คู่มือการบำรุงรักษาและดูแลระบบ

โครงการศึกษาการเพิ่มศักยภาพ
ศูนย์บัญชาการกรมทางหลวง ระยะที่ 3

สารบัญ

หน้า

บทที่ 1 การบำรุงรักษาระบบ....1
1) การบำรุงรักษาระบบเชื่อมโยงข้อมูล 1
2) การติดตั้งระบบจัดการ Body Camera 4
3) การติดตั้งระบบจัดการเครื่องคอมพิวเตอร์แม่ข่าย 7
4) การใช้งานระบบจัดการเครื่องคอมพิวเตอร์แม่ข่าย Proxmox VE 14
5) การใช้งาน ICC Bodycam Management 23
6) เครื่องคอมพิวเตอร์แม่ข่ายระบบศูนย์บัญชาการ กรมทางหลวง 37
บทที่ 2 แผนการบำรุงรักษา.... 51
1) ระบบซอฟต์แวร์และโปรแกรมประยุกต์ (System and application Software) 51
2) ระบบฐานข้อมูล (Database) 52
3) ระบบเครื่องคอมพิวเตอร์แม่ข่าย (On Premise) 52
บทที่ 3 แผนการซ่อมแซมแก้ไขระบบ 54
1) กระบวนการรับเรื่องแก้ไขปัญหา.... 54
2) ประเภทและนิยามของเหตุการณ์ปัญหา 55
3) วิธีการแก้ไขเหตุการณ์เบื้องต้น.... 56

สารบัญรูป

หน้า

รูปที่ 1 การติดตั้งเครื่อง Server ของ ICC (Rack 16) 39
รูปที่ 2 การกำหนด port ของ Firewall 39
รูปที่ 3 การกำหนด port ของ Switch L3 40
รูปที่ 4 การกำหนด port ของ Switch Manage 40
รูปที่ 5 การกำหนด port ของ Data Lake BI Gateway 41
รูปที่ 6 การกำหนด port ของ Database 41
รูปที่ 7 การกำหนด port ของ Streaming 41
รูปที่ 8 การกำหนด port ของ System Web 41
รูปที่ 9 การกำหนด port ของ Body Camera 42
รูปที่ 10 การกำหนด port ของ Databus Gateway 42
รูปที่ 11 การกำหนด port ของ Algorithm 42
รูปที่ 12 การกำหนด port ของ SSO (1) 42
รูปที่ 13 การกำหนด port ของ SSO (2) 43
รูปที่ 14 ขั้นตอนกระบวนการรับเรื่องร้องเรียน 54
รูปที่ 15 ช่องทางสำหรับประสานงานแก้ไขปัญหาระบบ 57

สารบัญตาราง

หน้า

ตารางที่ 1 รายการอุปกรณ์ที่เกี่ยวข้องในโครงการ 38
ตารางที่ 2 การออกแบบมาตรฐานเครื่องที่ใช้ในโครงการ 38
ตารางที่ 3 แสดงรายการ port ที่ได้รับจัดสรรในระบบ ICC 49
ตารางที่ 4 ตัวอย่างแบบฟอร์มสถานการณ์ทำงานของระบบ (System Health) 53
ตารางที่ 5 ข้อตกลงการให้บริการรักษาและดูแลระบบ (Service Level Agreement : SLA) 55

บทที่ 1
การบำรุงรักษาระบบ

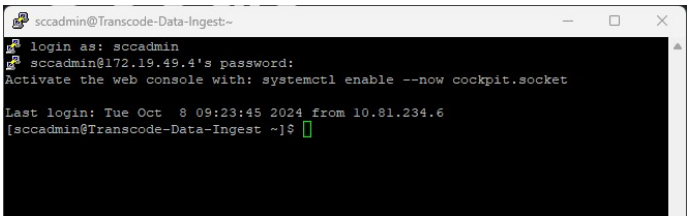
- การบำรุงรักษาระบบเชื่อมโยงข้อมูลและระบบถ่ายทอดสด
- การติดตั้งระบบจัดการ Body Camera
- การติดตั้งระบบจัดการเครื่องคอมพิวเตอร์แม่ข่าย

1) การบำรุงรักษาระบบเชื่อมโยงข้อมูล

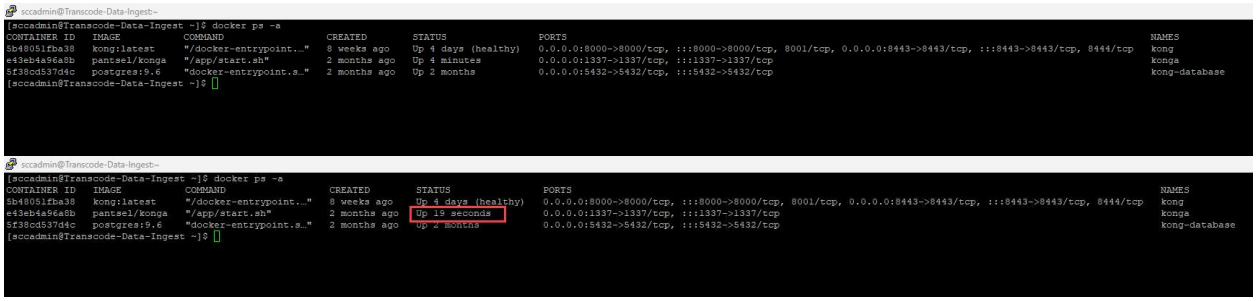
ปัจจุบันโครงการศึกษาการเพิ่มศักยภาพศูนย์บัญชาการกรมทางหลวง ระยะที่ 2 มีการใช้งานระบบ Kong API Gateway เพื่อใช้สำหรับดึงข้อมูลเข้ามาแสดงผลในระบบมีกระบวนการในการดำเนินการดังนี้

1.1) วิธีการบำรุงรักษาระบบเชื่อมโยงข้อมูล

- Secure Shell เข้าเครื่อง 172.19.49.4



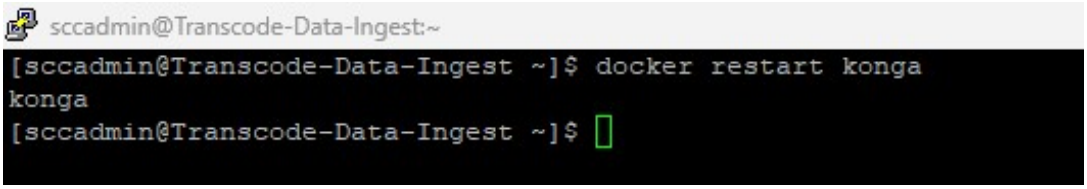
- พิมพ์คำสั่ง docker ps -a เพื่อดูสถานะของ Service โดยจะพบกับ Docker Container ทั้งหมด 3 containers ซึ่งจะสามารถดูสถานะของ Service ต่าง ๆ ได้ดังรูป



โดยประกอบไปด้วย

- kong คือ Container หลักที่ทำงานเป็น Kong service
- konga คือ Admin UI มีหน้าที่ให้ User สามารถจัดการ Kong ผ่านหน้า UI
- kong-database คือ Postgres Database ของ Kong service
- วิธีการ Restart Service สามารถทำได้โดย พิมพ์คำสั่ง docker restart <container name>

  โดย docker container จะทำการ restart ดังรูป



โดยสามารถเลือก Restart เฉพาะ Service ที่ต้องการได้ดังนี้

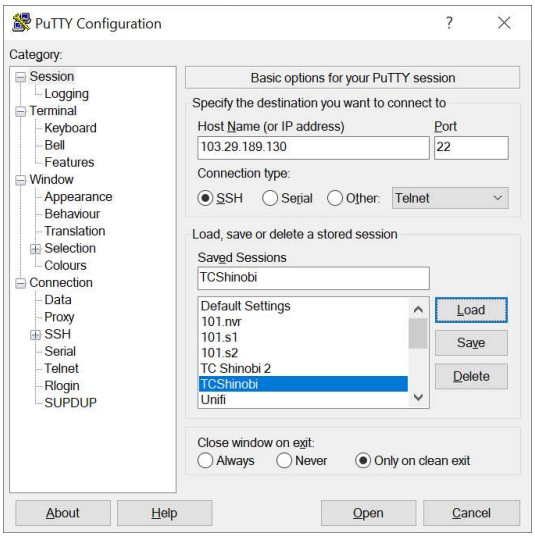
(1) docker restart kong

(2) docker restart konga

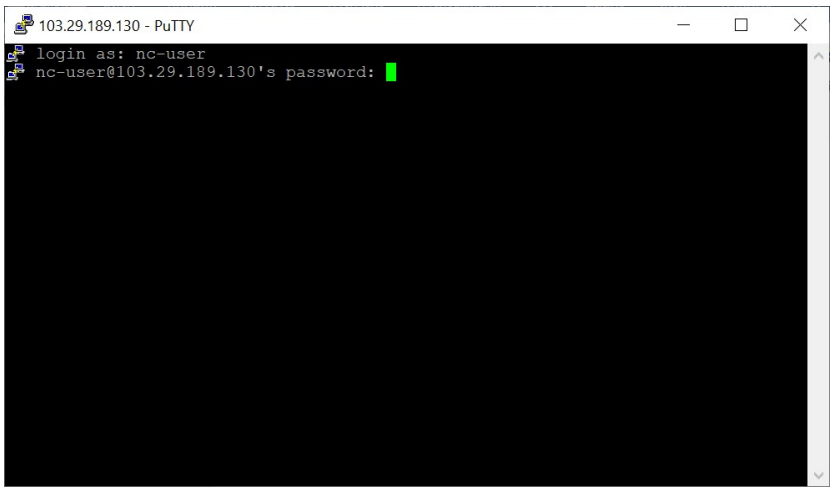
(3) docker restart kong-database

2.1) วิธีการบำรุงรักษาระบบถ่ายทอดสด

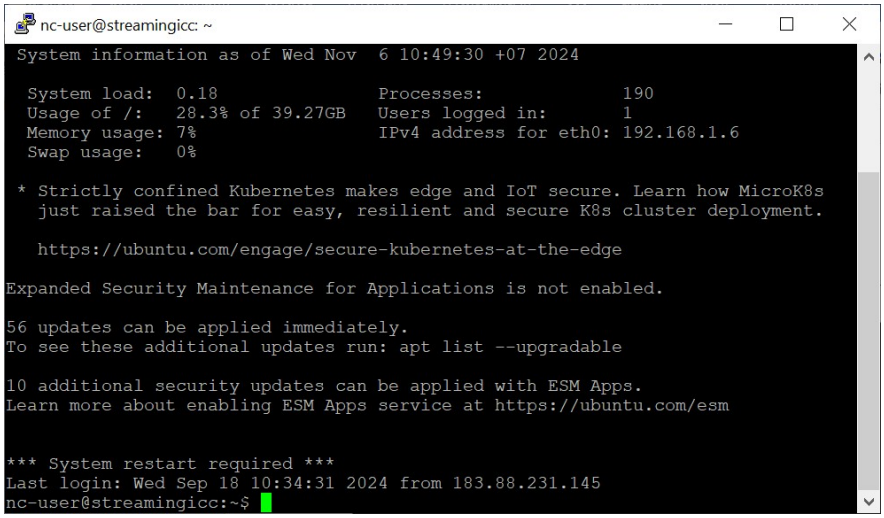
- เข้า ssh แล้วใช้ IP 103.29.189.130



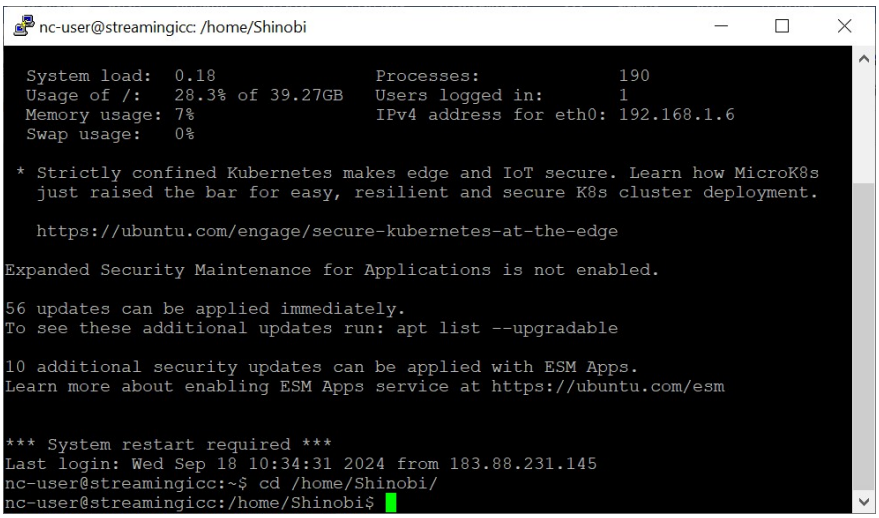
- เข้าหน้า Login



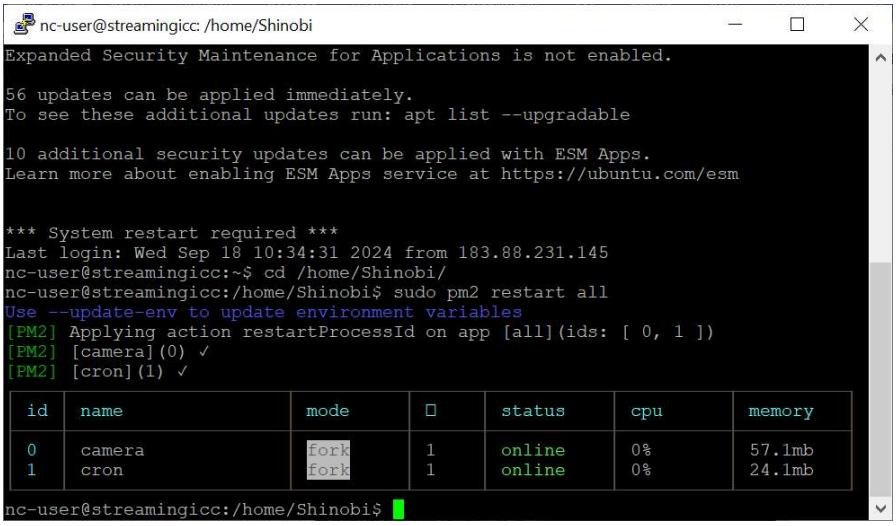
- login user: nc-user



- เข้าไปที่ cd /home/Shinobi



- ใช้คำสั่ง sudo pm2 restart all เพื่อ Restart การทำงาน



2) การติดตั้งระบบจัดการ Body Camera

2.1) ขั้นตอนการดาวน์โหลดจาก Google Drive

- https://drive.google.com/drive/folders/1xWlODKh7OXEIDwluKfumF8vshi1QGrQU?usp=sharing

  โปรแกรมที่ต้องดาวน์โหลด

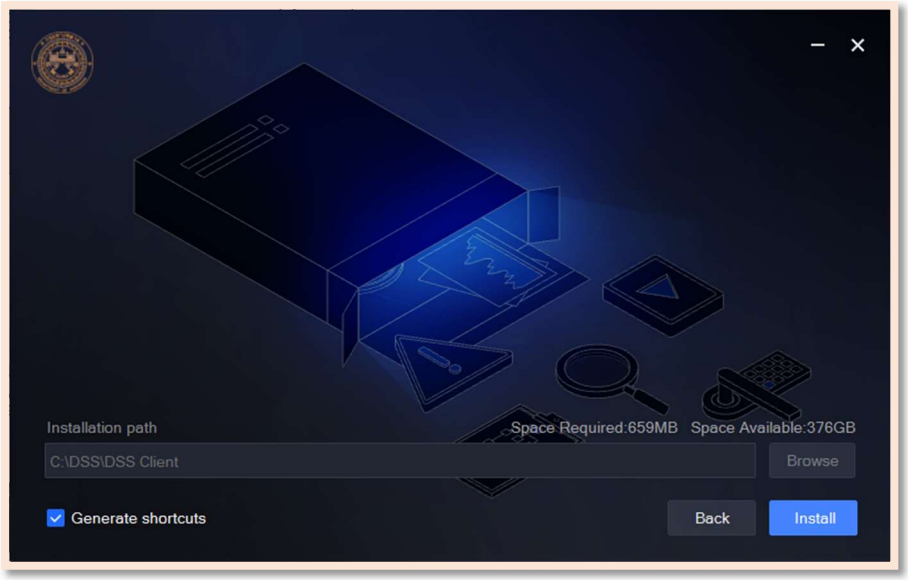
- General_ICCBodycamManagement_Win64_IS_V8.005.0000000.0.R.20240907DOH240913.exe
- Setup ICC App v1.0.4.msi

2.2) ขั้นตอนการติดตั้ง

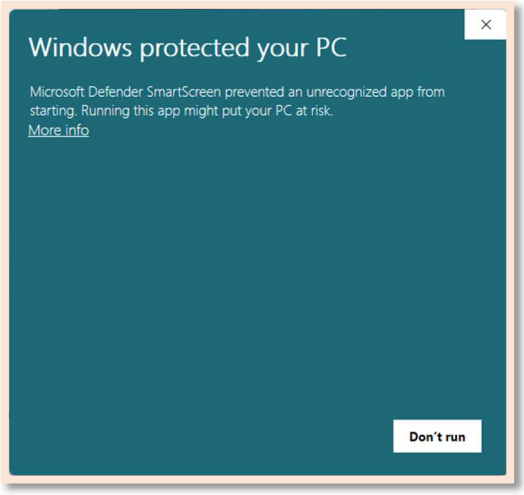
ICC Bodycam Management

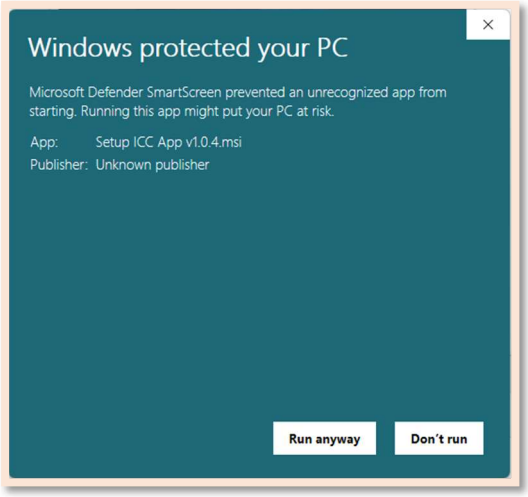
คลิกดาวน์โหลดโปรแกรมที่อยู่ใน Google Drive เมื่อทำการติดตั้งเรียบร้อยแล้ว เข้าระบบ คลิกยอมรับในช่องสี่เหลี่ยม และคลิกปุ่ม Next

- ทำการและคลิกปุ่ม Install

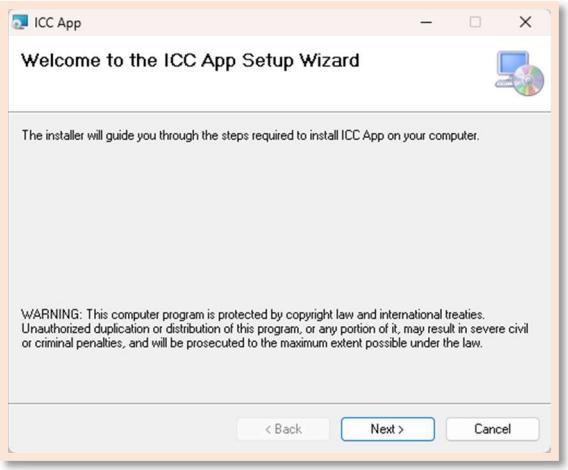


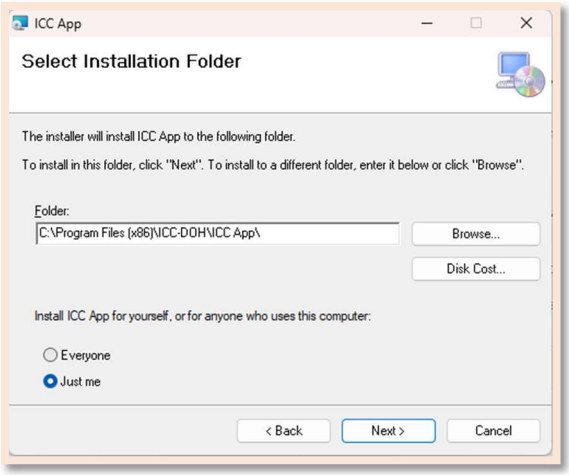
- เมื่อเปิดตัว ICC APP จะมีการแจ้งเตือนให้คลิกที่ More info แล้วทำการคลิกปุ่ม Run anyway

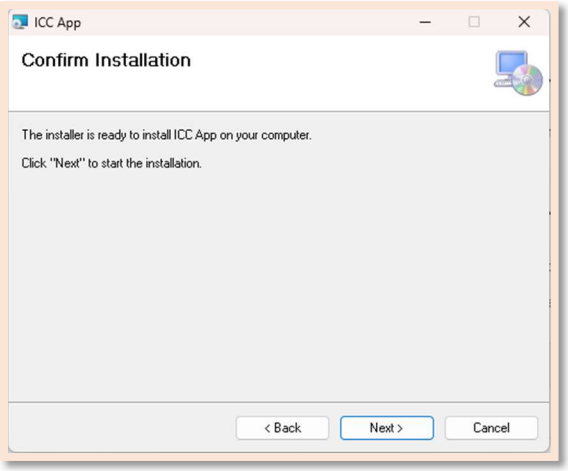


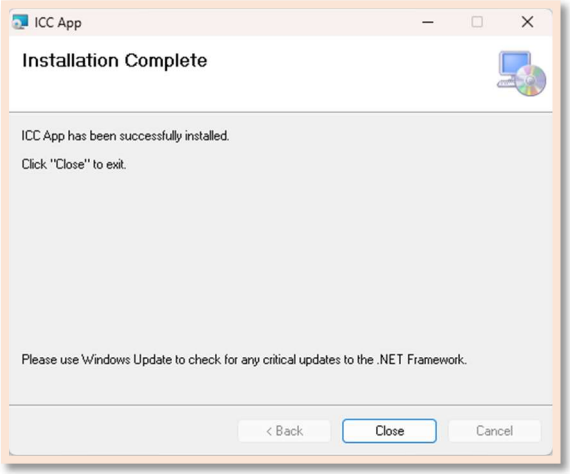


- ระบบจะแสดงหน้าจอตามภาพ ให้คลิกปุ่ม next จนถึงขั้นตอนติดตั้งสำเร็จ แล้วคลิกปุ่ม Close









หมายเหตุ : เมื่อติดตั้งเสร็จแล้วต้องมีการรีสตาร์ทเครื่องก่อนทุกครั้ง

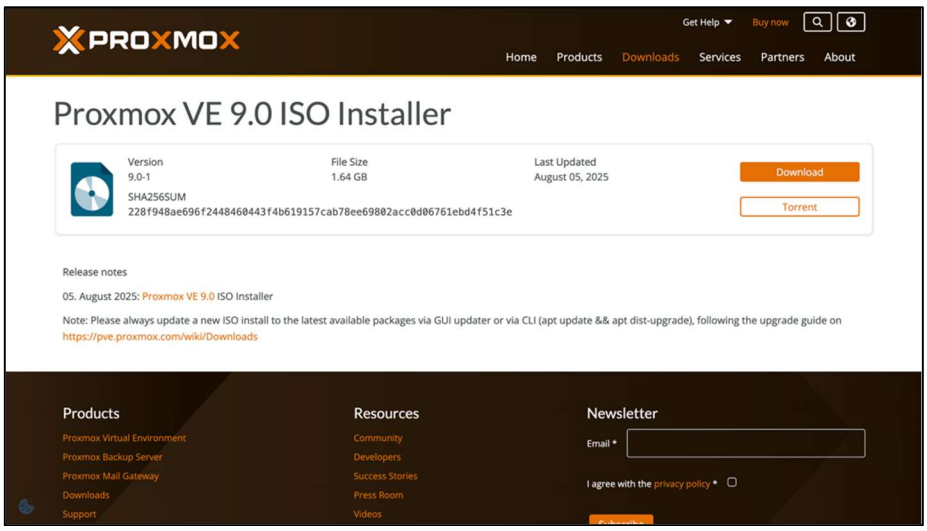
3) การติดตั้งระบบจัดการเครื่องคอมพิวเตอร์แม่ข่าย

3.1) การติดตั้งระบบปฏิบัติการ (OS) สำหรับจัดการ Virtual Machine (VM)

เป็นซอฟต์แวร์ Opensourceที่ใช้ทำเวอร์ชวลไลเซชั่นหรือคอนเทนเนอร์ สามารถทำงานได้คล้ายกับ VMware ESXi สามารถบริหารและจัดการข้อมูลทั้งหมดผ่านทางเว็บบราวเซอร์ และยังสามารถเขียน API เพื่อใช้จัดการระบบได้อีกด้วย และที่ขาดไม่ได้เลยคือ มันฟรีถ้าถามลงไปอีกว่ามันมีดีอะไรบ้าง บอกเลยว่ามีดีมากเพียงพอสำหรับระบบทั่วๆไปเลย ไม่ว่าจะเป็น การนำหลายๆเครื่องมาทำคลัสเตอร์กัน ซึ่งจะทำให้สามารถควบคุมทุกเครื่องจากศูนย์กลางได้ ไม่ต้องไปคอยเปิดแก้ทีละเครื่อง หรือแม้แต่สามารถย้ายเครื่องโดยไม่ต้องปิดเครื่องที่จะย้ายก็ได้ สามารถทำ Snapshot, Backup, Restore หรือแม้แต่ HA ได้ สำหรับรายละเอียดเพิ่มเติมที่นี่ https://www.proxmox.com/en/proxmox-virtual-environment/features

