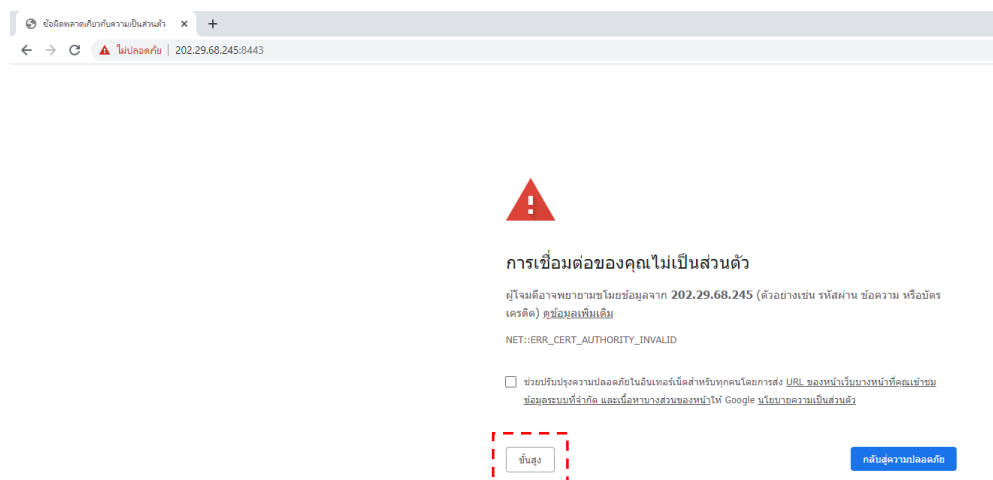


คู่มือการใช้งานระบบ VPN สถาบันเทคโนโลยีปทุมวัน

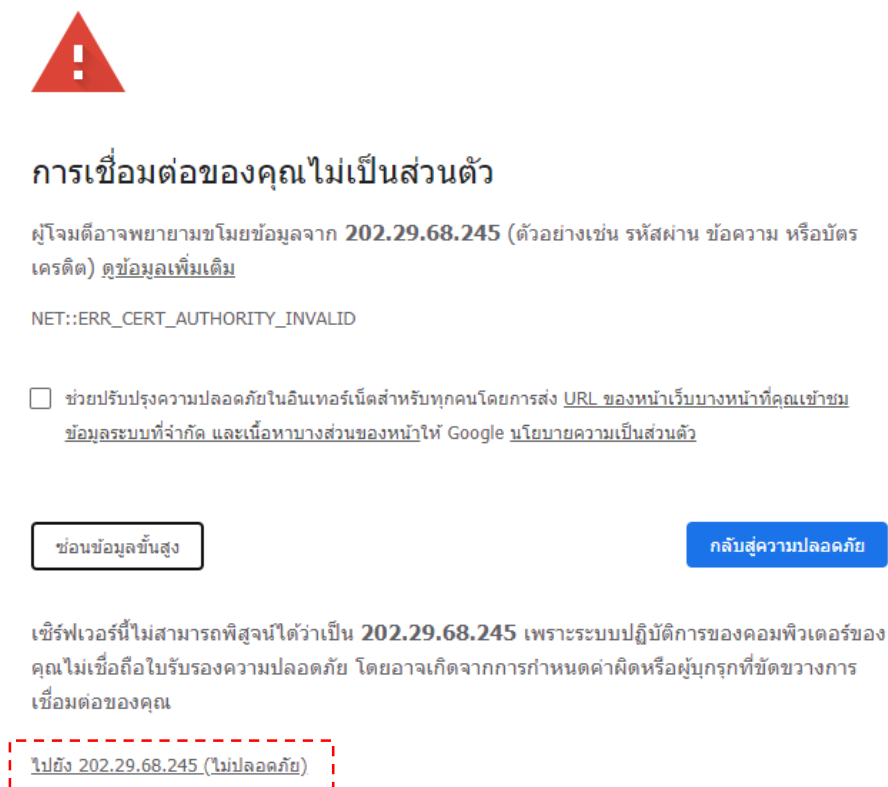
ผู้ใช้งานระบบ VPN ต้องสร้าง TOKEN ก่อนการใช้งานระบบ VPN โดยมีขั้นตอนดังนี้

1. สร้าง Token แบบ One-Time Password

1.1 เปิด Web Browser(Chrome) พิมพ์ : <https://202.29.68.245:8443> แล้วคลิกเลือกที่ “ขึ้นสูง”



1.2 คลิกที่ ไปยัง 202.29.68.245 (ไม่ปลอดภัย)



1.3 ลงชื่อเข้าใช้งาน

1.3.1 username สำหรับบุคลากร : sekxxx (username เดียวกันกับ PIT Account)

username สำหรับนักศึกษา : 6301XXXXXX (username คือรหัสประจำตัวนักศึกษา)

1.3.2 Password : รหัสผ่านเดียวกันกับ PIT Account เมื่อกรอกข้อมูลเรียบร้อยแล้วคลิก “Log in”

Enter your username and password and click Log In to authenticate.

