รายงานสรุปผลการพัฒนาระบบความปลอดภัยทางไซเบอร์

กลุ่มที่ 1: ระบบ Endpoint Detection and Response (EDR)

ข้อมูลกลุ่ม

1.	นายดำรงพล โจ่ยสา	นวก.คอมพิวเตอร์ปฏิบัติการ	รพ.เชียงรายประชานุคราะห์ เขต 1
2.	นายสุกฤษฎิ์ ปัญญาคม	นวก.คอมพิวเตอร์	สสจ.ลำปาง เขต 1
3.	นายอนุสร สุริยนต์	นักทรัพยากรบุคคล	รพ.กำแพงเพชร เขต 3
4.	นายบุญลักษณ์ มงคลลักษมี	จพง.สาธารณสุขชำนาญงาน	สสจ.นครปฐม เขต 5
5.	นายนนธภพ ยาระพัฒน์	นวก.คอมพิวเตอร์ปฏิบัติการ	รพ.เถิน เขต 1
6.	นายจตุชัย ศรีคำม้วน	จพง.เครื่องคอมพิวเตอร์	รพ.นครพนม เขต 8
7.	นายกฤษฎา แต้มทอง	นวก.คอมพิวเตอร์ปฏิบัติการ	รพ.กระบี่ เขต 11
8.	นายอับดุลฮาฟิต หะยีหะเต็ง	นวก.คอมพิวเตอร์ชำนาญการ	รพ.ยะลา เขต 12
9.	นายวิศรุต วัชระเสนีย์	นวก.คอมพิวเตอร์ปฏิบัติการ	รพ.ลำพูน เขต 1
10.	นายทัชชกร นามน้อย	นวก.คอมพิวเตอร์ปฏิบัติการ	รพ.แม่สาย เขต 1
11.	นายกิตติภพ ยาวิเลิง	นวก.คอมพิวเตอร์ปฏิบัติการ	รพ.เวียงแก่น เขต 1
12.	นายเกียรติกำจร รู้ทำนอง	นวก.คอมพิวเตอร์ปฏิบัติการ	รพ.เวียงเชียงรุ้ง เขต 1
13.	นางสาวปิยะธิดา วัชระภาสร	นวก.คอมพิวเตอร์ชำนาญการ	รพ.เชียงรายประชานุคราะห์ เขต 1

1. การวิเคราะห์ปัญหาและความต้องการ

1.1. **ปัญหาที่พบในปัจจุบัน**

1.1.1. ปัจจุบันภัยคุกคามด้านไซเบอร์เพิ่มขึ้นเป็นจำนวนมากทำให้เกิดเหตุการณ์ตามข่าวต่างๆ เช่น ข้อมูล รพ.โดน Hack ,ข้อมูล รพ.ถูกเข้ารหัส(Ransom ware), ข้อมูลบัตรเครดิต, facebook ถูก hack, ข้อมูลถูกนำไป

1.1.2. เกณฑ์ประเมิน Cybersecurity บังคับให้ใช้งาน Software ระบบ EDR

1.1.3. เกณฑ์ประเมิน รพ.อัจฉริยะปีงบประมาณ 68 ให้มีการติดตั้ง Antivirus ทุกเครื่อง

1.2. ความต้องการของระบบ

1.2.1. มอบการป้องกันเชิงรุกต่อภัยคุกคามและการโจมตีขั้นสูง

ซอฟต์แวร์ EDR ช่วยป้องกัน และปกป้องเครือข่ายจากการโจมตีทางไซเบอร์เชิงรุก ด้วยการตรวจจับ และกำจัดภัยคุกคามก่อนที่จะสร้างความเสียหายหรือทำให้ข้อมูลสำคัญรั่วไหล ระบบนี้จะตรวจสอบกิจกรรมของอุปกรณ์ปลายทางและพฤติกรรมของผู้ใช้อย่างต่อเนื่อง ทำให้สามารถระบุภัยคุกคามรูปแบบใหม่ๆ ที่อาจเกิดขึ้นได้ โดยคุณสมบัตินี้มีความสำคัญอย่างยิ่ง เนื่องจากภัยคุกคามทางไซเบอร์มีการพัฒนาอยู่ตลอดเวลา และมักมีความซับซ้อนเกินกว่าที่ระบบป้องกันอุปกรณ์ปลายทางแบบดั้งเดิมจะตรวจพบได้ ด้วยเหตุนี้ ระบบ EDR จึงช่วยให้สามารถตรวจจับ และรับมือกับการบุกรุกดังกล่าวได้อย่างรวดเร็ว และมีประสิทธิภาพ

1.2.2. การเพิ่มขึ้นของการทำงานแบบผสมผสาน (Hybrid Work) ส่งผลให้เครือข่ายมีช่องโหว่มากขึ้น

การแพร่ระบาดของโควิด-19 ได้เปลี่ยนแปลงวิถีชีวิตของเราอย่างมาก แม้ในโลกหลังการระบาด หลายบริษัทยังคงเลือกใช้รูปแบบการทำงานแบบผสมผสานหรือการทำงานทางไกลเพื่อเพิ่มประสิทธิภาพ

อย่างไรก็ตาม การเพิ่มขึ้นอย่างรวดเร็วของอุปกรณ์ปลายทางเครือข่ายก็นำมาซึ่งช่องโหว่ที่มากขึ้นด้วยเช่นกัน เมื่อผู้คนทำงานจากบ้านหรือสถานที่นอกสำนักงานมากขึ้น ส่งผลให้พื้นที่ที่อาจถูกโจมตีผ่านอุปกรณ์ปลายทางขยายวงกว้างขึ้นตามไปด้วย เพราะอุปกรณ์ปลายทางเหล่านี้สามารถกลายเป็นช่องทางสำหรับการโจมตีทางไซเบอร์ได้ ดังนั้นระบบ EDR จึงช่วยให้มั่นใจว่า เครือข่ายภายในองค์กรยังคงได้รับการปกป้อง ไม่ว่าจะเข้าถึงจากที่ใดก็ตาม

1.2.3. แฮคเกอร์อาจซ่อนตัวอยู่ในระบบเป็นเวลานาน

ปัจจุบันการโจมตีทางไซเบอร์สามารถดำเนินการได้อย่างเงียบเชียบภายในเครือข่าย และมักสร้างเส้นทางลับ (Backdoor) สำหรับเข้าถึงจากภายนอกเอาไว้ ด้วยศักยภาพในการค้นพบช่องโหว่ของซอฟแวร์ระบบปฏิบัติการ (Operative System) จากแหล่งภายนอกนี้ ส่งผลให้ระบบ EDR มีความสำคัญอย่างยิ่งสำหรับการตรวจจับภายในอย่างทันท่วงที และมีประสิทธิภาพ

1.2.4. รับรองการปฏิบัติตามกฎระเบียบ (Regulatory Compliance)

ภาครัฐตระหนักดีว่า การโจมตีทางไซเบอร์สามารถสร้างความเสียหายต่อประชาชนและประเทศชาติ ดังนั้นจึงได้กำหนดกรอบกฎระเบียบที่เข้มงวด ซึ่งบริษัทต่างๆ จำเป็นต้องจัดให้มีการป้องกันข้อมูลที่เพียงพอสำหรับลูกค้า หลายประเทศมีบทลงโทษที่รุนแรงสำหรับการละเมิดกฎระเบียบด้านความปลอดภัยทางไซเบอร์ โดยเฉพาะองค์กรที่ต้องจัดการข้อมูลที่ละเอียดอ่อน ซึ่งจึงจำเป็นต้องใช้ระบบรักษาความปลอดภัยทางไซเบอร์ขั้นสูง ส่งผลให้การนำระบบ EDR มาใช้ไม่เพียงแสดงถึงความมุ่งมั่นในการปฏิบัติตามข้อกำหนด แต่ยังช่วยป้องกันองค์กรจากค่าปรับมหาศาลที่อาจเกิดขึ้นจากการละเมิดความปลอดภัยของข้อมูล

1.2.5. โซลูชันอันชาญฉลาดที่สามารถนำไปใช้ได้จริง

การมีระบบรักษาความปลอดภัยระดับสูงไม่ได้รับประกันการรั่วไหลของข้อมูล และตีความข้อมูลที่เกี่ยวข้องกับการถูกละเมิดได้อย่างมีประสิทธิภาพ ในขณะที่โซลูชัน EDR ช่วยให้การประมวลผล และการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องเป็นไปอย่างรวดเร็ว เพื่อป้องกันช่องโหว่ที่มีอยู่ นอกจากนี้ การเข้าถึงข้อมูลด้านความปลอดภัยเพียงอย่างเดียวยังไม่เพียงพอด้วยเช่นกัน เพราะการตรวจจับ และการตอบสนองต่ออุปกรณ์ปลายทางถือเป็นปัจจัยสำคัญสำหรับข้อมูลเชิงลึกที่สามารถนำไปใช้ได้จริง และสำหรับมาตรการรับมือที่มีประสิทธิภาพ โดยมีทั้งเครื่องมือการวิเคราะห์ และแนวทางปฏิบัติจากผู้เชี่ยวชาญในด้านความปลอดภัยทางไซเบอร์

1.2.6. ป้องกันการสูญเสียทางการเงิน และข้อมูลรั่วไหลจากการโจมตีทางไซเบอร์

เหตุการณ์ด้านความปลอดภัยสามารถส่งผลกระทบทางการเงินต่อองค์กรได้ ไม่ว่าจะเป็นความเสียหายต่อชื่อเสียงหรือค่าปรับจากการละเมิดกฎระเบียบ การโจมตีทางไซเบอร์ทำให้องค์กรเกิดค่าใช้จ่าย และสูญเสียรายได้ แต่ระบบ EDR สามารถมอบการป้องกันแบบครอบคลุมที่ช่วยป้องกันการโจมตีทางไซเบอร์หรือการสูญเสียข้อมูลที่มีค่าใช้จ่ายสูงได้ ซึ่งช่วยลดต้นทุนโดยรวมในการรักษาความปลอดภัยทางไซเบอร์

1.2.7. คุ้มค่าคุ้มราคา

หากปราศจากความสามารถในการป้องกันที่ครอบคลุม กระบวนการแก้ไขปัญหาอาจยุ่งยากและมีค่าใช้จ่ายสูง ในขณะที่ระบบ EDR สามารถช่วยลดระยะเวลา และค่าใช้จ่ายเหล่านี้ได้ เพื่อลดความจำเป็นในการใช้มาตรการรุนแรง เช่น การปรับปรุงหรืออัปเดตซอฟแวร์ภายในระบบทั้งหมด พร้อมช่วยให้การดำเนินงานเป็นไปอย่างต่อเนื่องโดยไม่หยุดชะงัก

2. การออกแบบระบบ

ทางเลือกการออกแบบระบบ

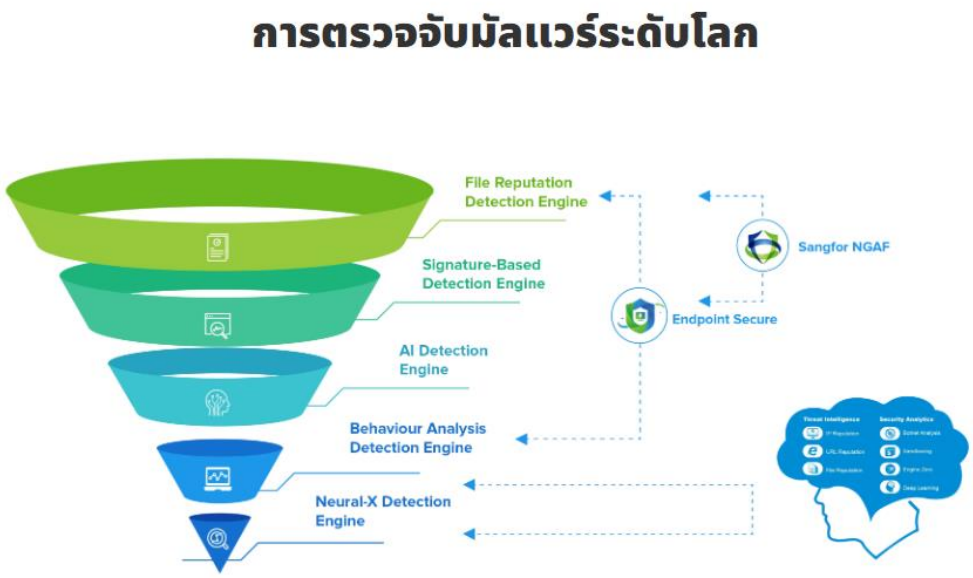
- สำรวจจำนวน EDR Client ที่ต้องใช้งาน
- จัดหา software EDR ที่ตรงความต้องการ
- ของบประมาณจัดซื้อ จำนวนเครื่องx700
- เลือก Solution on-premise/ on-cloud

2.1. on-Premise

- ติดตั้ง software management server
- จัดการ license และการตั้งค่า
- โหลดไฟล์ติดตั้งลงเครื่องลูก

2.2. on-Cloud

- จัดการ license และการตั้งค่า
- โหลดไฟล์ติดตั้งลงเครื่องลูก



3. การพัฒนาและติดตั้ง

3.1. วิธีการติดตั้ง ES , EDR Manager (On Premise) เตรียม ES Manager โดยใช้ Spec ดังนี้

1-5000 Endpoints

CPU >= 8 Core

RAM >= 16 GB

Disk >= 512 GB (Thin Provisioning) หรือ >= 1TB*

3.2. สร้าง VM ตาม Requirement ข้างต้น โดยจะมีระบบตรวจสอบว่า Spec ห้ามต่ำกว่า 8Core 8GB ตั้งแต่ ISO ของ ES3.7.2 ได้เปลี่ยน Linux Distro เป็น Ubuntu 20.04

3.3. หลังจากที่ Boot VM ด้วย ISO ระบบจะทำการติดตั้ง Endpoint Secure Manager อัตโนมัติ

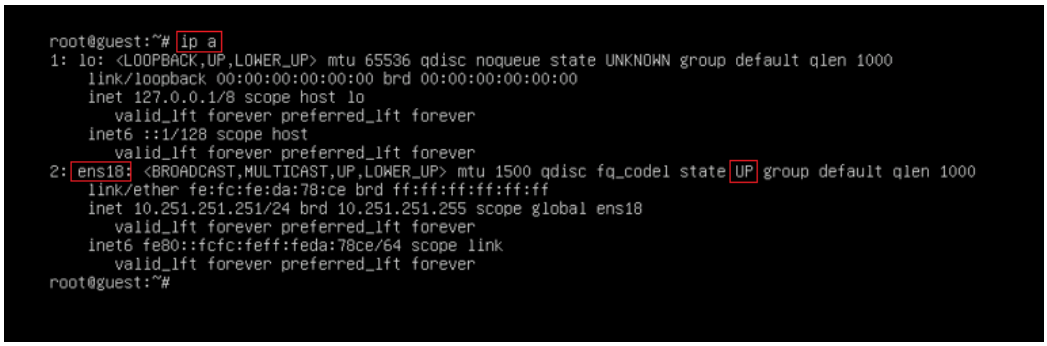
หากทำการติดตั้งบน Sangfor HCI จะต้องไปปรับ BIOS Option ให้เป็น UEFI ก่อน จึงจะสามารถเริ่มติดตั้งได้