ขั้นตอนที่ 1

ดาวน์โหลดตัว Proxmox VE กันก่อน โดยไปที่ https:/www.proxmox.com/en/downloads เลื่อนลงไปหา Proxmox VE 9.0 ISO Installer (ถ้ามีใหม่กว่านี้ก็จะเลือกอันที่ใหม่กว่านี้ก็ได้)

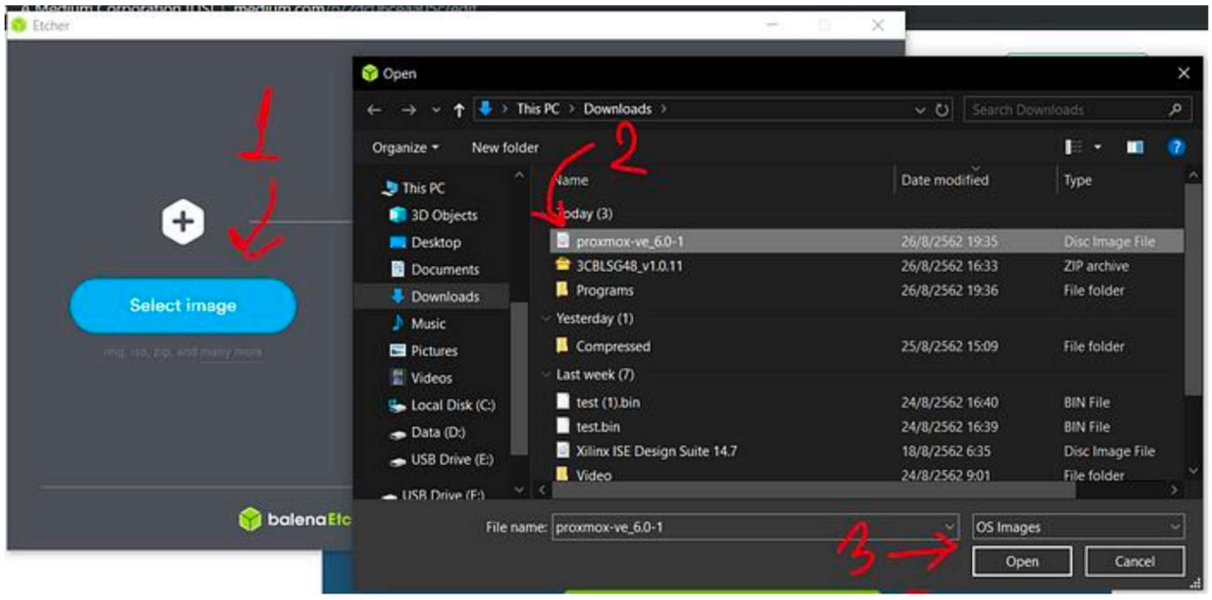


ขั้นตอนที่ 2

นำไฟล์นี้ไปใส่ USB ไดรฟ์ หรือสื่ออื่นๆ เพื่อให้เครื่องเซิฟเวอร์ ติดตั้งไฟล์ได้ ในที่นี้จะใส่ไปใน USB ไดรฟ์ โดยโหลดโปรแกรม balenaEtcher ก่อน (ไม่สามารถใช้โปรแกรม Rufus หรือ UNetbootin ได้) เข้าไปที่ https://www.balena.io/etcher/ แล้วกด Download เมื่อโหลดเสร็จแล้วให้ทำการติดตั้งโปรแกรม

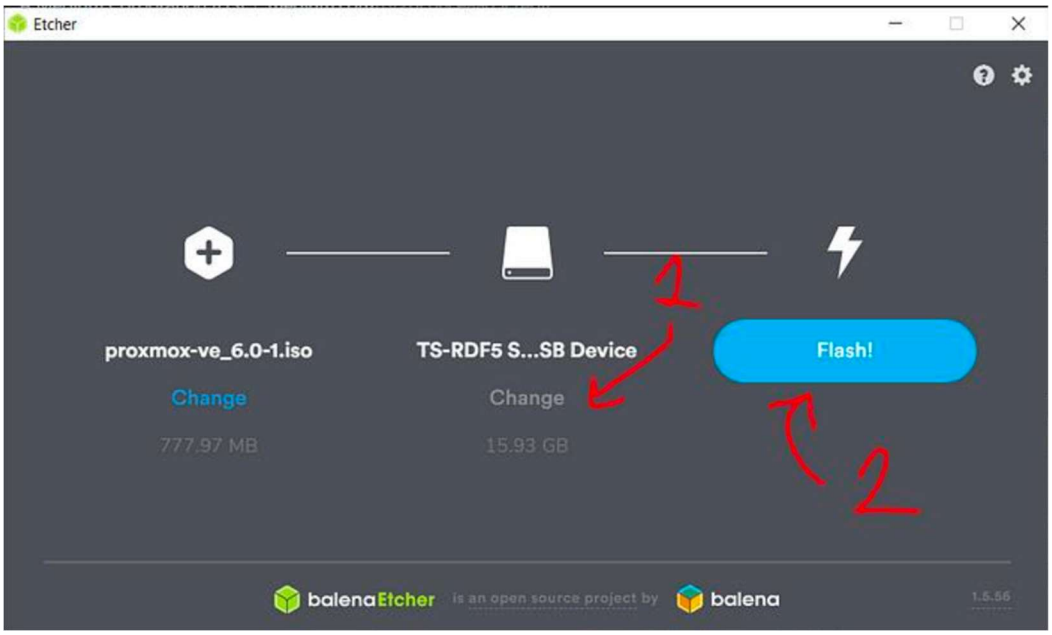
ขั้นตอนที่ 3

เมื่อติดโปรแกรม balenaEtcher เสร็จ โปรแกรมจะถูกเปิดขึ้นมาโดยอัตโนมัติ ให้กด Select Image แล้วเลือกไฟล์ Proxmox VE ที่เราโหลดมาในขั้นตอนแรก จากนั้นให้กด Open



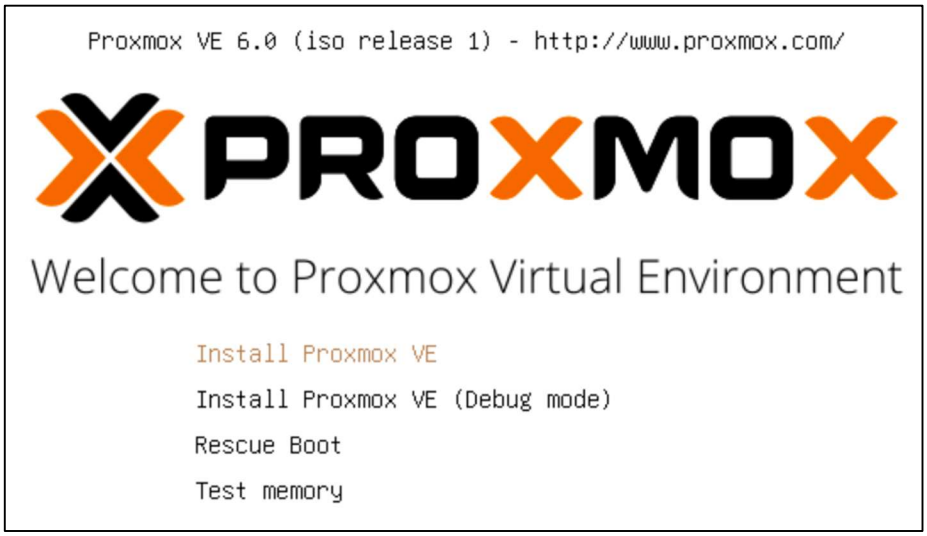
ขั้นตอนที่ 4

ให้เลือกไดรฟ์ที่เราต้องการจะเขียนตัวติดตั้งลงไป จากนั้นจึงกด Flash! แล้วก็รอจนโปรแกรมทำการเขียนข้อมูลลงไดรฟ์จนเสร็จ จากนั้นก็ปิดโปรแกรมไปเลย ไม่ได้ใช้แล้ว แล้วก็นำไปบูตที่เครื่องเซิฟเวอร์ที่ต้องการจะติดตั้ง ซึ่งขั้นตอนนี้จะแตกต่างกันไปตามแต่ละผู้ผลิตเซิฟเวอร์ จึงขอข้ามไป



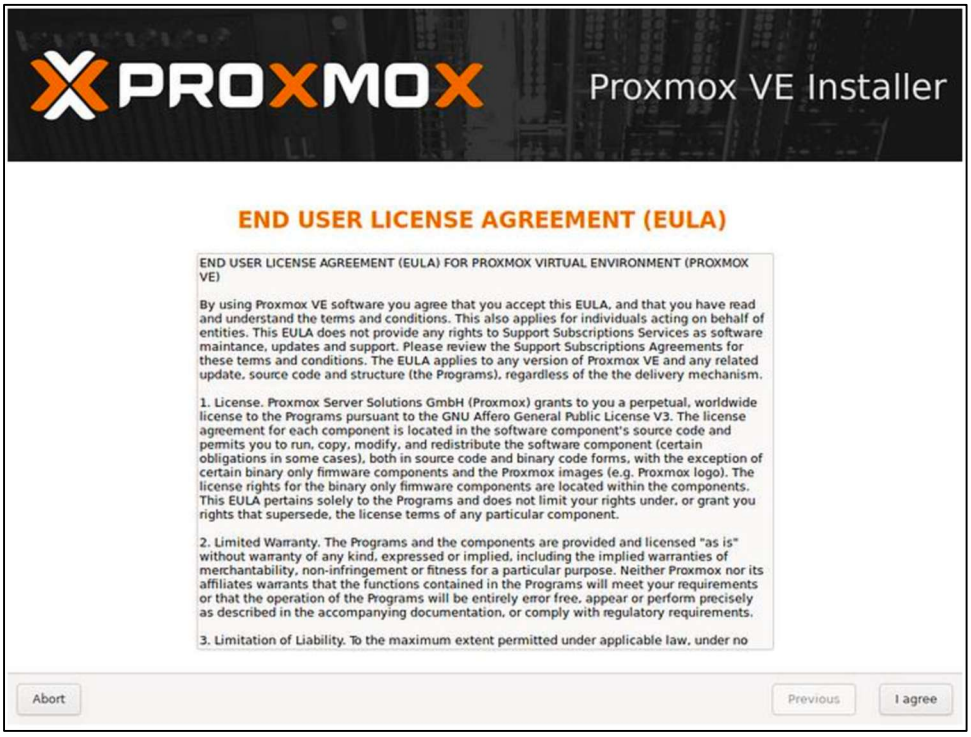
ขั้นตอนที่ 5

เมื่อบูตตัวติดตั้งขึ้นมาจะเจอหน้าตามด้านล่างนี้ ให้เลือก Install Proxmox VE (สำหรับในกรณีไม่มีไม่มีเมาส์มีแต่คีย์บอร์ด สามารถกด ALT ตามด้วยตัวอักษรที่ถูกขีดเส้นใต้ในข้อความของปุ่มที่ต้องการกด เช่น ALT+N สำหรับการกด Next หรือสามารถกด CTRL+ Tab สำหรับการกด Tab แบบปกติ)



ขั้นตอนที่ 6

จากนั้นก็จะเจอหน้าให้อ่านข้อตกลงสิทธิการใช้งานของผู้ใช้งาน ซึ่งเราสามารถอ่านก็ได้หรือไม่อ่านก็ได้ ถ้าดูจนพอใจแล้วก็ให้กด I agree เพื่อบอกว่าเรายอมรับข้อตกลงนี้

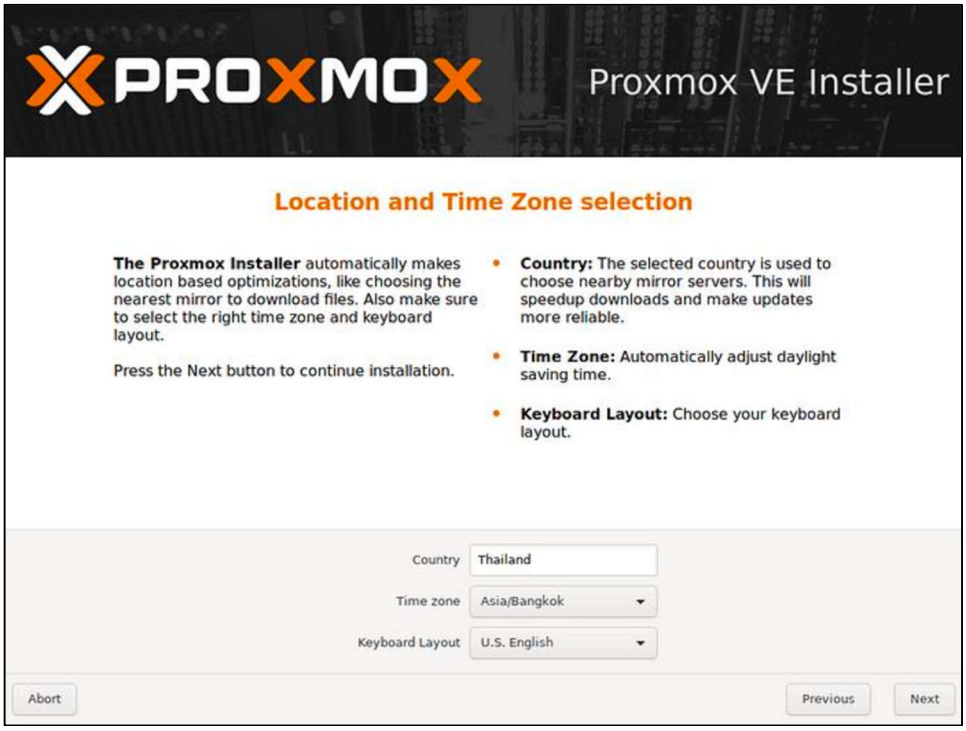


ขั้นตอนที่ 7

ทำการเลือกที่ที่เราต้องการติดตั้ง แล้วก็กด Next

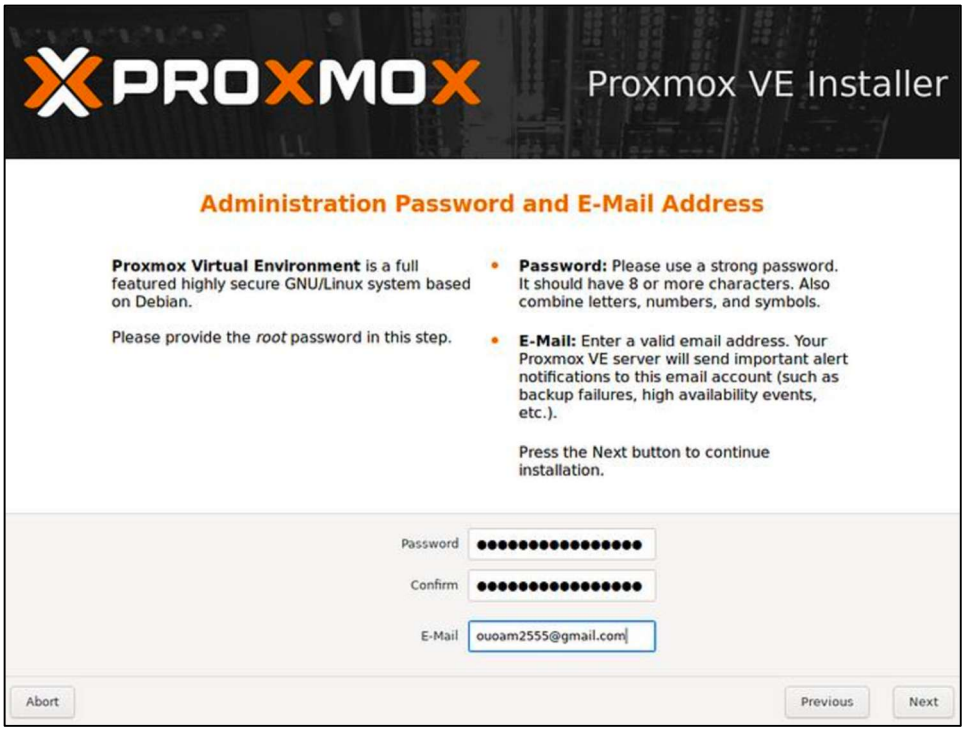
ขั้นตอนที่ 8

ทำการเลือกประเทศและเขตเวลาที่เราอยู่ อย่างในตัวอย่างจะเลือกเป็นประเทศไทยและมีเขตเวลาเป็นกรุงเทพฯ



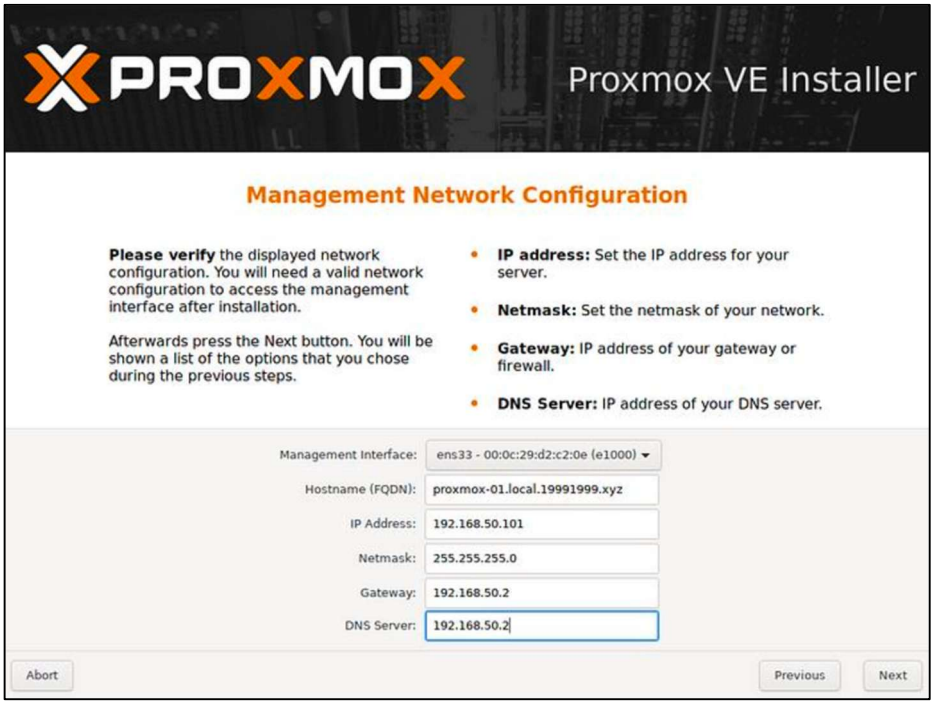
ขั้นตอนที่ 9

ทำการตั้งรหัสผ่านสำหรับผู้ใช้ root และ E-Mail เพื่อไว้รับการแจ้งเตือนต่าง ๆ



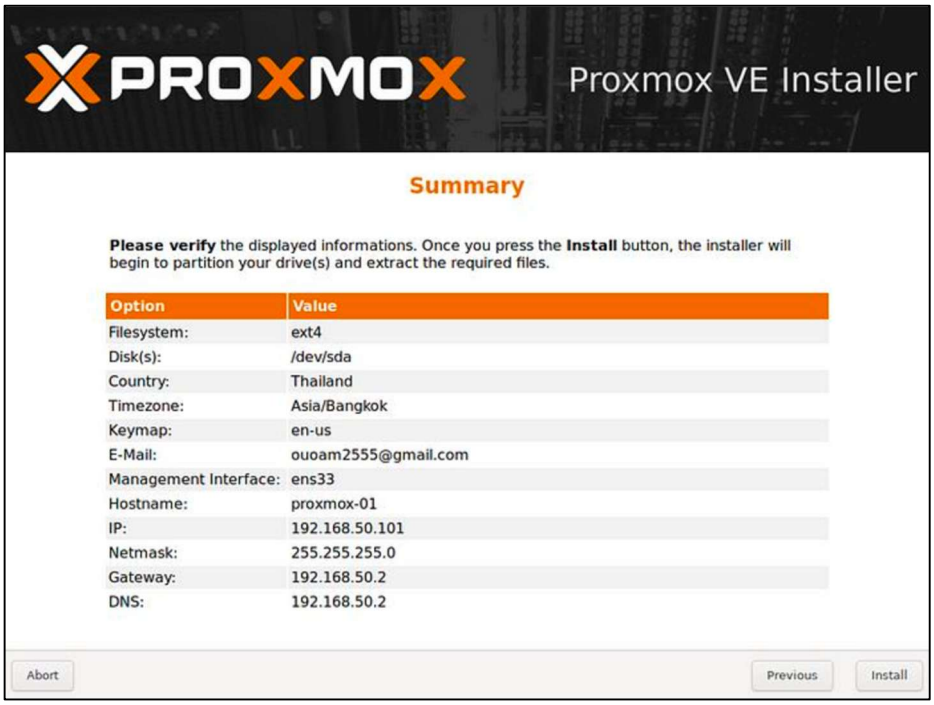
ขั้นตอนที่ 10

ทำการตั้งค่าช่องทางที่จะเอาไว้ควบคุมเครื่องว่าจะเอาเป็นอินเตอร์เฟสไหน ตั้งค่าชื่อเครื่อง อย่างในตัวอย่างที่ทำ เครื่องจะชื่อว่า proxmox-01 และตั้งค่าเน็ตเวิร์ค



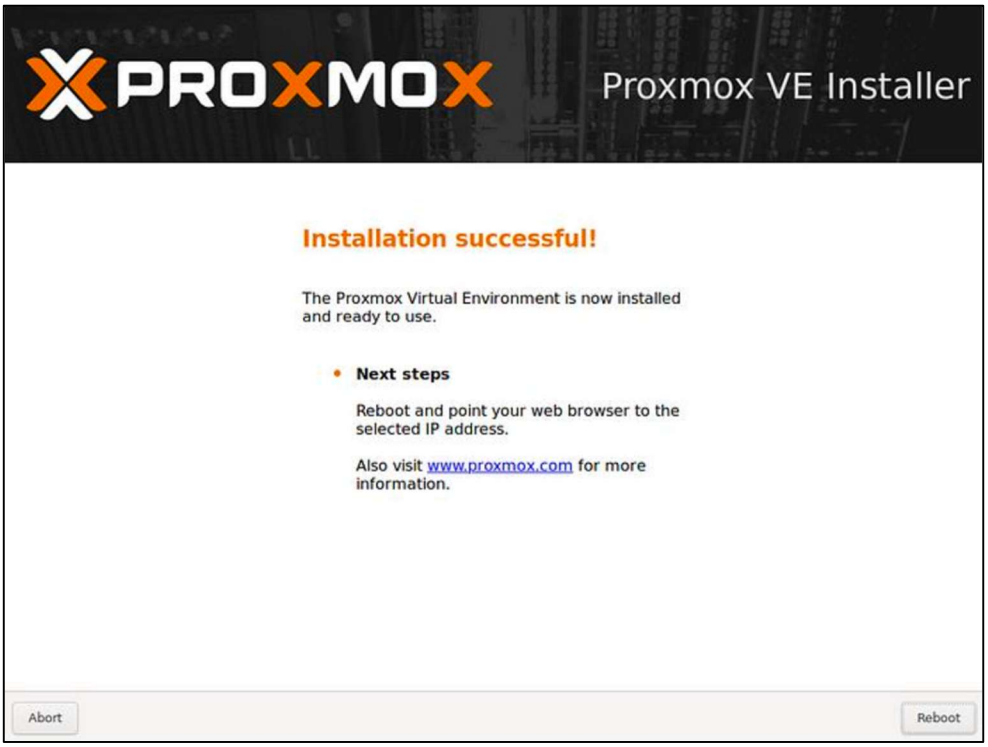
ขั้นตอนที่ 11

ทำการตรวจสอบการตั้งค่าว่าถูกต้องหรือไม่ ถ้าถูกและกด install



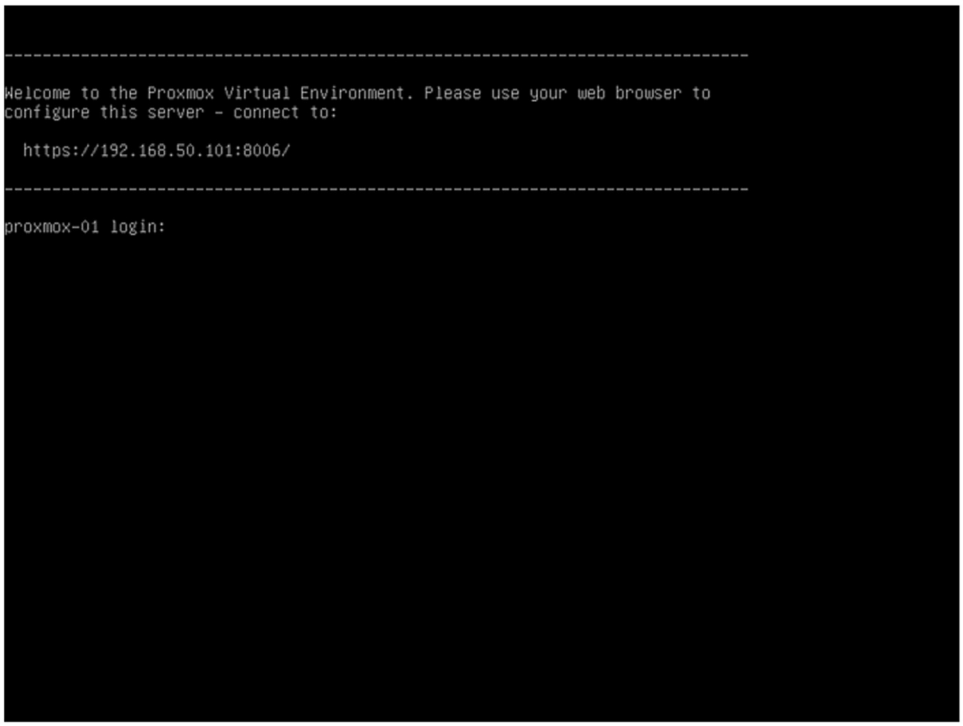
ขั้นตอนที่ 12

เมื่อติดตั้งเสร็จกด Reboot



ขั้นตอนที่ 13

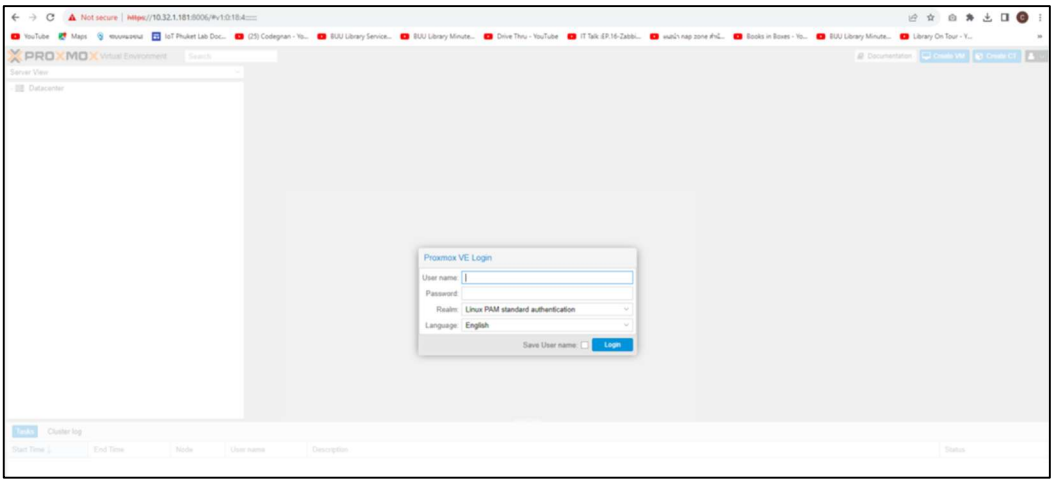
เมื่อ Reboot เสร็จจะขึ้นหน้าตามด้านล่างนี้ ก็แสดงว่าสามารถเริ่มใช้งานได้