Please sign in

Username

Password

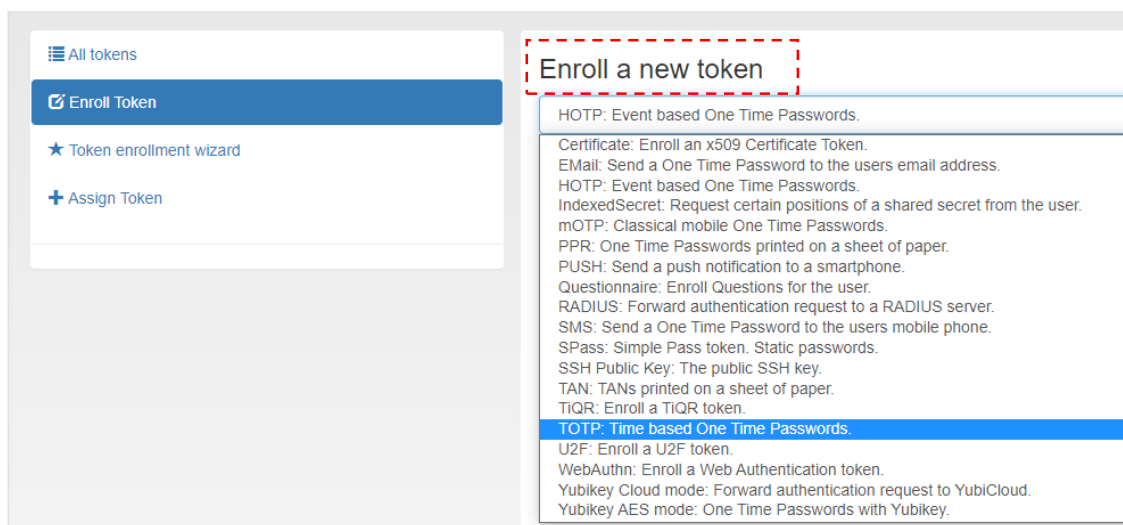
Log In

1.4 คลิกไปที่ Enroll Token (เพื่อทำการเริ่มต้นการสร้าง Token)

total tokens: 4

serial	type	active	description	failcounter
OATH0003123C	hotp	active	pakin.r	0
OATH0004EFA1	hotp	active	pakin.r	0
OATH00055E61	hotp	active	pakin.r	0
OATH0006DE1E	hotp	active	pakin.r	0

1.5 หัวข้อ Enroll a new token ให้เลือกเป็น “TOTP : Time based One Time Passwords.”

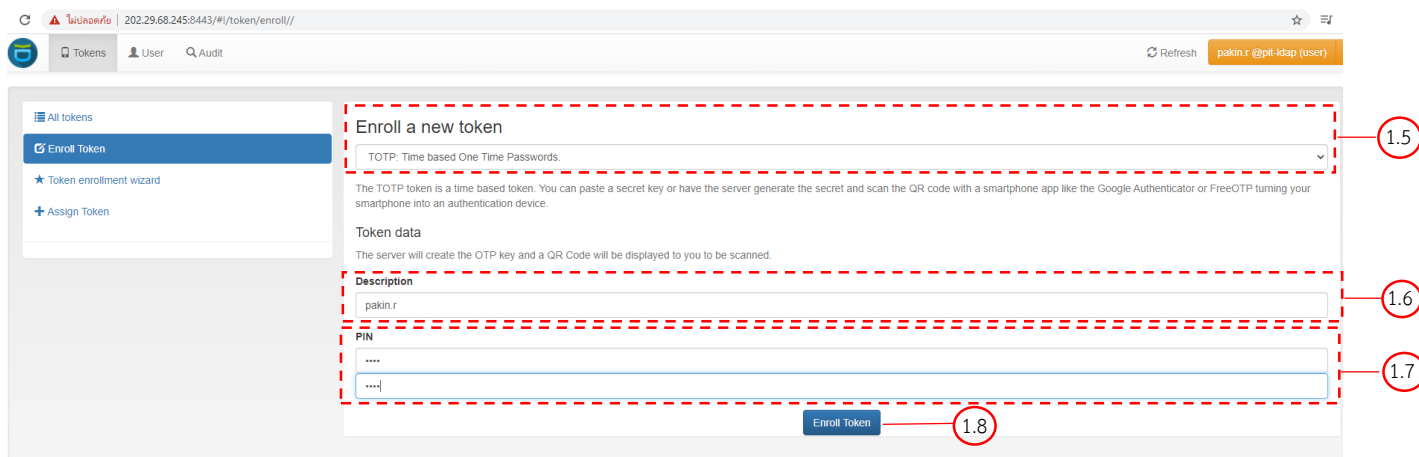


1.6 หัวข้อ Description สำหรับ บุคลากรให้กรอก username : sekxxx

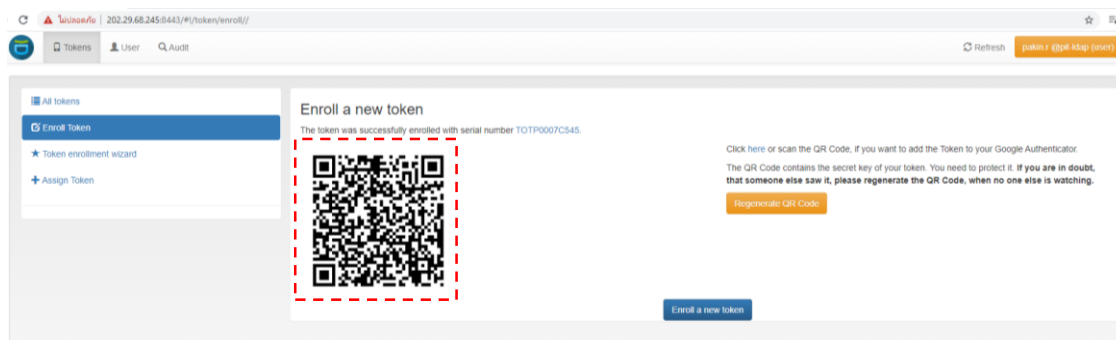
นักศึกษาให้กรอกรหัสนักศึกษา : 6301xxxxxx

1.7 หัวข้อ PIN พิมพ์ตัวเลข 4 หลัก (กำหนดด้วยตนเอง ตัวอย่างเช่น 1234) ในช่อง Type a password และ พิมพ์ตัวเลข 4 หลัก (อีกครั้ง) ในช่อง Repeat password