ถ้าหน้า Console ขึ้นว่า guest login: แสดงว่าติดตั้งเสร็จแล้ว

3.4. Login ที่ console ของ Sangfor ES Manager ได้โดยใช้ข้อมูลดังต่อไปนี้

Username: root Password: great@cause

3.5. ใช้คำสั่ง ip a เพื่อตรวจสอบชื่อ interface เช่น ens18 หรือ ens160 และดูสถานะของ interface (UP/DOWN)

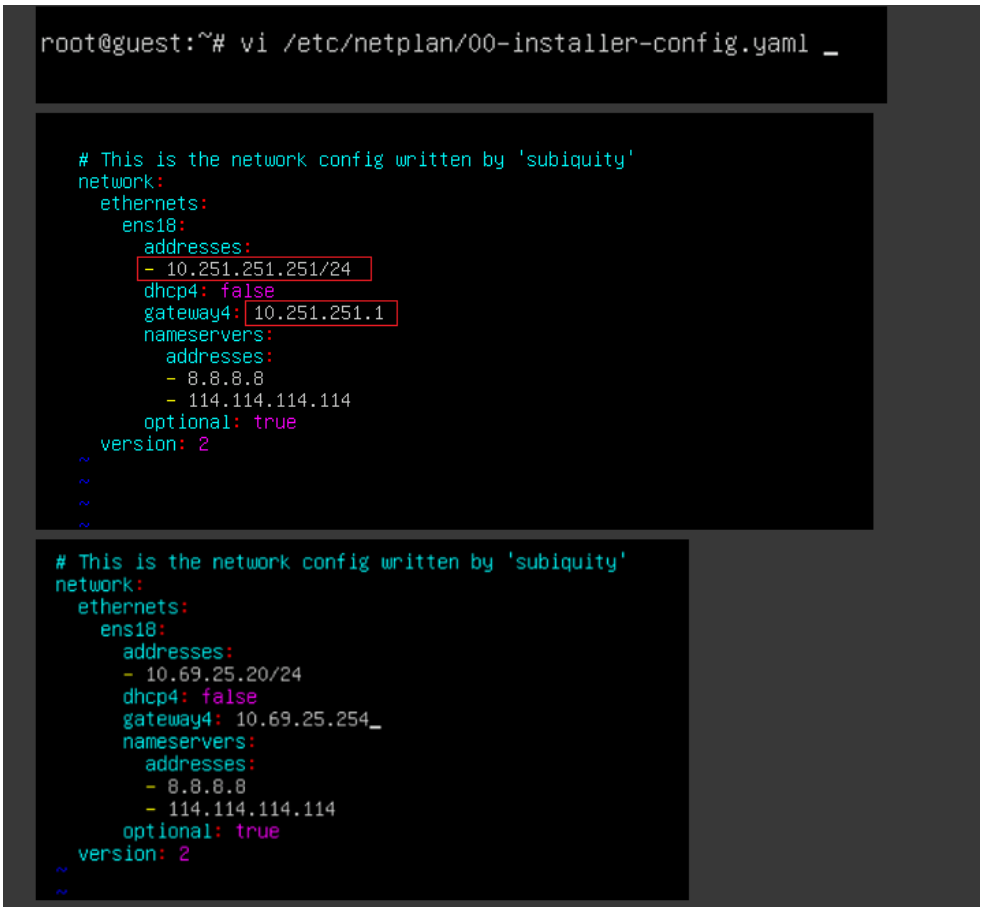


ถ้าไม่ up ให้ใช้คำสั่ง เพื่อ on interface ขึ้นมา จึงจะเห็น IP

```
ip link set up ens18        (หรือ eth0 แล้วแต่เครื่อง)
netplan apply
```

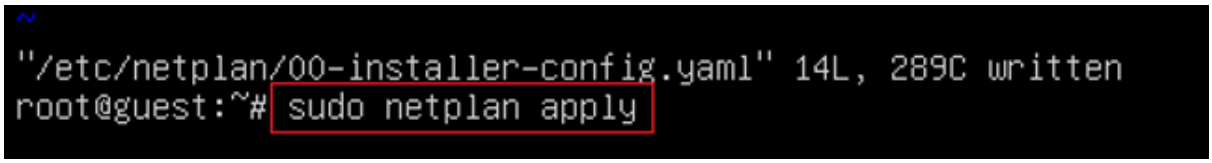
3.6. ใช้คำสั่ง vi /etc/netplan/00-installer-config.yaml เพื่อตั้งค่า IP, Subnet, Gateway

*recheck ว่า ens[xx] ในข้อ4 กับ ข้อ5 ตรงกันหรือไม่ ถ้าไม่ตรงให้แก้ .yaml ให้ตรงกับผล ip a

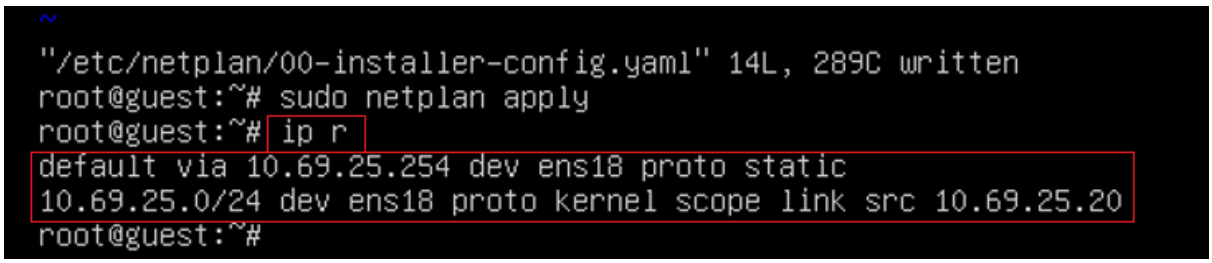


กรณีใช้ vi :- กด i เพื่อเข้าโหมด insert เพื่อแก้ไขข้อมูลในไฟล์ - กด ESC เพื่อออกจากโหมด insert - พิมพ์ :wq และ enter เพื่อ write และ quit ออกจาก ไฟล์นี้ (ถ้าต้องการออกโดยที่ไม่save พิมพ์ :q และ enter)

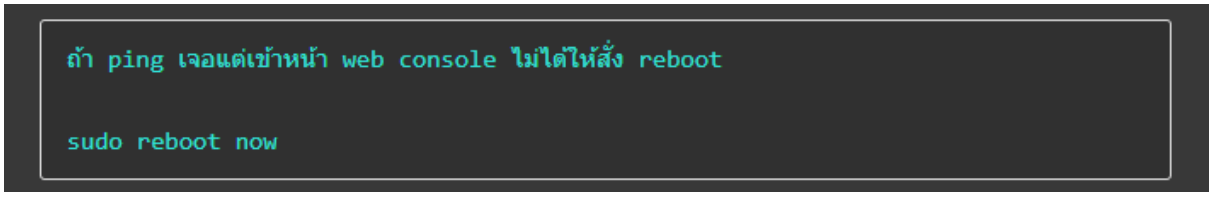
3.7. ใช้คำสั่ง sudo netplan apply



3.8. ใช้คำสั่ง **ip r** เพื่อเช็คการตั้งค่า

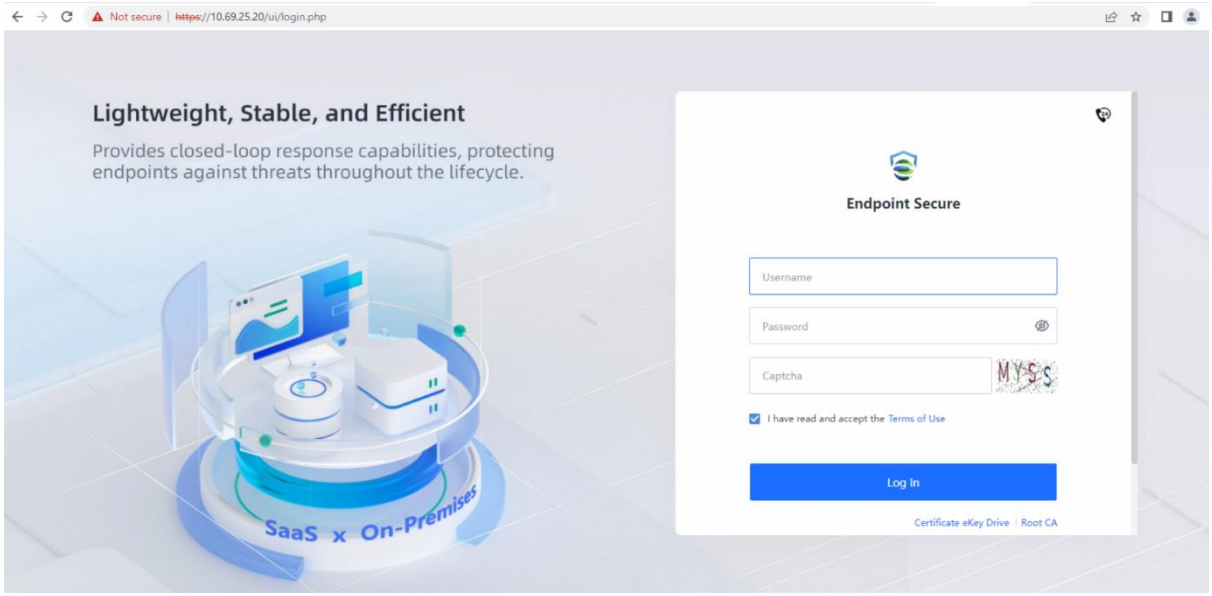


3.9. ทดลอง **ping** ไป gateway เพื่อตรวจสอบการเชื่อมต่อ



3.10. เข้าหน้า Web Console เพื่อบริหารจัดการ ได้ที่ https://ip-es-manager

โดยใช้ **username: admin password: admin**

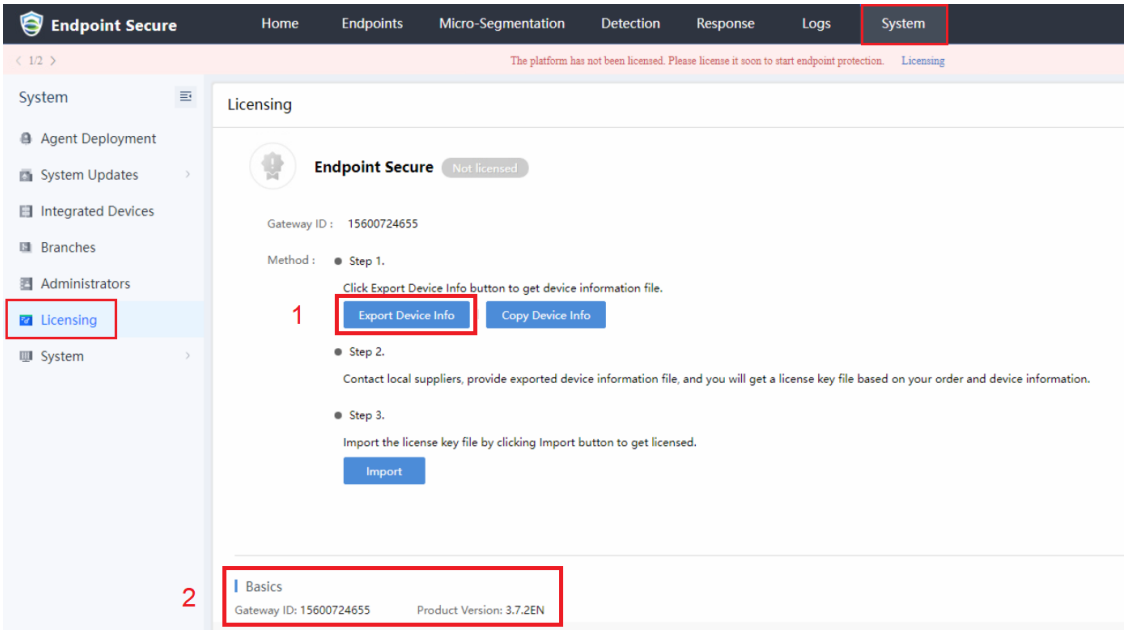


3.11. ไปที่เมนู **System > Licensing** ดังรูป เพื่อดำเนินการแจ้งค่า **Gateway ID**, และ **Export Device Info** เพื่อนำมาดำเนินการขอ License

>> ส่งมาที่ support.thailand@sangfor.com >> หัวข้อ : Generate ES Manager License - ชื่อลูกค้า

1. Export Device Info File
2. ES Version:
3. Gateway ID:
4. Enduser:
5. Partner:
6. Standard or Ultimate License:
7. ใบ Service Letter (ถ้าเป็นแบบซื้อ)

- กรณี License POC จะได้สูงสุด 90 Agents



3.12. เมื่อได้ License แล้ว ให้นำมา Import ในหน้า WebUI ES Manager

4. **ผลการทดสอบ**
   - software EDR ราคาตามตามเกณฑ์ ICT
   - คุณสมบัติตามเกณฑ์ software EDR ด้าน Cyber security
   - ป้องกัน ransom ware ได้
   - ป้องกันการใช้ software crack ได้
   - ป้องกัน การติดตั้ง app/คำสั่งที่เป็นอันตรายต่อเครื่อง ได้
   - ไม่กินทรัพยากรเครื่อง
   - รองรับการทำงาน OS เก่าๆที่ไม่สามารถอัพเดต security patch (แต่จำเป็นยังคงต้องใช้งาน)
   - มีระบบ Central Managemenet
   - ป้องกันการปิด antivirus ได้
5. **แผนการบำรุงรักษาโครงสร้างพื้นฐานทางด้านไอทีด้วย 6 มาตรการด้านความปลอดภัย**
   - ต้องมีการจัดทำแผนการจัดซื้อ/ต่ออายุ สินทรัพย์ประเภท software ทุกปีเพื่อให้ สามารถปกป้องสินทรัพย์และสามารถใช้งานได้ต่อเนื่อง
6. **ข้อเสนอแนะ**
   - **ใน version เก่าไม่ support linux**
   - **High false alarm (Garner peer insight)**
   - **การตั้งค่าความปลอดภัยไม่ยืดหยุ่น**
7. **แนวทางพัฒนาต่อ**
   - ต้องทำการนโยบายทางด้าน cybersecurity ควบคู่ไปด้วยอย่างเข้มข้น เพื่อให้ software สามารถทำงานได้มีประสิทธิภาพสูงสุด