4) การใช้งานระบบจัดการเครื่องคอมพิวเตอร์แม่ข่าย Proxmox VE

4.1) การเข้าใช้งานระบบ

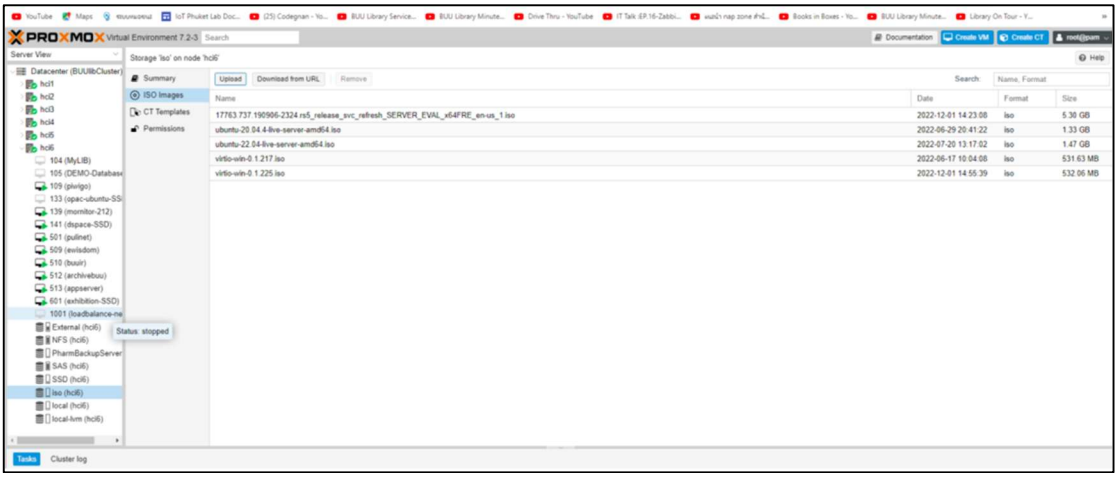
URL https://10.32.1.181:8006/ หรือ https://10.32.1.182-186:8006/ (เป็นช่องทางมาตรฐานที่สำหรับเข้าใช้งาน Proxmox) ส่วน user และ password ให้ใช้ตามที่สร้างไว้ในเบื้องต้น



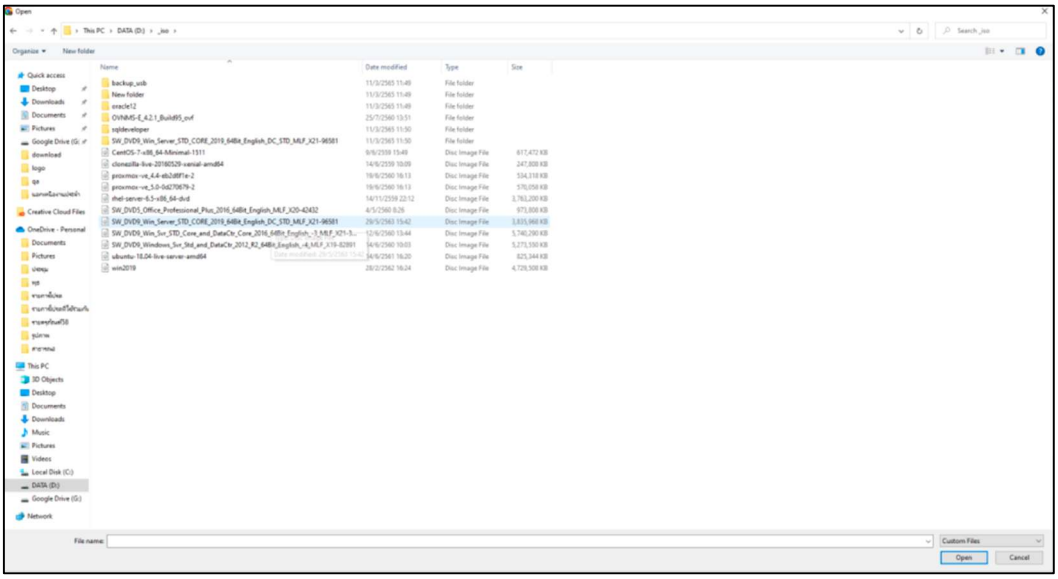
4.2) Upload ไฟล์ .iso

ก่อนสร้าง VM ต้อง Upload ไฟล์ .iso ของ OS ที่ต้องการติดตั้ง ไปไว้ในเว็บ PROXMOX ก่อน ดังนี้

- เลือกเมนู Local > ISO Images
- รอให้ Upload เสร็จ Proxmox ก็จะมีไฟล์ .iso สำหรับติดตั้ง OS แล้ว



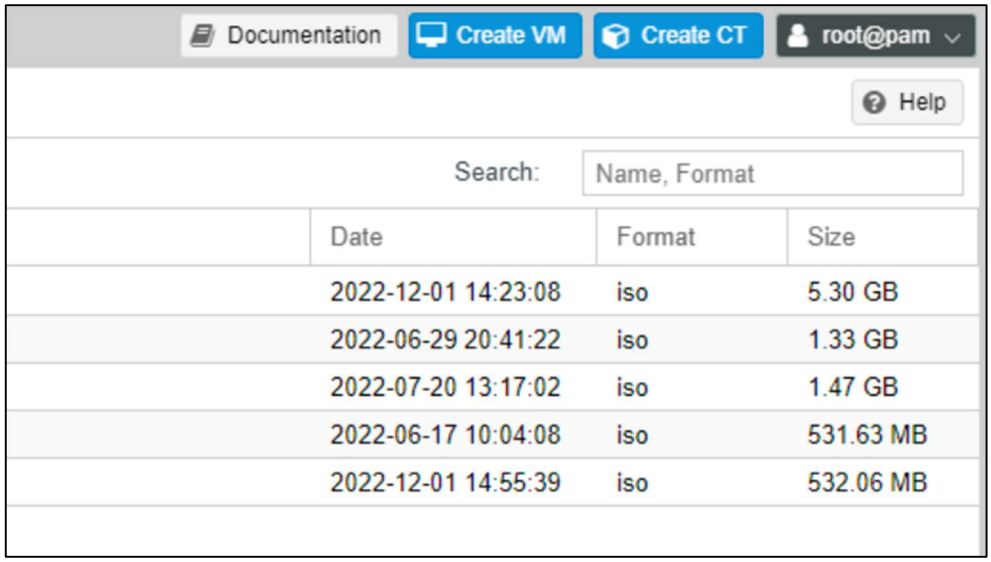
กดปุ่ม Upload ด้านบน แล้วเลือกไฟล์ .iso ที่ต้องการ และรอให้ Upload เสร็จ Proxmox ก็จะมีไฟล์ .iso สำหรับติดตั้ง OS



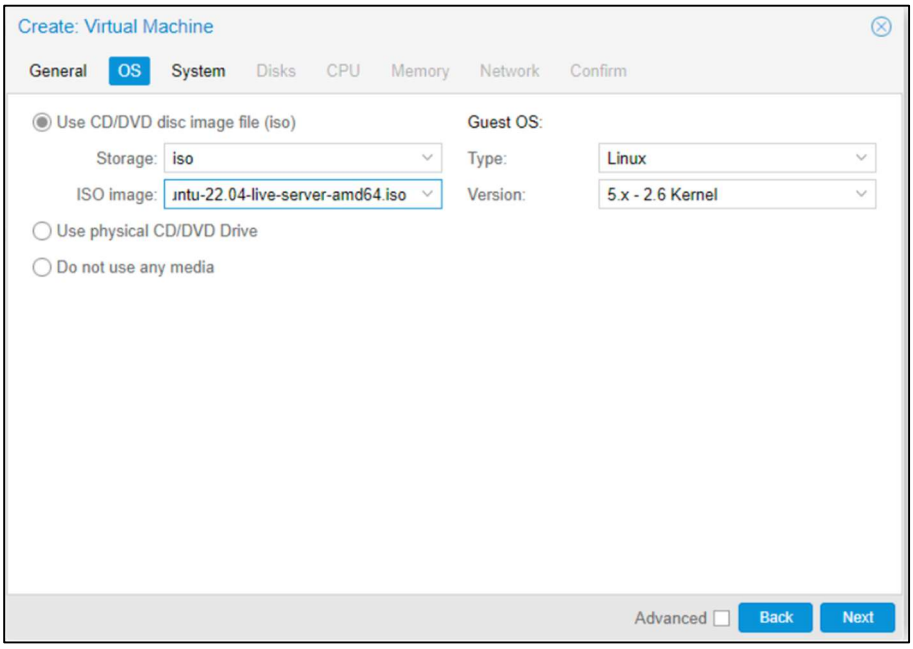
4.3) การสร้าง VM

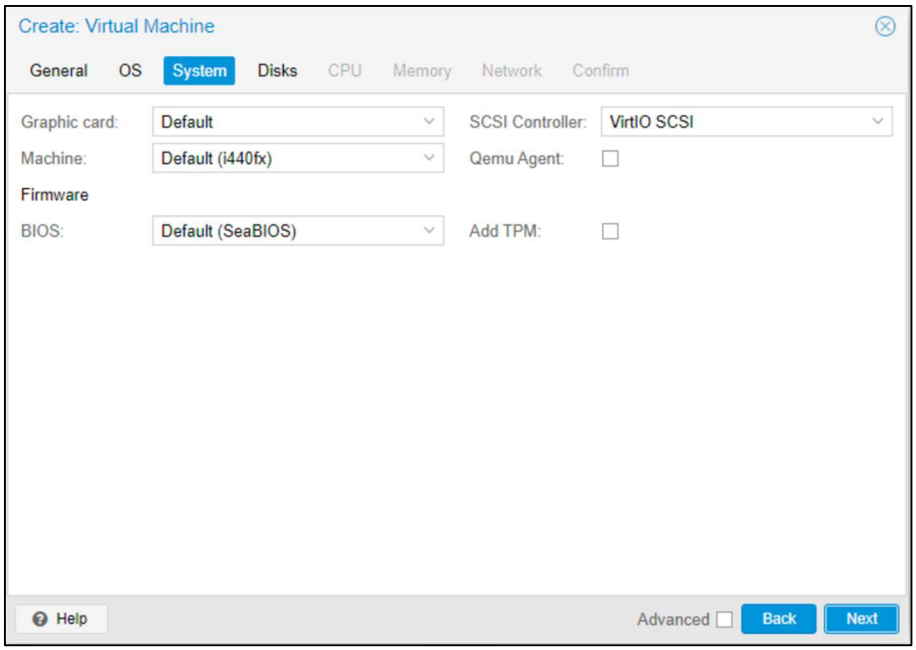
VM ของ PROXMOX จะมีหมายเลขประจำ VM โดย VM ตัวแรกจะเริ่มต้นที่เลข 100 และบวก 1 ไปเรื่อยๆ เป็น 101 , 102 , 103 , ...

- ตั้งหมายเลข VM เองได้ แต่ VM จะต้องมีหมายเลขที่ไม่ซ้ำกัน
- กดปุ่ม Create VM (มุมบนขวา Web UI)



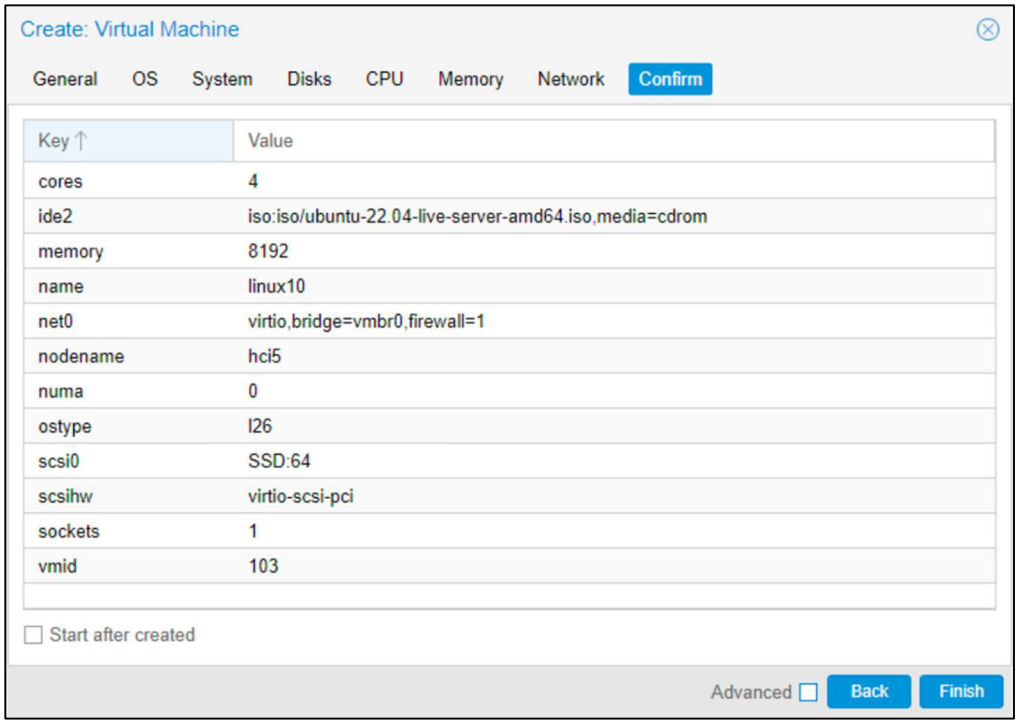
เลือกไฟล์ .iso ของ OS ที่ต้องการติดตั้ง (ตัวอย่างที่เลือกไฟล์Ubuntu-22.04-live-server-amd64.iso) และเลือกตาม Default ของระบบที่ให้มา



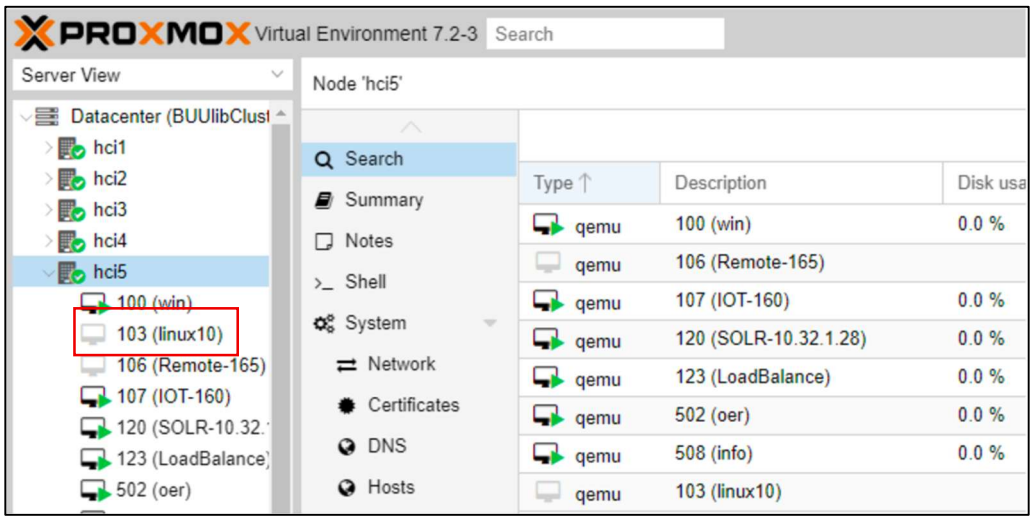


ในหัวข้ออื่น ๆ ส่วนที่เหลือให้ใส่ตามความต้องการพื้นฐานของระบบ Disk, CPU, Memory, Network

เมื่อกำหนดทรัพยากรต่าง ๆ ที่จำเป็นแล้ว จะเข้าสู่หน้า Confirm ซึ่งสรุปรายการทั้งหมด

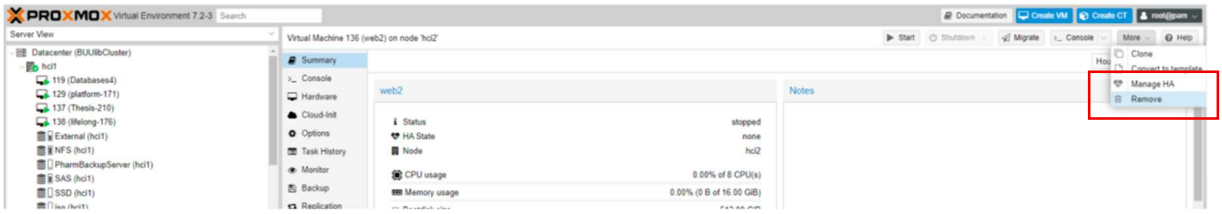


กดปุ่ม Finish แล้ว PROXMOX ก็จะสร้าง VM ให้เรา โดยจะมี VM ชื่อ 103 (linux10) อยู่ทางซ้ายมือของเมนู

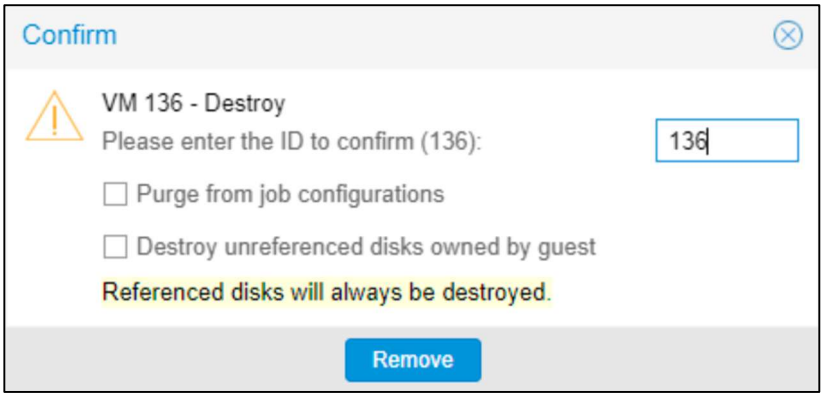


4.4) การลบ VM

หากต้องการลบ VM 136 ชื่อ web2 จากนั้นคลิกที่เมนู More Remove อยู่มุมขวาบน

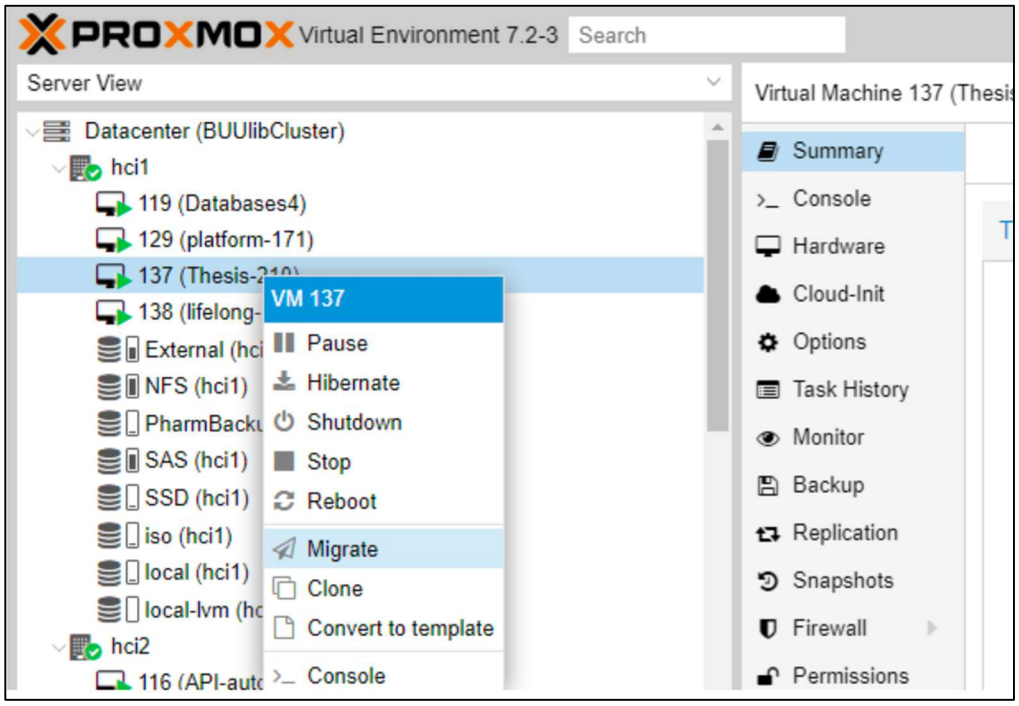


ระบบจะขึ้น Popup แล้วพิมพ์หมายเลข VM คือ 136 ในช่องสี่เหลี่ยมแล้วกดปุ่ม Remove

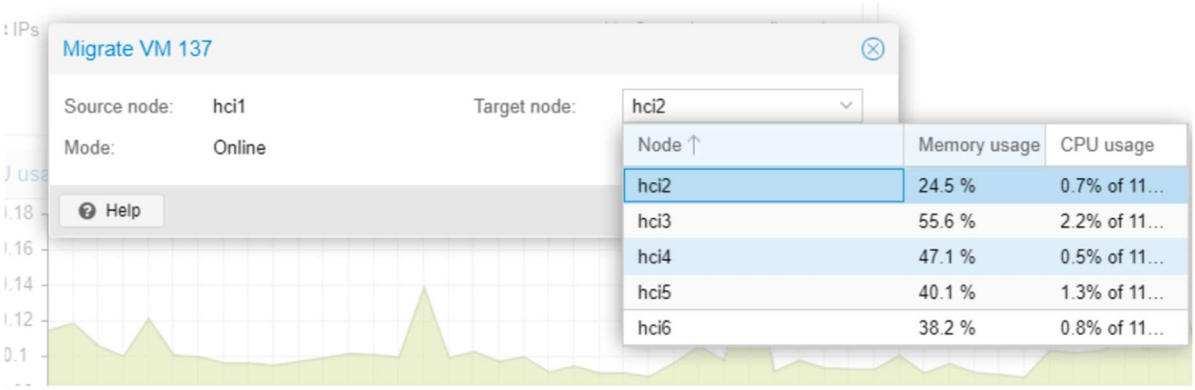


4.5) การทำ Migrate VM

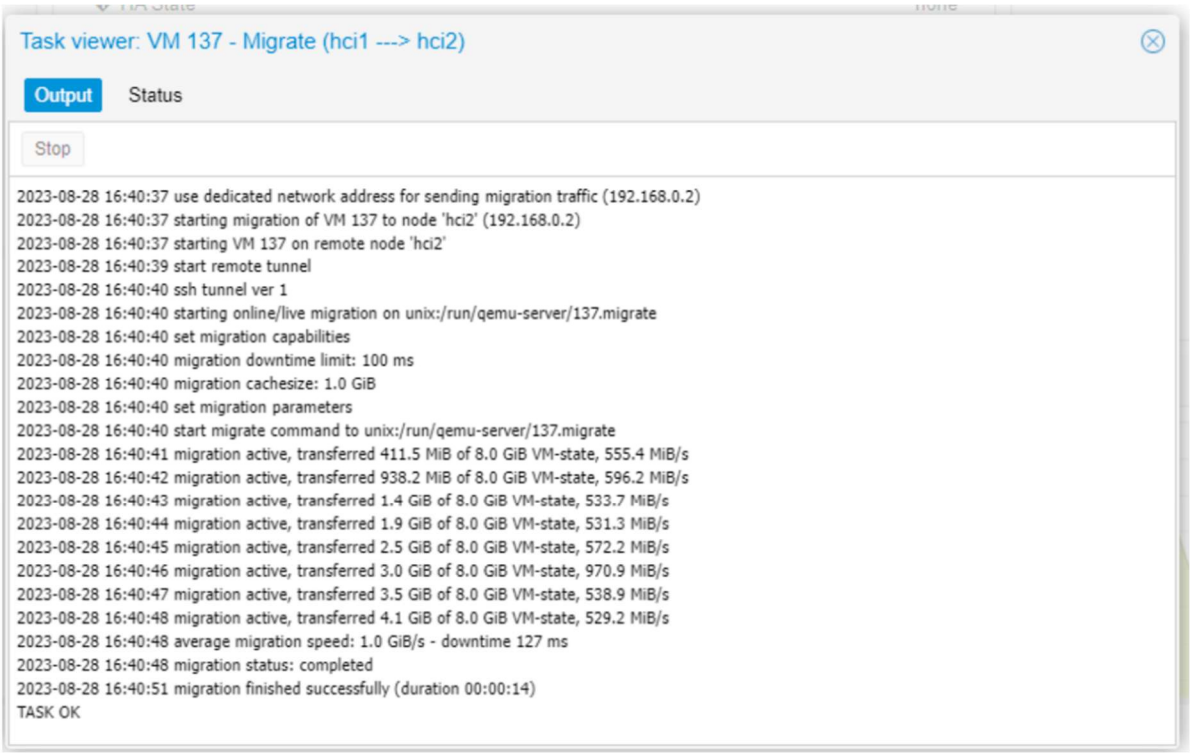
คือการย้าย VM จาก HCI ไปยังอีก HCI หนึ่ง อย่างเช่น Migrate VM 137 จาก HCI 1 ไปยัง HCI 2 เป็นต้น โดย คลิกที่ VM 137 แล้วคลิกขวา เลือกเมนู Migrate