1.8 คลิกที่ Enroll Token



1.9 ผู้ใช้งานจะได้รับ QR Code จากระบบเพื่อรับ one-time password (OTP)

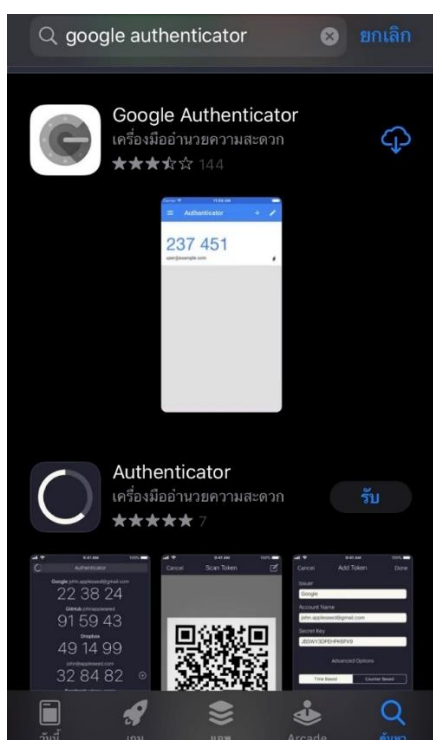


2. การติดตั้ง Google Authenticator

Google Authenticator คือ แอปพลิเคชันเพิ่มความปลอดภัยของบัญชีผู้ใช้งาน และเพื่อรับรหัสการเข้าใช้งาน VPN ของสถาบัน โดยรหัสผ่านจาก Google Authenticator จะมีอายุการใช้งานเพียง 1 นาทีเท่านั้น เมื่อรหัสปรากฏครบ 1 นาที แล้ว ทางแอปจะกำหนดรหัสใหม่เพื่อมาทดแทนของเดิมที่หมดอายุการใช้งาน

2.1 ให้ผู้ใช้งานดาวน์โหลด **Google Authenticator** ได้จาก Play Store สำหรับมือถือระบบ Android หรือ App Store สำหรับมือถือระบบ iOS

2.1.1 เลือกไปที่ เริ่มการติดตั้ง



หน้าจอ App Store



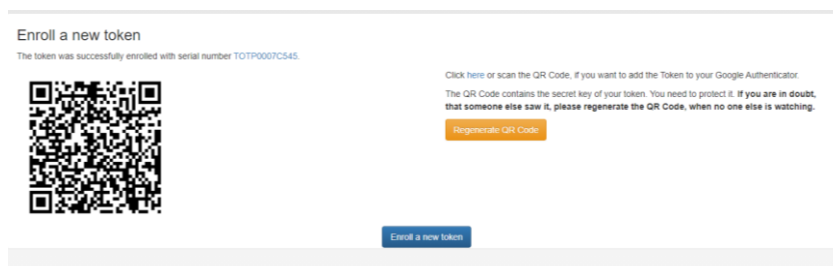
หน้าจอ Play Store

2.1.2 เลือกปุ่มสแกนบาร์โค้ด

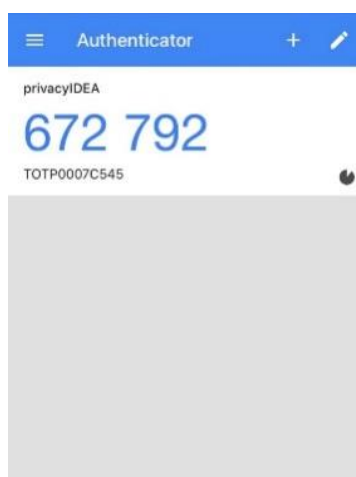


2.1.3 ผู้ใช้งานสแกน QR code ที่ได้รับจาก Token ในข้อที่ 1.9 เพื่อจะได้รับ

หมายเลข PrivacyIDEA

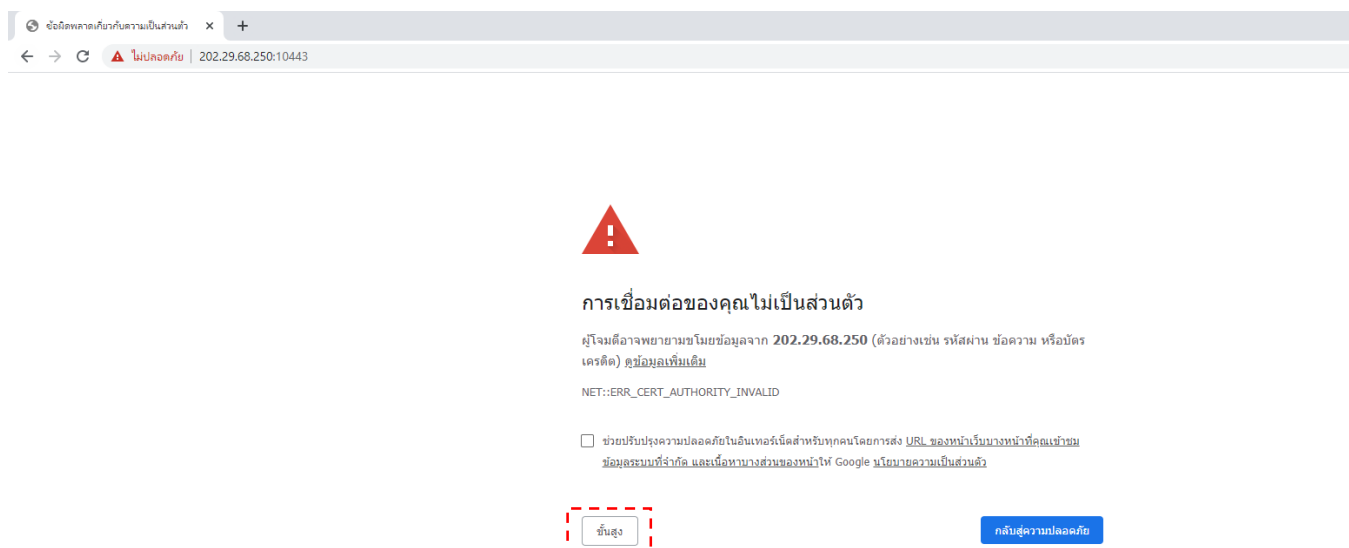


2.1.4 ผู้ใช้งานจะได้รับหมายเลข PrivacyIDEA เป็นตัวเลข 6 หลัก เพื่อนำไปเป็น OTP Password ในการ Log on การติดตั้ง Cisco AnyConnect Secure (ชุดตัวเลข 6 หลักจะเปลี่ยนทุก 1 นาที)

