



การติดตั้งและตั้งค่า

CMU GlobalProtect VPN

สำหรับผู้รับบริการ



เชื่อมต่อได้ทั่วโลก
เข้าถึงเครือข่ายมหาวิทยาลัย
ได้อย่างปลอดภัย



ปลอดภัย มั่นใจ
เข้ารหัสข้อมูลด้วยมาตรฐาน
ระดับสากล



เสถียร รวดเร็ว
เชื่อมต่อได้เสถียร
ทุกที่ ทุกเวลา



รองรับทุกอุปกรณ์
ใช้งานได้บน Windows,
macOS, iOS และ Android



สำหรับผู้รับบริการ



กลุ่มภารกิจเทคโนโลยีดิจิทัล
และสื่อการเรียนรู้ (DTLM)

คำนำ

คู่มือการปฏิบัติงานกลุ่มภารกิจเทคโนโลยีดิจิทัลและสื่อการเรียนรู้ เรื่อง “การติดตั้งและตั้งค่า CMU GlobalProtect VPN สำหรับผู้รับบริการ” ฉบับนี้ กลุ่มภารกิจเทคโนโลยีดิจิทัลได้จัดทำขึ้นเพื่อเป็นแนวทางที่ชัดเจนและเป็นมาตรฐานเดียวกันสำหรับผู้ใช้งานในการเข้าถึงระบบเครือข่ายของมหาวิทยาลัยผ่านเครือข่ายส่วนตัวเสมือน (VPN) อย่างถูกต้อง ปลอดภัย และมีประสิทธิภาพ โดยครอบคลุมขั้นตอนสำคัญตั้งแต่การเตรียมความพร้อม การติดตั้งโปรแกรม ไปจนถึงการตั้งค่าและการเชื่อมต่อใช้งานบนอุปกรณ์ประเภทต่าง ๆ

การใช้งาน CMU GlobalProtect VPN มีบทบาทสำคัญในการสนับสนุนการทำงานจากภายนอกเครือข่ายมหาวิทยาลัย ช่วยให้บุคลากร นักศึกษาและผู้ที่เกี่ยวข้องสามารถเข้าถึงทรัพยากรสารสนเทศและระบบงานภายในได้อย่างปลอดภัย ลดความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล และสอดคล้องกับนโยบายด้านเทคโนโลยีสารสนเทศขององค์กร

ผู้จัดทำหวังเป็นอย่างยิ่งว่าคู่มือฉบับนี้จะช่วยอำนวยความสะดวกให้แก่ผู้ใช้งานทุกระดับ ให้สามารถปฏิบัติตามขั้นตอนได้อย่างถูกต้อง ลดปัญหาที่อาจเกิดขึ้นระหว่างการติดตั้งและใช้งาน รวมถึงช่วยเพิ่มประสิทธิภาพในการเข้าถึงระบบเครือข่ายของมหาวิทยาลัยได้อย่างต่อเนื่องและมั่นคง หากมีข้อเสนอแนะเพิ่มเติม ผู้จัดทำยินดีน้อมรับเพื่อนำไปปรับปรุงคู่มือให้มีความสมบูรณ์ยิ่งขึ้นต่อไป

กลุ่มภารกิจเทคโนโลยีดิจิทัลและสื่อการเรียนรู้

มกราคม 2569

สารบัญ

หน้า

คำนำ

1. หลักการและเหตุผล	3
2. วัตถุประสงค์	3
3. ขอบเขต	3
4. คำจำกัดความ	4
5. หน้าที่ความรับผิดชอบ	4
6. ผังกระบวนการ	5
7. วิธีการขั้นตอนการขอรับบริการ	6
8. ระยะเวลาดำเนินการ	12
9. ช่องทางการให้บริการ	12
10. ค่าธรรมเนียม	12
11. รายการเอกสารหลักฐานประกอบการยื่นคำขอรับบริการ	12
12. กฎหมายที่เกี่ยวข้อง	12
13. มาตรฐานงานและข้อตกลงในการใช้งาน	12
14. ระบบติดตามประเมินผลและเอกสารอ้างอิง	12
15. ภาคผนวก	13

คู่มือการปฏิบัติงานกลุ่มภารกิจเทคโนโลยีสารสนเทศและสื่อการเรียนรู้: การติดตั้งและตั้งค่า CMU

GlobalProtect VPN สำหรับผู้ขอรับบริการ

1. หลักการและเหตุผล

ในระบบนิเวศดิจิทัลของมหาวิทยาลัยเชียงใหม่ การเข้าถึงทรัพยากรสารสนเทศอย่างปลอดภัยเป็นกลยุทธ์สำคัญที่สนับสนุนการวิจัยและการเรียนการสอน เครือข่ายส่วนตัวเสมือน หรือ VPN (Virtual Private Network) คือเทคโนโลยีโครงสร้างพื้นฐานที่ใช้เทคนิคการทำ Tunneling วิ่งบนเครือข่ายอินเทอร์เน็ตสาธารณะ เพื่อสร้างช่องทางรับส่งข้อมูลที่มีการเข้ารหัสความปลอดภัยสูงเสมือนผู้ใช้งานเชื่อมต่ออยู่ภายในเครือข่ายของมหาวิทยาลัยโดยตรง