จากนั้นเลือก HCI 2 เป็น Target node(ปลายทาง) แล้วคลิกปุ่ม Migrate

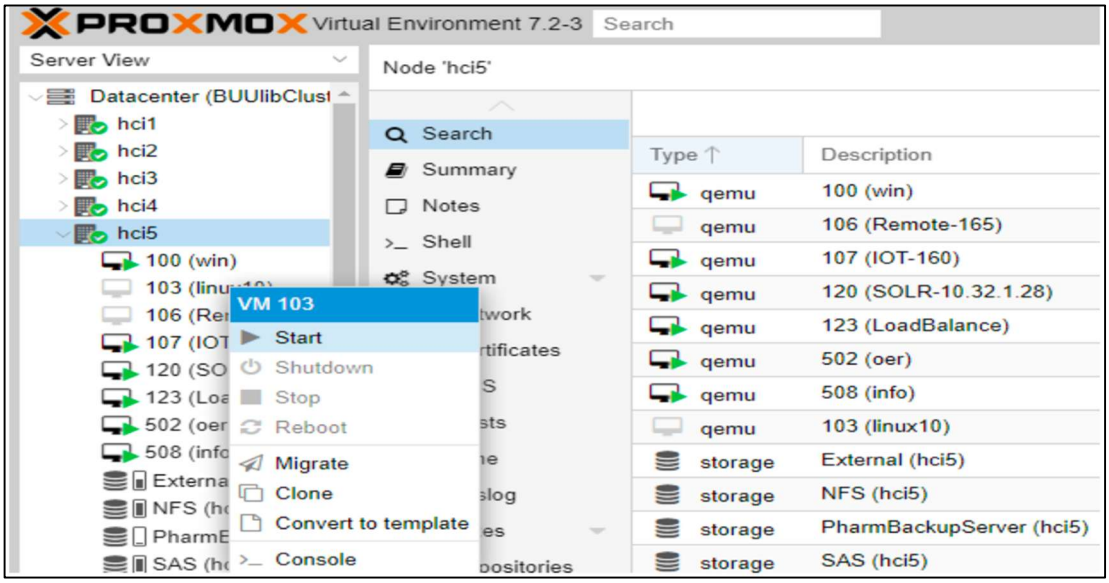


ระบบจะขึ้น Task viewer การ Migrate

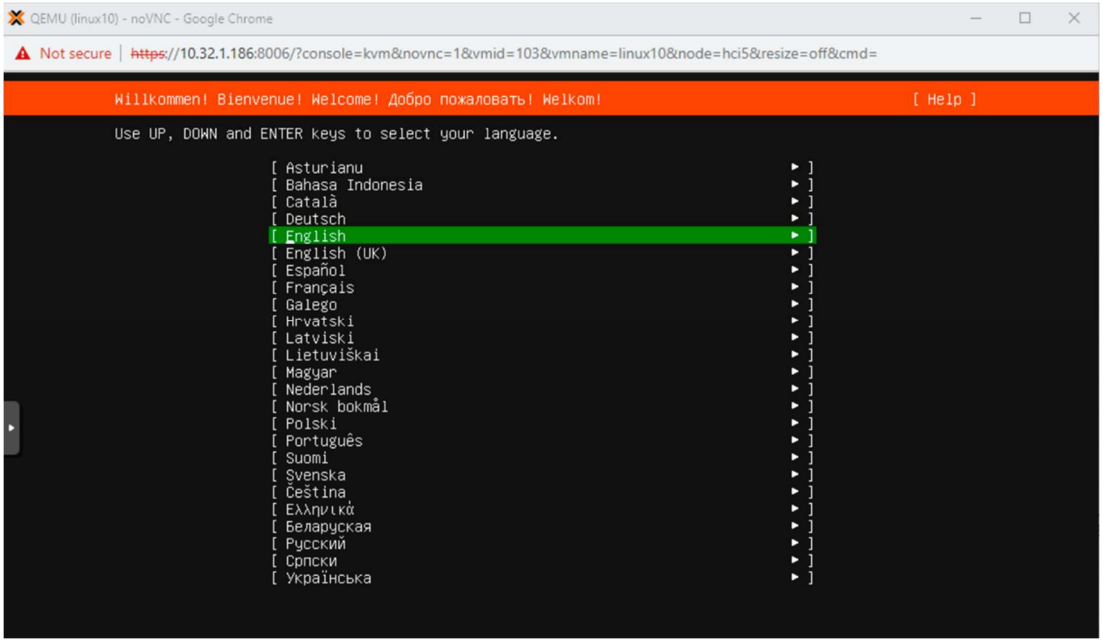


4.6) เริ่ม Start VM

คลิกขวาที่ VM ที่เมนูทางซ้าย แล้วกดปุ่ม Start



เลือก VM เมนูทางซ้าย 103 (linux10) > กดเมนู Console ติดตั้ง OS จนเสร็จเรียบร้อย VM ก็พร้อมใช้งานทันที



4.7) การตั้ง IP Address , Subnet , Gateway , DNS ใน VM

มี 2 กรณี คือ Static IP Address กับ Dynamic IP Address (ตัวอย่าง เช่น Static IP Address)

IP Address = 10.32.1.211 (ต้องตั้ง IP Address ไม่ซ้ำกัน)

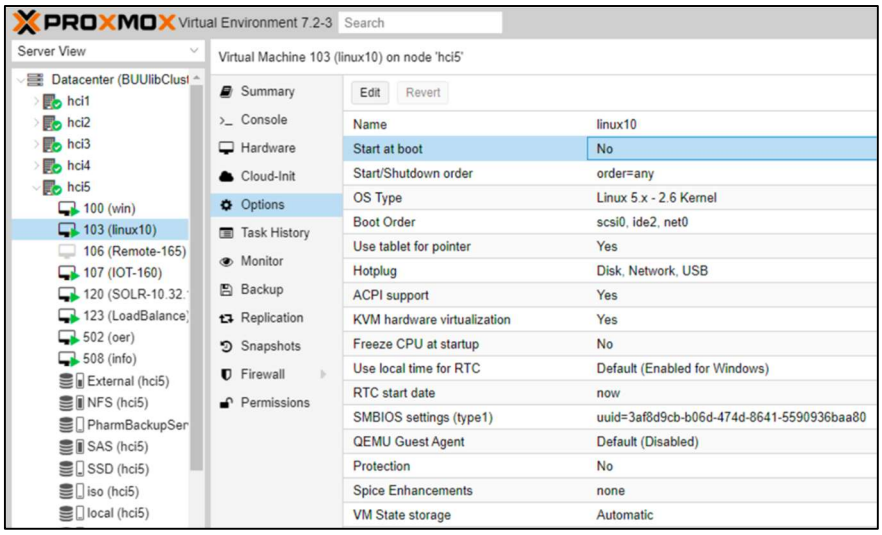
Supnet = 255.255.255.0

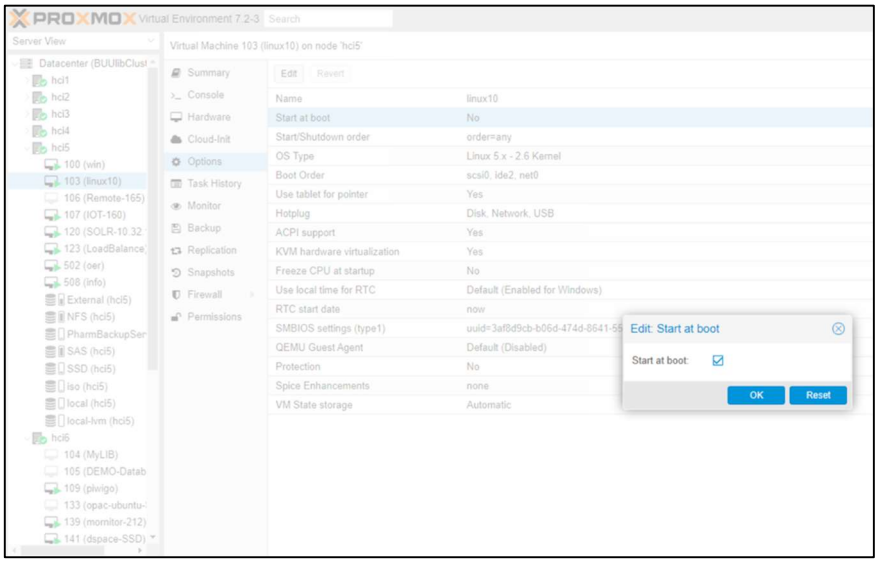
Gate way = 10.32.1.1

DNS = 10.32.1.7

4.8) ตั้งให้ VM ทำงานอัตโนมัติ (Auto Start)

ทุกครั้งที่ Restart PROXMOX (Reboot เครื่อง) VM ที่เราสร้างขึ้นมาใหม่จะไม่ Auto Start หาก PROXMOX วิธีตั้งให้ VM รัน Auto คือ เลือก VM เมนูทางซ้าย 103 (linux10) > กดเมนู Options



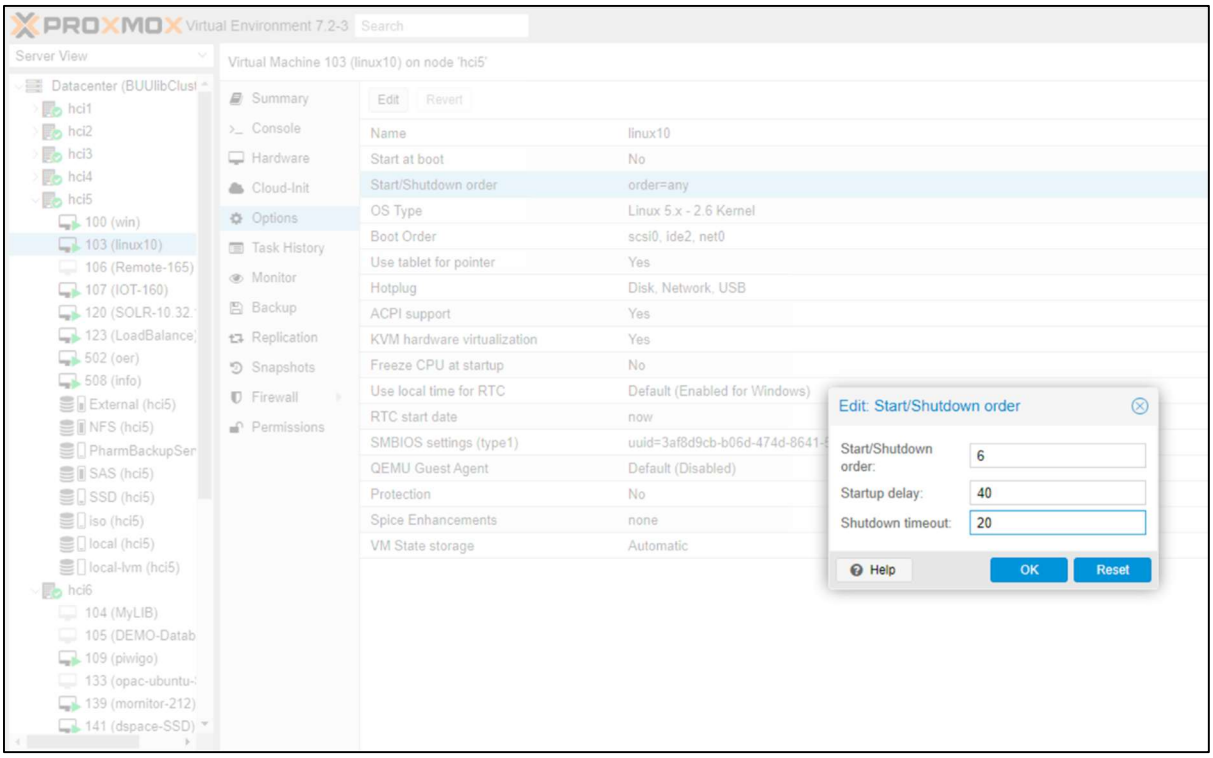


4.9) ตั้งให้ VM แต่ละตัว เริ่ม Start ในช่วงเวลาต่างกัน

ในหลายๆกรณีที่สร้าง VM ไว้หลายตัว แล้วต้องการให้บาง VM รันก่อน VM อื่น เช่น ให้ VM ที่เป็น Database (Start) ก่อน VM ที่เป็น Web Server เป็นต้น สามารถกำหนดได้ว่าจะให้ VM แต่ละตัว Auto Start

- สั่งให้ Start ก่อน – หลังได้
- สั่งให้ Start ช้าหรือเร็วได้
- สั่งให้ shutdown VM ช้าหรือเร็วได้

โดยเลือก VM เมนูทางซ้าย 103 (linux10) > กดเมนู Options > คลิก เลือกที่ Start/Shutdown order แล้วกดปุ่ม Edit (ด้านบน)

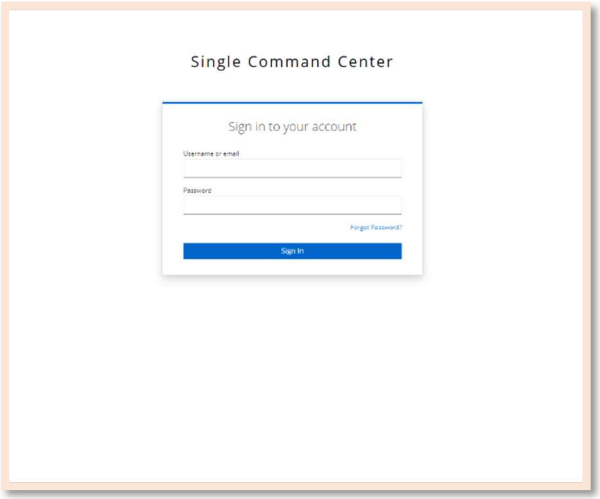


5) การใช้งาน ICC Bodycam Management

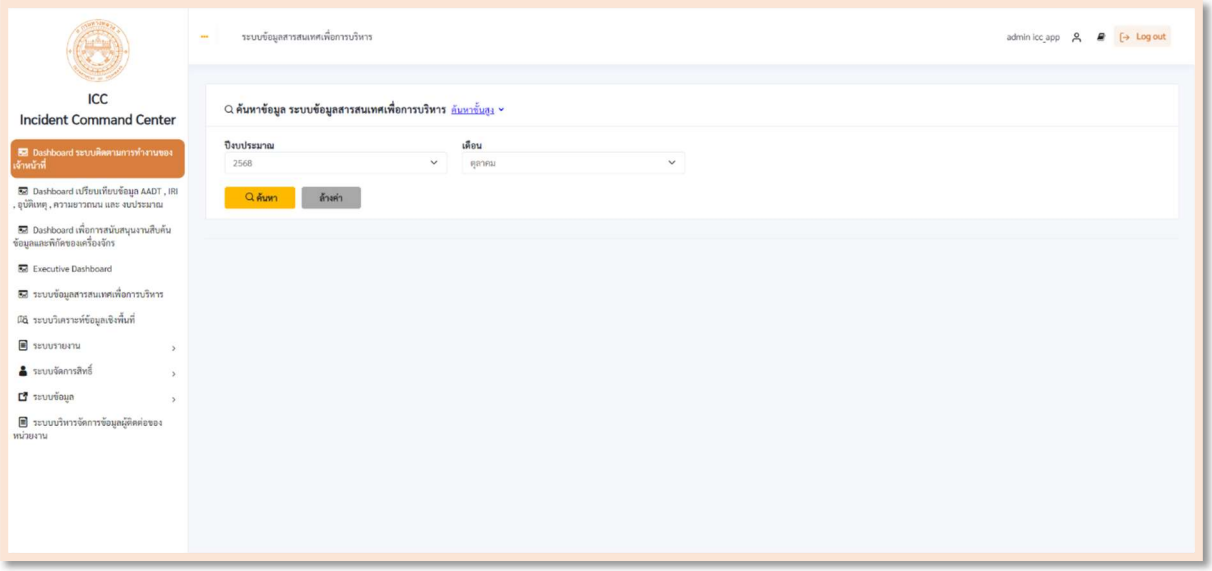
ผู้ใช้สามารถเข้าผ่านหน้าเว็บไซต์ icc.doh.go.th แล้วทำการเข้าสู่ระบบให้เรียบร้อย

ชื่อผู้ใช้ : admin_icc_app

รหัสผ่าน : password.

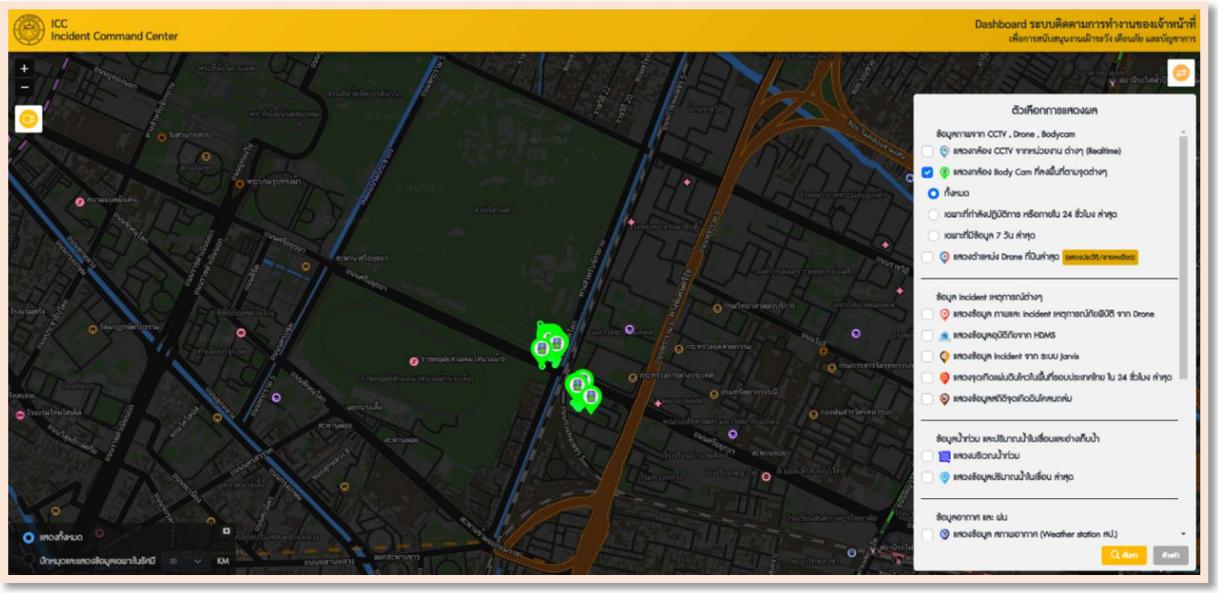


เมื่อทำการเข้าสู่ระบบแล้วจะแสดงหน้า Dashboard ของหน้าเว็บไซต์ ให้ไปที Dashboard ระบบติดตามการทำงานของเจ้าหน้าที่

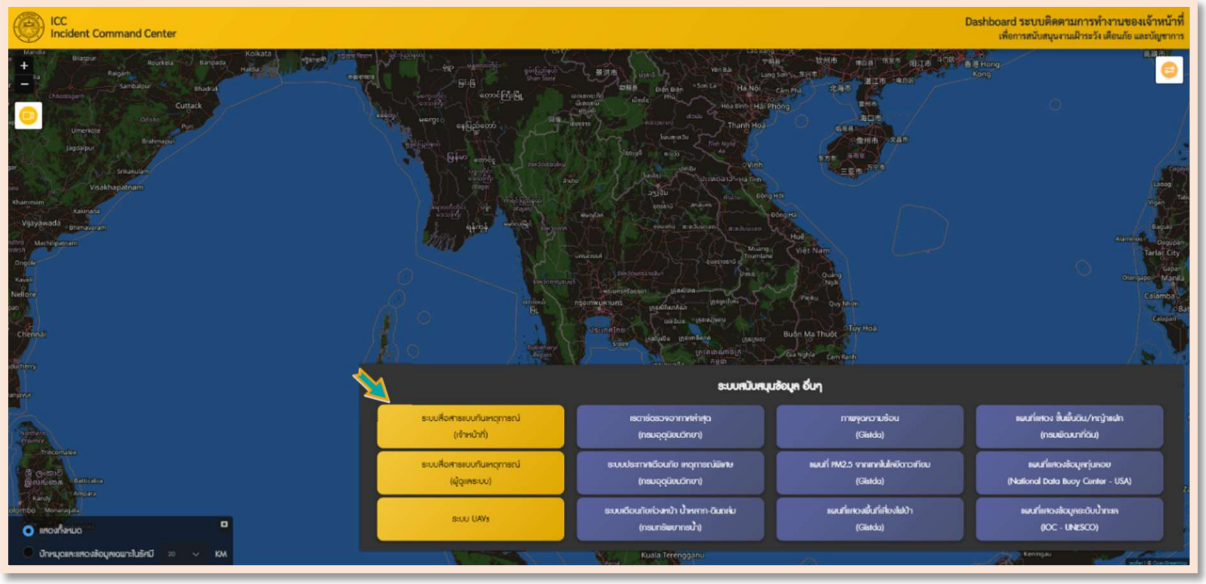


Dashboard ระบบติดตามการทำงานของเจ้าหน้าที่ ส่วนที่จะมี 3 จุดหลัก ๆ

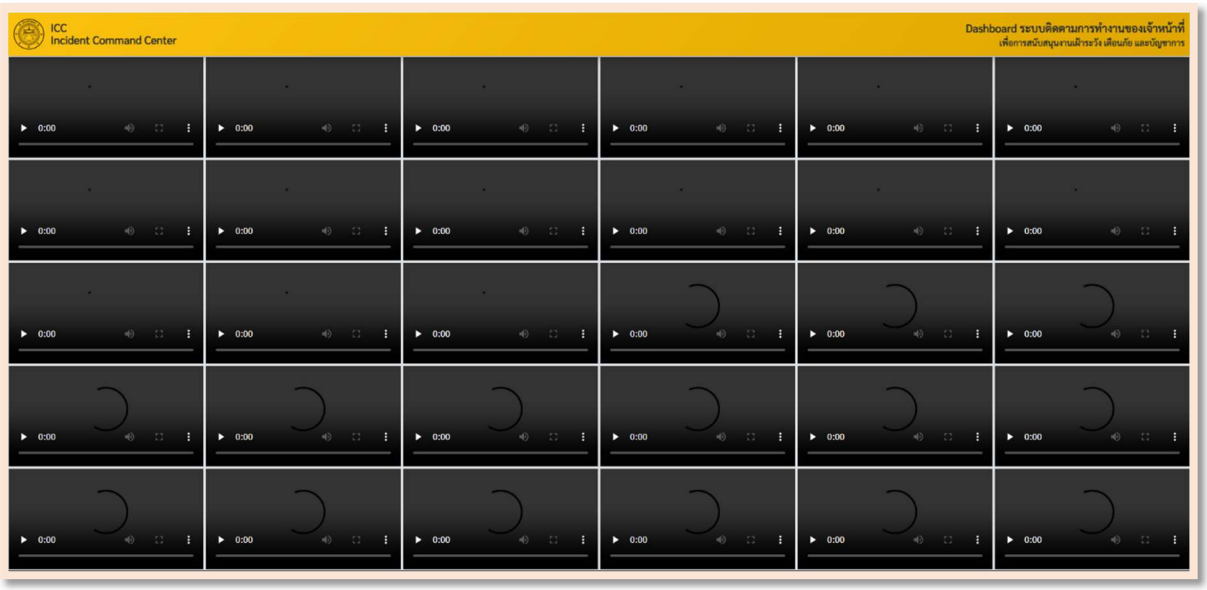
- แสดงกล้อง Body Cam ที่ลงพื้นที่ตามจุดต่างๆ เป็นฟังก์ชันทีจะระบุจุดทีอุปกรณ์อยู่