---คู่มือ---

การตั้งค่า Security Protection Policy ใน Endpoint Secure Manager

หลังจากที่ได้ติดตั้ง Endpoint Secure Manager และ Agent ไปยังเครื่อง Endpoint แล้วสามารถปรับแต่ง policy ด้านความปลอดภัยได้โดยสามารถแยกการตั้งค่าตามgroup ได้

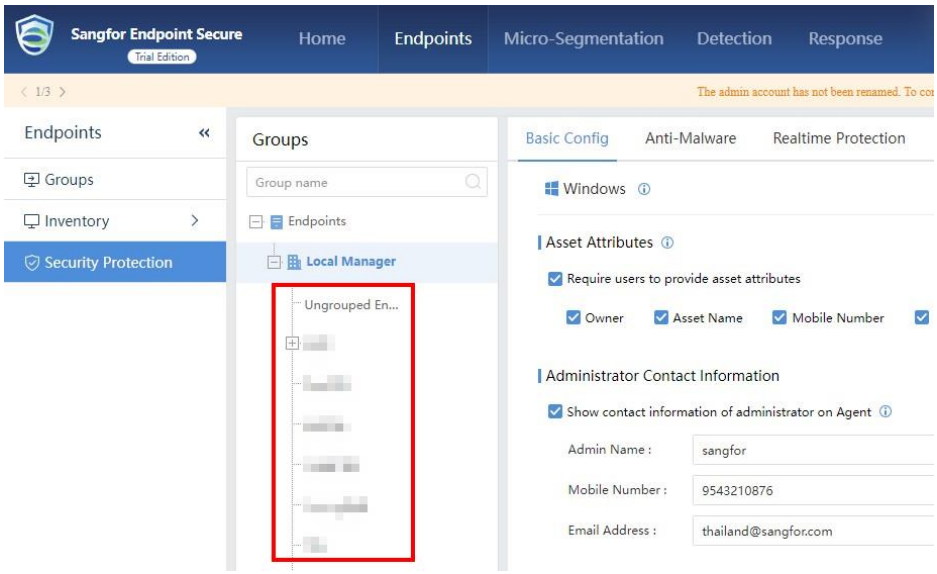
การตั้งค่าGroup

ไปที่ Endpoint > Groups

- สามารถจัด group ให้กับ endpointใหม่ๆ ตามIPได้ (Auto Grouping)
- สามารถเลือก endpoint แล้ว move เข้าไปที่groupที่ต้องการได้

การตั้งค่า Security Protection ตาม Group

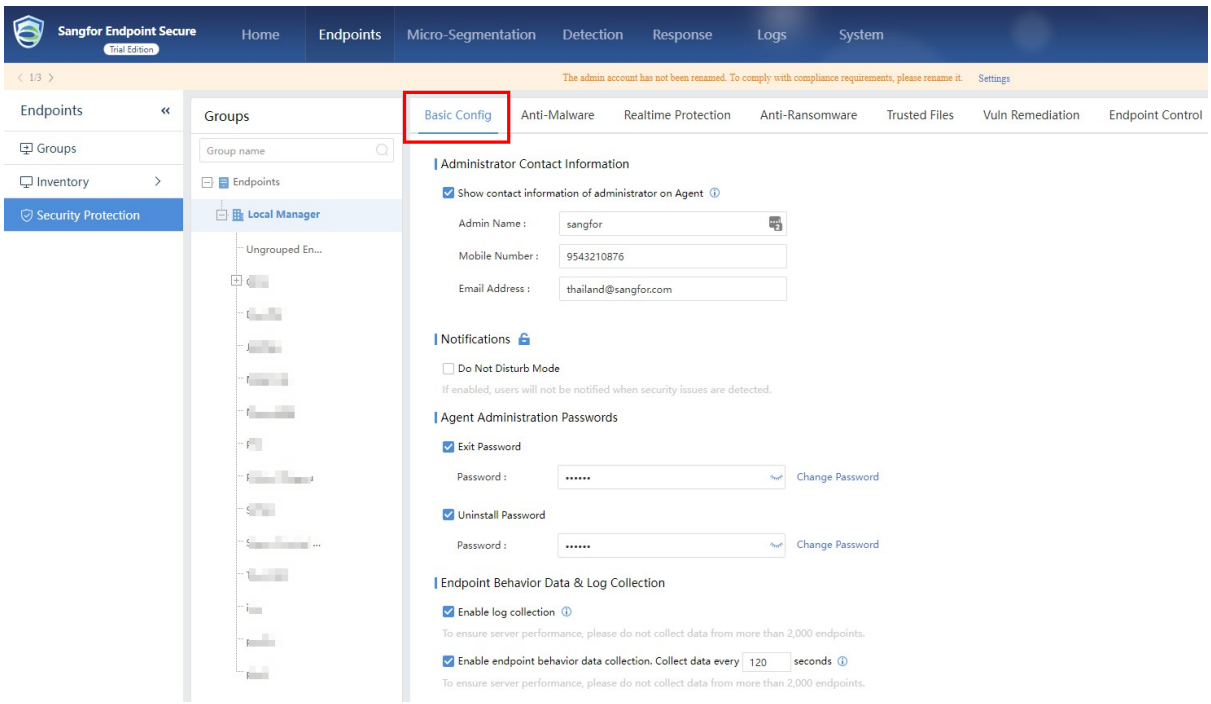
- สามารถตั้ง policy สำหรับ แต่ละ group ได้ โดยเลือกที่group จากนั้นtabต่างๆด้านขวาจะเป็นของ group ที่เลือก



Tab ต่างๆใน Security Protection

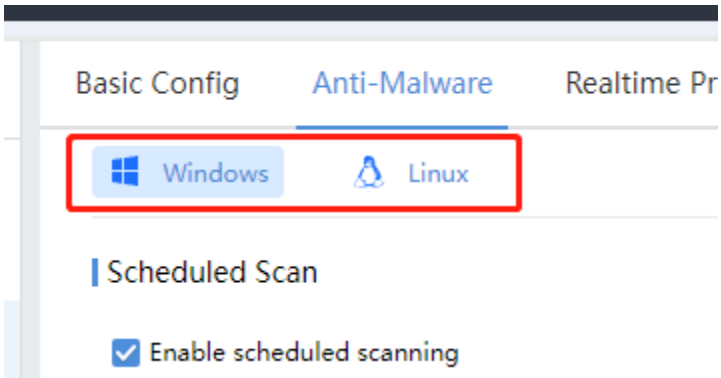
1. Basics

- เลือกที่จะเก็บข้อมูลเจ้าของ endpoint
- รหัส เพื่อปิดprogram
- รหัส เพื่อถอนprogram

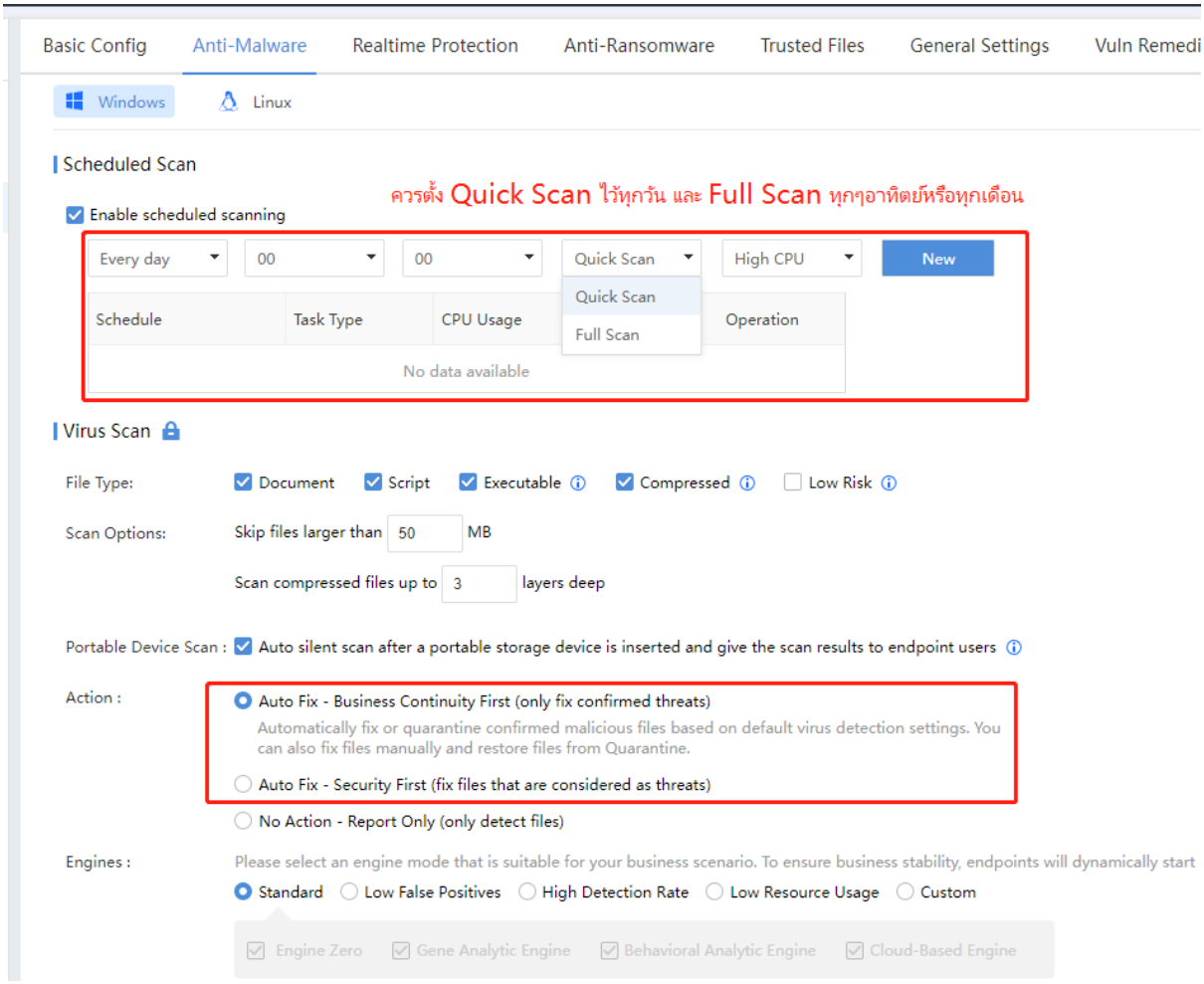


2.Malware

- สามารถเลือก ประเภทของendpoint เช่น Windows หรือ Linux

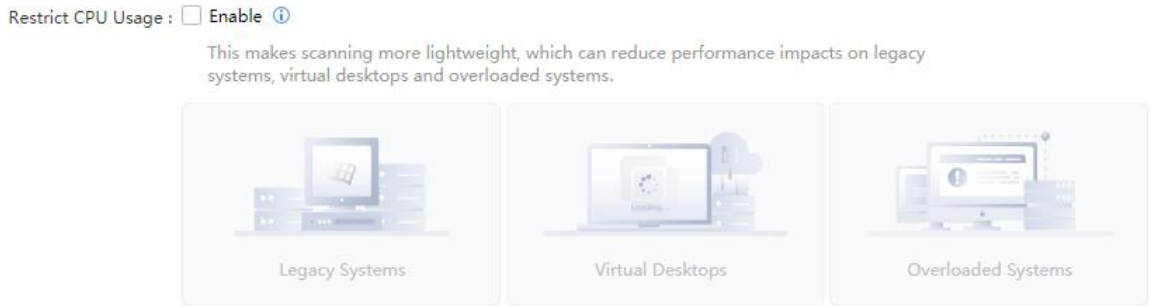


- การตั้ง Scheduled Scan และระดับการ take action

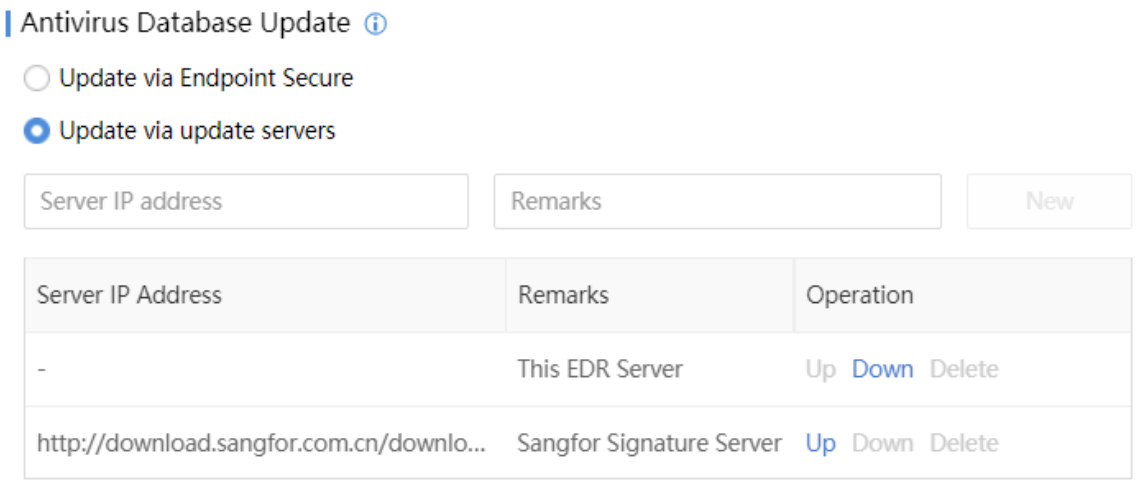


- Business Continuity First - แก้ไขและกักไฟล์ที่อยู่ในฐานข้อมูลว่าคือthreat
- Security First - แก้ไขและกักไฟล์ที่สงสัยว่ามีความเสี่ยงทั้งหมดที่เจอ ถ้าไม่ใช่ก็ค่อยไปปลดจาก Fixed ในหน้า Responseอีกที
- No Action - Report Only - ไม่ทำการแก้ไข แต่จะแจ้งในtab Response อย่างเดียว

- ตั้งค่าสำหรับ Endpoint ที่ไม่สามารถใช้งานResourceมาก

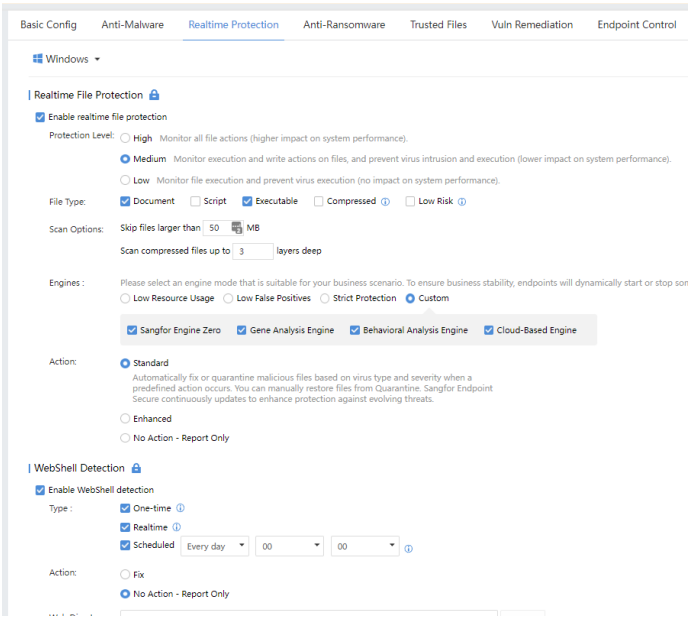


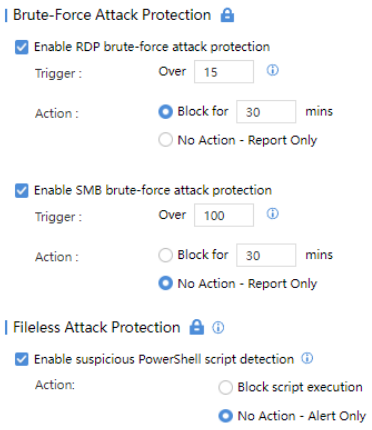
- เลือกว่าให้update database ของ antivirus จากที่ไหน



3.Realtime Protection - ตั้งค่าการทำงานของagent (คล้ายๆ antivirus)

- ตั้งค่าการป้องกันแบบ Realtime รวมถึง WebShell Detection, Brute-Force Attack Detection, Ransomware Protection (Honeypot), Fileless Attack Protection.