เทคโนโลยีนี้มีความจำเป็นอย่างยิ่งในการเข้าถึงทรัพยากรที่มีลิขสิทธิ์และจำกัดสิทธิ์เฉพาะภายในสถาบัน เช่น ฐานข้อมูลงานวิจัยระดับนานาชาติ บทความวิชาการของสำนักหอสมุด และระบบการเรียนการสอนออนไลน์ อย่างไรก็ตาม เพื่อเป็นการ "ลดภาระให้กับ GlobalProtect Server" โดยไม่จำเป็น ระบบได้ทำการปิดกั้นการเชื่อมต่อจากเครือข่ายภายในมหาวิทยาลัย (เช่น Jumbo Net หรือ Wired LAN) เนื่องจากเครือข่ายดังกล่าวสามารถเข้าถึงทรัพยากรได้โดยตรงอยู่แล้ว คู่มือฉบับนี้จึงจัดทำขึ้นเพื่อให้การใช้งาน GlobalProtect VPN ผ่าน CMU Account เป็นไปอย่างถูกต้องตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ

2. วัตถุประสงค์

1. เพื่อเป็นแนวทางมาตรฐาน (Standard Operating Procedure) ในการติดตั้งและตั้งค่าซอฟต์แวร์ GlobalProtect VPN สำหรับบุคลากรและนักศึกษา
2. เพื่อให้มั่นใจว่าการเข้าถึงทรัพยากรเครือข่ายเป็นไปตามข้อกำหนด ระเบียบ และหลักเกณฑ์ด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย
3. เพื่อลดความผิดพลาดในกระบวนการติดตั้งและช่วยให้ผู้ใช้งานสามารถปฏิบัติตามขั้นตอนทางเทคนิคที่ซับซ้อนได้อย่างถูกต้อง

3. ขอบเขต

คู่มือการปฏิบัติงานฉบับนี้ครอบคลุมกระบวนการตั้งแต่การตรวจสอบความพร้อมของระบบปฏิบัติการ การเลือกไฟล์ติดตั้งที่ถูกต้อง การตั้งค่าสิทธิ์ความปลอดภัย (Security Permissions) การยืนยันตัวตน ไปจนถึงกระบวนการสิ้นสุดการเชื่อมต่อ โดยครอบคลุม:

* ระบบปฏิบัติการ: Windows (32-bit และ 64-bit), macOS, iOS, Android และ Linux

* กลุ่มเป้าหมาย: นักศึกษาและบุคลากร (CMU Account) และบุคคลภายนอก (Guest Account)

* ระยะเวลาดำเนินงาน: การใช้งานจากเครือข่ายภายนอกมหาวิทยาลัยเชียงใหม่เท่านั้น

4. คำจำกัดความ

VPN หมายถึง เครือข่ายส่วนตัวเสมือนที่เชื่อมต่อจากภายนอกเข้ามาเสมือนใช้งานอยู่ในระบบเครือข่ายของมหาวิทยาลัย

Tunneling หมายถึง เทคนิคการสร้างช่องทางรับส่งข้อมูลที่ปลอดภัยบนเครือข่ายสาธารณะ

GlobalProtect หมายถึง ซอฟต์แวร์ไคลเอนต์มาตรฐานที่ใช้ในการเชื่อมต่อ VPN ของมหาวิทยาลัยเชียงใหม่

CMU Account หมายถึง บัญชีผู้ใช้ไอทีส่วนบุคคลที่ออกโดยสำนักบริการเทคโนโลยีสารสนเทศ

ITSC หมายถึง สำนักบริการเทคโนโลยีสารสนเทศ (Information Technology Service Center)

System Type หมายถึง ประเภทสถาปัตยกรรมของระบบปฏิบัติการ (32-bit หรือ 64-bit)

ผู้รับบริการ หมายถึง บุคลากรและนักศึกษามหาวิทยาลัยเชียงใหม่

5. หน้าที่ความรับผิดชอบ

เพื่อให้การดำเนินงานสอดคล้องตามลำดับชั้นการบริหารจัดการ (Hierarchy of Authority) จึงกำหนดหน้าที่ดังนี้:

1. สำนักบริการเทคโนโลยีสารสนเทศ (ITSC):

ผู้ดูแลระบบ (System Administrator): รับผิดชอบการจัดเตรียมเครื่องแม่ข่าย จัดหาซอฟต์แวร์ และควบคุมสิทธิ์การเข้าถึงเว็บไซต์ที่ได้รับอนุญาต