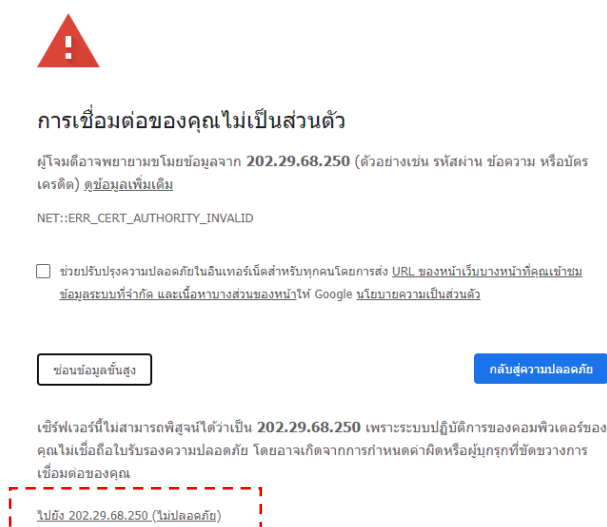


3.การติดตั้งและใช้งานโปรแกรม VPN Cisco AnyConnect Secure สำหรับ Windows 10

3.1 เปิด Web Browser พิมพ์ : <https://202.29.68.250:10443> แล้วคลิกเลือกที่ “ขึ้นสูง”



3.2 คลิกเลือกที่ 202.29.68.250 (ไม่ปลอดภัย)