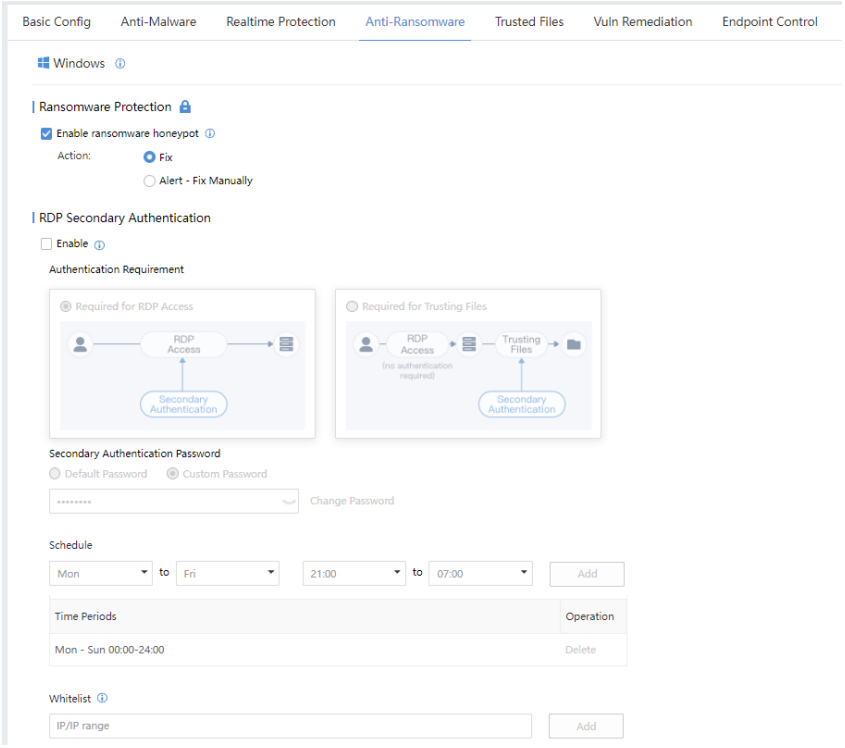




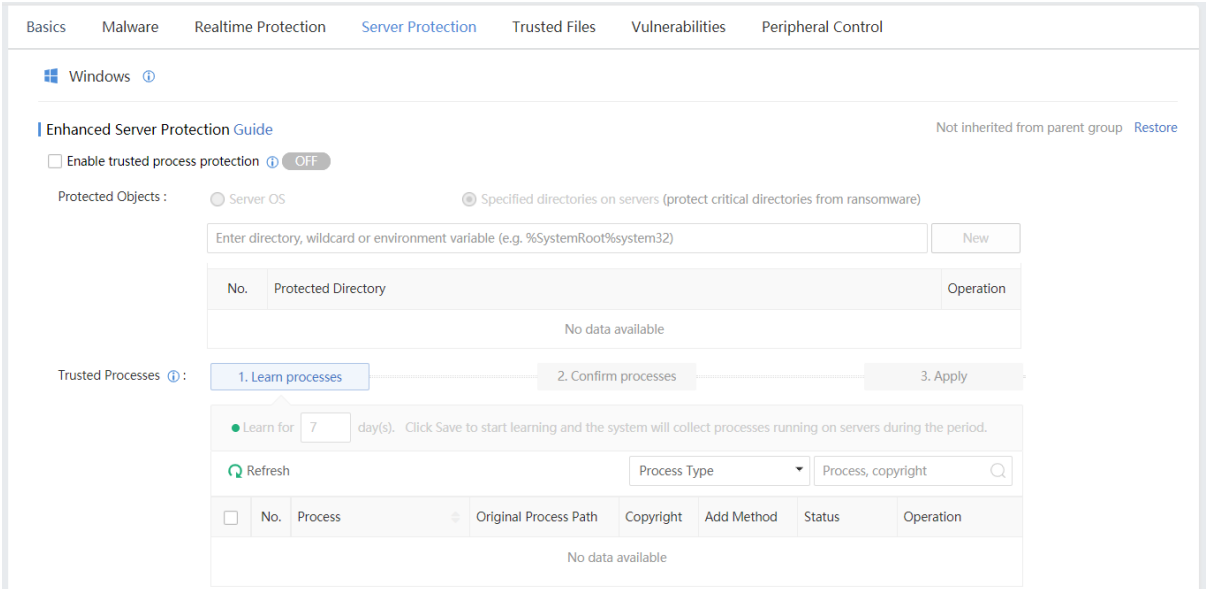
4.Anti-Ransomware - การป้องกัน Ransomware

- Ransomware Honeypot - เป็นการวางไฟล์เหยื่อล่อ ถ้ามีprocess มา Encrypt จะทำการ Suspend ทิ้งถ้าตั้งค่าไว้ที่ Fix

- RDP Secondary Authentication - เมื่อ RDP เข้า server จะต้องใช้รหัสผ่านอีกชุดจาก ES Manager เพื่อเข้าถึงตัว OS (RDP เข้าServerแล้วติดรหัสผ่าน) สามารถตั้งช่วงเวลา Active 2FA ได้ หรือทำ whitelist source ip ได้ ที่ไม่ต้องโดน 2FA ดูรหัสที่จะใช้เข้าใช้งานจากหน้า ES Manager และสามารถกด Copy ออกไปได้



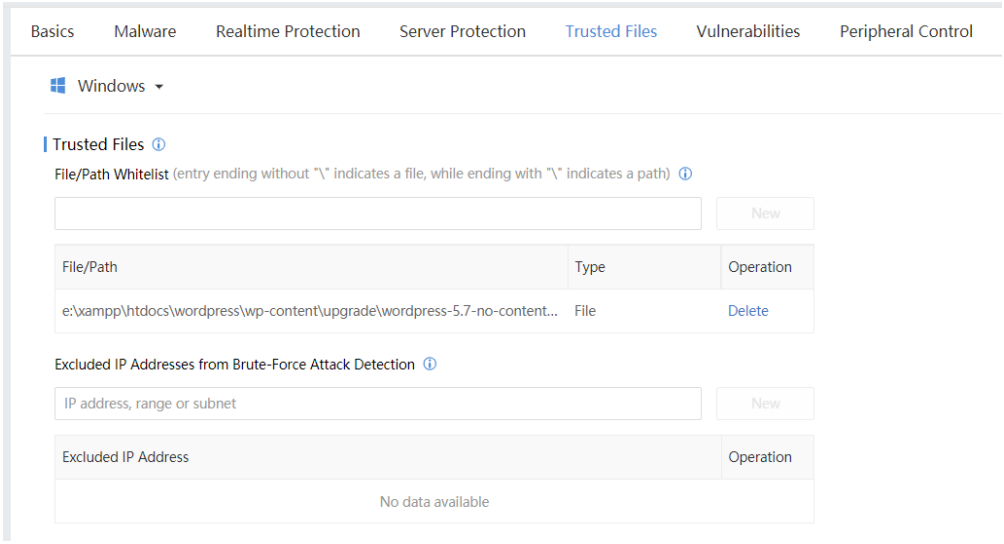
- Enhanced Server Protection - มีผลเฉพาะกับ Windows Server - จะการ Learn process ที่ run อยู่บนserverนั้นๆ และจะไม่อนุญาตให้processนอกเหนือจากนั้นrunได้ ใช้ในกรณีต้องการความปลอดภัยขั้นสูง
- โดยจะlearning process ตามจำนวนวันที่กำหนด และรอคำยืนยันเพื่อดำเนินการใช้งานต่อไป



5.Trusted Files

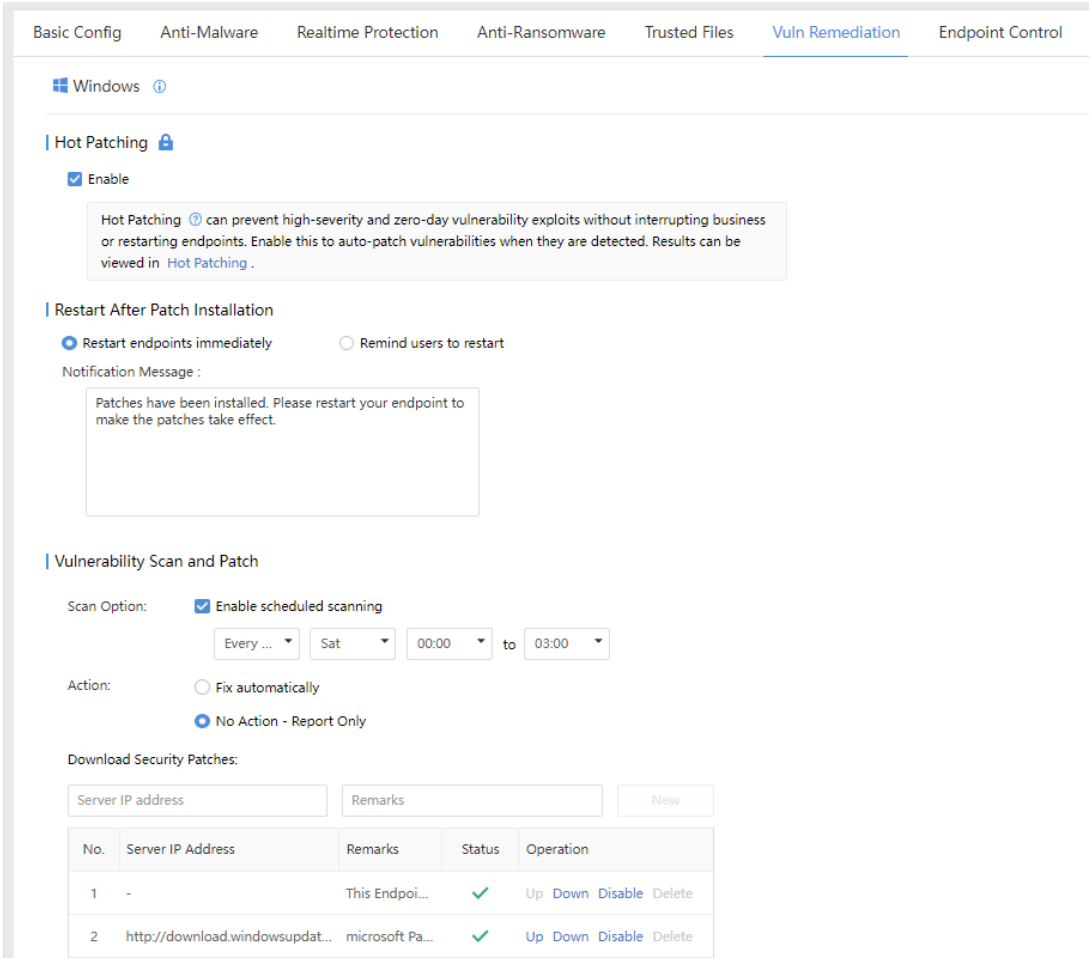
- เลือก File หรือ Path ที่ต้องการจะwhitelist

- IP ที่จะให้exclude จากการตรวจจับ Brute-Force Attack



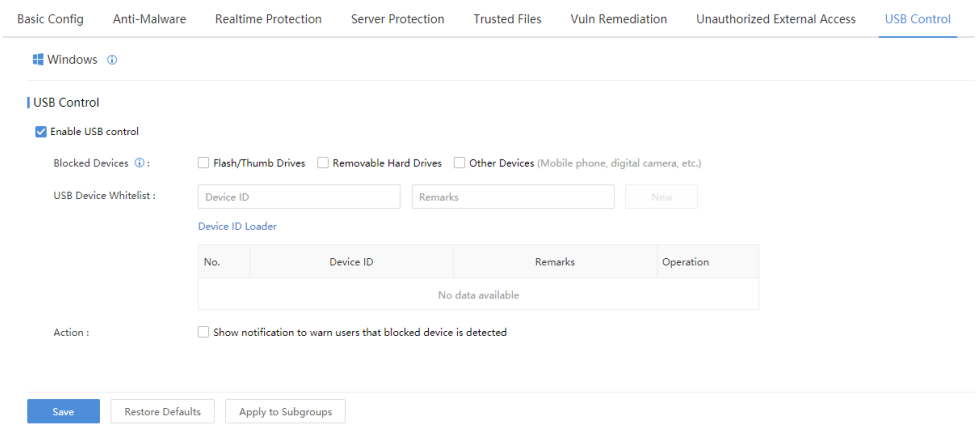
6.Vuln Remediation

- ตั้งค่า Hot Patching ซึ่งเป็นการป้องกันช่องโหว่ Windows ที่มีความสำคัญด้วย Patch เสมือน โดยไม่ต้องReboot/ติดตั้งpatch
- สามารถสั่ง Schedule Scan ช่องโหว่ของ OS เช่น Patch ของ windows ที่ยังไม่ได้ลง ตามวันและช่วงเวลาที่กำหนด
- เลือกว่าจะให้ Download patch os จากที่ไหน เช่น ผ่านES Manager หรือจาก websiteของMicrosoftเอง