ITSC Helpdesk: สนับสนุนทางเทคนิคและแก้ไขปัญหาการใช้งานให้กับผู้ใช้

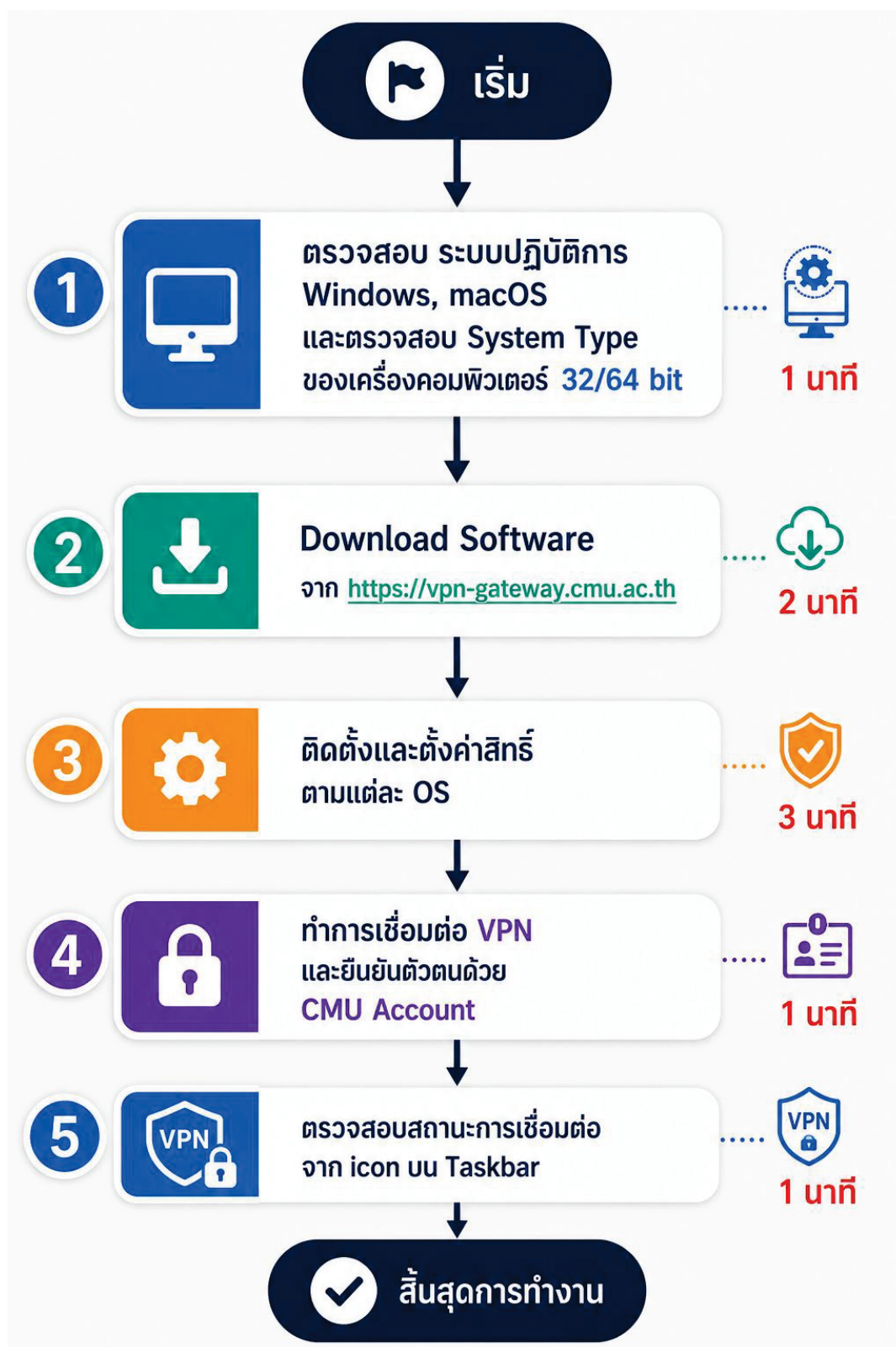
2. ผู้ใช้งาน (User):

บุคลากรและนักศึกษาของคณะเศรษฐศาสตร์

การปฏิบัติตาม (Compliance): ติดตั้งและใช้งานซอฟต์แวร์ตามขั้นตอนในคู่มืออย่างเคร่งครัด

ความรับผิดชอบ (Accountability): รับผิดชอบต่อบัญชี CMU Account ของตนแต่เพียงผู้เดียว ไม่แจกจ่ายให้ผู้อื่น และต้องปฏิบัติตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