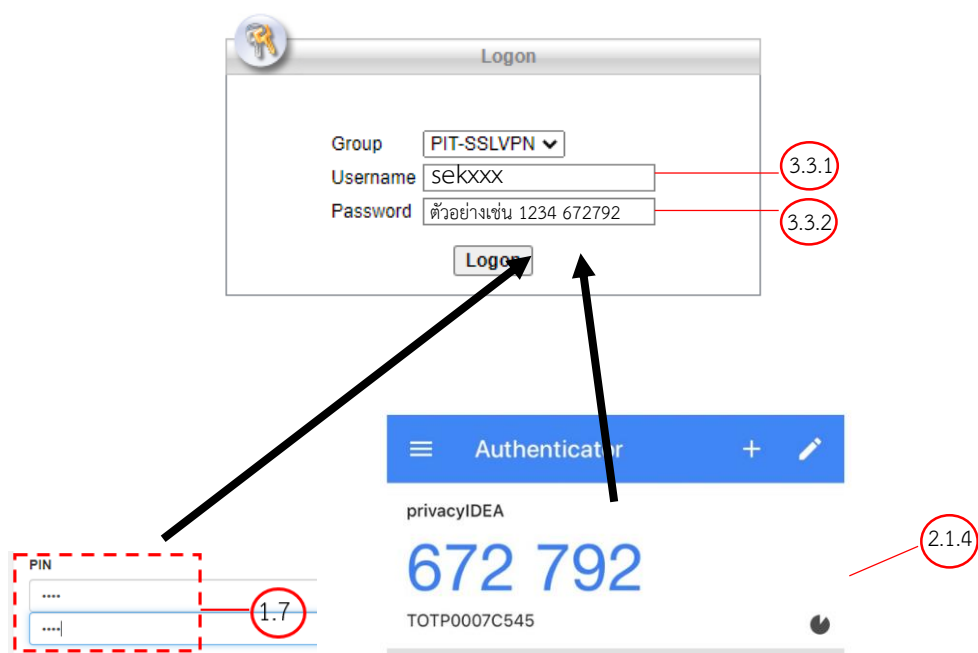
3.3 ลงชื่อเข้าใช้งาน

3.3.1 username สำหรับบุคลากร : sekxxx

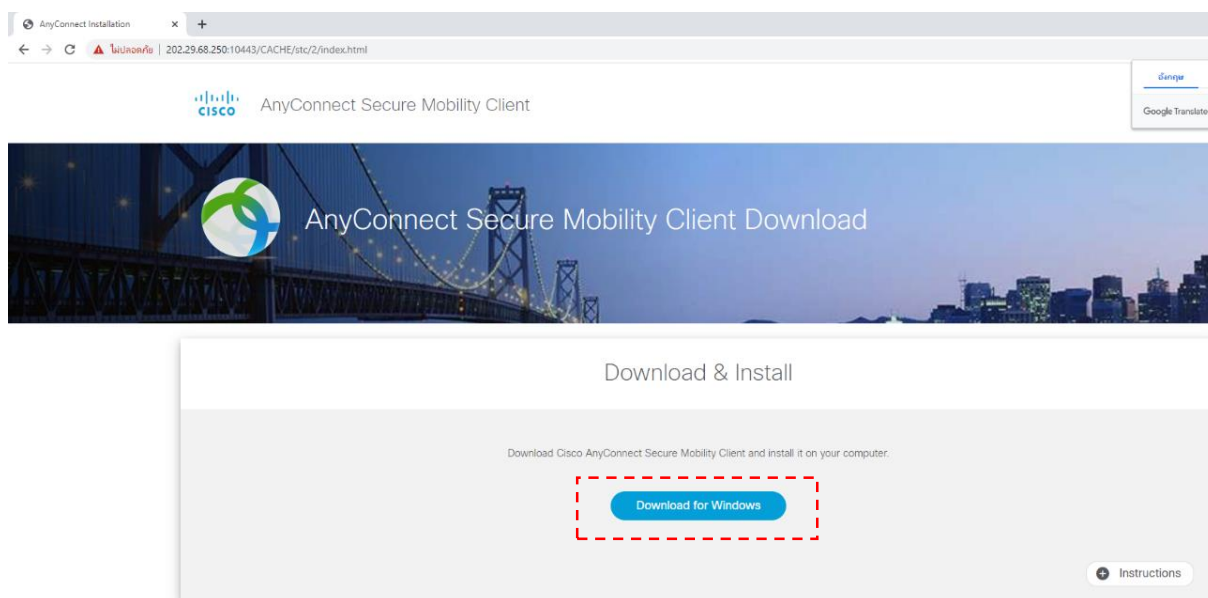
username สำหรับนักศึกษา : 6301XXXXXX

3.3.2 Password : PIN (4 หลัก) + OTP (6 หลัก)

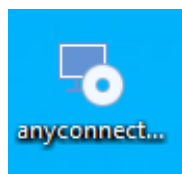
นำเลข PIN 4 หลัก ที่กำหนดในหัวข้อ 1.7 และเลข 6 หลัก จาก privacyIDEA จากหัวข้อ 2.1.4 เมื่อกรอกข้อมูลเรียบร้อยแล้วคลิก “Log on”



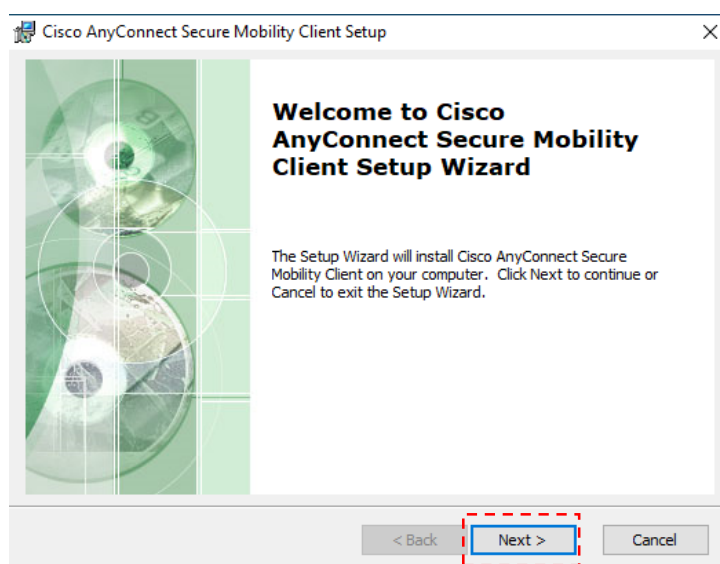
3.4 คลิกเลือก Download for Windows เพื่อทำการติดตั้ง : AnyConnect SSLVPN Client



3.5 ติดตั้งโปรแกรม AnyConnect SSLVPN Client

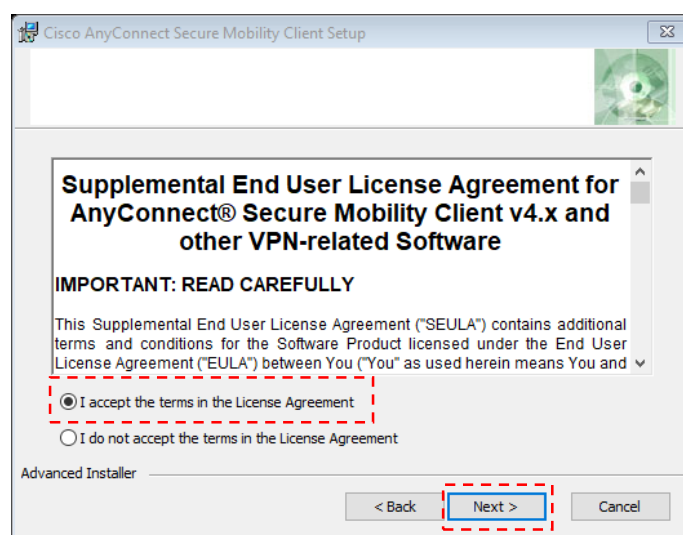


3.6 คลิกเลือก “Next”

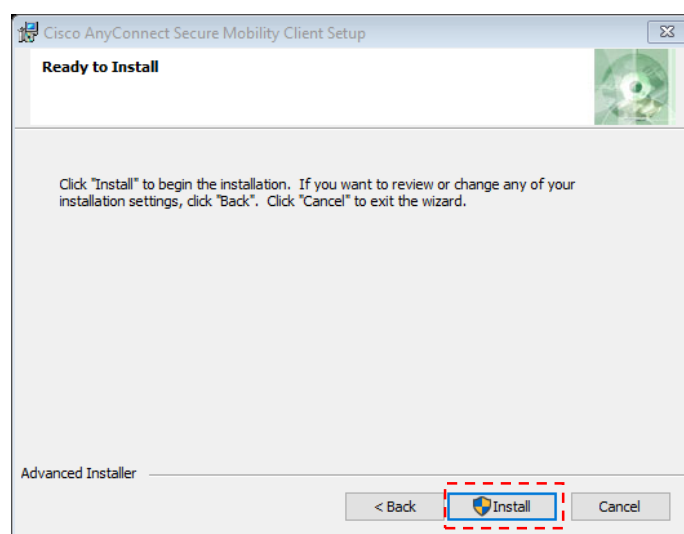


3.7 คลิกเลือก “I accept the terms in the License Agreement”