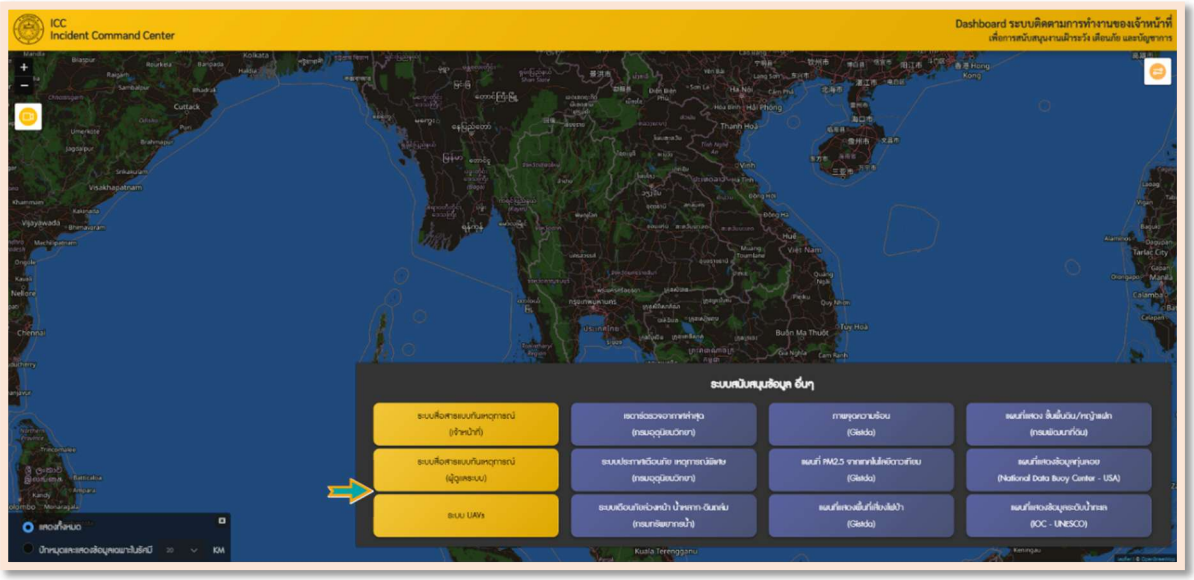
- ระบบสื่อสารแบบทันเหตุการณ์ (เจ้าหน้าที่) จะเป็นฟังก์ชันที่สามารถดูภาพ Stem สดจากตัว Body Cam มาแสดงทั้งหมด 30 เครื่อง สามารถหาฟังก์ชันที icon ตรงมุมล่างขวาของหน้าเว็บไซต์



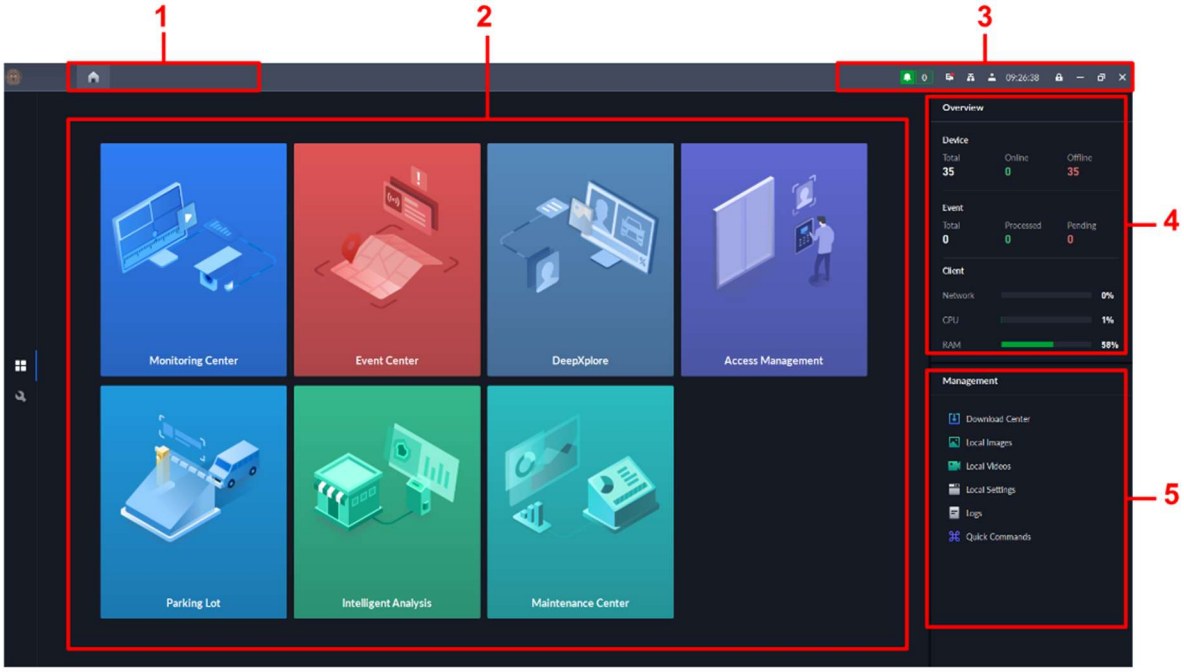
- หน้าต่างแสดงภาพ Stem ทั้ง 30 เครื่อง



- ระบบสื่อสารแบบทันเหตุการณ์ (ผู้ดูแลระบบ) จะเป็นส่วนที่เชื่อมกับ ICC Bodycam Management เมื่อเลือกฟังก์ชันนี้ จะทำการเรียก ICC Bodycam Management ขึ้นมาแล้วเข้าสู่ระบบโดยอัตโนมัติ



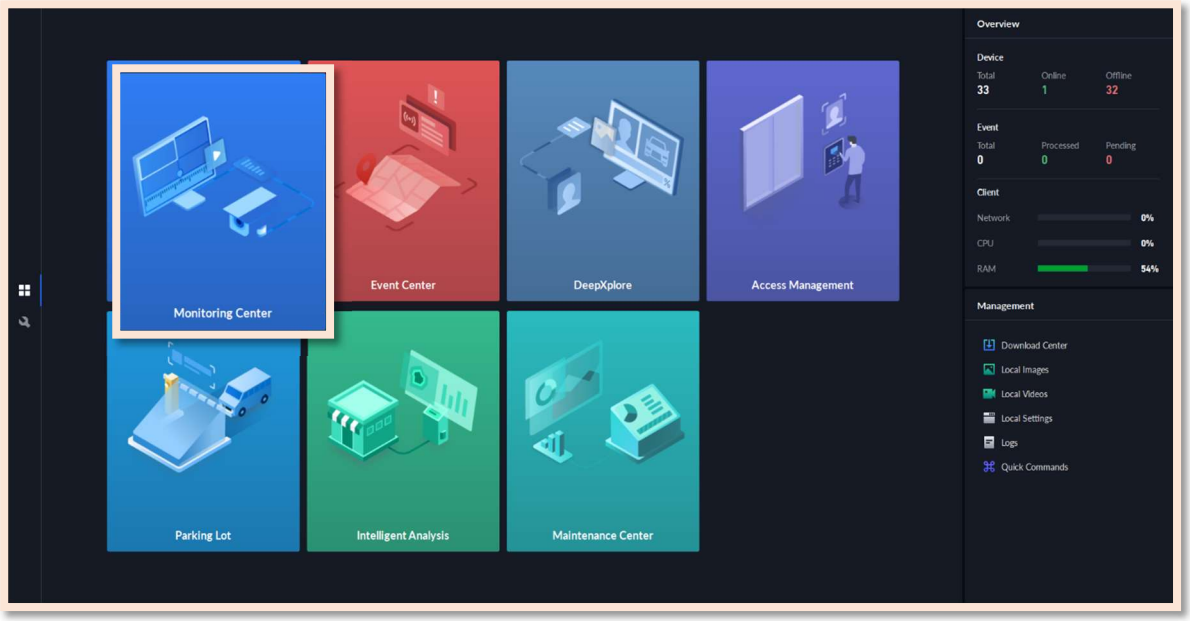
หน้าต่างโปรแกรม ICC Bodycam Management



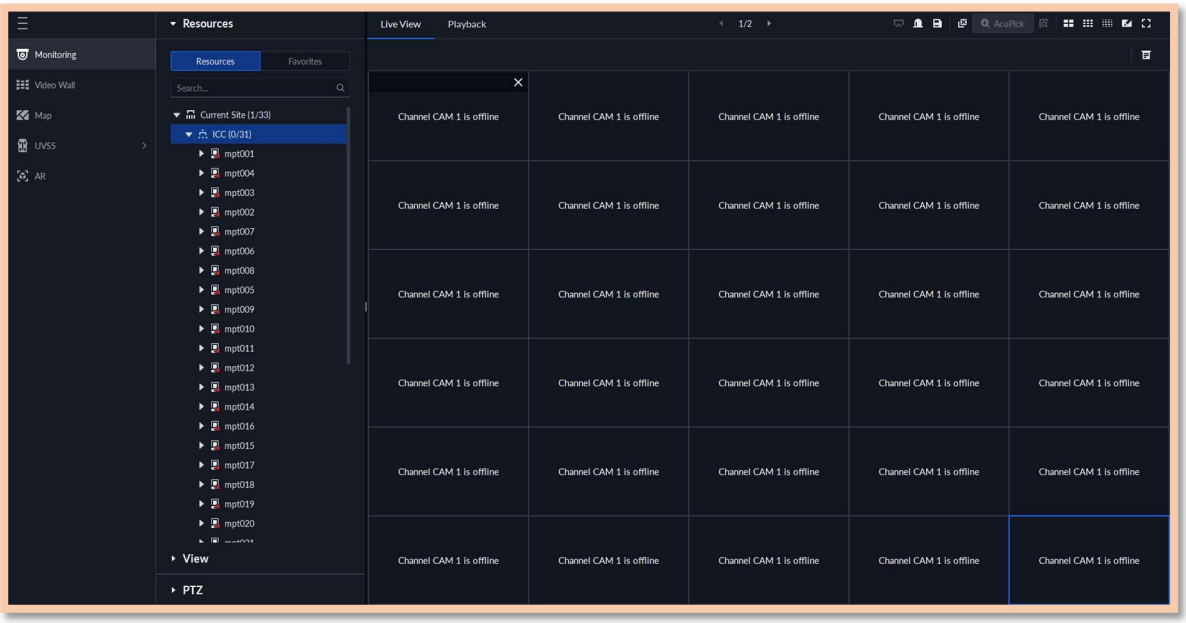
ลำดับ	ชื่อ	คุณสมบัติ
1.	Tab	- แสดงชื่อของแท็บทั้งหมดที่ถูกเปิด
2.	Applications	- ตัวเลือกการใช้งาน การจัดการการเข้าถึง การวิเคราะห์อัจฉริยะ และการควบคุมทางเข้า
3.	System Settings	- เปิดหรือปิดเสียงสัญญาณเตือน - แสดงจำนวนการแจ้งเตือน คลิกไอคอนเพื่อไปที่ Event Center เพื่อดูข้อความของระบบ เช่น ข้อมูลของอุปกรณ์ถูกแก้ไขหรือถูกลบ - ข้อมูลผู้ใช้: คลิกไอคอน จากนั้นคุณสามารถเข้าสู่ระบบหน้าเว็บได้โดยการคลิกที่ที่อยู่ IP ของระบบ เปลี่ยนรหัสผ่าน ล็อกไคลเอนต์ และออกจากระบบ • คลิกที่อยู่ IP ของแพลตฟอร์มเพื่อไปที่หน้าเว็บ • คลิกเปลี่ยนรหัสผ่านเพื่อเปลี่ยนรหัสผ่านผู้ใช้ • คลิกเกี่ยวกับเพื่อดูข้อมูลเวอร์ชัน
4.	Overview	- จำนวนอุปกรณ์รวมทั้งออฟไลน์และออนไลน์ - จำนวนเหตุการณ์ทั้งหมดที่ได้รับการประมวลผลและรอดำเนินการ - เครือข่ายไคลเอนต์ การใช้งาน CPU และ RAM
5.	Management	- ดาวน์โหลดวิดีโอ - ตรวจสอบภาพและวิดีโอในพื้นที่ - การตั้งค่าสำหรับวิดีโอ สแนปช็อต วิดีโอวอลล์ สัญญาณเตือน ความปลอดภัย และปุ่มลัด - ดูและจัดการบันทึก - ปรับแต่งคำสั่ง HTTP ด่วน สำหรับรายละเอียด

(1) ฟังก์ชั่นที่ต้องใช้ของ ICC Bodycam Management

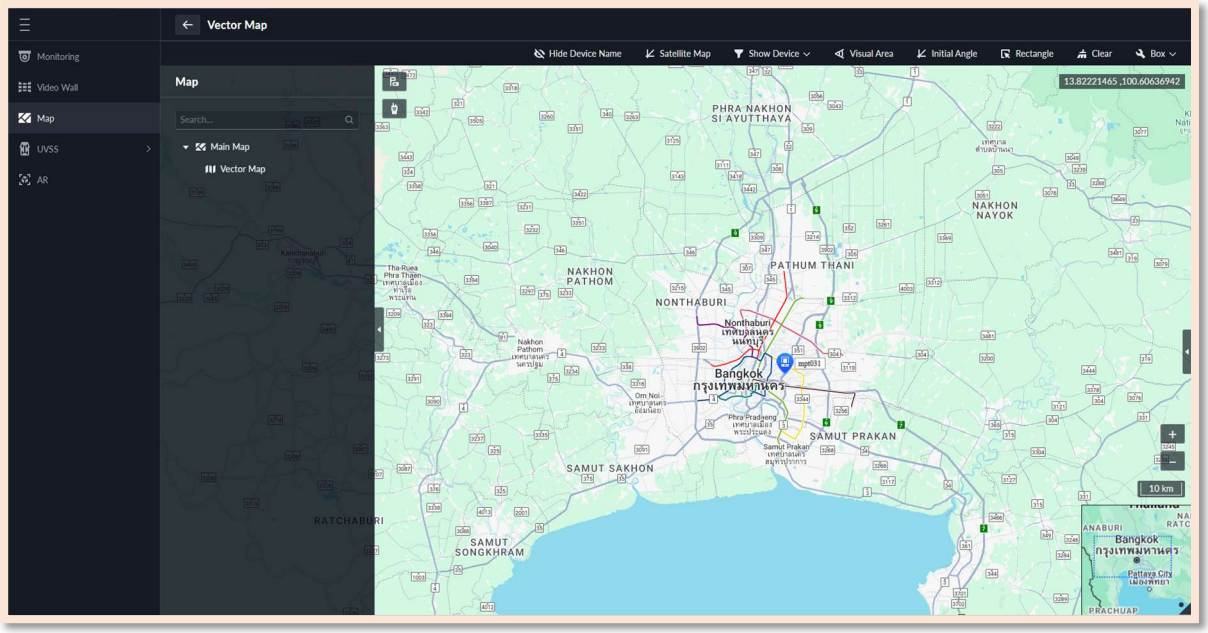
Monitoring canter คือ ฟังก์ชันที่สามารถ ดู Stem สื่อสาร โต้ตอบ กับ Body cam ได้ และยังสามารถสร้าง Gorp Talk ผ่านตัวฟังก์ชันนี้ได้ เช่นกัน



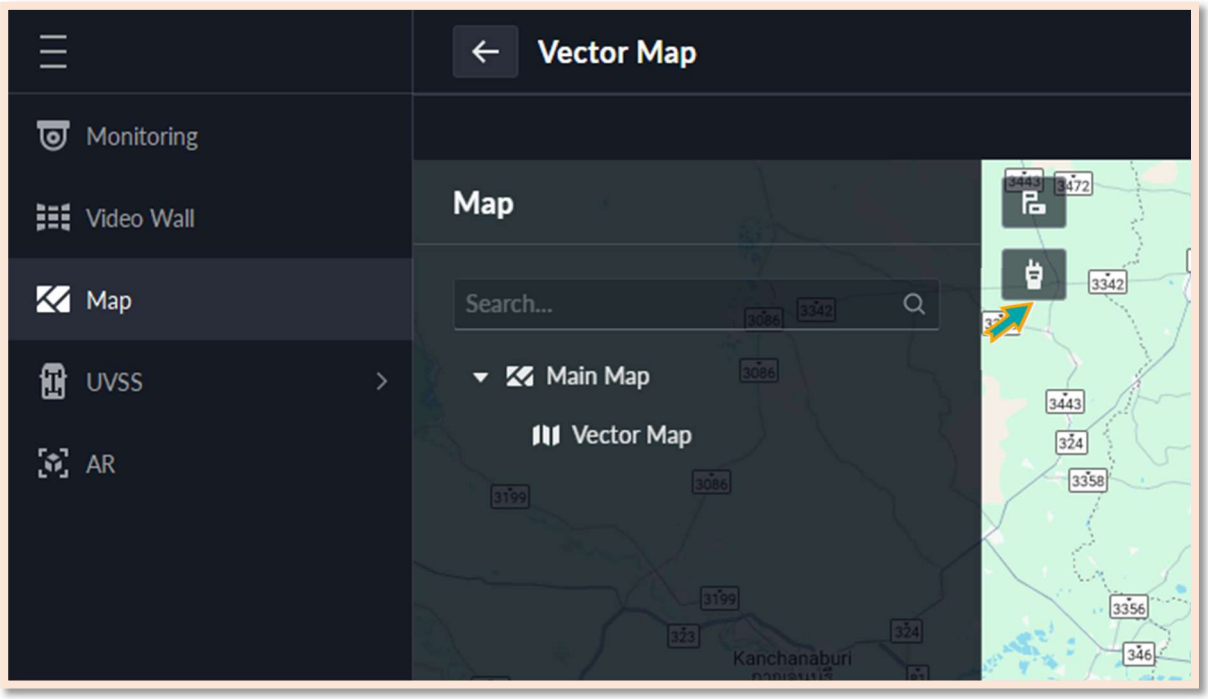
Monitoring จะสามารถเรียกดู Stem สด จาก Body cam ได้ 30 เครื่องเหมือนกับในหน้าระบบสื่อสารแบบทันเหตุการณ์ (เจ้าหน้าที่) แต่ที่ต่างจากเว็บไซต์ คือ จะยังสามารถสื่อสารกับ Body cam ได้โปรตรงโดยไม่ต้องผ่าน Group Talk (ผู้ดูแลระบบ)



Map เป็นฟังก์ชันเรียกดูอุปกรณ์ ที่ออนไลน์ทั้งหมดได้ และยังมีฟังก์ชัน Group Talk ที่สามารถสร้างกลุ่มให้กับ Body cam เพื่อให้สามารถสื่อกสารกันได้

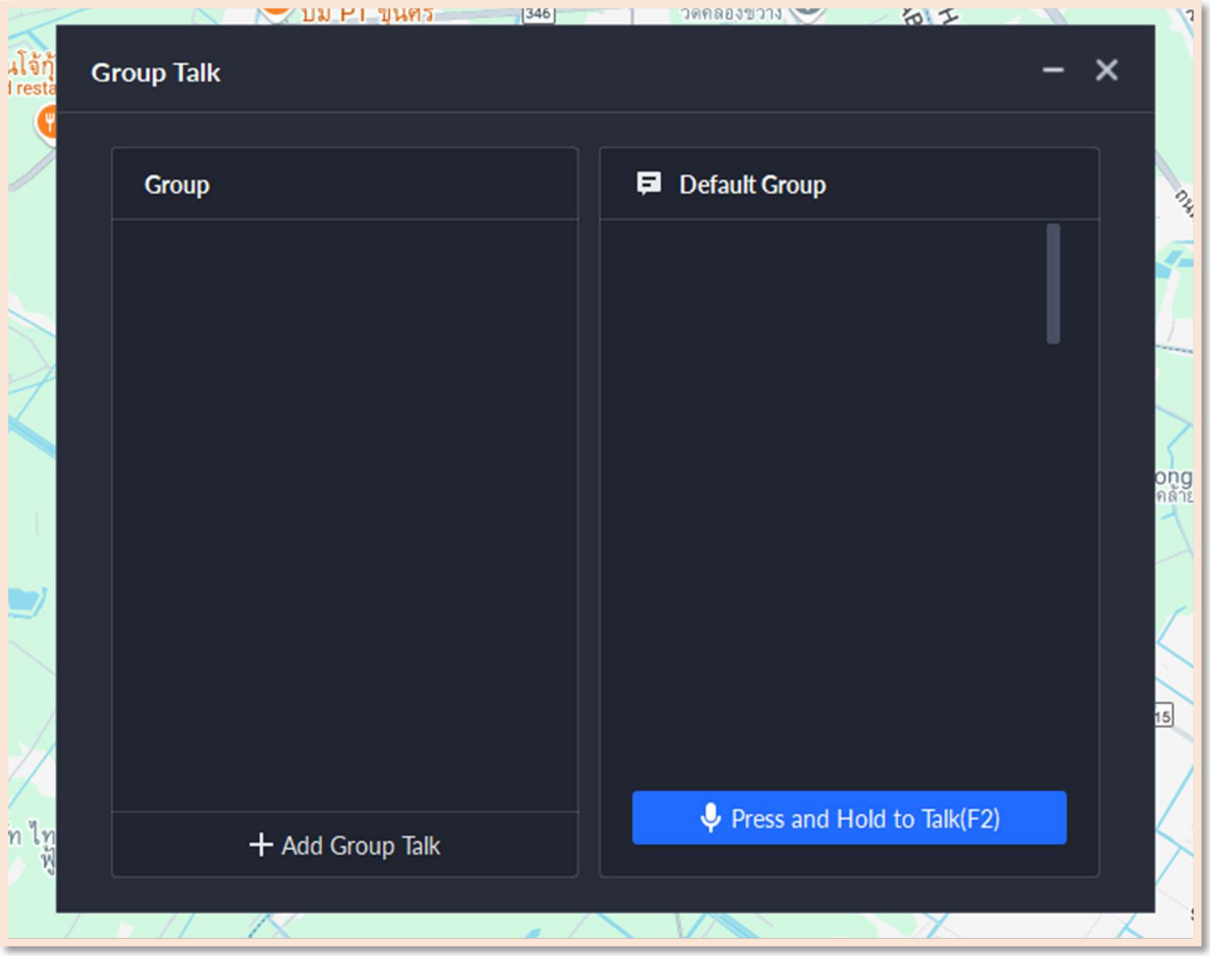


Group Talk ฟังก์ชันสร้างกลุ่มการสื่อสารระหว่าง Body cam กับ Body cam ด้วยกัน สามารถสร้างได้ด้วยการกดที่ปุ่ม PTT ของตัวเครื่อง



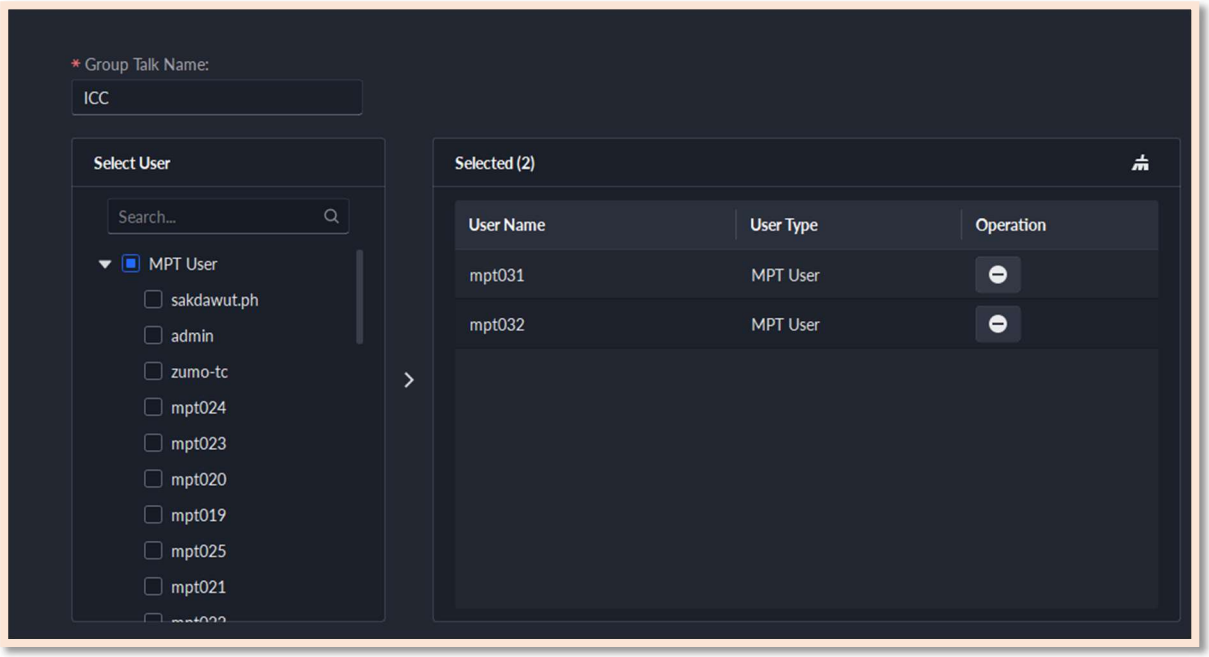
1) การสร้าง Group Talk มีขั้นตอนดังนี้

เมื่อคลิกที่ฟังก์ชัน Gorp Talk จะแสดง POP UP หน้าต่างการสร้างขึ้นมา ให้ทำการคลิกปุ่ม + Add Gorp Talk