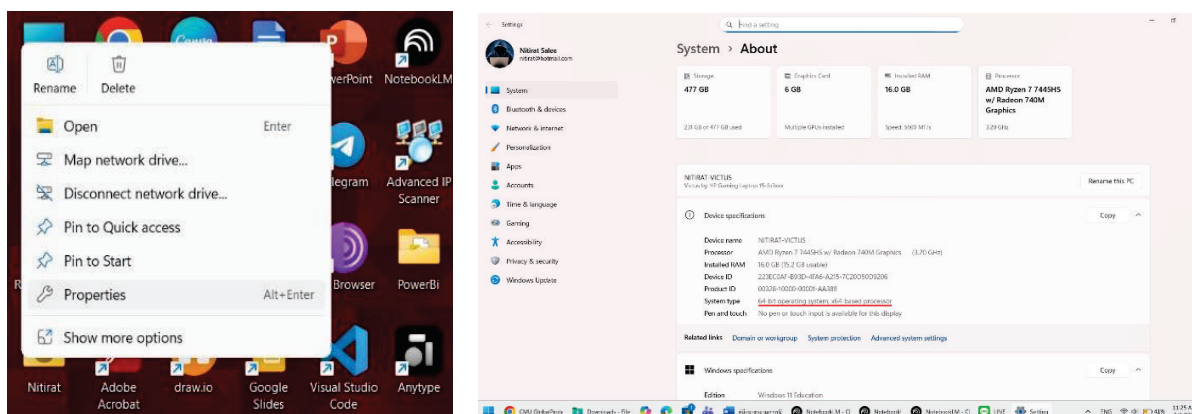
6. ผังกระบวนการงาน



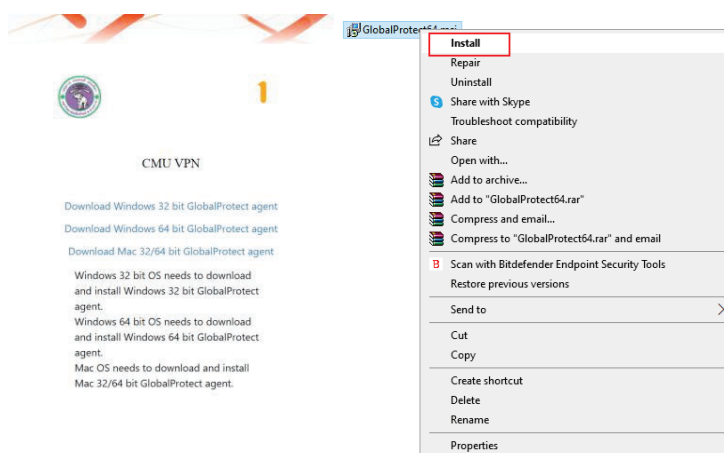
7. วิธีการขั้นตอนการขอรับบริการ

7.1 สำหรับระบบปฏิบัติการ Windows

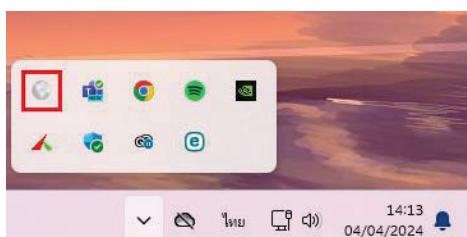
1. การตรวจสอบ System Type: คลิกขวาที่ This PC หรือ My Computer เลือก Properties ตรวจสอบว่าระบบเป็น 32-bit หรือ 64-bit (สำคัญมาก: การเลือกไฟล์ผิดรุ่นจะทำให้เกิด Installation Failure)