7.Endpoint Control

- การป้องกันการใช้งาน USB เช่น อุปกรณ์USB (Flash Drive), Removable Drives (Hard Drive), หรือ Portable Devices (Mobile Phone, Camera)
- Keyboard และ Mouse จะไม่ถูกBlockจากหัวข้อนี้ (จะBlockเฉพาะประเภทที่มีStorage)
- สามารถทำwhitelistได้สำหรับบางอุปกรณ์ที่ต้องการ [การตั้งค่า Block USB และ Whitelist USB]
- การแค่เลือก Enable USB Control จะยังไม่ Block จะต้องเลือก Device ด้วย



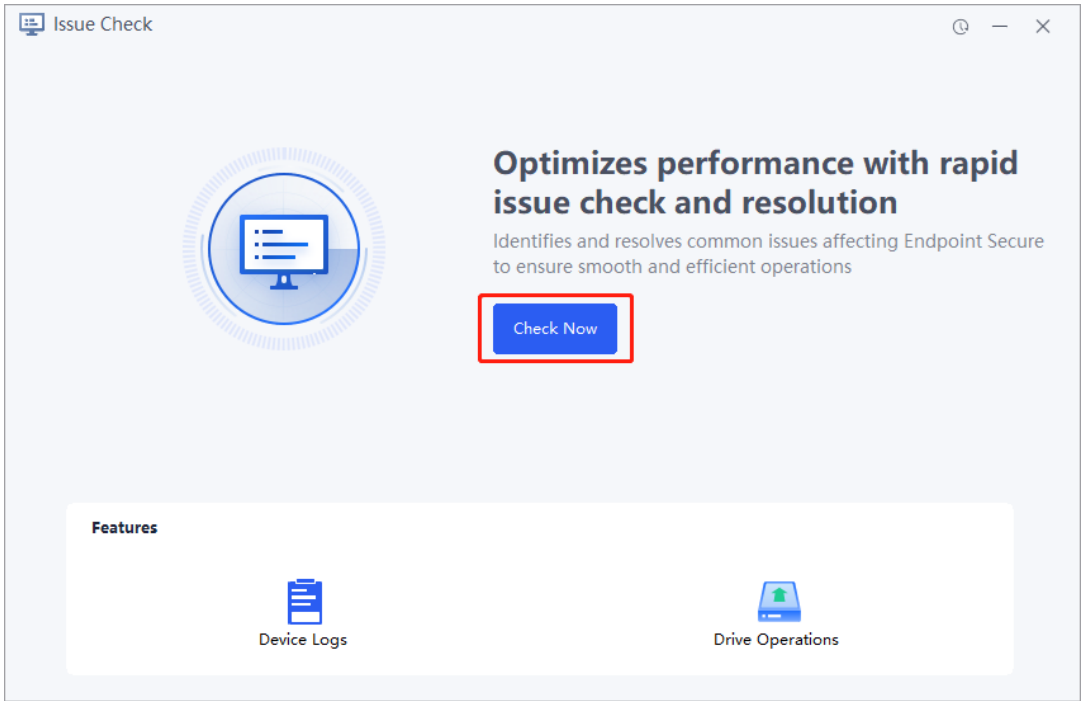
การเก็บ Log ES Agent ด้วย EDR Diagnostic Tool

วิธีการ Run Tool

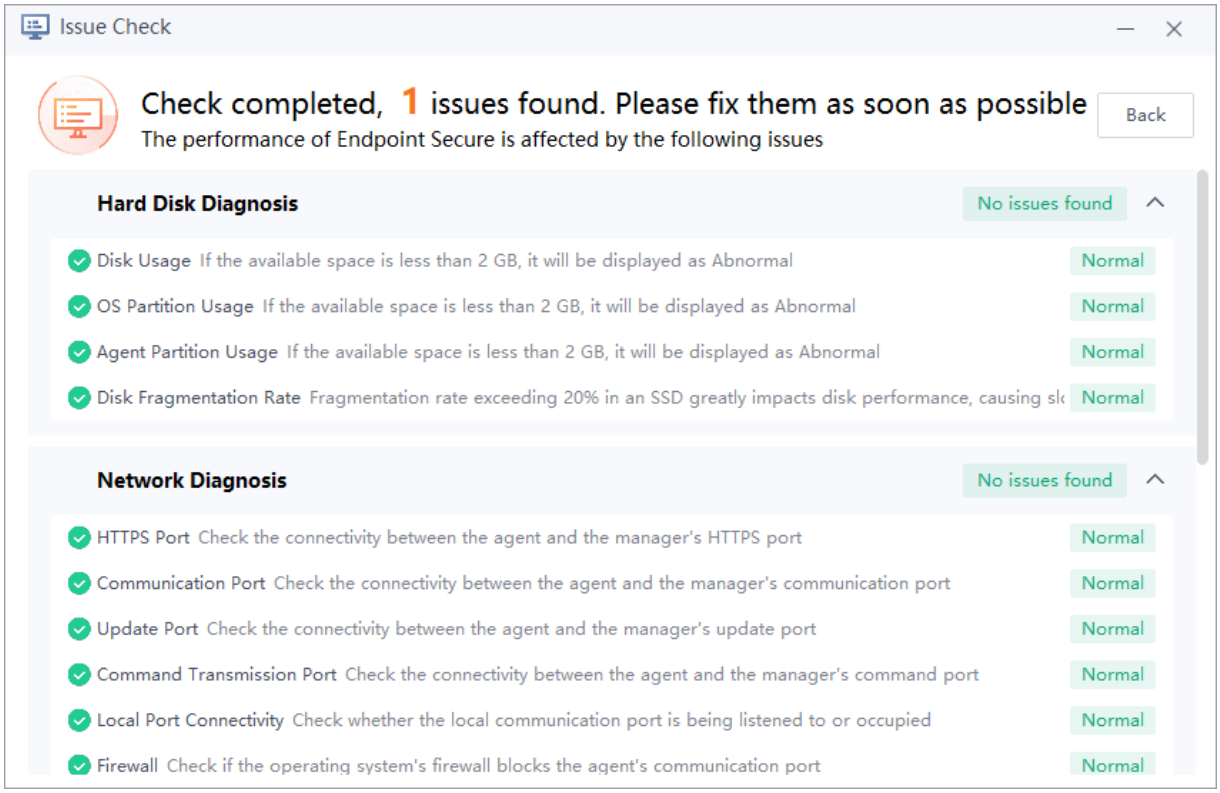
1. Download File ตามแนบด้านล่างใน Attachment
2. Run as Administrator