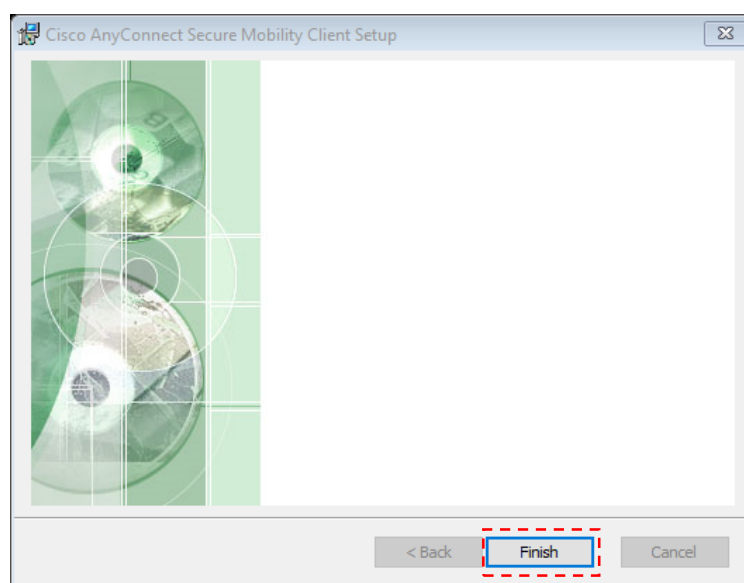
3.8 คลิก Next



3.9 คลิกเพื่อ Install



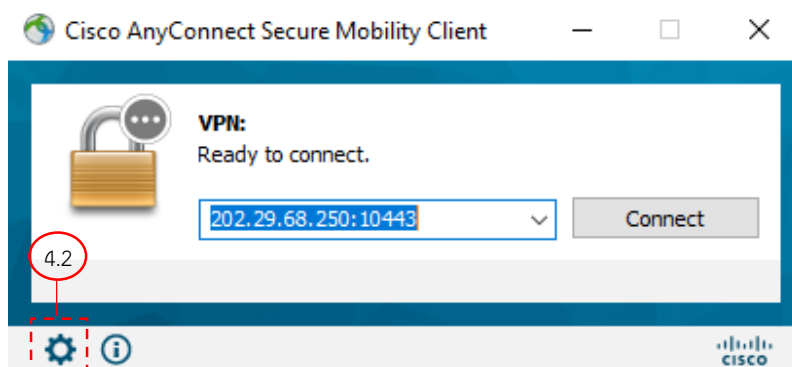
3.10 คลิกเลือก Finish



4.การใช้งานโปรแกรม Cisco AnyConnect Secure

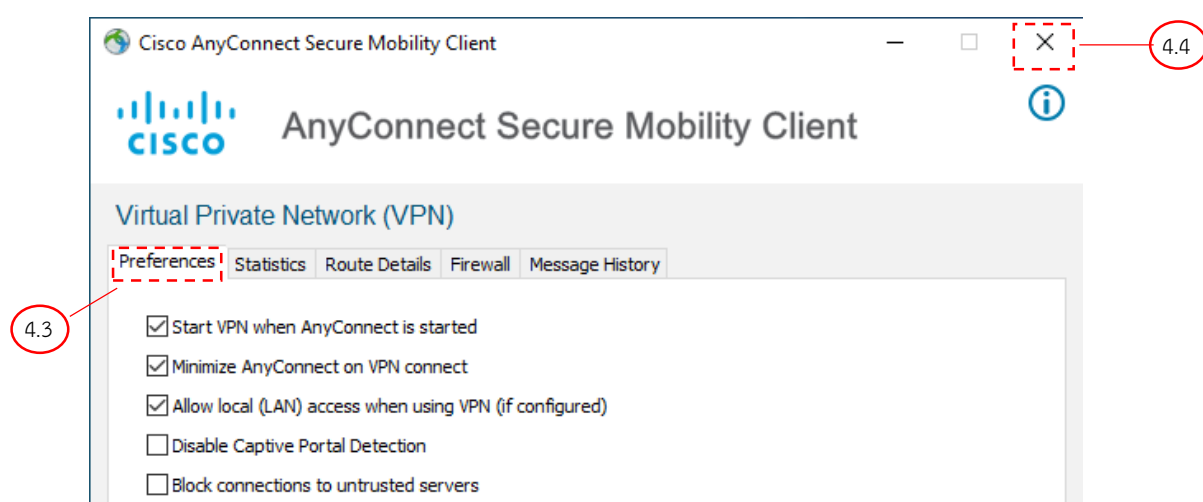
4.1 คลิกเลือก Icon โปรแกรม Cisco AnyConnect Secure