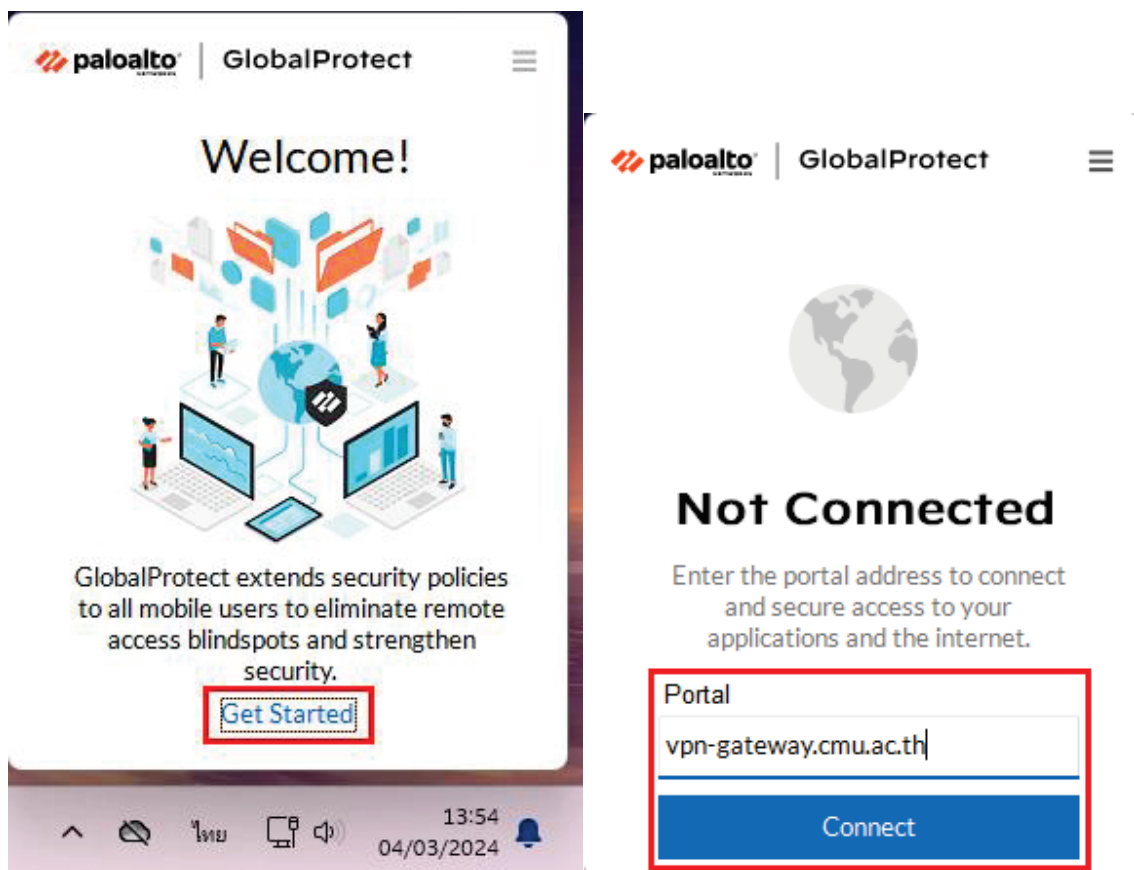


2. การติดตั้ง: เข้าไปที่ <https://vpn-gateway.cmu.ac.th> ล็อกอินด้วย CMU Account และดาวน์โหลดไฟล์รุ่นที่ถูกต้อง จากนั้นคลิกขวาที่ไฟล์ เลือก Install กด Next ตามขั้นตอนจนถึง Close

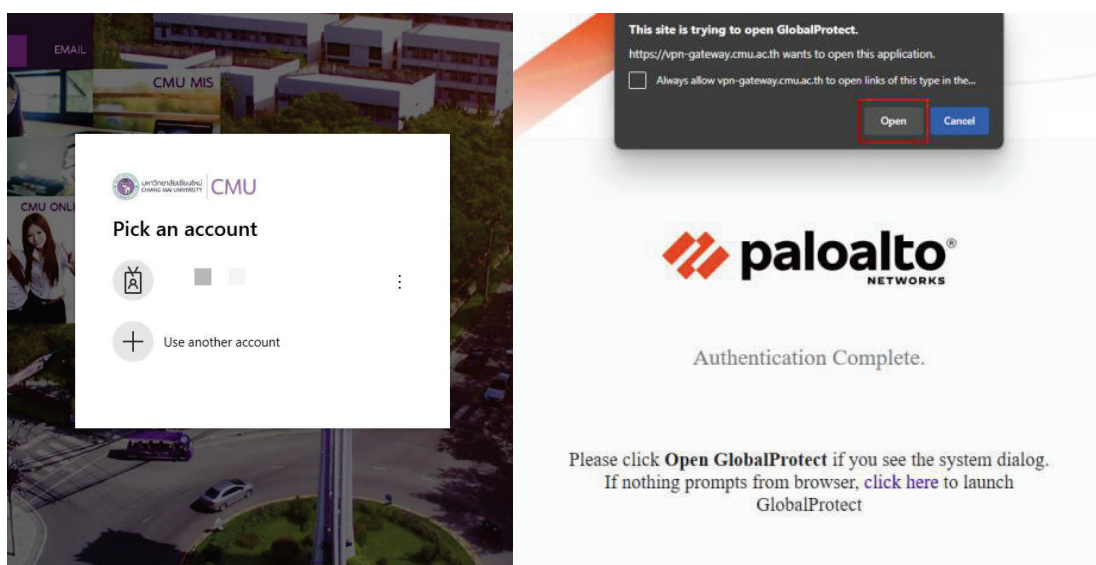


3. การเชื่อมต่อ: คลิกไอคอน GlobalProtect ที่ System tray กด Get Started กรอก Portal: vpn-gateway.cmu.ac.th แล้วกด Connect





4. Web Login: เมื่อเบราว์เซอร์แสดงขึ้น ให้ล็อกอินด้วย CMU Account จากนั้นในหน้าเว็บ Palo Alto ให้คลิกคำว่า "Open" เพื่อส่งคำสั่งกลับมายังโปรแกรม GlobalProtect



7.2 สำหรับระบบปฏิบัติการ macOS

1. การติดตั้ง: ดาวน์โหลดไฟล์ GlobalProtect.pkg และดำเนินการติดตั้งจนเสร็จสิ้น



1

CMU VPN

[Download Windows 32 bit GlobalProtect agent](#)

[Download Windows 64 bit GlobalProtect agent](#)

[Download Mac 32/64 bit GlobalProtect agent](#)