Issue Check

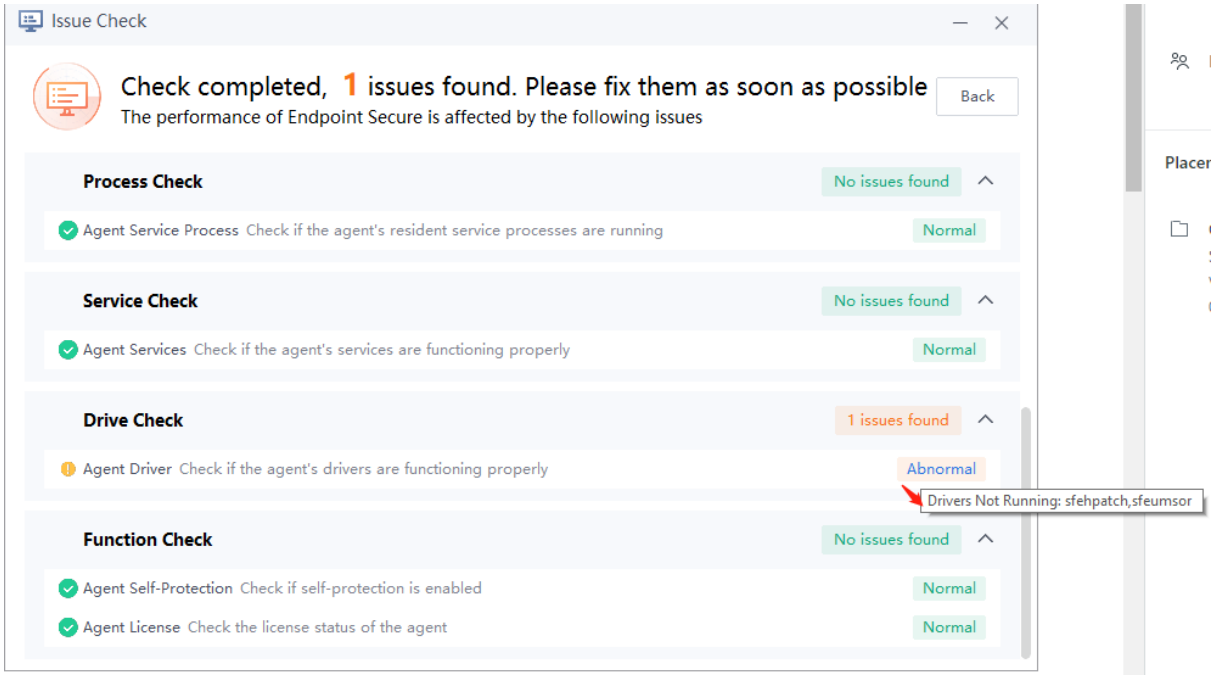
1. กด Check Now



2. Screenshot ผิด

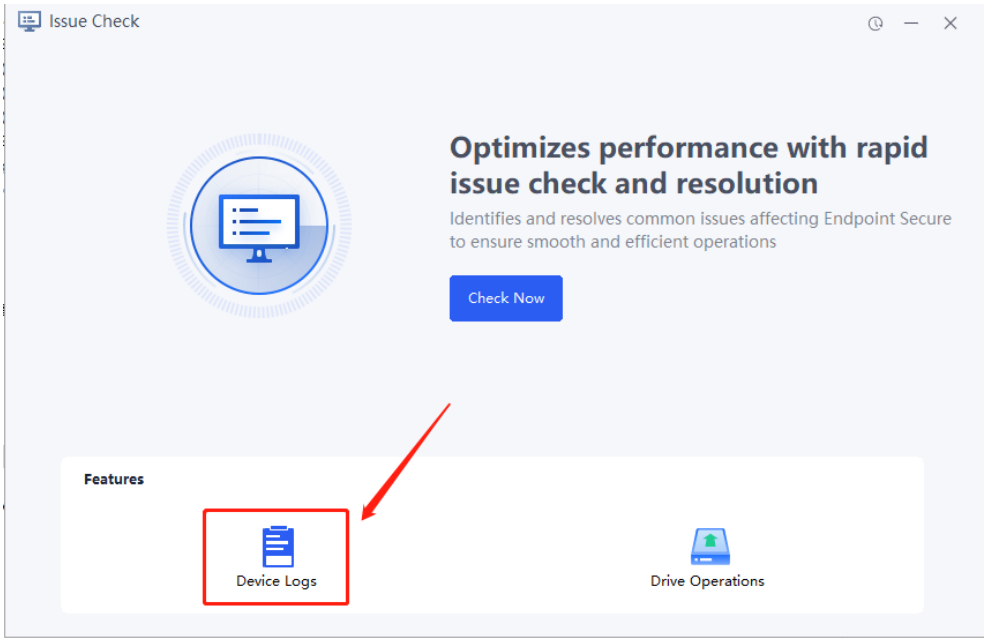


Screenshot Abnormal issue

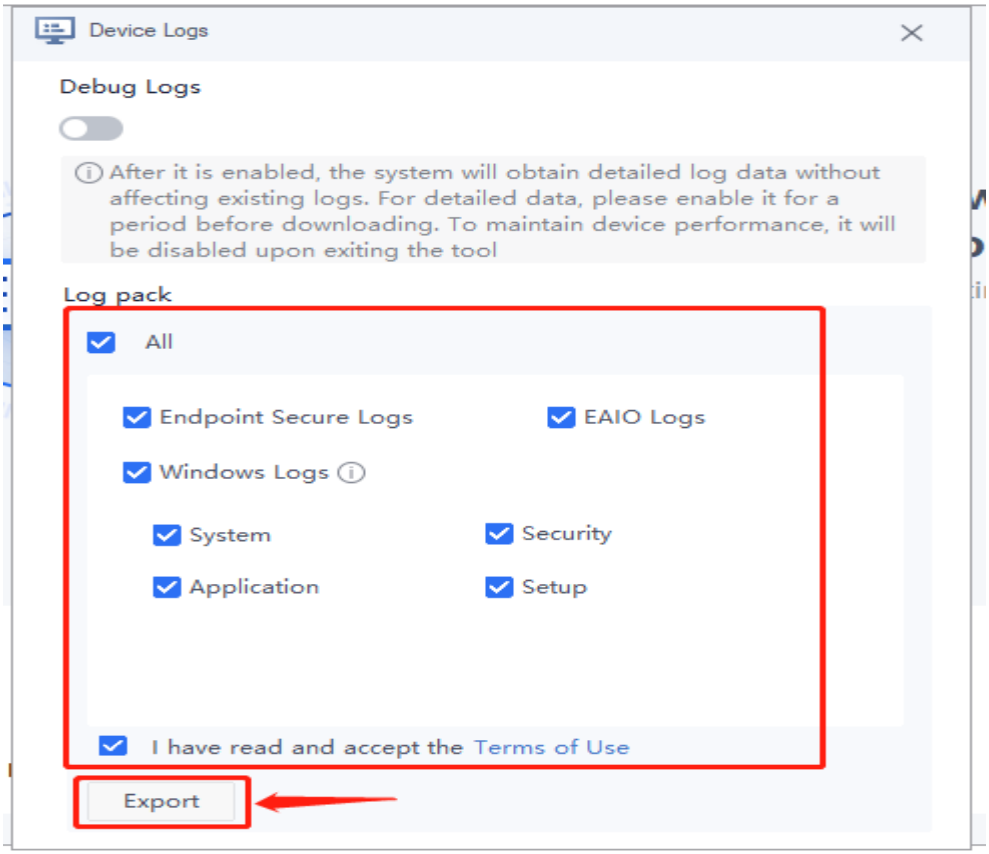


การเก็บ Log

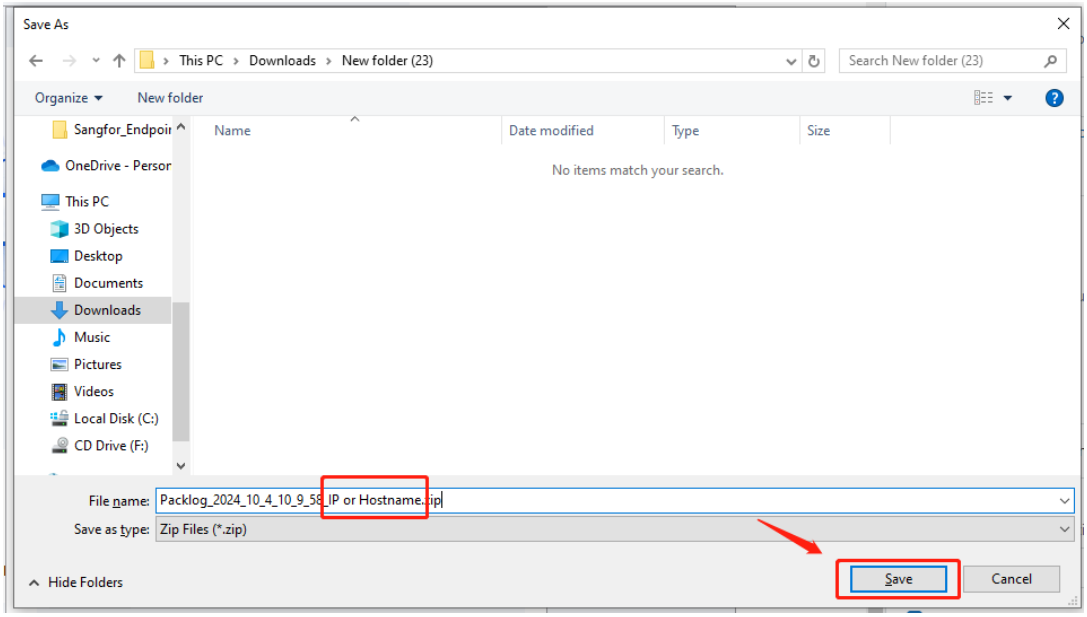
1. กด Device Logs



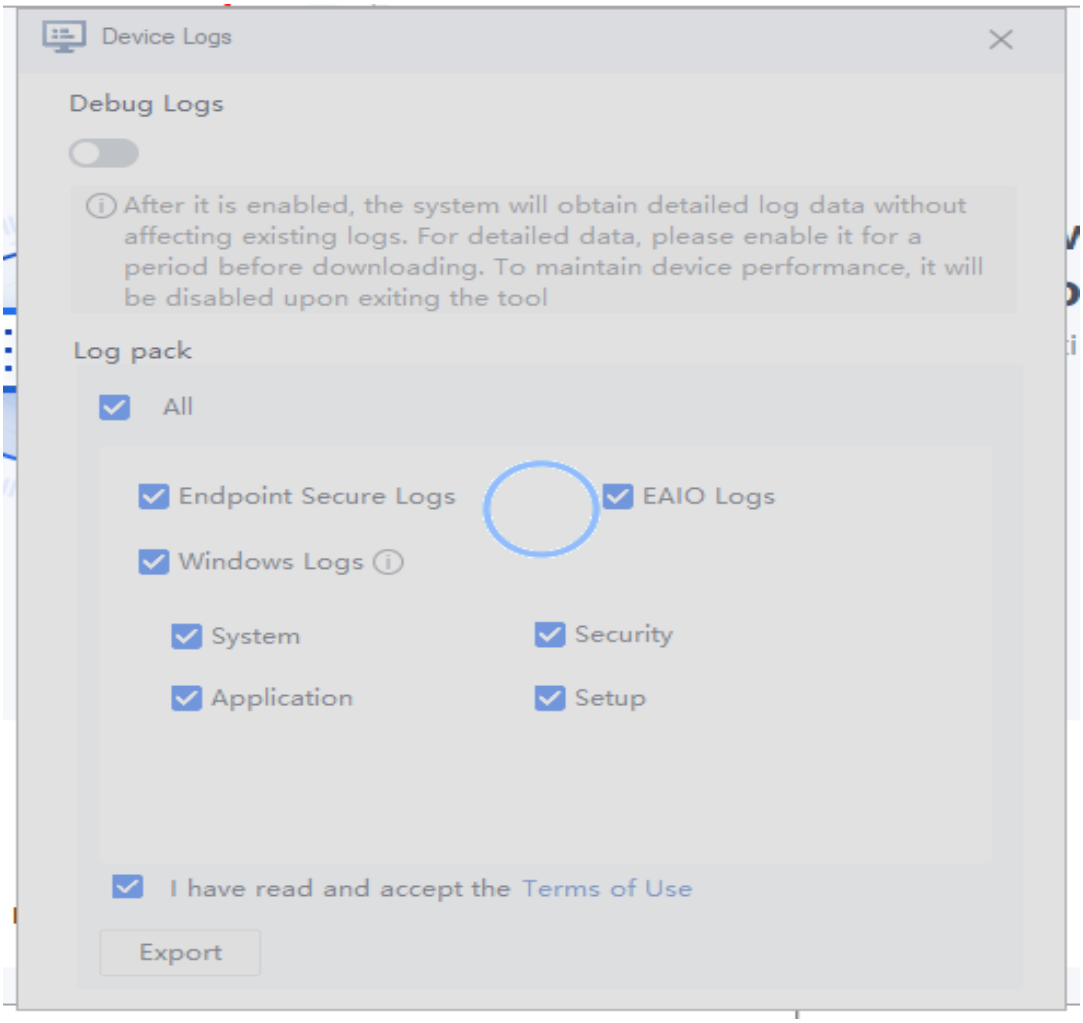
2. กดเลือก Log pack all แล้วกด Export



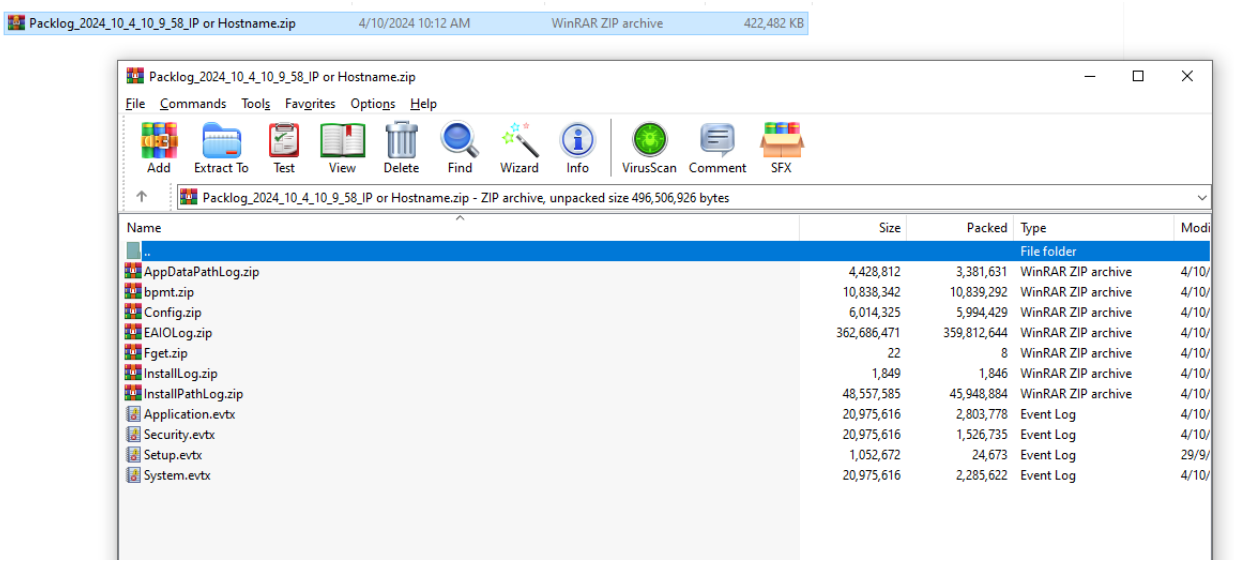
3. เพิ่มชื่อเครื่อง หรือ IP ในชื่อไฟล์ ZIP จากนั้นกด Save



4. รอระบบดำเนินการ

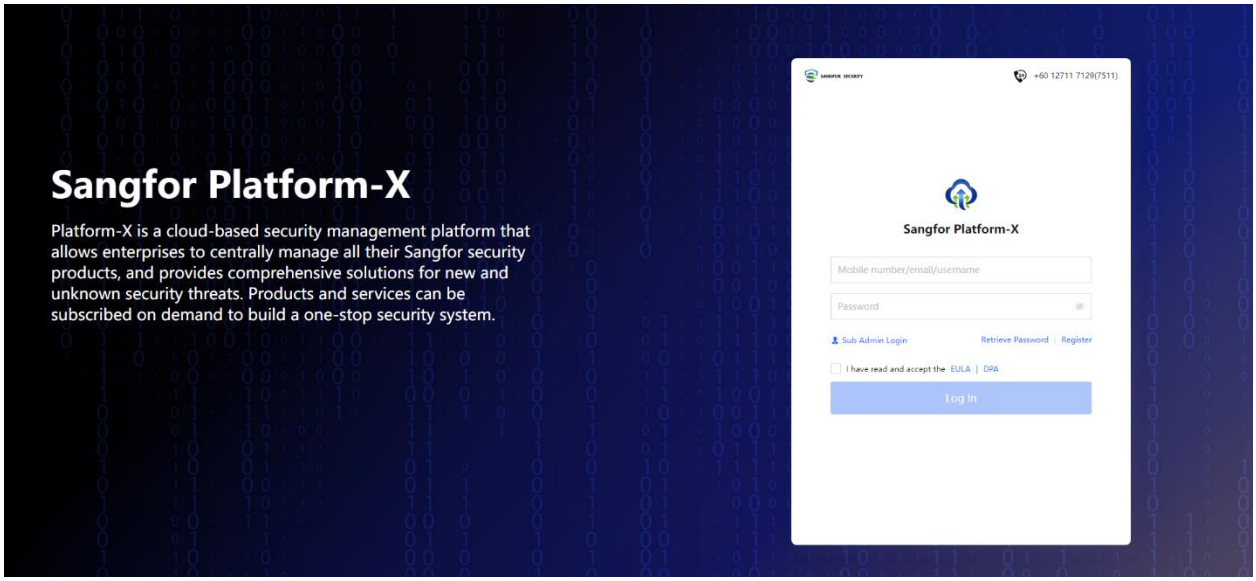


5. ตัวอย่างไฟล์ เพื่อนำส่งให้ Support โดยระบุวันเวลาที่พบปัญหา (ถ้ามี)



การควบคุมการเข้าถึง Endpoint Group ด้วย Account Sub Admin

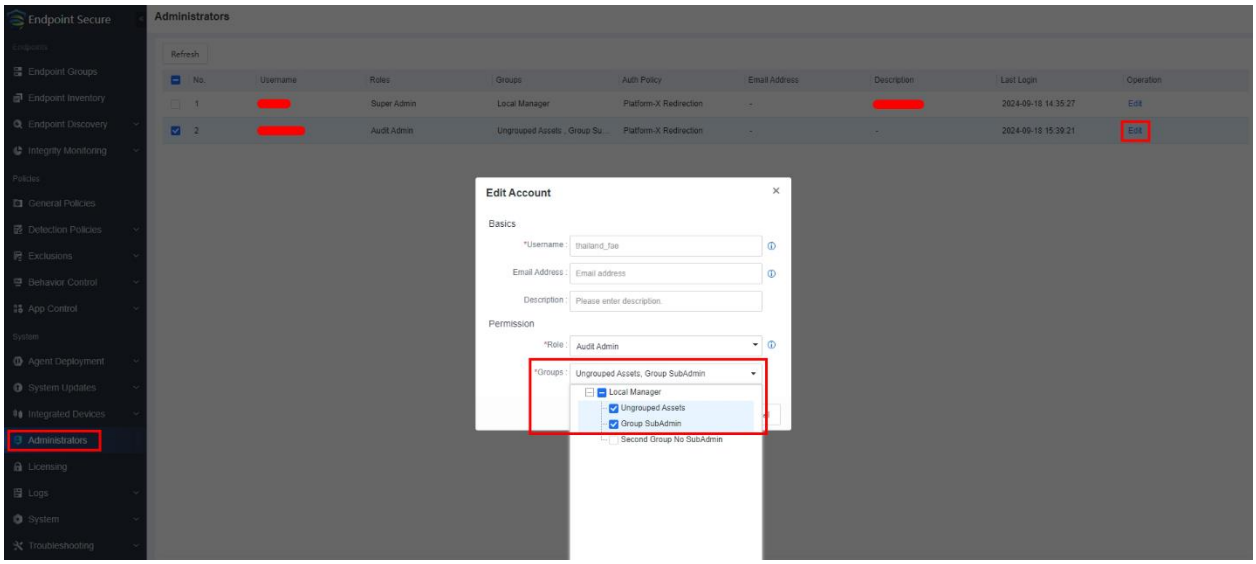
1. Login เข้า Platform-X ด้วย Account Admin

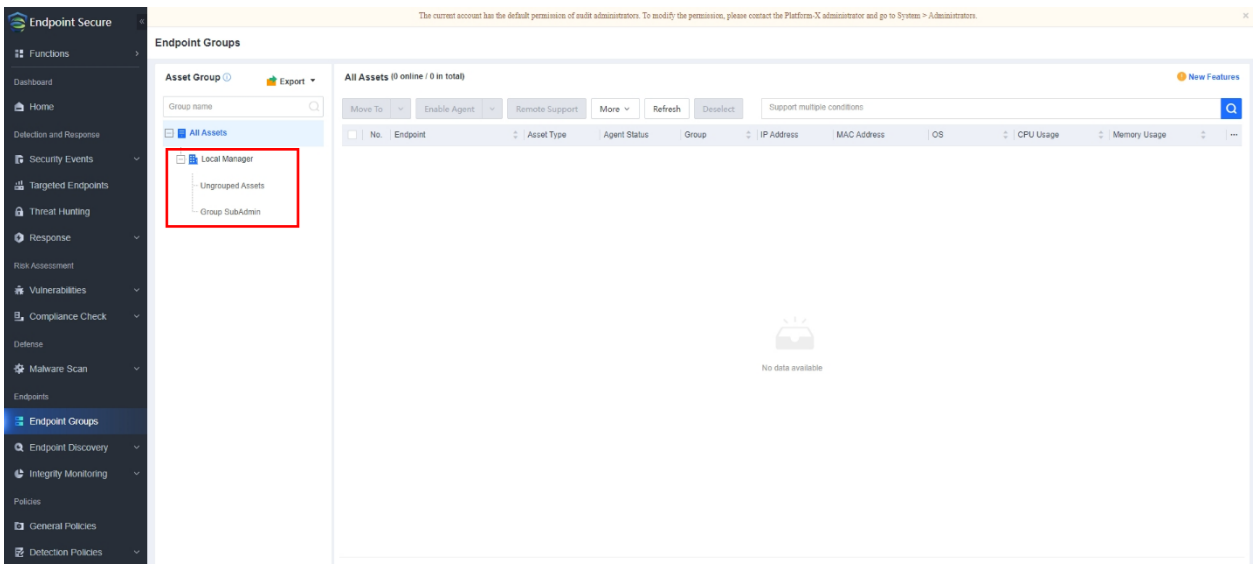


2. กด Visit เข้า Endpoint Secure

3. เข้าไปตั้งค่าที่ System > Administrator โดยต้องใช้สิทธิ์ Account Platform-X ที่เป็น Super Admin