4.2 คลิกไปที่



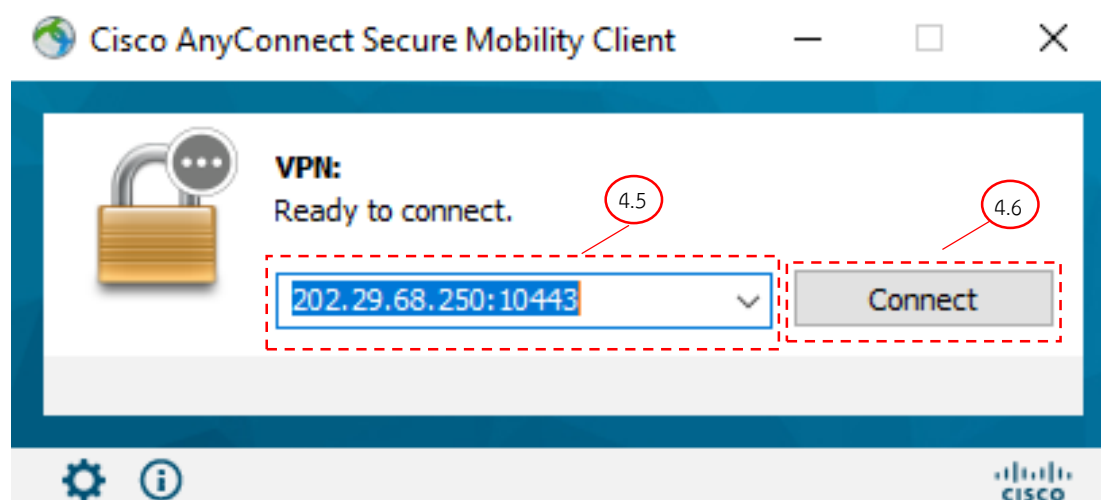
4.3 ให้คลิกเลือก Preferences กำหนดตัวเลือกตามรูปด้านล่าง

4.4.คลิกที่เครื่องหมายปิดหน้าจอ

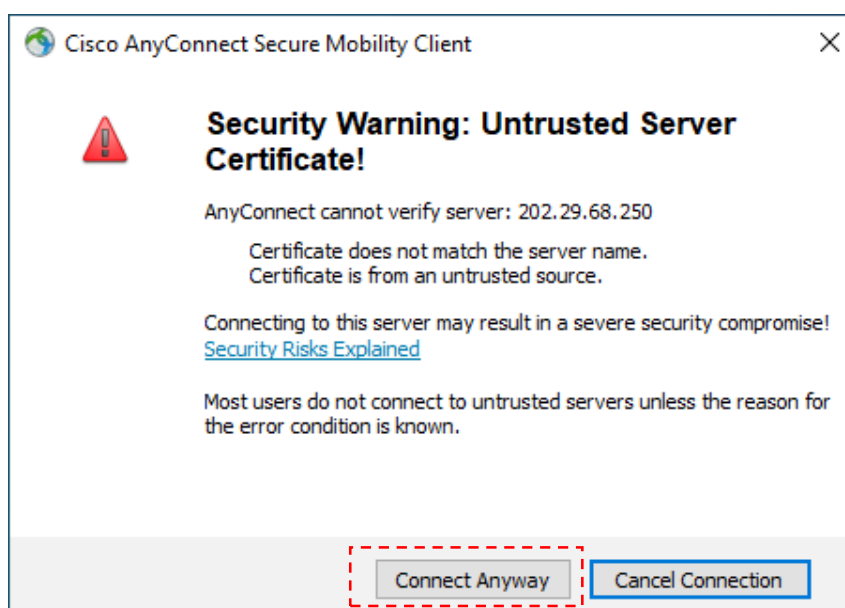


4.5 กรอกเลข “202.29.68.250:10443” ในช่องว่าง

4.6 คลิกเลือก Connect



4.7 คลิกเลือก Connect Anyway



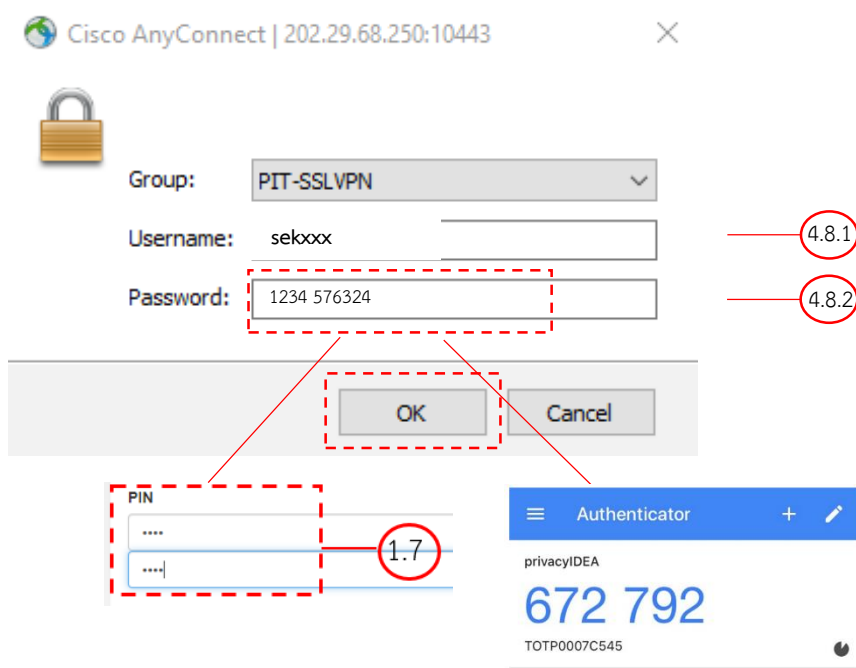
4.8 ลงชื่อเข้าใช้งาน

4.8.1 username สำหรับบุคลากร : sekxxx

username สำหรับนักศึกษา : 6301XXXXXX

4.8.2 Password : PIN (4 หลัก) + OTP (6 หลัก)

นำเลข PIN 4 หลัก ที่กำหนดในหัวข้อ 1.7 และเลข 6 หลัก จาก privacyIDEA จากหัวข้อ 2.1.4 เมื่อกรอกข้อมูลเรียบร้อยแล้วคลิก “Log on”