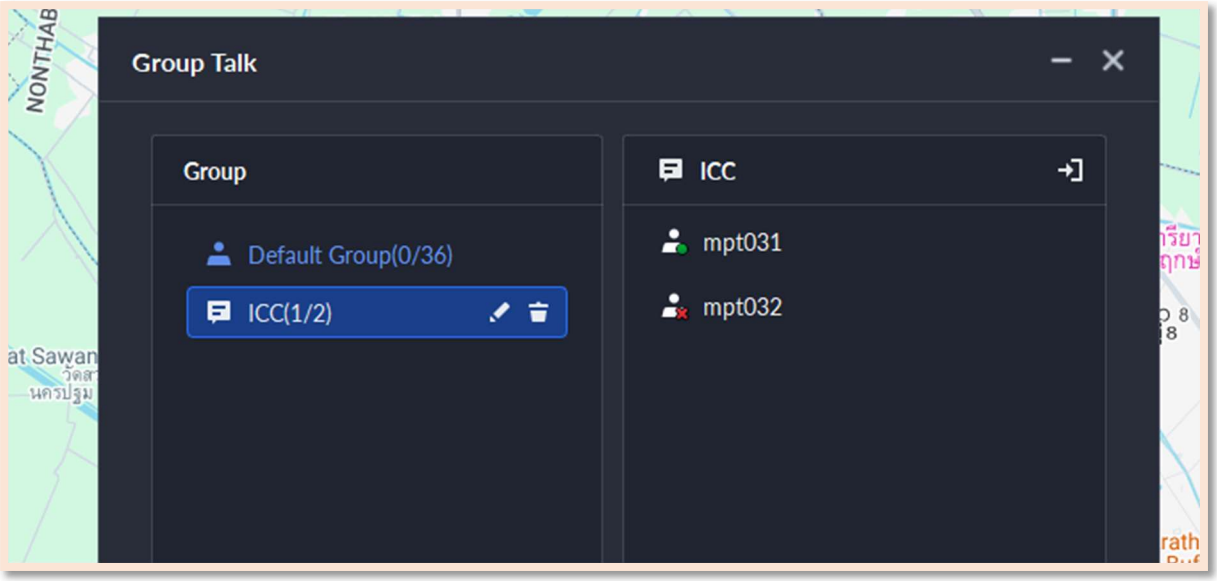


เมื่อเข้าสู่หน้าต่าง + Add Group Talk ต่อไปคือ

1. สร้างชื่อกลุ่มที่ Group Talk Name
2. เลือก Body cam ที่ต้องการ
3. คลิก OK เพื่อสร้าง Group

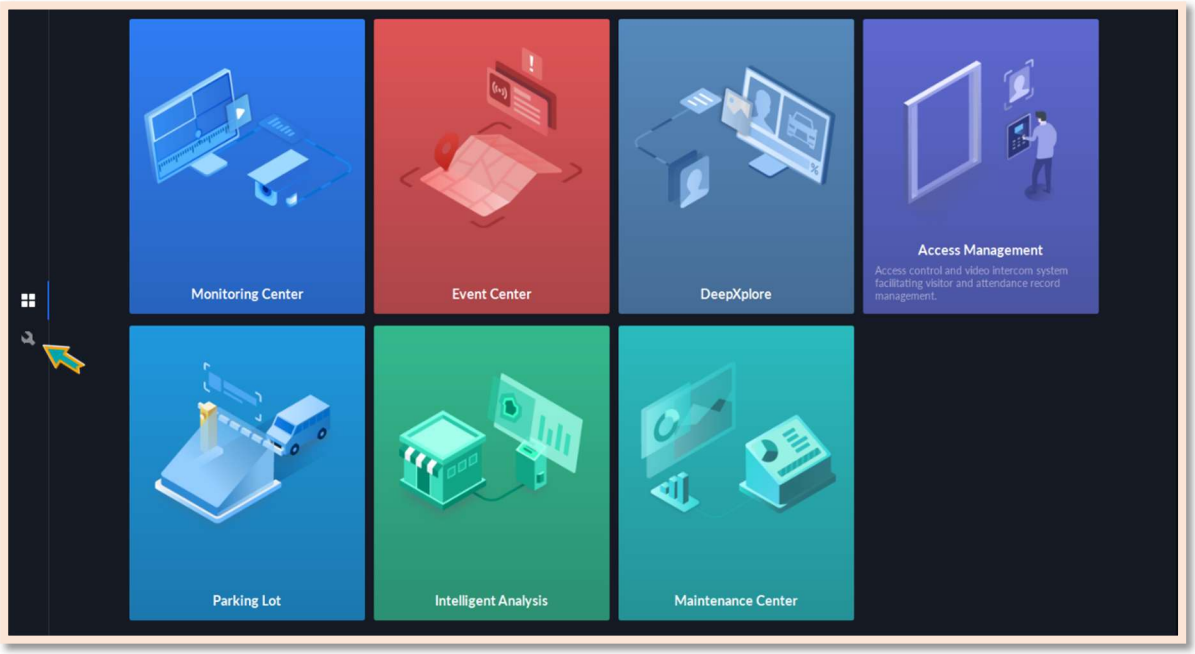


ตัวอุปกรณ์ที่เลือกจะสามารถอยู่ได้แค่ 1 กลุ่มเท่านั้น
เมื่อสร้างเสร็จ ฟังก์ชัน Gorp Talk จะแสดง Group ที่สร้างและ ตัวอุปกรณ์ที่อยู่ใน Group นั้น ๆ



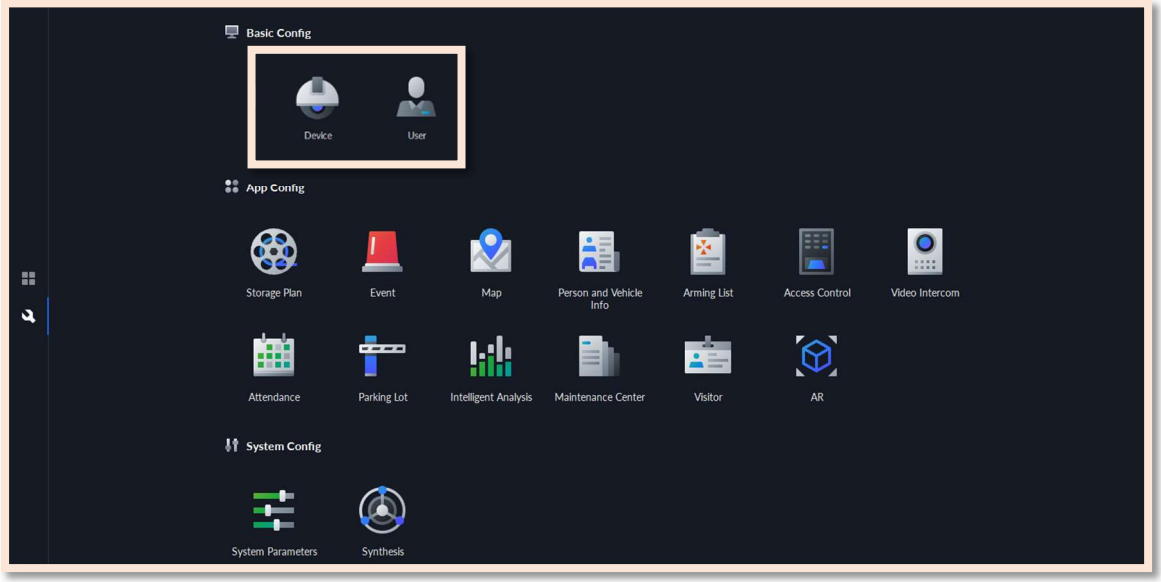
2) วิธีเพิ่ม Device และ User

ให้ไปที่ Configuration จะอยู่ที่ด้านซ้ายของจอ



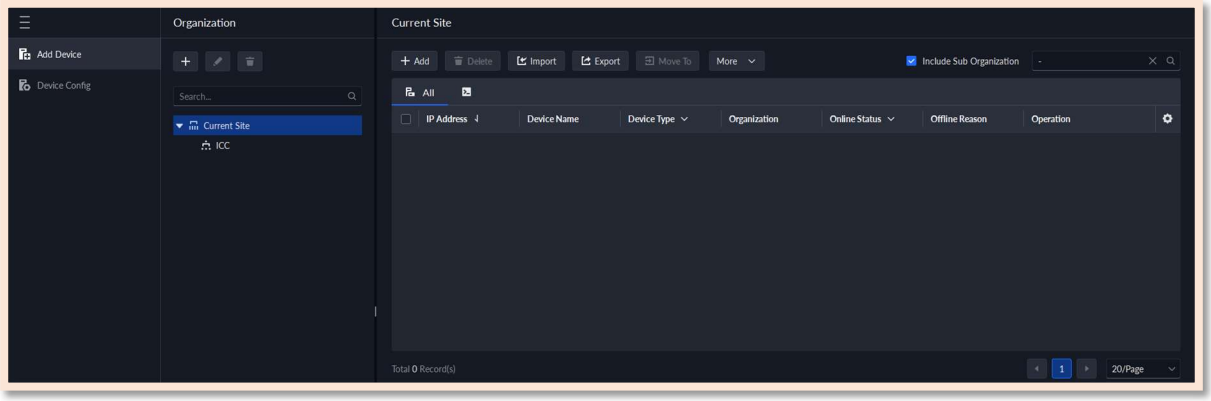
เลือก Basic Config

- กรณีจะเพิ่มอุปกรณ์ให้เลือก Device หรือ กรณีจะเพิ่มผู้ใช้งานให้เลือก User



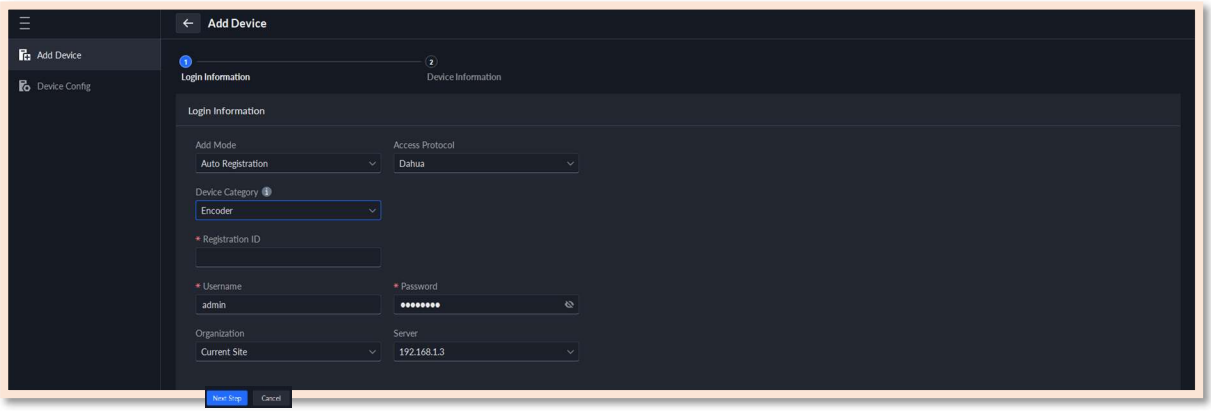
3) ขั้นตอนการเพิ่ม Device

ทำการเลือก Device จะแสดงหน้าต่างการ Add Device



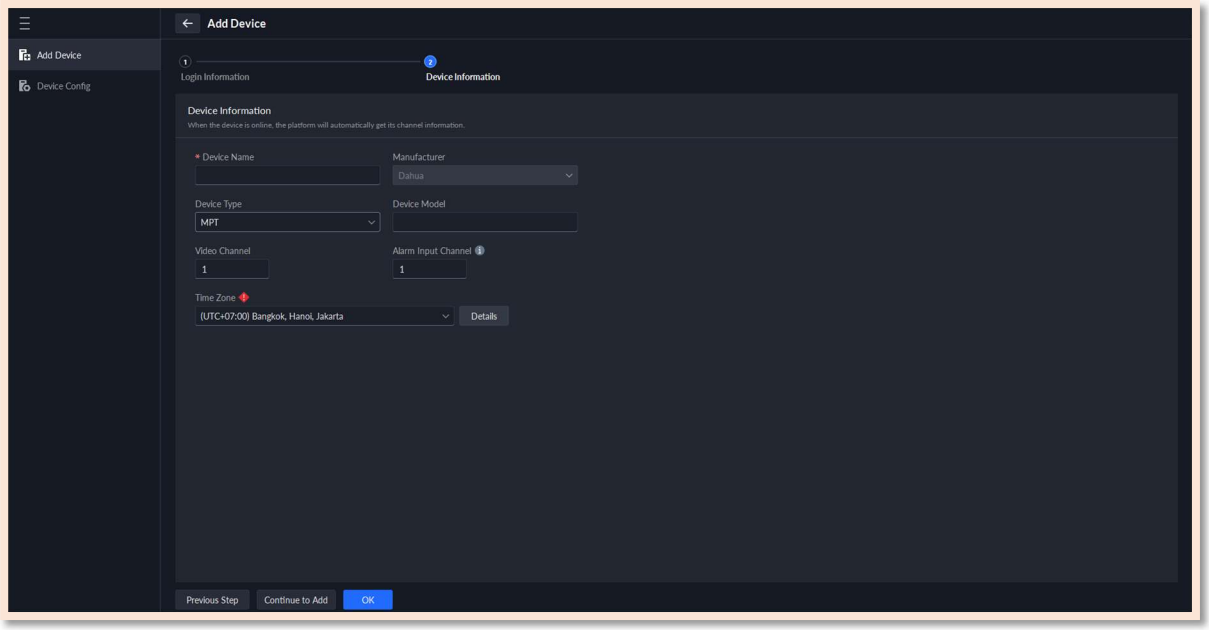
ให้ไปที +Add เพื่อทำการเพิ่ม Device ที่ต้องการสร้างให้กับ Body cam โดยเพิ่มข้อมูล Login Information

- Add Mode = Auto Registration
- Access Protocol = Dahua
- Device Category = Encoder
- Registration ID = ตั้งชื่ออุปกรณ์
- Username = admin
- Password = Admin001
- Organization = เลือกกลุ่มอุปกรณ์
- Server = ตามค่าเริ่มต้น แล้วกด Next Step เพื่อไปยังขั้นตอนถัดไป



เพิ่มข้อมูล Device Information

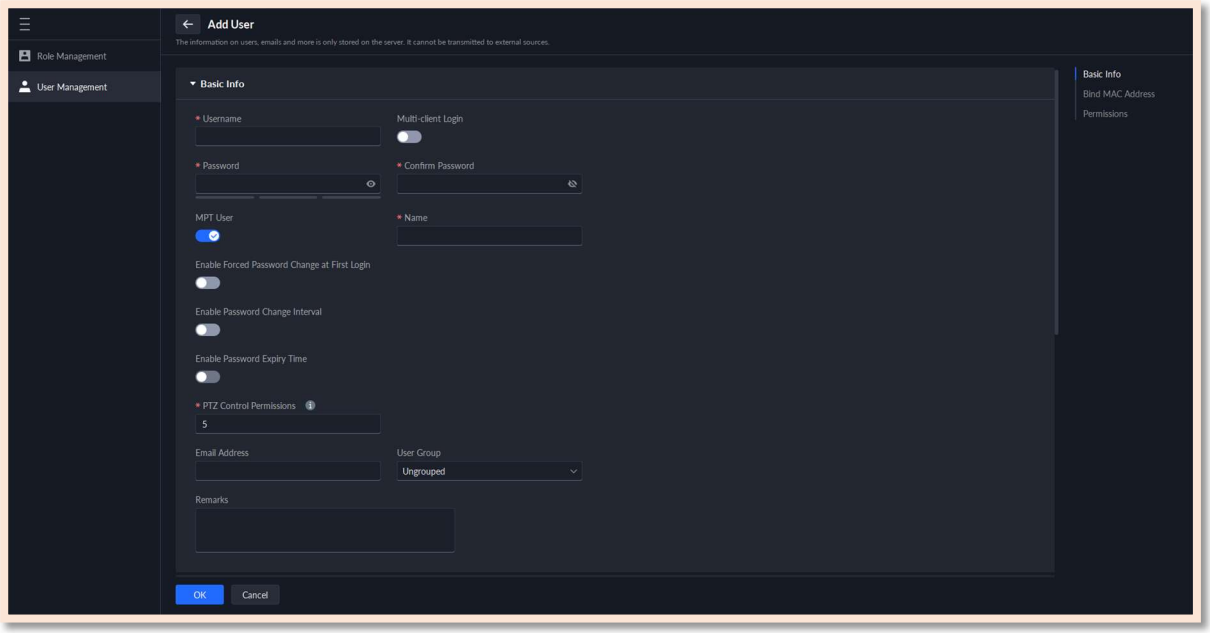
- Device name : ตั้งชื่ออุปกรณ์
- Manufacturer : ค่าเริ่มต้น
- Device Type : MPT
- Device Model : ว่าง
- Video Channel : 1
- Alam Input Channel : 1



4) ขั้นตอนการเพิ่ม User Basic Info (ข้อมูลพื้นฐาน)

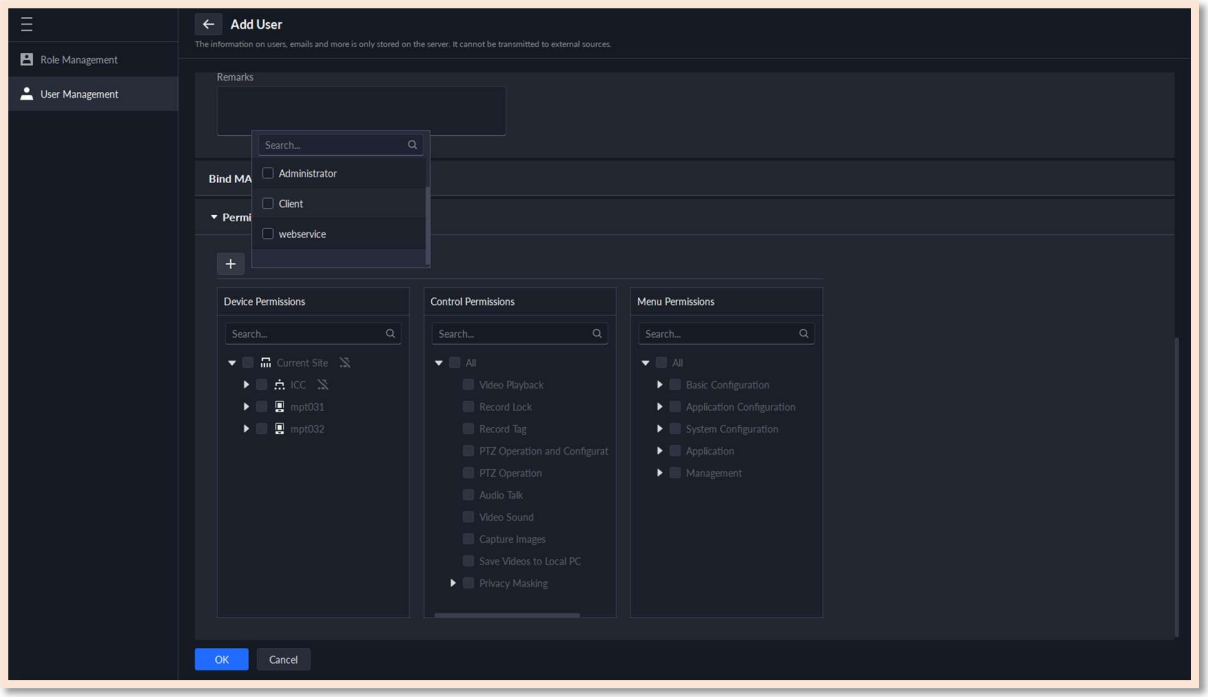
- Username : ชื่อผู้ใช้
- Password : รหัสผ่าน
- Confirm Password : ยืนยันรหัสผ่าน
- Name : ชื่อระบุอุปกรณ์

เมื่อกรอกข้อมูลข้างต้นแล้ว ให้ทำการ เปิด MPT User แล้วทำการปิดฟังก์ชันอื่น ๆ ทั้งหมด



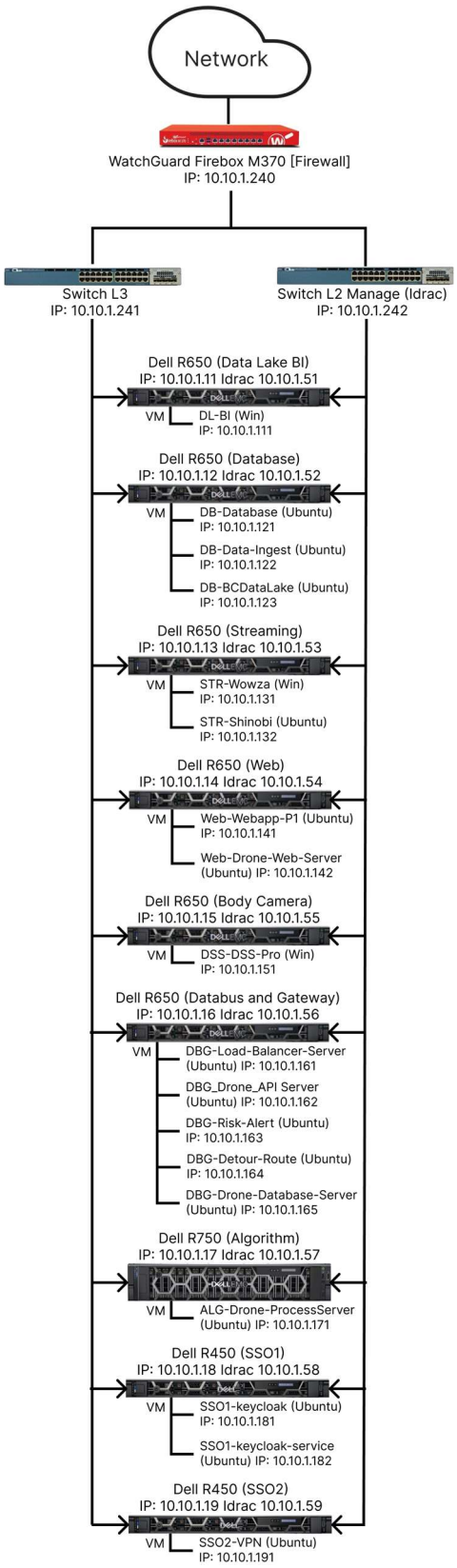
5) Permissions (สิทธิ์)

เป็นการจัดการประเภทของ และสิทธิ์ของ User ส่วนนี้ถ้าหากเป็นของ Body Cam จะให้สิทธิ์ Client



6) เครื่องคอมพิวเตอร์แม่ข่ายระบบศูนย์บัญชาการ กรมทางหลวง

ภาพรวม (Overview)

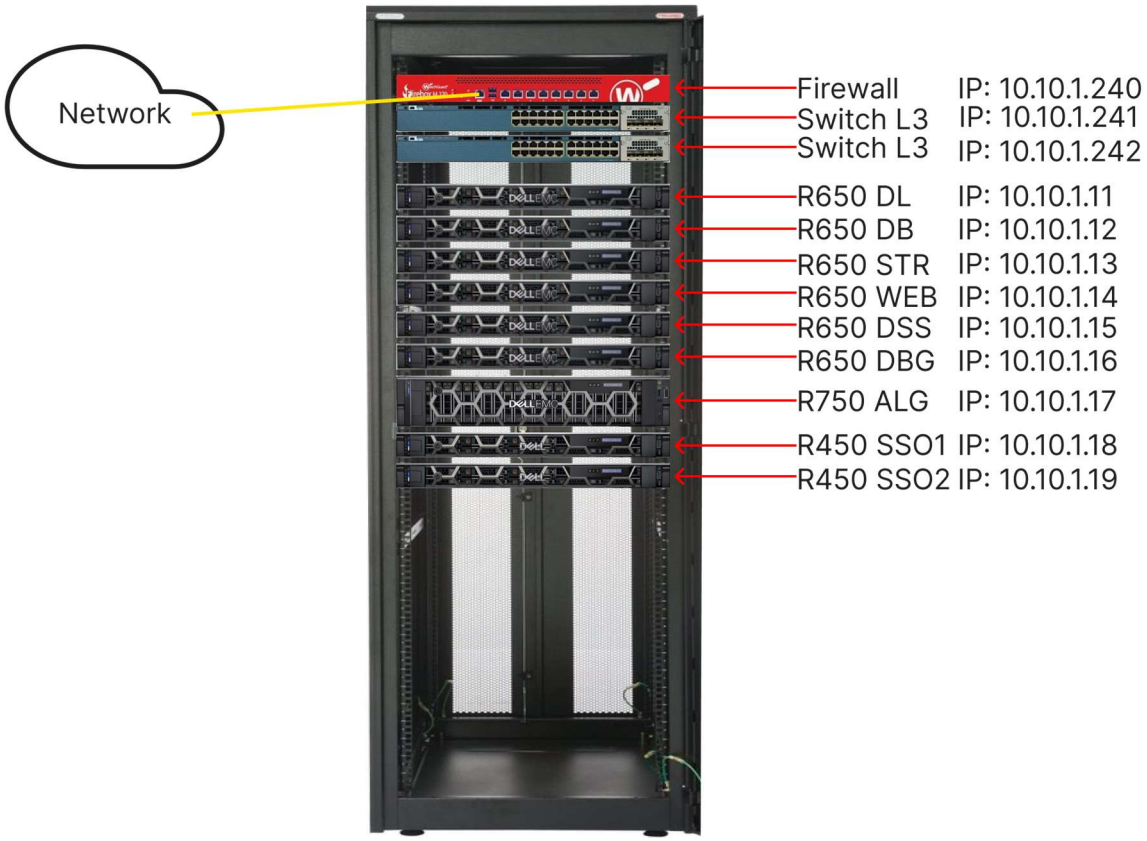


ตารางที่ 1 รายการอุปกรณ์ที่เกี่ยวข้องในโครงการ

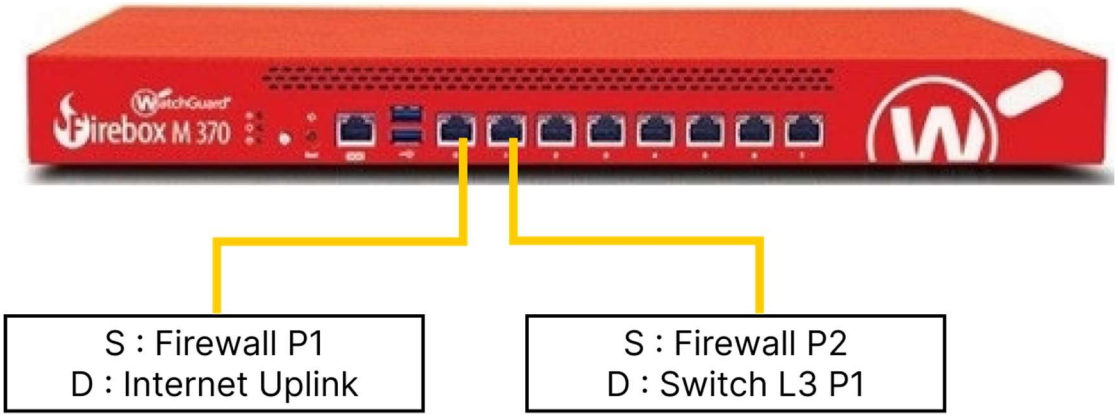
ลำดับที่	รายการอุปกรณ์	Serial Number
1.	Dell PowerEdge R650	19N8L94
2.	Dell PowerEdge R650	B8N8L94
3.	Dell PowerEdge R650	49N8L94
4.	Dell PowerEdge R650	99N8L94
5.	Dell PowerEdge R650	89N8L94
6.	Dell PowerEdge R650	9CP8L94
7.	Dell PowerEdge R750	39N8L94
8.	Dell PowerEdge R450	59N8L94
9.	Dell PowerEdge R450	69N8L94
10.	WatchGuardFirewall	801307F18-32AE
11.	Cisco L3 Switch (1)	FDO1536K1SG
12.	Cisco L3 Switch (2)	FDO1536P1WY