4. Edit Sub-Admin Account ที่ต้องการ เลือก Group ที่ต้องการให้อยู่ในสิทธิ์ของ Sub Admin นั้น ๆ (โดยสามารถเลือกได้มากกว่า 1 Group)

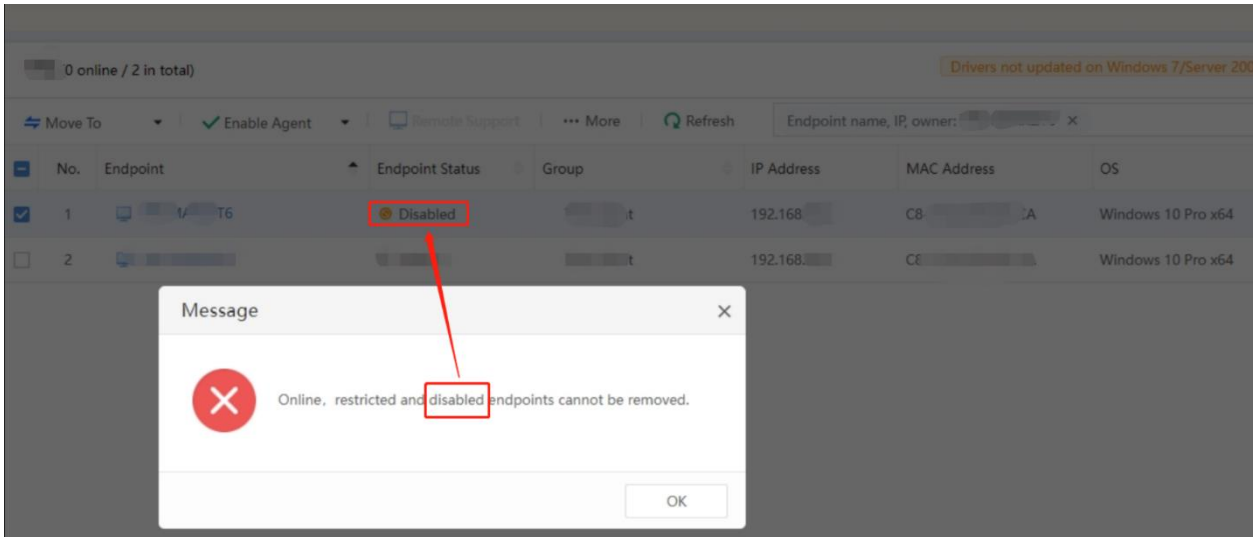




ไม่สามารถลบ Agent ที่เป็นสถานะ Disabled ได้

อาการ:

มีรายการ Agent ที่อยู่ในสถานะ Disabled ไม่สามารถกด Delete Agent ได้จากบน Manager



สาเหตุ:

เครื่องที่เป็นสถานะ Online, Restricted หรือ Disabled จะไม่สามารถกด Delete ออกได้

วิธีแก้ไข:

- จะต้องทำให้เป็น Offline, Uninstalled ก่อน โดยการ Enable Agent ขึ้นมา ทั้งนี้ Agent รายการดังกล่าวจะต้องมีตัวตนจริง และสามารถเชื่อมต่อไปที่ Manager ได้
- **หากเป็นเครื่องที่ต้องการลบ**ให้ติดต่อเปิดเคสเข้ามาที่ Support เพื่อดำเนินการลบAgent จาก Database ออก

โดยหากเป็นแบบ Manager แบบ On Cloud ต้องมีข้อมูลต่อไปนี้

1. Corp ID:
2. Hostname ที่ต้องการให้นำออก
3. Agent ID ที่ต้องการให้นำออก (การเช็ค Agent ID)
4. ภาพ Screenshot ว่าAgent อยู่ในสถานะ Disabled และ ลบไม่ได้

หากเป็น On Premise ให้แทน Corp ID ด้วย Gateway ID และ เปิดเคสเข้ามาที่ Support

ไม่สามารถแก้ไข Setting ที่ ES Agent ได้

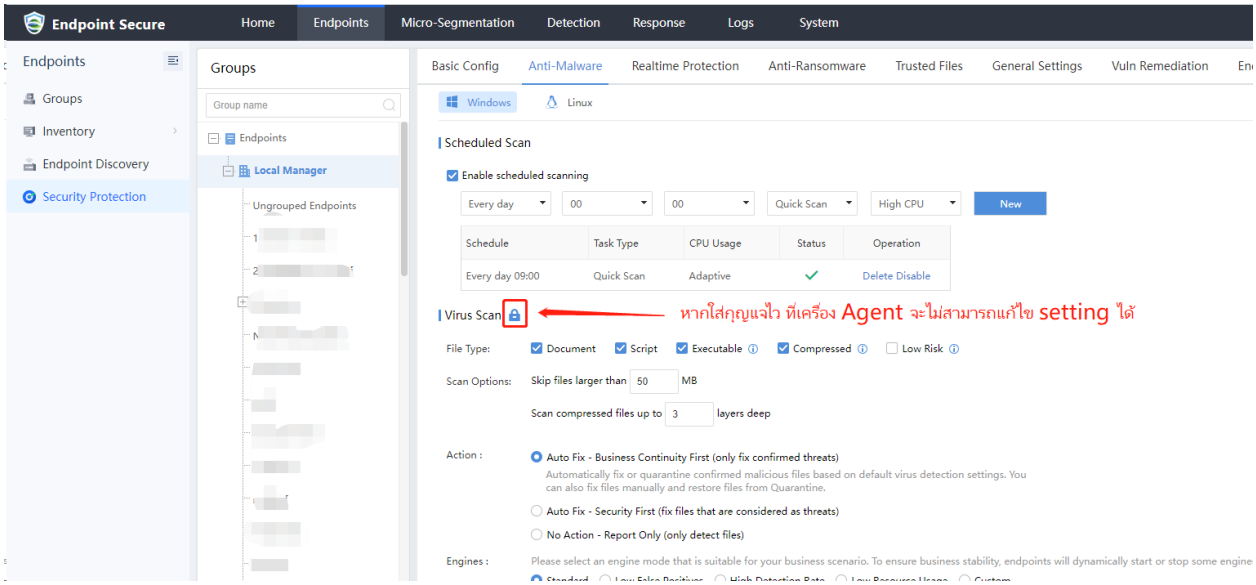
ภาพตัวอย่างอาการ:

Changes to some entries are prohibited by admin

วิธีแก้ไข:

1. ไปที่ Security Protection (หรือ General Policies) และหา module ที่ต้องการให้แก้ไข

2. กดที่แม่กุญแจเพื่อปลด Lock ให้ User สามารถแก้ไข Setting เองได้



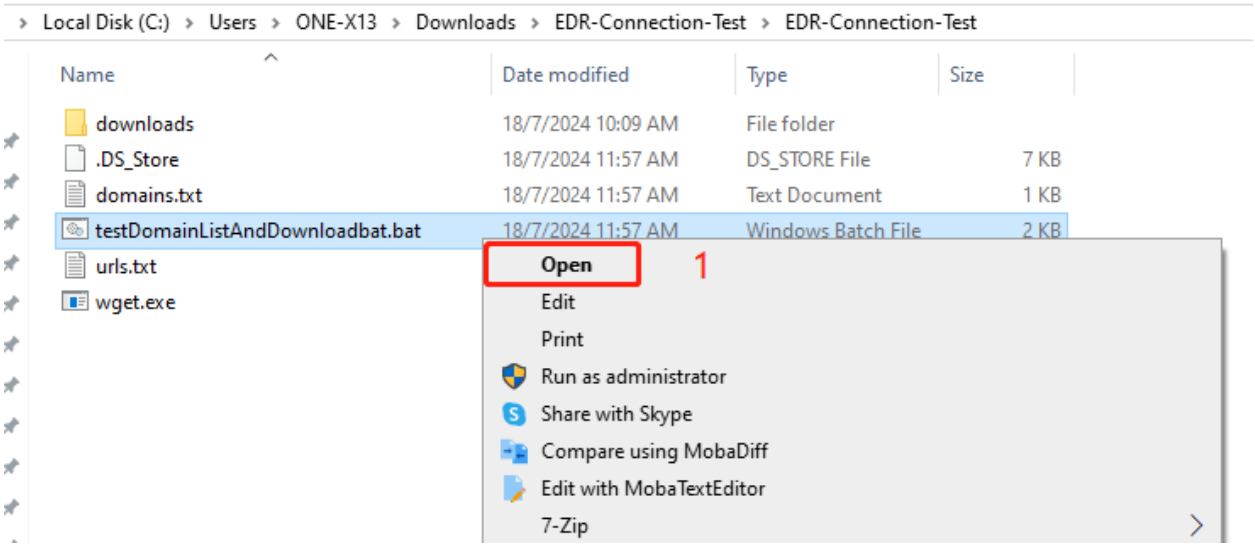
การตรวจสอบการเชื่อมต่อ SAAS Endpoint Secure