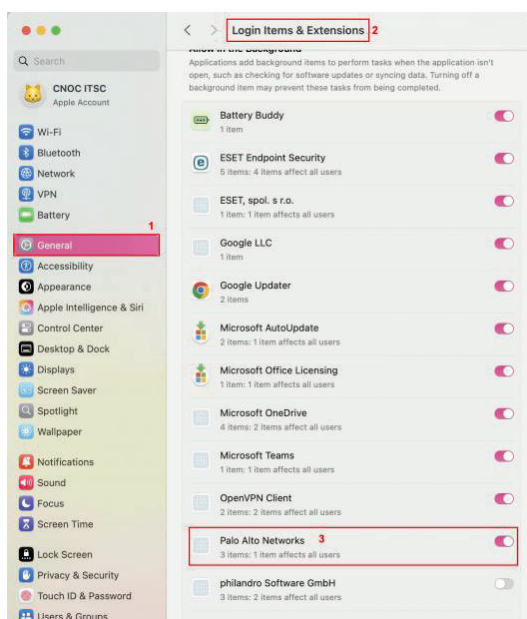
Windows 32 bit OS needs to download and install Windows 32 bit GlobalProtect agent.

Windows 64 bit OS needs to download and install Windows 64 bit GlobalProtect agent.

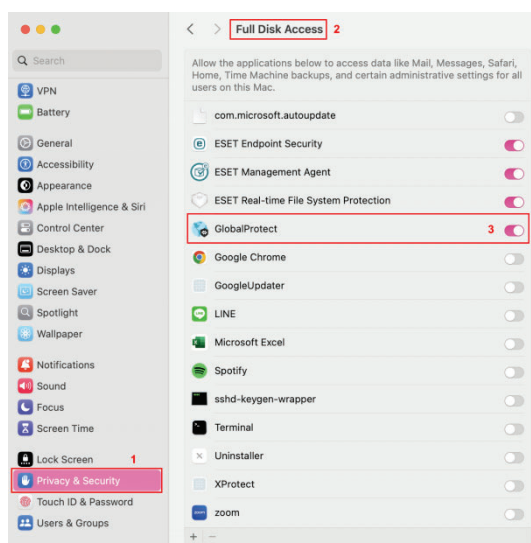
Mac OS needs to download and install Mac 32/64 bit GlobalProtect agent.

2. การตั้งค่าสิทธิ์ระบบ:

* ไปที่ System Settings > General > Login Items เปิดการทำงาน Palo Alto Networks



* ไปที่ System Settings > Privacy & Security > Full Disk Access เปิดการทำงาน GlobalProtect



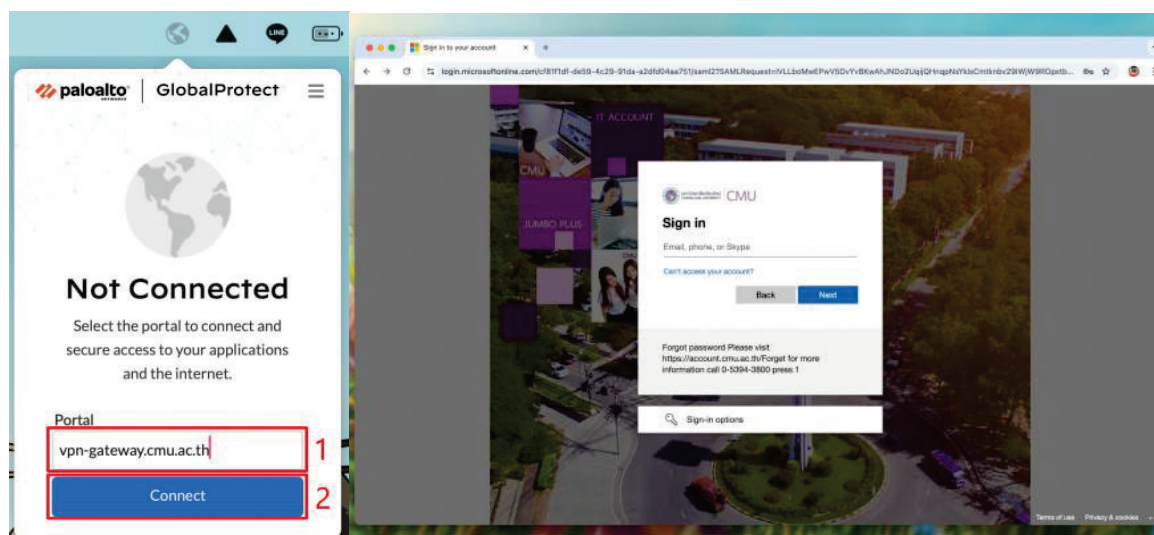
3. การปลดล็อค System Extension:

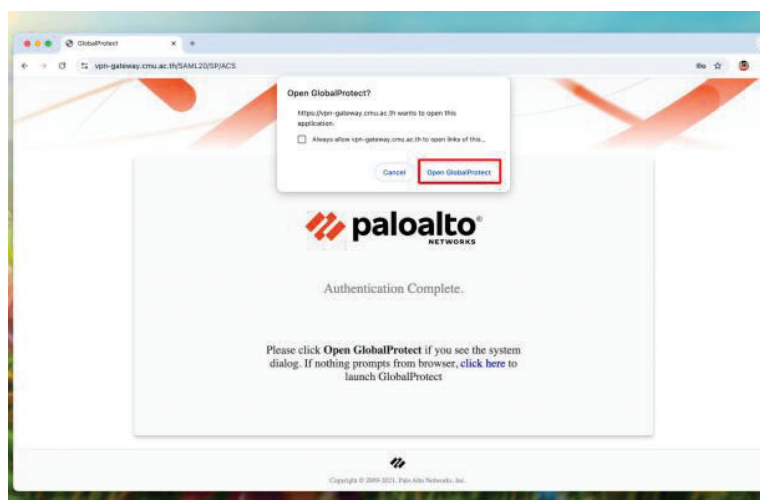
* หากพบหน้าต่าง System Extension Blocked ให้เลือก Open Security Preferences

* ที่เมนู General ให้คลิกที่ สัญลักษณ์แม่กุญแจ (Lock Icon) ด้านล่าง ใส่รหัสผ่านเครื่องเพื่อ Unlock

* กดปุ่ม Allow ทั้งหมด 2 ครั้ง ตามที่ระบบแจ้งเตือน จากนั้นคลิกสัญลักษณ์แม่กุญแจอีกครั้งเพื่อล็อคให้เรียบร้อย

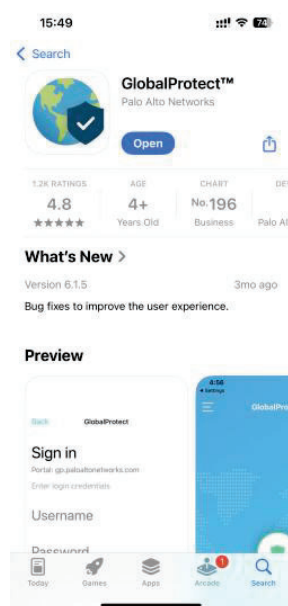
4. การเชื่อมต่อ: กรอก Portal Address และยืนยันตัวตนผ่าน Web Browser ตามลำดับ



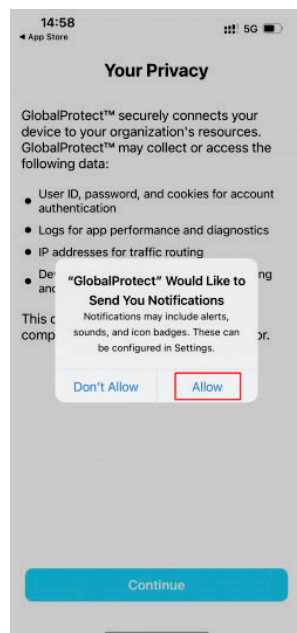


7.3 สำหรับระบบปฏิบัติการพกพา (iOS และ Android)

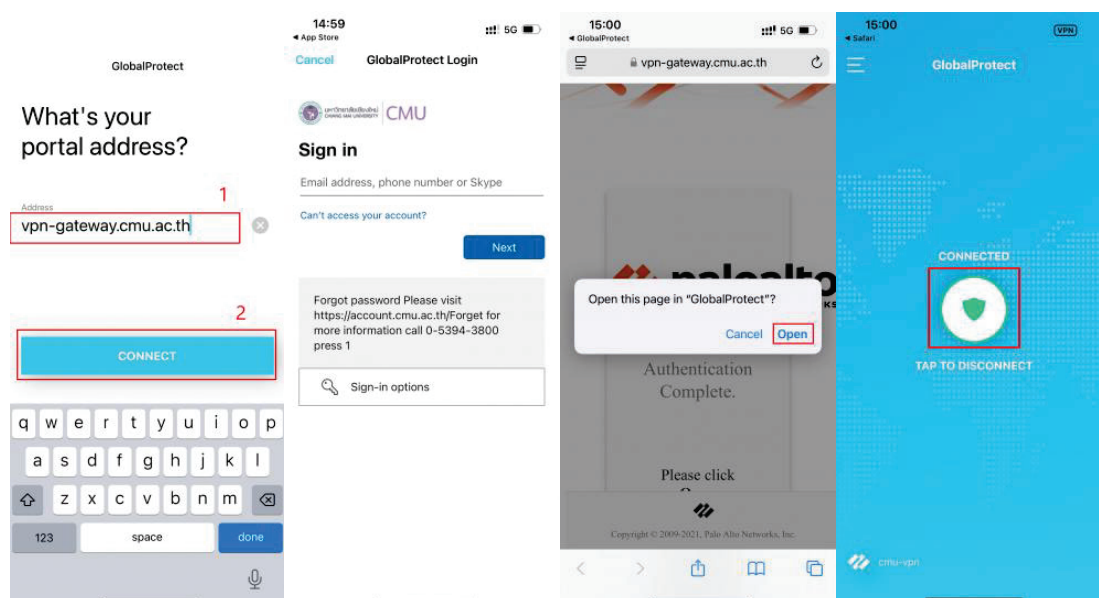
1. ดาวน์โหลด: ติดตั้งแอปพลิเคชัน GlobalProtect จาก App Store หรือ Play Store