ตารางที่ 2 การออกแบบมาตรฐานเครื่องที่ใช้ในโครงการ

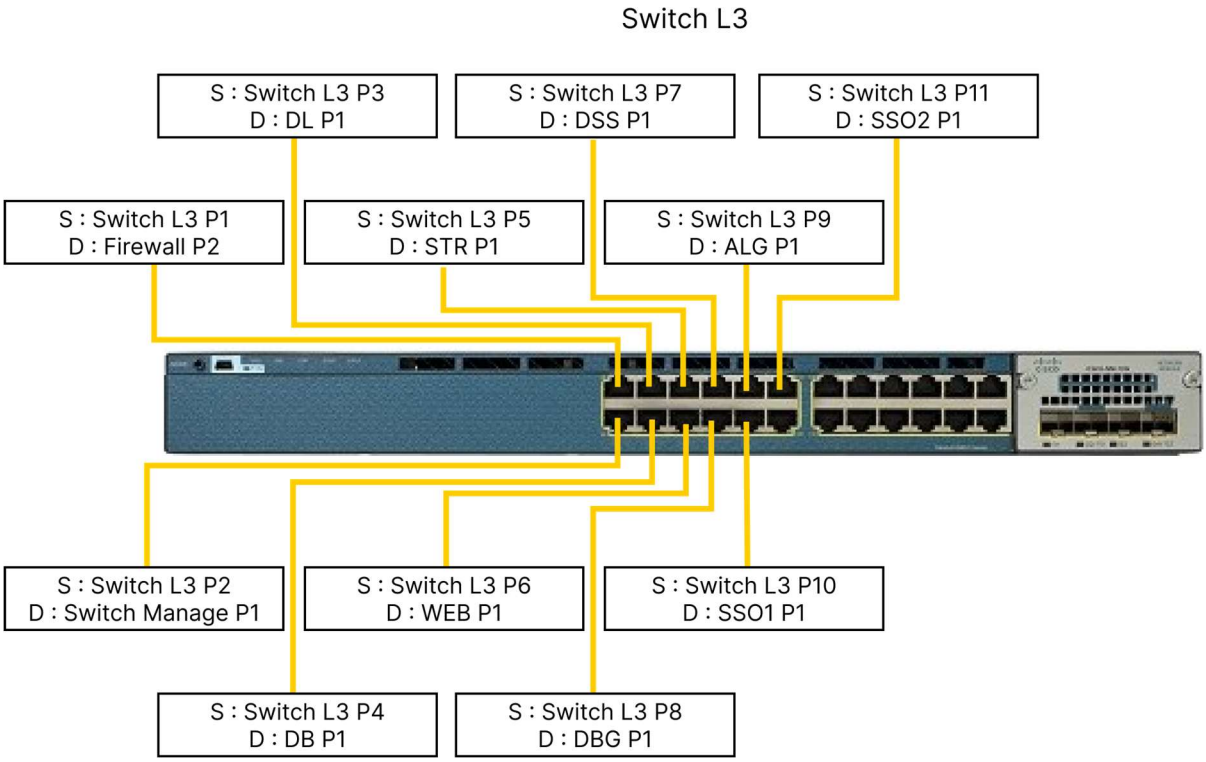
รหัสย่อ	ชื่อเครื่องแม่ข่าย	คำอธิบาย	IP Address
DLG	Data Lake BI Gateway	รวบรวมข้อมูล เพื่อใช้กับ Power BI	10.10.1.11
DB	Database	ฐานข้อมูลหลักในระบบ ICC	10.10.1.12
STR	Streaming	ติดตั้งระบบงานด้าน Streaming	10.10.1.13
WEB	สำหรับ System Web	ติดตั้ง ICC App ระยะที่ 1-3	10.10.1.14
DSS	Body Camera	สำหรับเก็บภาพและวีดีโอ	10.10.1.15
DBG	Databus and Gateway	สำหรับใช้เป็น Service Gateway	10.10.1.16
ALG	Algorithm	การวิเคราะห์และประมวลผลภาพ	10.10.1.17
SSO1	SSO1	ติดตั้ง Keycloak Prod	10.10.1.18
SSO2	SSO2	ติดตั้ง Keycloak โซนทดสอบ และ Ovpn	10.10.1.19
WG	WatchGuardFirewall	Firewall กั้นระหว่าง DOH กับ ICC	10.10.1.240
L3SW1	Cisco L3 Switch (1)	สำหรับ Switch L3	10.10.1.241
L3SW2	Cisco L3 Switch (2)	Switch Manage	10.10.1.242



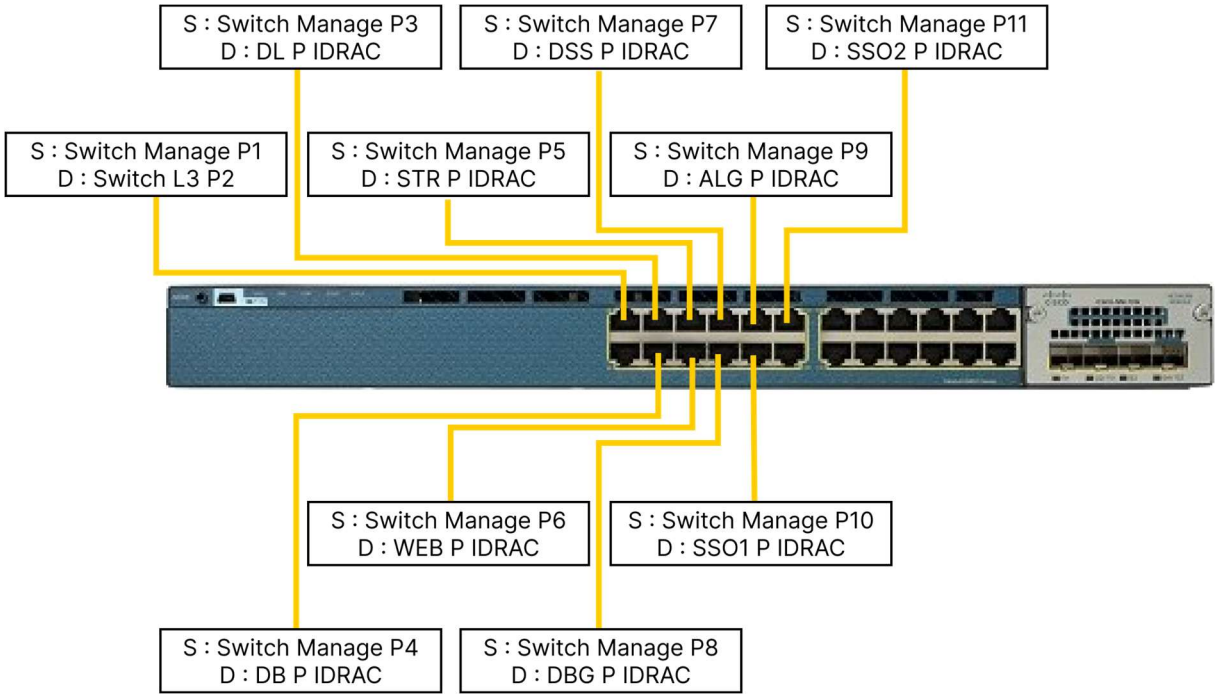
รูปที่ 1 การติดตั้งเครื่อง Server ของ ICC (Rack 16)



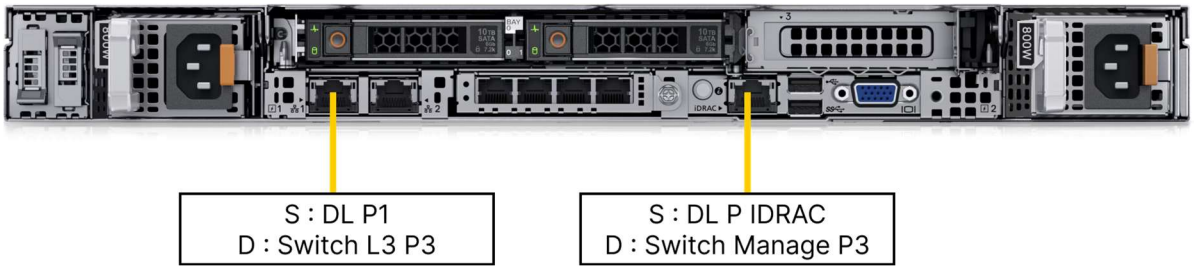
รูปที่ 2 การกำหนด port ของ Firewall



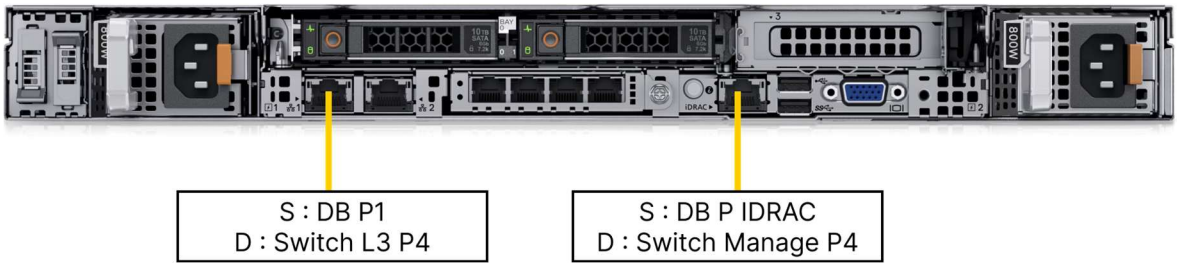
รูปที่ 3 การกำหนด port ของ Switch L3



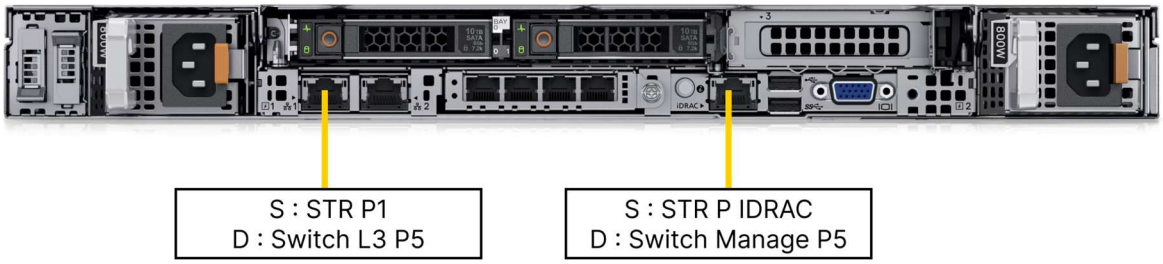
รูปที่ 4 การกำหนด port ของ Switch Manage



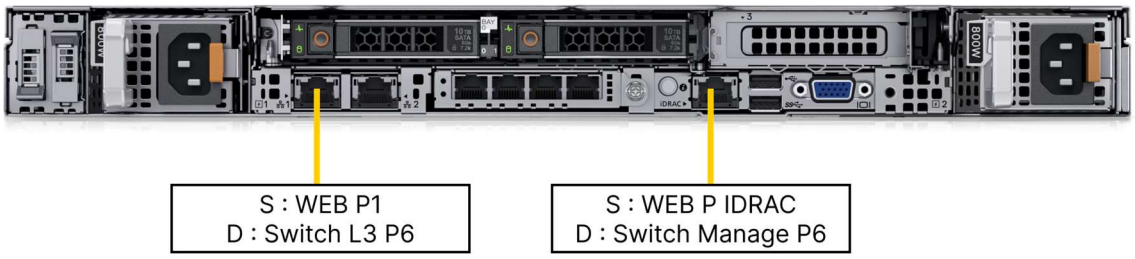
รูปที่ 5 การกำหนด port ของ Data Lake BI Gateway



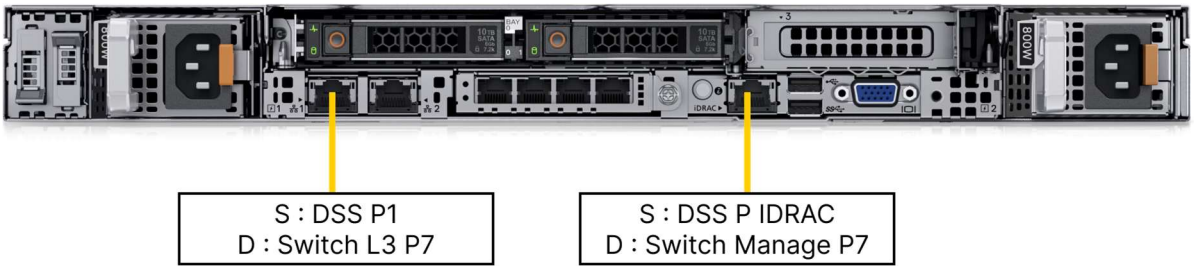
รูปที่ 6 การกำหนด port ของ Database



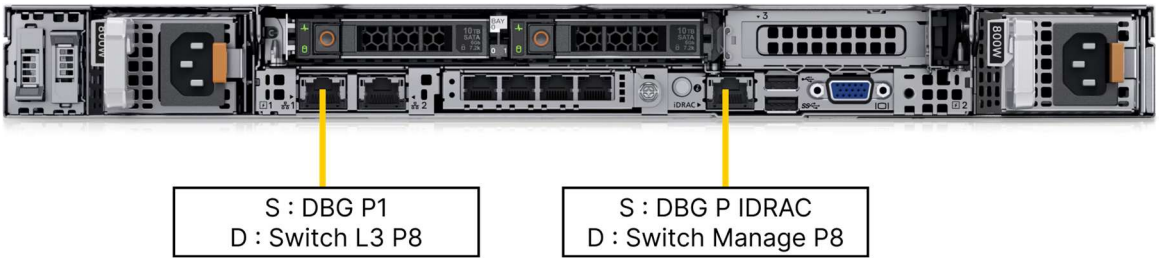
รูปที่ 7 การกำหนด port ของ Streaming



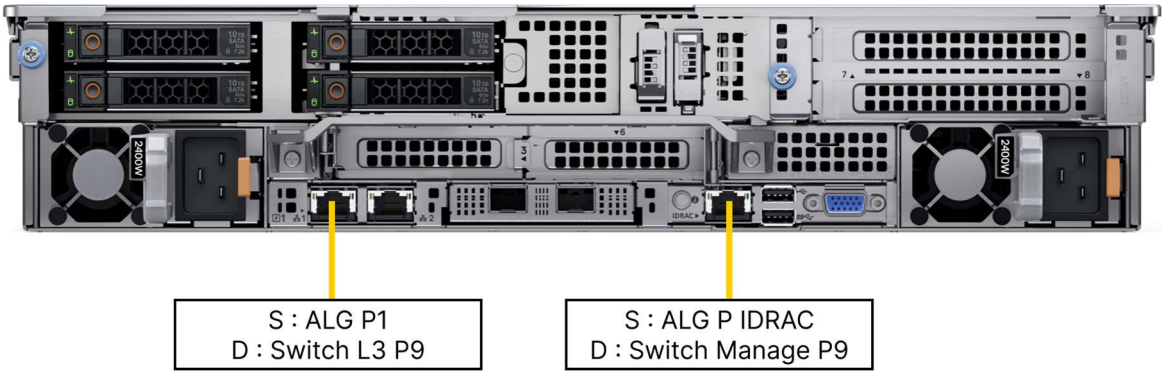
รูปที่ 8 การกำหนด port ของ System Web



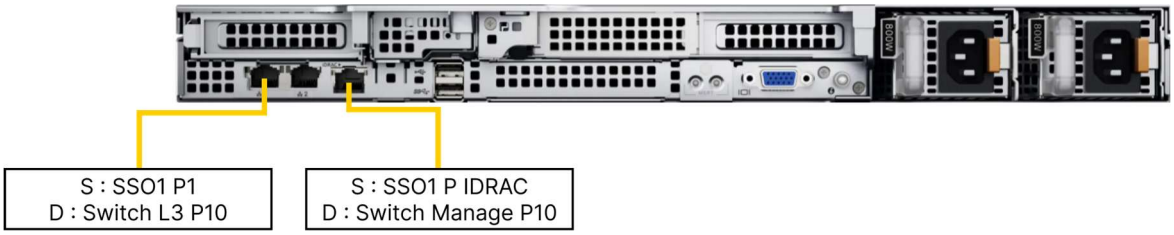
รูปที่ 9 การกำหนด port ของ Body Camera



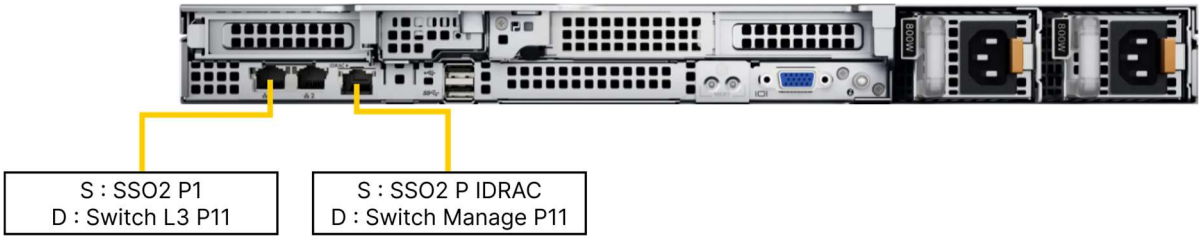
รูปที่ 10 การกำหนด port ของ Databus Gateway



รูปที่ 11 การกำหนด port ของ Algorithm



รูปที่ 12 การกำหนด port ของ SSO (1)



รูปที่ 13 การกำหนด port ของ SSO (2)

รายละเอียดเครื่องคอมพิวเตอร์แม่ข่ายเครื่องที่ 1

เครื่องแม่ข่าย : Data Lake BI Gateway	**IP Address : 10.10.1.11**	
1) Brand Name Dell PowerEdge R650		
2) CPU Speed : 2.4 GHz	Type : Intel Xeon Gold	
3) RAM : จำนวน 2 หน่วย รวม 32 GB	Size : 16 GB/Pcs	
4) HDD : จำนวน 6 หน่วย รวม 9.68 TB	RAID Type : 0,1,5	
5) LAN : จำนวน 1 หน่วย	Speed : 10 GB Base-T	
6) Mouse	☐ Yes	☑ No
7) Key Board	☐ Yes	☑ No
8) Monitor	☐ Yes	☑ No

หมายเหตุ : เครื่องคอมพิวเตอร์แม่ข่ายแบบที่ 2 เพิ่ม SSD ขนาดความจุ 1.92 TB จำนวน 4 หน่วย

รายละเอียดเครื่องคอมพิวเตอร์แม่ข่ายเครื่องที่ 2

เครื่องแม่ข่าย : Database	**IP Address : 10.10.1.12**	
1) Brand Name Dell PowerEdge R650		
2) CPU Speed : 2.4 GHz	Type : Intel Xeon Gold	
3) RAM : จำนวน 2 หน่วย รวม 32 GB	Size : 16 GB/Pcs	
4) HDD : จำนวน 6 หน่วย รวม 9.68 TB	RAID Type : 0,1,5	
5) LAN : จำนวน 1 หน่วย	Speed : 10 GB Base-T	
6) Mouse	☐ Yes	☑ No
7) Key Board	☐ Yes	☑ No
8) Monitor	☐ Yes	☑ No

หมายเหตุ : เครื่องคอมพิวเตอร์แม่ข่ายแบบที่ 2 เพิ่ม SSD ขนาดความจุ 1.92 TB จำนวน 4 หน่วย

รายละเอียดเครื่องคอมพิวเตอร์แม่ข่ายเครื่องที่ 3

เครื่องแม่ข่าย : Streaming	**IP Address : 10.10.1.13**	
1) Brand Name Dell PowerEdge R650		
2) CPU Speed : 2.4 GHz	Type : Intel Xeon Gold	
3) RAM : จำนวน 8 หน่วย รวม 256 GB	Size : 32 GB/Pcs	
4) HDD : จำนวน 3 หน่วย รวม 6 TB	RAID Type : 0,1,5	
5) LAN : จำนวน 1 หน่วย	Speed : 10 GB Base-T	
6) Mouse	☐ Yes	☑ No
7) Key Board	☐ Yes	☑ No
8) Monitor	☐ Yes	☑ No

หมายเหตุ : เครื่องคอมพิวเตอร์แม่ข่ายแบบที่ 2 เพิ่ม RAM ขนาดความจุ 32GB จำนวน 7 หน่วย

รายละเอียดเครื่องคอมพิวเตอร์แม่ข่ายเครื่องที่ 4

เครื่องแม่ข่าย : System Web	**IP Address : 10.10.1.14**	
1) Brand Name Dell PowerEdge R650		
2) CPU Speed : 2.4 GHz	Type : Intel Xeon Gold	
3) RAM : จำนวน 2 หน่วย รวม 32 GB	Size : 16 GB/Pcs	
4) HDD : จำนวน 3 หน่วย รวม 6 TB	RAID Type : 0,1,5	
5) LAN : จำนวน 1 หน่วย	Speed : 10 GB Base-T	
6) Mouse	☐ Yes	☑ No
7) Key Board	☐ Yes	☑ No
8) Monitor	☐ Yes	☑ No

หมายเหตุ : เครื่องคอมพิวเตอร์แม่ข่ายแบบที่ 2 เพิ่ม RAM ขนาดความจุ 32GB จำนวน 7 หน่วย

รายละเอียดเครื่องคอมพิวเตอร์แม่ข่ายเครื่องที่ 5

เครื่องแม่ข่าย : Body Camera	**IP Address : 10.10.1.15**	
1) Brand Name Dell PowerEdge R650		
2) CPU Speed : 2.4 GHz	Type : Intel Xeon Gold	
3) RAM : จำนวน 2 หน่วย รวม 32 GB	Size : 16 GB/Pcs	
4) HDD : จำนวน 6 หน่วย รวม 9.68 TB	RAID Type : 0,1,5	
5) LAN : จำนวน 1 หน่วย	Speed : 10 GB Base-T	
6) Mouse	☐ Yes	☑ No
7) Key Board	☐ Yes	☑ No
8) Monitor	☐ Yes	☑ No

หมายเหตุ : เครื่องคอมพิวเตอร์แม่ข่ายแบบที่ 2 เพิ่ม SSD ขนาดความจุ 1.92 TB จำนวน 4 หน่วย

รายละเอียดเครื่องคอมพิวเตอร์แม่ข่ายเครื่องที่ 6

เครื่องแม่ข่าย : Databus and Gateway	**IP Address : 10.10.1.16**	
1) Brand Name Dell PowerEdge R650		
2) CPU Speed : 2.4 GHz	Type : Intel Xeon Gold	
3) RAM : จำนวน 8 หน่วย รวม 256 GB	Size : 32 GB/Pcs	
4) HDD : จำนวน 3 หน่วย รวม 6 TB	RAID Type : 0,1,5	
5) LAN : จำนวน 1 หน่วย	Speed : 10 GB Base-T	
6) Mouse	☐ Yes	☑ No
7) Key Board	☐ Yes	☑ No
8) Monitor	☐ Yes	☑ No

หมายเหตุ : เครื่องคอมพิวเตอร์แม่ข่ายแบบที่ 2 เพิ่ม RAM ขนาดความจุ 32GB จำนวน 7 หน่วย