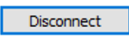


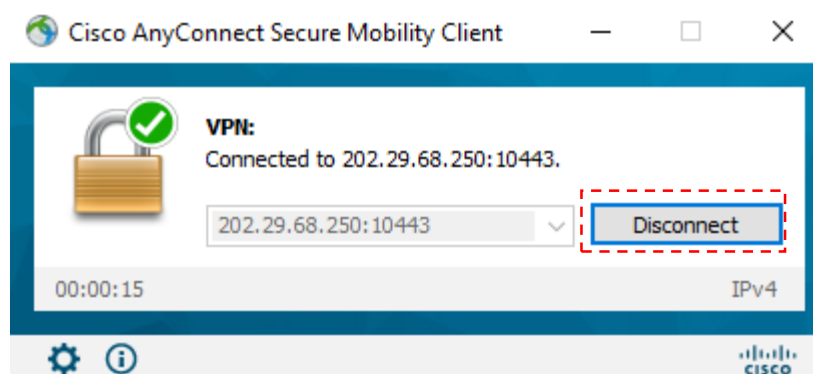
4.9 ระบบ VPN พร้อมใช้งาน Iconอยู่ที่มุมด้านขวา  ของหน้าจอ



5. จากนั้น ผู้รับบริการจะสามารถเข้าถึงบริการภายในต่าง ๆ ของสถาบันได้ โดยเมื่อสิ้นสุดการใช้งาน ให้ทำการคลิก ไอคอน “Disconnect” เพื่อสิ้นสุดการ เชื่อมต่อระบบ

5.1 คลิกไอคอน อยู่ที่มุมด้านขวาของหน้าจอ 

5.2 คลิกไอคอน  เพื่อหยุดการใช้งาน

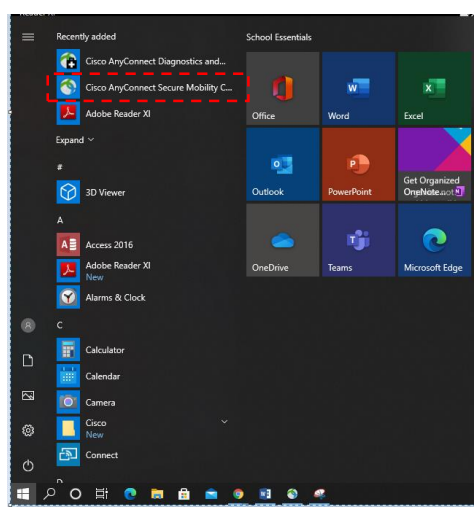


6. สำหรับการใช้งานครั้งถัดไป ให้เปิดโปรแกรม Cisco AnyConnect Secure

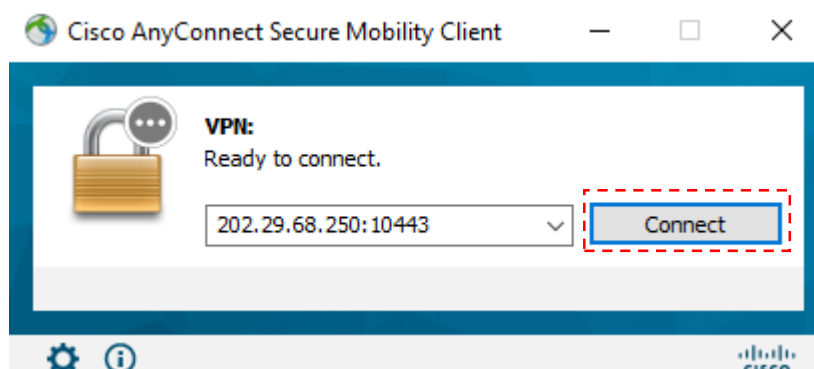
6.1 เปิดมือถือเข้าใช้งานแอป Google Authentication เพื่อนำหมายเลข PrivacyIDEA เป็นตัวเลข

6 หลักมาใช้ในการ เข้าใช้งาน โปรแกรม Cisco AnyConnect Secure Mobility client

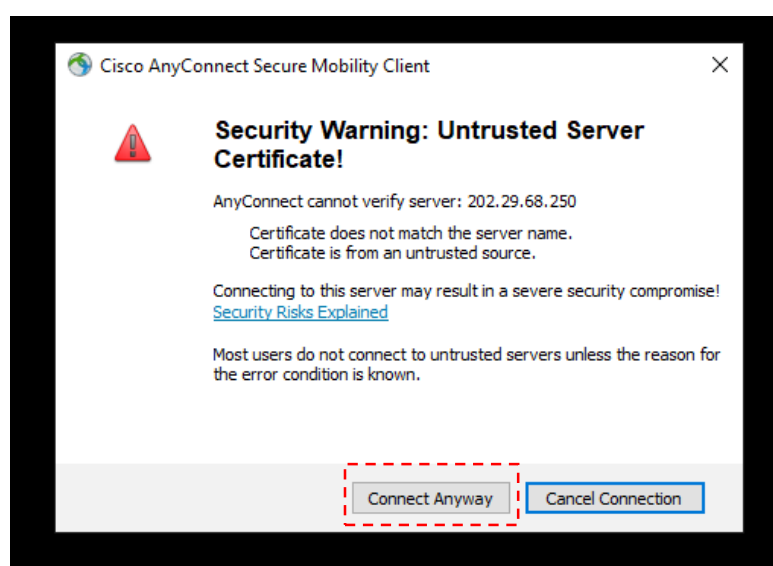
6.2 คลิก Start และ เลือกโปรแกรม Cisco AnyConnect Secure Mobility client



6.3 คลิก Connect



6.4 คลิก Connect Anyway



6.5 ลงชื่อเข้าใช้งาน

6.5.1 username สำหรับบุคลากร : sekxxx

username สำหรับนักศึกษา : 6301XXXXXX

6.5.2 Password : นำเลข PIN 4 หลัก ที่กำหนดในหัวข้อ 1.7 และเลข 6 หลัก จาก One Time Password จากหัวข้อ 2.1.4 เมื่อกรอกข้อมูลเรียบร้อยแล้วคลิก “OK”