2. การอนุญาตสิทธิ์: เปิดแอปฯ และกด Allow หรือ ตกลง เพื่ออนุญาตการแจ้งเตือนและการสร้างการเชื่อมต่อ VPN



3. การเชื่อมต่อ: พิมพ์ Portal: vpn-gateway.cmu.ac.th กด Connect และล็อกอินด้วย CMU Account



7.4 สำหรับ Linux และ Guest Account

* Linux: ดาวน์โหลดซอฟต์แวร์ผ่านลิงก์เฉพาะในหน้าระบบเครือข่ายของ ITSC และปฏิบัติตามคำสั่งการติดตั้งใน Terminal <[download](#)>

* Guest Account: เลือกใช้งานผ่านเมนู "GlobalProtect for Guest Account" บนหน้าเว็บ Portal

8. ระยะเวลาที่ใช้ในการขอรับบริการ

8 นาที

9. ช่องทางการให้บริการ

ผู้ขอรับบริการสามารถติดต่อ ขอรับคำปรึกษา หรือสอบถามรายละเอียดการติดตั้งและตั้งค่า CMU GlobalProtect VPN ได้ที่ห้องกลุ่มภารกิจเทคโนโลยีดิจิทัลและสื่อการเรียนรู้ ชั้น 1 อาคาร 1 คณะเศรษฐศาสตร์ และดาวน์โหลดซอฟต์แวร์ที่เว็บไซต์ <https://vpn-gateway.cmu.ac.th>

10. ค่าธรรมเนียม

ไม่มีการชำระค่าธรรมเนียม

11. รายการเอกสารประกอบการยื่นคำขอรับบริการ

ไม่มีรายการเอกสารที่ต้องใช้ในการขอรับบริการ

12. กฎหมายที่เกี่ยวข้อง

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

13. มาตรฐานงานและข้อตกลงการใช้งาน

การยืนยันตัวตน	ต้องผ่านการตรวจสอบสิทธิ์ด้วยบัญชี CMU Account ทุกครั้งก่อนเริ่ม Tunneling
ขอบเขตการเข้าถึง เท่านั้น	อนุญาตให้เข้าถึงเฉพาะเว็บไซต์และทรัพยากรทางการศึกษาที่มหาวิทยาลัยกำหนด
ความมั่นคงปลอดภัย ย้อนกลับ	ข้อมูลจราจรคอมพิวเตอร์ถูกบันทึกตาม พรบ. คอมพิวเตอร์ฯ 2550 เพื่อการตรวจสอบ

การสิ้นสุดการใช้งาน ผู้ใช้งานต้องทำการ Logout จากระบบถาวรเมื่อเลิกใช้งานเพื่อป้องกันการสวมสิทธิ์

14. ระบบติดตามประเมินผลและเอกสารอ้างอิง

ระบบติดตาม: สังเกตไอคอนรูปลูกโลก (GlobalProtect) บนแถบสถานะ หากเชื่อมต่อสำเร็จต้องแสดงสีเขียวหรือสถานะ "Connected"

เอกสารอ้างอิง:

ฐานข้อมูลความรู้ระบบเครือข่าย: <https://network.cmu.ac.th/wiki>

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไขเพิ่มเติม

15. ภาคผนวก

ช่องทางการสนับสนุน: ติดต่อ ITSC Helpdesk สำหรับปัญหาการเข้าใช้งานระบบ

ลิงก์สำคัญ:

หน้าหลัก Portal: <https://vpn-gateway.cmu.ac.th>

การออกจากระบบถาวร (Permanent Logout): <https://mail.cmu.ac.th>

แบบฟอร์มและบันทึก:

บันทึกการเข้าใช้งาน (User Login Logs): บันทึกโดยอัตโนมัติในระบบ Central Log ของมหาวิทยาลัย ตามกฎหมาย

คู่มือการปฏิบัติงานกลุ่มภารกิจเทคโนโลยีดิจิทัลและสื่อการเรียนรู้
การติดตั้งและตั้งค่า CMU GlobalProtect VPN สำหรับผู้รับบริการ

(ลงชื่อ).....ผู้รายงาน

(นายนิติรัฐ สาลี)

หัวหน้ากลุ่มภารกิจดิจิทัลและสื่อการเรียนรู้

(ลงชื่อ).....ผู้รับรองรายงาน

(รองศาสตราจารย์ ดร.รสริน โอสถานันต์กุล)

คณบดีคณะเศรษฐศาสตร์

หมายเหตุ: ให้ผู้บริหารสูงสุดของหน่วยงานหรือผู้รักษาราชการแทน เป็นผู้รับรองรายงานการเผยแพร่ลงเว็บไซต์