รายละเอียดเครื่องคอมพิวเตอร์แม่ข่ายเครื่องที่ 7

เครื่องแม่ข่าย : Algorithm	IP Address : 10.10.1.17	
1) Brand Name Dell PowerEdge R750		
2) CPU Speed : 2.4 GHz	Type : Intel Xeon Gold	
3) RAM : จำนวน 2 หน่วย รวม 128 GB	Size : 16 GB/Pcs	
4) HDD : จำนวน 3 หน่วย รวม 6 TB	RAID Type : 0,1,5	
5) LAN : จำนวน 1 หน่วย	Speed : 10 GB Base-T	
6) GPU : จำนวน 2 หน่วย รวม 24 GB	Size : 12 GB/Pcs	
7) Mouse	☐ Yes	☑ No
8) Key Board	☐ Yes	☑ No
9) Monitor	☐ Yes	☑ No

หมายเหตุ :

รายละเอียดเครื่องคอมพิวเตอร์แม่ข่ายเครื่องที่ 8

เครื่องแม่ข่าย : SSO1	IP Address : 10.10.1.18	
1) Brand Name Dell PowerEdge R450		
2) CPU Speed : 2.2 GHz	Type : Intel Xeon Silver	
3) RAM : จำนวน 1 หน่วย รวม 16 GB	Size : 16 GB/Pcs	
4) HDD : จำนวน 1 หน่วย รวม 1 TB	RAID Type : 0,1,5	
5) LAN : จำนวน 1 หน่วย	Speed : 10 GB Base-T	
6) Mouse	☐ Yes	☑ No
7) Key Board	☐ Yes	☑ No
8) Monitor	☐ Yes	☑ No

หมายเหตุ :

รายละเอียดเครื่องคอมพิวเตอร์แม่ข่ายเครื่องที่ 9

เครื่องแม่ข่าย : SSO2	**IP Address : 10.10.1.19**	
1) Brand Name Dell PowerEdge R450		
2) CPU Speed : 2.2 GHz	Type : Intel Xeon Silver	
3) RAM : จำนวน 1 หน่วย รวม 16 GB	Size : 16 GB/Pcs	
4) HDD : จำนวน 1 หน่วย รวม 1 TB	RAID Type : 0,1,5	
5) LAN : จำนวน 1 หน่วย	Speed : 10 GB Base-T	
6) Mouse	☐ Yes	☑ No
7) Key Board	☐ Yes	☑ No
8) Monitor	☐ Yes	☑ No

หมายเหตุ :

รายละเอียดอุปกรณ์อื่นๆ

อุปกรณ์ : Firewall	**IP Address : 10.10.1.240**
ยี่ห้อ : WatchGuard **รหัสเครื่อง : 801307F18-32AE**	**รุ่น : M370**

อุปกรณ์ : L3 Switch (1)	**IP Address : 10.10.1.241**
ยี่ห้อ : CISCO **รหัสเครื่อง : FDO1536K1SG**	**รุ่น : C3560X-24TS-**

อุปกรณ์ : L3 Switch (2)	**IP Address : 10.10.1.242**
ยี่ห้อ : CISCO **รหัสเครื่อง : FDO1536P1WY**	**รุ่น : C3560X-24TS-**

ตารางที่ 3 แสดงรายการ port ที่ได้รับจัดสรรในระบบ ICC

No.	ระบบงาน	Source IP Address	Service Source Port	Destination IP Address	Service Destination Port	Application
1	ICC	103.215.233.166	80	172.16.211.61	80	http
2	ICC		443		443	https
3	ICC		8899		8899	
4	ICC		3306		3306	
5	ICC		27017		27017	
6	ICC		2210-2219		2210-2219	
7	DSS Server		3389		3389	
8	MQ-mqtt		1883		1883	MQ-mqtt
9	MQ-openwire		61616		61616	MQ-openwire
10	RTSP		9100		9100	RTSP
11	RTSP over TLS		9102		9102	RTSP over TLS
12	RTSP		9320		9320	RTSP
13	RTSP over TLS		9300		9300	RTSP over TLS
14	RTP		40000-50000		40000-50000	RTP
15	SIP Registration		5080		5080	SIP Registration
16	UDP		2000-30000		2000-30000	UDP
17	TCP		9005		9005	TCP
18	TCP		9500		9500	TCP

No.	ระบบงาน	Source IP Address	Service Source Port	Destination IP Address	Service Destination Port	Application
19	TCP		9399		9399	TCP
20	UDP		5084		5084	UDP
21	UDP		30000-30240		30000-30240	UDP
22	Video Stream		8088		8088	http
23	Open VPN		1194		1194	
24	TC CNX		2208		2208	
25	Detour		8000		8000	
26	Drone Web		8089		8089	
27	Drone API		8443		8443	
28	Drone DB		5432		5432	
29	Drone ALG		2209		2209	

บทที่ 2
แผนการบำรุงรักษา

- ระบบซอฟต์แวร์และโปรแกรมประยุกต์ (System and application Software)
- ระบบฐานข้อมูล (Database)
- ระบบเครื่องคอมพิวเตอร์แม่ข่าย

1) ระบบซอฟต์แวร์และโปรแกรมประยุกต์ (System and application Software)

1.1) การสำรองข้อมูล

ในการบำรุงรักษาระบบงานต้นแบบ ซึ่งดำเนินงานอยู่บนเครื่องคอมพิวเตอร์แม่ข่ายแบบคลาวด์ (Cloud Server) แบ่งการบำรุงรักษาระบบออกเป็น 2 ส่วน ได้แก่ บำรุงรักษาระบบเครื่องคอมพิวเตอร์แม่ข่ายแบบคลาวด์ (Cloud Server) และบำรุงรักษาส่วนของซอฟต์แวร์ระบบศูนย์บัญชาการเหตุการณ์ (Web Application) มีรายละเอียดดังนี้

1.2) การบำรุงรักษาระบบเครื่องคอมพิวเตอร์แม่ข่ายแบบคลาวด์ (Cloud Server)

สำหรับระบบ Cloud ที่ใช้งานจะมีบริการการทำ Snapshot ซึ่งเป็นบริการที่จะเก็บสถานะของระบบในเวลาที่กำหนดให้ และสามารถย้อนสถานะของระบบกลับมาเป็นช่วงที่ทำ Snapshot ไว้ได้เมื่อระบบเกิดปัญหา ก็เป็นวิธีการหนึ่งที่ผู้ให้บริการ Cloud ช่วยให้ระบบมีความปลอดภัยสูงขึ้น

1.3) การบำรุงรักษาส่วนของซอฟต์แวร์ระบบศูนย์บัญชาการเหตุการณ์ (Web Application)

แต่ในขอบเขตความรับผิดชอบในการดูแลส่วนซอฟต์แวร์ระบบศูนย์บัญชาการเหตุการณ์ ที่เป็น Web Application ควรมีการดำเนินการสำรองข้อมูลในส่วนของ Application ต่าง ๆ อย่างสม่ำเสมอ เพื่อความปลอดภัยในการใช้งานระบบเพิ่มมากขึ้น โดยการสำรองข้อมูล Application ควรทำทุก ๆ 1 เดือน

1.4) การทดสอบกู้คืนระบบ

เนื่องจากระบบงานของระบบศูนย์บัญชาการเหตุการณ์ แบ่งการทำงานออกเป็นส่วนๆ ซึ่งแต่ละ Module จะทำงานแยกส่วนออกจากกันอย่างชัดเจน ผู้ดูแลระบบทำการทดสอบการกู้คืนระบบ Application ต่าง ๆ อย่างสม่ำเสมอ โดยทดสอบการกู้คืนระบบแบบแยกส่วนแต่ละ Module แล้วทดสอบการทำงานแบบแยกส่วน เพื่อให้มั่นใจได้ว่า Application ที่ทำการสำรองไว้นั้น จะสามารถนำมากู้คืนระบบกลับมาทำงานได้เป็นปกติได้ โดยระยะเวลาของการทดสอบการกู้คืนระบบควรมีการทำปีละ 1 ครั้ง

2) ระบบฐานข้อมูล (Database)

2.1) การสำรองข้อมูล : สำหรับข้อมูลในฐานข้อมูลของระบบ แบ่งออกเป็น 2 ส่วนหลัก ได้แก่

- ข้อมูลที่มีการเชื่อมโยงความสัมพันธ์ (SQL) มีการเปลี่ยนแปลงข้อมูลน้อย เช่น ข้อมูลหมายเลขทางหลวง ตอนควบคุม สำนักทางหลวง แขวงทางหลวง และหมวดทางหลวง
- ข้อมูลที่ไม่มีความสัมพันธ์ระหว่างกัน (NOSQL) มีการไหลเวียนข้อมูลในปริมาณมาก และต้องมีการนำข้อมูลมาแสดงผล เช่น ข้อมูลภัยพิบัติ และข้อมูลอุบัติเหตุ ข้อมูลแผนงาน จากลักษณะข้อมูลข้างต้นระบบศูนย์บัญชาการเหตุการณ์มีการรับจากระบบต่างๆ ผ่านการทำ data ingestion ขั้นตอนการนำข้อมูลดิบ (Raw data) จากแหล่งต่างๆเข้ามา ซึ่งอาจต้องใช้เทคโนโลยีที่แตกต่างกันสำหรับแหล่งข้อมูลหลากหลายชนิด

ในการสำรองข้อมูลนี้จะมุ่งเน้นการสำรองข้อมูลพื้นฐานเป็นหลัก ส่วนข้อมูลที่นำมาใช้ในการประมวลผลนั้นจะทำการสำรองโดยกำหนดนโยบายให้สำรองข้อมูลเพียงบางส่วนเท่านั้น

2.2) การทดสอบการกู้คืนข้อมูล : เป็นการนำข้อมูลที่ได้สำรองไว้ มาทดลองติดตั้งในระบบสำรอง เพื่อทดลองว่าข้อมูลที่ทำการสำรองไว้นั้นสามารถนำมากู้คืนได้อย่างสมบูรณ์ โดยการทดสอบการกู้คืนข้อมูลควรทำอย่างน้อยปีละ 1 ครั้ง

2.3) การลบข้อมูลที่ไม่ได้ใช้งานออกจากระบบ : เนื่องจากการพัฒนาระบบศูนย์บัญชาการเหตุการณ์ในระยะที่ 2 เป็นการทำงานกับข้อมูลปริมาณมหาศาล ในการพัฒนาระบบมีการสร้างหน่วยเก็บข้อมูลชั่วคราว (Temporary Data) ทำให้การเก็บข้อมูลดังกล่าวลดทอนประสิทธิภาพของระบบฐานข้อมูล ในการบำรุงรักษาระบบจึงควรมีการลบข้อมูลชั่วคราวและข้อมูลที่ไม่ได้ใช้งานออก ซึ่งการดำเนินการดังกล่าวสามารถทำทุก ๆ สัปดาห์

3) ระบบเครื่องคอมพิวเตอร์แม่ข่าย (On Premise)

การวิเคราะห์ความสมบูรณ์ของระบบเครื่องคอมพิวเตอร์แม่ข่าย รวมถึงประสิทธิภาพโดยรวมของระบบปกติแล้วพิจารณาข้อมูลจากหลายส่วน ซึ่งส่วนมากล้วนเกี่ยวข้องกับ หน่วยประมวลผลกลาง หน่วยความจำชั่วคราว พื้นที่เก็บข้อมูลที่ใช้ และอัตราการถ่ายโอนข้อมูล เพื่อง่ายต่อการบำรุงรักษา จึงกำหนดเกณฑ์พื้นฐานโดยมีรายละเอียดดังนี้

- การใช้งานหน่วยประมวลผลกลางโดยเฉลี่ยไม่ควรเกินร้อยละ 80
- หน่วยความจำชั่วคราว (Memory) ที่ใช้งานโดยเฉลี่ย ไม่ควรเกินร้อยละ 80
- พื้นที่เก็บข้อมูลที่ใช้ (Storage) สำหรับระบบเครื่องคอมพิวเตอร์แม่ข่าย ไม่ควรเกินร้อยละ 80
- พื้นที่เก็บข้อมูลที่ใช้ (Storage) สำหรับเครื่องฐานข้อมูล และเก็บรูปภาพ ไม่ควรเกินร้อยละ 95
- อัตราการถ่ายโอนข้อมูล (Bandwidth) ที่ใช้งาน ไม่ควรเกินร้อนละ 80

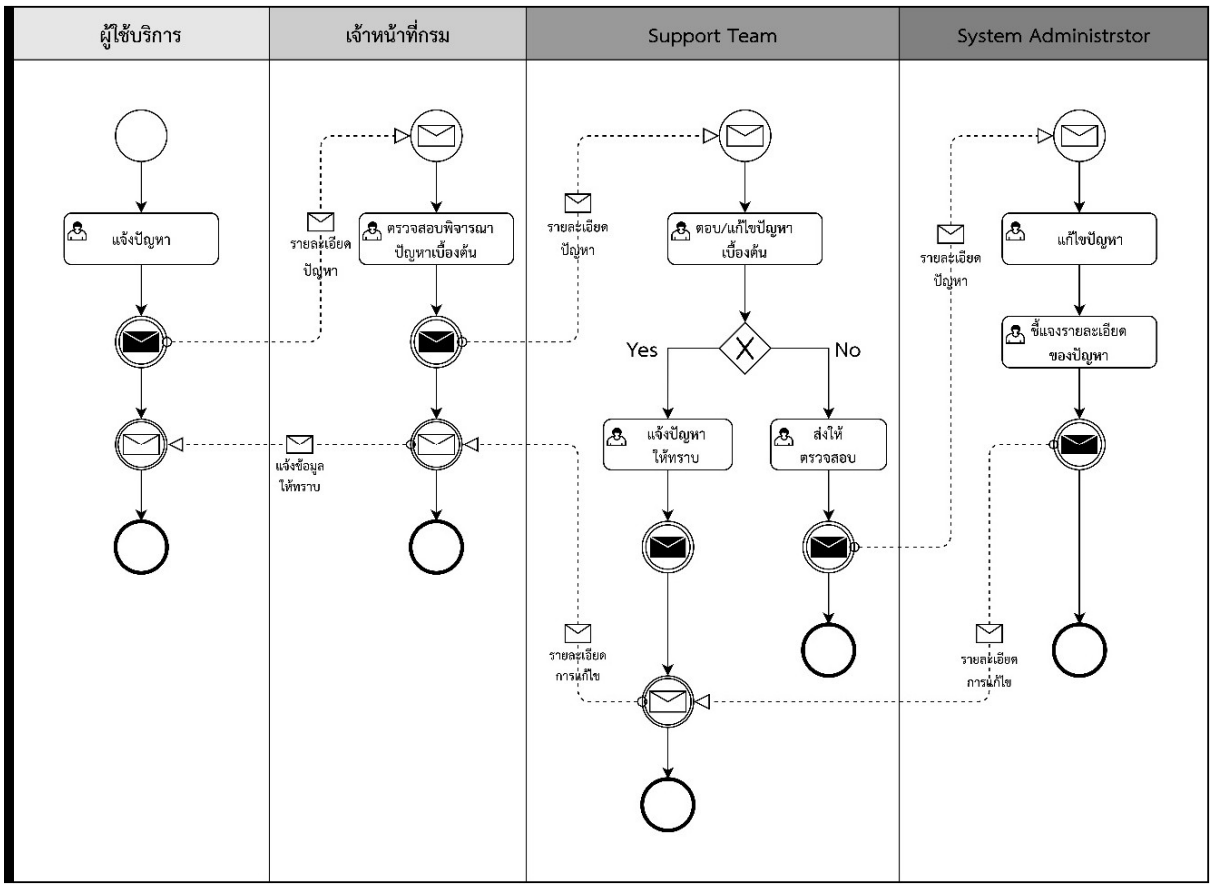
ตารางที่ 4 ตัวอย่างแบบฟอร์มสถานการณ์ทำงานของระบบ (System Health)

บริการ	การเรียกใช้งานเดือนที่แล้ว			การเรียกใช้งานเดือนนี้			Uptime
	Min	Avg	Max	Min	Avg	Max	

บทที่ 3
แผนการซ่อมแซมแก้ไขระบบ

- กระบวนการรับเรื่องแก้ไขปัญหา
- ประเภทและนิยามของเหตุการณ์ปัญหา
- วิธีการแก้ไขเหตุการณ์เบื้องต้น

1) กระบวนการรับเรื่องแก้ไขปัญหา



รูปที่ 14 ขั้นตอนกระบวนการรับเรื่องร้องเรียน

ขั้นตอนที่ 1 ผู้ใช้งานแจ้งรายละเอียดปัญหาผ่านช่องทางที่กำหนด

ขั้นตอนที่ 2 เจ้าหน้าที่ประสานงานตรวจสอบและรายงานปัญหาตามรอบเวลาของลักษณะเหตุการณ์ กรณีที่ไม่สามารถดำเนินการหรือแก้ไขเหตุการณ์ได้เองจะดำเนินการส่งเรื่องต่อไปยังทีมแอดมินให้ช่วยแก้ไข

ขั้นตอนที่ 3 ทีมแอดมินรับเรื่องต่อจากเจ้าหน้าที่ประสานงานเพื่อดำเนินการแก้ไขปัญหาเหตุการณ์ที่เป็นไปตามรอบดำเนินงานต่อไป

2) ประเภทและนิยามของเหตุการณ์ปัญหา

การช่วยเหลือแก้ไขปัญหาจะดำเนินการแบบระยะไกล (Remote Assistance) ในวันและเวลาที่มีการใช้งานระบบ โดยที่ปรึกษาได้จัดทำข้อตกลงในการให้บริการรักษา และดูแลระบบ (Service Level Agreement : SLA) ดังนี้

ตารางที่ 5 ข้อตกลงการให้บริการรักษาและดูแลระบบ (Service Level Agreement : SLA)

ลำดับ	ขั้นตอนการดำเนินการเมื่อระบบขัดข้อง	เวลาดำเนินการ
1	รับแจ้ง/พบปัญหาระบบขัดข้องผ่านทางหมายเลขโทรศัพท์ของเจ้าหน้าที่รับแจ้งปัญหา และผ่านแอปพลิเคชันไลน์ (Line) เพื่อสอบถามรายละเอียดหรือตัวอย่างหน้าจอการของปัญหา	● ***รับแจ้งทันทีในช่วงเวลาทำการปกติ*** ● การตอบกลับ(Response Time) *นอกเวลาทำการ* แบ่งออกเป็น 4 ประเภท ดังนี้ (1) เร่งด่วนและสำคัญ ภายใน 60 - 120 นาที หลังจากได้รับแจ้ง (2) เร่งด่วนและไม่สำคัญ ภายใน 2 - 4 ชั่วโมง หลังจากได้รับแจ้ง (3) ไม่เร่งด่วนและสำคัญ ภายใน 24 ชั่วโมง หลังจากได้รับแจ้ง (4) ไม่เร่งด่วนและไม่สำคัญ ภายในเวลาทำการปกติถัดไป หลังจากได้รับแจ้ง
2	ตรวจสอบสาเหตุการเกิดปัญหา และประเมินระดับความเร่งด่วนและสำคัญของปัญหา	ดำเนินการภายใน 30 นาที หลังการรับแจ้ง
3	วิเคราะห์ผลกระทบของปัญหา และประเมินเวลาการแก้ไขปัญหา	ดำเนินการภายใน 30 นาที หรือภายใน 60 นาที หลังการรับแจ้ง
4	แจ้งข้อมูลแก่ผู้ว่าจ้างให้ทราบถึง ● ปัญหาที่เกิดขึ้น ● สาเหตุการเกิดปัญหา ● ผลกระทบของปัญหา ● วิธีการแก้ไขปัญหา ● ระยะเวลาที่ดำเนินการแก้ไขโดยประมาณ ● ความคืบหน้าการแก้ไขปัญหา (กรณีใช้ระยะเวลาแก้ไขมากกว่า 30 นาที)	ดำเนินการภายใน 60 นาที หรือภายใน 90 นาที หลังการรับแจ้ง และความคืบหน้าการแก้ไขปัญหาทุก ๆ 30 นาที ตั้งแต่เริ่มดำเนินการแก้ไขจนการแก้ไขเสร็จสิ้น
5	ดำเนินการแก้ไขปัญหา	ภายใน 60 นาที หรือ 120 นาทีหลังการรับแจ้ง หรือตามกรณีของปัญหา
	กรณีเกิดข้อขัดข้องต้องกู้คืนระบบด้วยข้อมูลที่ Backup ไว้	ภายใน 60 นาที หรือ 240 นาทีหลังการรับแจ้ง หรือตามกรณีของปัญหา
6	แจ้งผลการแก้ไขระบบขัดข้องหลังการแก้ไขเสร็จแก่ผู้ว่าจ้าง	ทันทีที่ดำเนินการแก้ไขเสร็จ

ลำดับ	ขั้นตอนการดำเนินการเมื่อระบบขัดข้อง	เวลาดำเนินการ
7	อัปเดตระบบส่วนที่แก้ไข	หลังแจ้งผลการแก้ไขแก่ผู้ว่าจ้าง หรือภายในเวลาที่ผู้ว่าจ้างแจ้งให้อัปเดตส่วนที่แก้ไขตามกรณี

3) วิธีการแก้ไขเหตุการณ์เบื้องต้น

เนื่องจากระบบศูนย์บัญชาการเหตุการณ์ เป็นระบบที่มีการเช่าใช้โครงสร้างพื้นฐานบน Cloud ซึ่งจะมีผู้ให้บริการจะเป็นผู้ดูแลส่วนของเครื่อง VM และระบบเครือข่าย ส่วนที่ปรึกษาเป็นผู้ดูแลระบบจะให้บริการดูแลเฉพาะในส่วนระบบศูนย์บัญชาการเหตุการณ์ (Web Application) เมื่อเกิดปัญหาในระบบ จึงต้องทำการตรวจสอบปัญหาว่าสาเหตุของปัญหาเกิดขึ้นในส่วนของโครงสร้างพื้นฐานหรือเกิดขึ้นจากระบบ ขั้นตอนในการแก้ปัญหาเบื้องต้นของระบบ จึงมีขั้นตอนดังนี้

1. ตรวจสอบสาเหตุของปัญหา โดยตรวจสอบสถานะการทำงานของระบบจากระบบ Monitoring ที่ได้ติดตั้งไว้เพื่อตรวจสอบการทำงานของระบบ ซึ่งสามารถตรวจสอบความผิดปกติในระบบได้หลาย ๆ ข้อ แต่ในกรณีที่ไม่ใช้ระบบ monitoring จะสามารถทดสอบการทำงานของระบบทีละส่วนดังนี้
    - ทดสอบความพร้อมใช้งานของระบบเครือข่ายของ Cloud โดยการเปิดหน้าเว็บเพจของระบบ หรือเปิดหน้าเว็บเพจของผู้ให้บริการ Cloud ที่อยู่ใน Datacenter เดียวกันตามลำดับเพื่อทดสอบว่าระบบเครือข่ายพร้อมใช้งานหรือไม่ โดยหากไม่สามารถเปิดหน้าเว็บเพจได้ จะหมายถึงปัญหาเกิดขึ้นที่ระบบเครือข่าย สามารถแจ้งผู้ให้บริการได้ทันที
    - ในกรณีที่สามารถเปิดหน้า Static Page ของอุปกรณ์ Proxy และเปิดหน้าเว็บเพจของผู้ให้บริการ Cloud ที่อยู่ใน Datacenter เดียวกันได้ แต่ไม่สามารถเปิดหน้าเว็บเพจของระบบศูนย์บัญชาการได้ อาจเกิดจาก 2 สาเหตุคือที่อุปกรณ์ Proxy หรือที่เครื่องแม่ข่ายของระบบ การตรวจสอบเพื่อระบุตำแหน่งสามารถทำได้โดยใช้โปรแกรม Remote Desktop เพื่อทดลองเข้าใช้งานเครื่องแม่ข่ายแล้วเปิดหน้าเว็บเพจของระบบบนเครื่องแม่ข่าย ถ้าสามารถทำงานได้ ก็สามารถระบุได้ว่าอุปกรณ์ Proxy ทำงานผิดปกติ
2. ในกรณีที่เป็นปัญหาด้านระบบเครือข่าย หรือ VM บน Cloud ให้ติดต่อเจ้าหน้าที่ของผู้ให้บริการ
3. ในกรณีที่เป็นปัญหาด้าน Application ให้ตรวจสอบการทำงานเพิ่มเติมดังนี้
    - ตรวจสอบการเข้าถึงระบบ โดยทดลองเปิด Web Application จากภายในระบบเครือข่ายของผู้ให้บริการ ถ้าสามารถใช้งานได้ให้ตรวจสอบส่วนอื่น ๆ ต่อ หากไม่สามารถเปิดได้ ให้ตรวจสอบการทำงานของ web server ว่าทำงานเป็นปกติหรือไม่
    - ตรวจสอบการทำงานของระบบฐานข้อมูล โดยสามารถตรวจสอบว่าระบบสามารถใช้งานได้หรือไม่จากการทดสอบเปิด web application แล้วเปิดหน้าเว็บที่เป็น dynamic content ที่มีการเรียกใช้ข้อมูลจากฐานข้อมูล ถ้าสามารถเปิดใช้งานได้แสดงว่าฐานข้อมูลสามารถทำงานได้ปกติ ความผิดปกติที่เกิดขึ้นอาจเกิดจากข้อมูลไม่ครบถ้วน

ช่องทางติดต่อประสานงานเพื่อแจ้งปัญหาการใช้งาน

รูปที่ 15 ช่องทางสำหรับประสานงานแก้ไขปัญหาระบบ