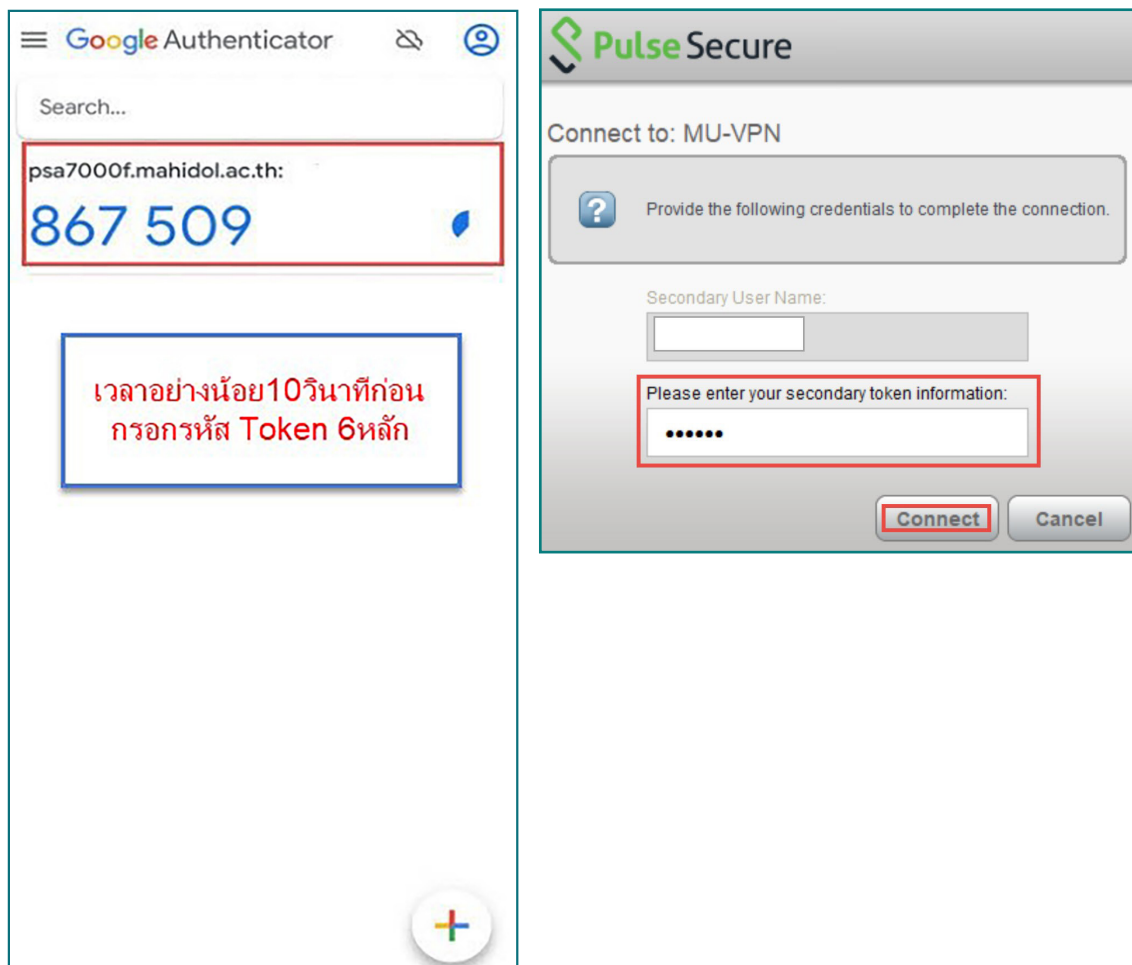
ภาพประกอบที่ 11 กรอก Username และ Password เพื่อเข้าระบบ



3. หลังจาก Login สำเร็จระบบจะแสดงหน้าให้กรอกรหัส Secondary Token (ตามรูปที่ 12) ให้ทำการเปิด Application Google Authenticator บนอุปกรณ์สื่อสารที่ได้ทำการลงทะเบียนไว้ จากนั้นนำรหัส 6 หลักบนหน้าจอ Application มากรอกในช่อง Secondary Token แล้วกด Connect

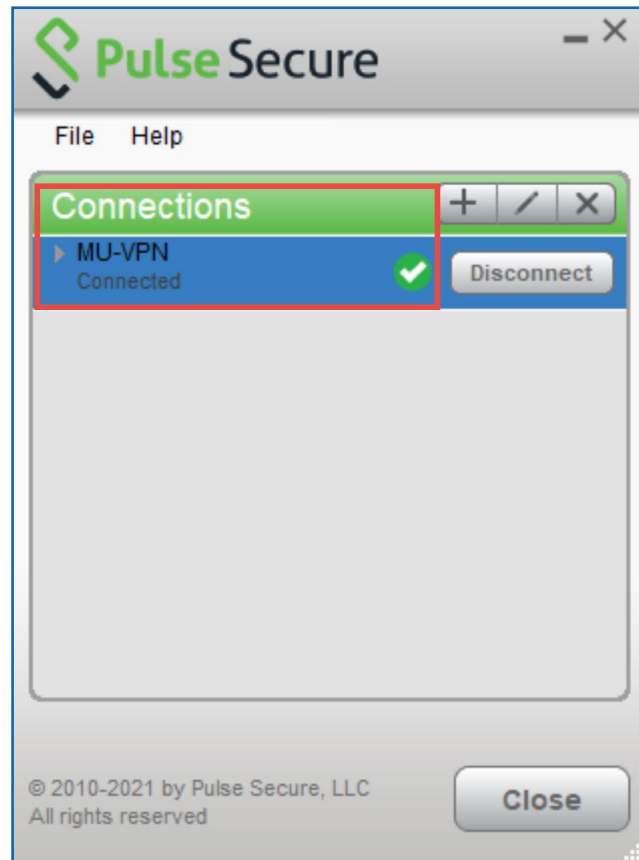
****หมายเหตุ**

- ถ้าใส่รหัสยืนยันจาก Application Authenticator ผิดเกิน 5 ครั้ง ระบบจะ Lock การใช้งาน VPN
- หากถูก Lock สามารถปลด Lock ได้ได้ที่ Email: consult@mahidol.ac.th



ภาพประกอบที่ 12 กรอกรหัส Secondary Token แล้วจะขึ้นว่า Login สำเร็จ

4. เมื่อยืนยันรหัส 6 หลัก สำเร็จ จะแสดงสถานะ Connected ตามรูปที่ 13 สามารถใช้งาน VPN ได้ตามปกติ



ภาพประกอบที่ 13 แสดงสถานะ Connected แล้วจะใช้งาน VPN ได้

ข้อจำกัดในการใช้งานระบบ VPN

1. การเชื่อมต่อ VPN 1 ครั้งสามารถใช้งานนาน สูงสุด 3 ชั่วโมง หลังจากนั้นระบบจะตัดการเชื่อมต่อโดยอัตโนมัติ
2. หากมีการเชื่อมต่อระบบ VPN ไว้ แต่ไม่มีการใช้งานเกิน 30 นาที ระบบจะตัดการเชื่อมต่อโดยอัตโนมัติ
3. หากถูกตัดการเชื่อมต่อ ต้องทำการเข้าใช้งานใหม่ พร้อมกรอกรหัส 2-FA อีกครั้ง