การเช็ค connection ระหว่าง Client EDR ไปที่ SaaS EDR Sangfor

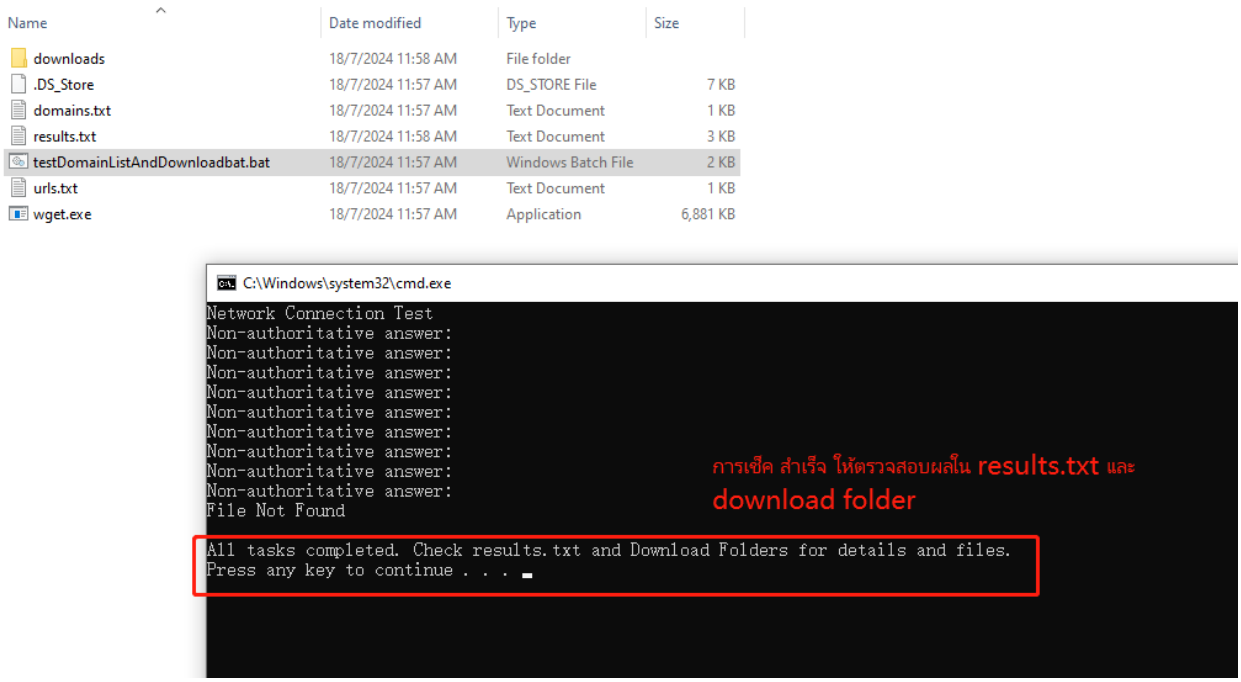
1. Download Script ในการทดสอบ

https://fs.vrc.demo.sangfor.co.th/index.php/s/ppHQ75RnqYKqszA

2. Run File testDomainListAndDownloadbat.bat

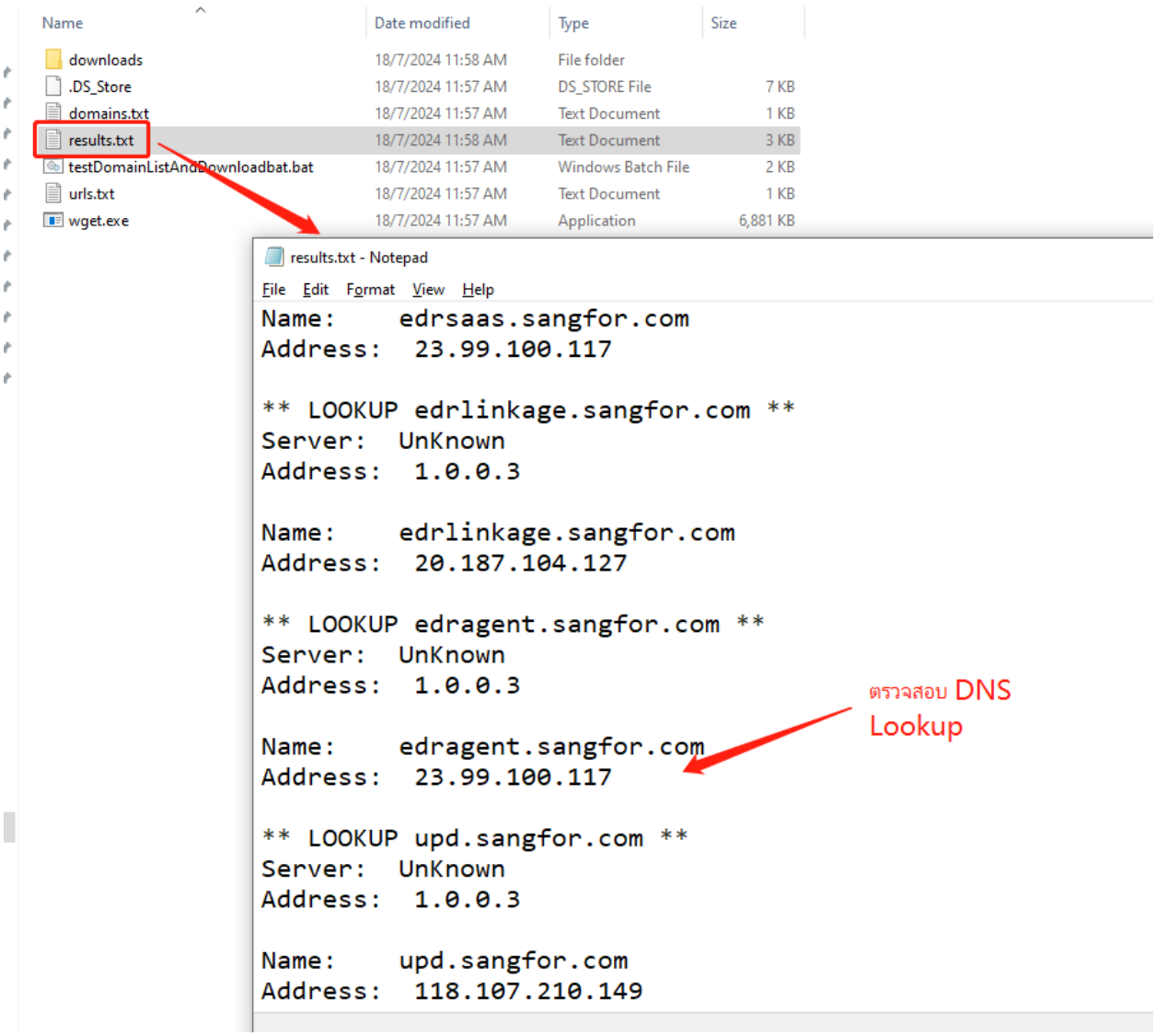


3. ตรวจสอบว่าการ Run สำเร็จ

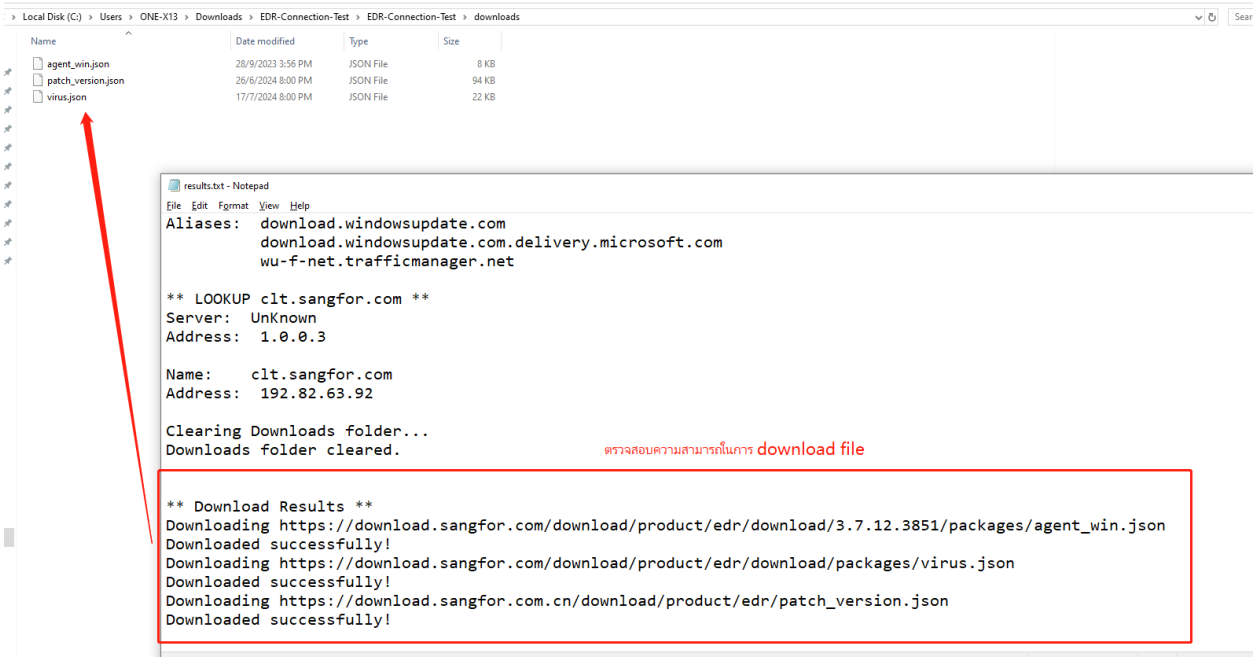


4. กดดูผลการทดสอบที่ results.txt

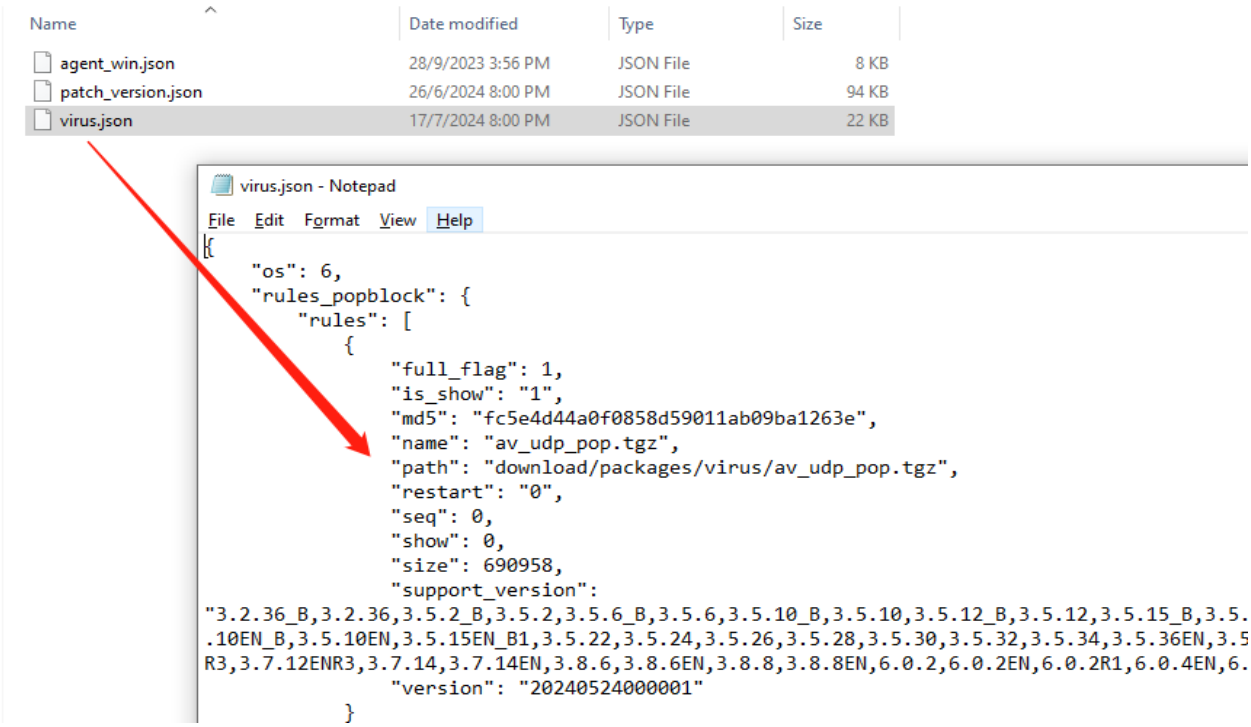
โดยจะมี 2 ส่วน คือ การ DNS Lookup และ การ download file



5. ตรวจสอบไฟล์ที่ Download มาว่าได้เนื้อความเป็น .json ปกติหรือไม่



เปิดไฟล์ .json ด้วย notepad



หากไม่สามารถ DNS Lookup ได้ให้ตรวจสอบที่ DNS Server ว่าสามารถ solve url ที่ต้องใช้ได้หรือไม่

หากติดที่การ download file ให้ตรวจสอบว่ามี Firewall หรือเครื่องมีความสามารถ Download File ได้หรือไม่ โดยที่ไม่ผ่าน Proxy

Uninstall Endpoint Secure ด้วย Agent Uninstaller

หมายเหตุ

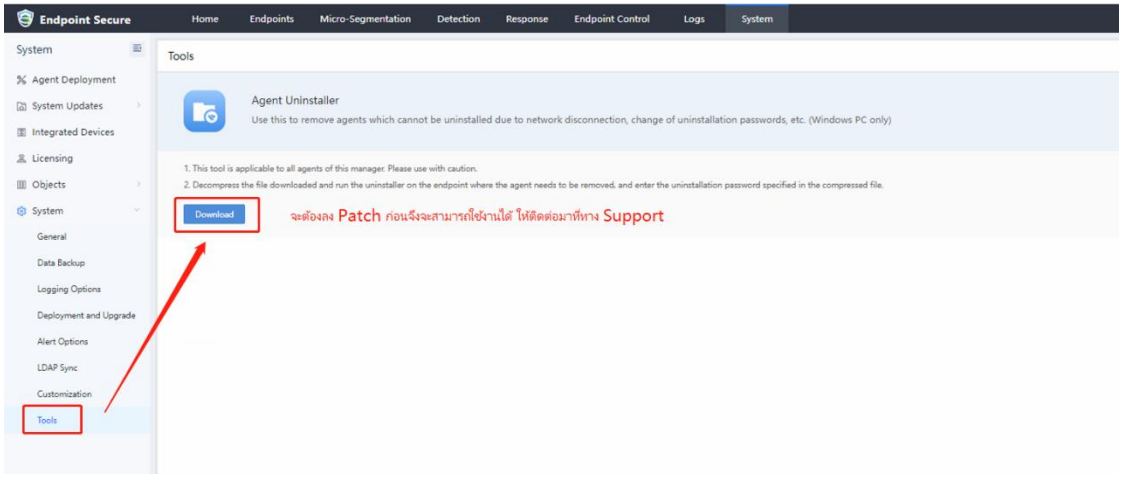
Tool นี้จะใช้งานได้เฉพาะกับ Agent ที่เคยชี้มาที่ Manager ตัวที่ Download Tool ออกมาเท่านั้น ไม่สามารถใช้ถอนเครื่องจาก Manager อื่นได้

การเตรียมก่อนใช้งาน

หากมีความประสงค์ในการใช้งาน Tool นี้ให้ติดต่อ Support เพื่อลง Patch เพื่อให้ใช้งานได้

ขั้นตอนการใช้งาน

1. Download Tool จากหน้า Manager หรือใช้ไฟล์ที่ทาง Support ส่งให้



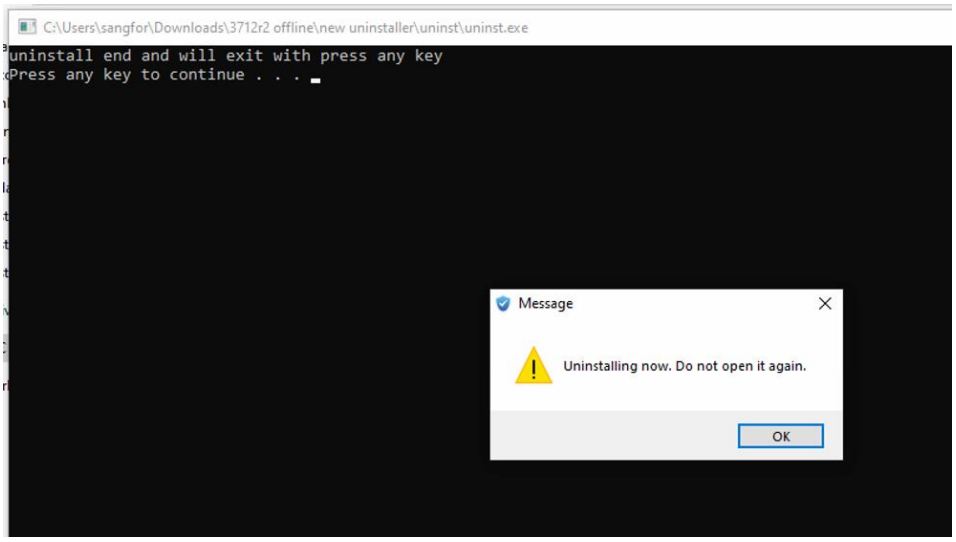
2. ตรวจสอบไฟล์ uninst.ini ว่ามี key3 แล้ว

เนื่องจากบาง Version มี Known Issue ที่จะไม่สามารถดึง Key 3 เพื่อให้ tool นำมาใช้งานได้

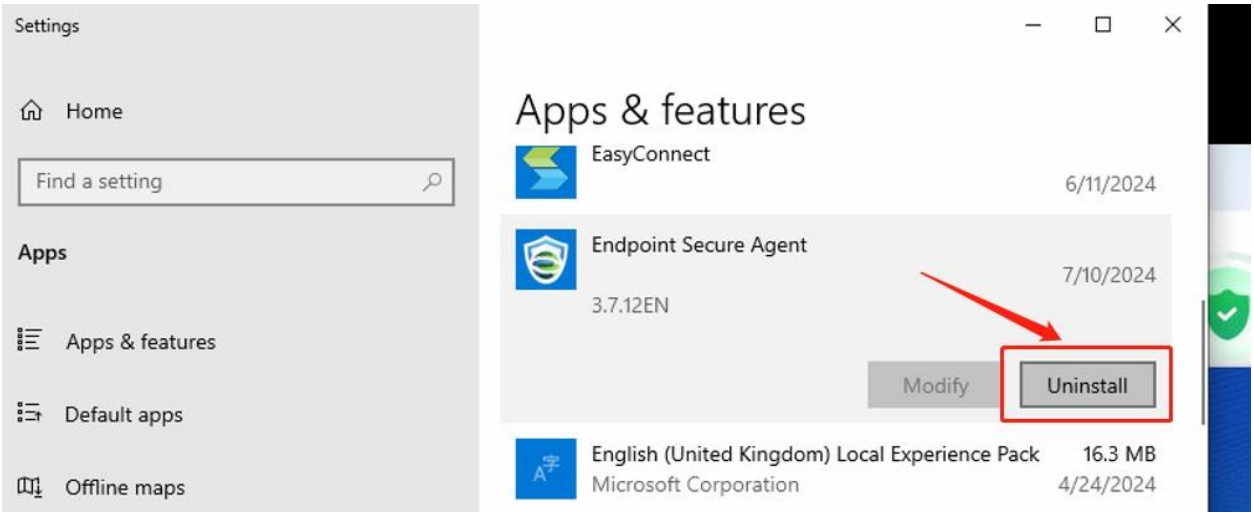
ให้ติดต่อ support เพื่อดำเนินการแก้ไขต่อไป

3. Run ตัว uninst.exe (ถ้า run ได้ถูกต้องขึ้น Messege ตามภาพด้านล่าง)

หากขึ้น error อื่นๆ อาจจะเพราะไฟล์ uninstall ไม่สมบูรณ์ หรือagent ไม่ได้อยู่ใน scope ของ Manager ที่ใช้งานปัจจุบัน)

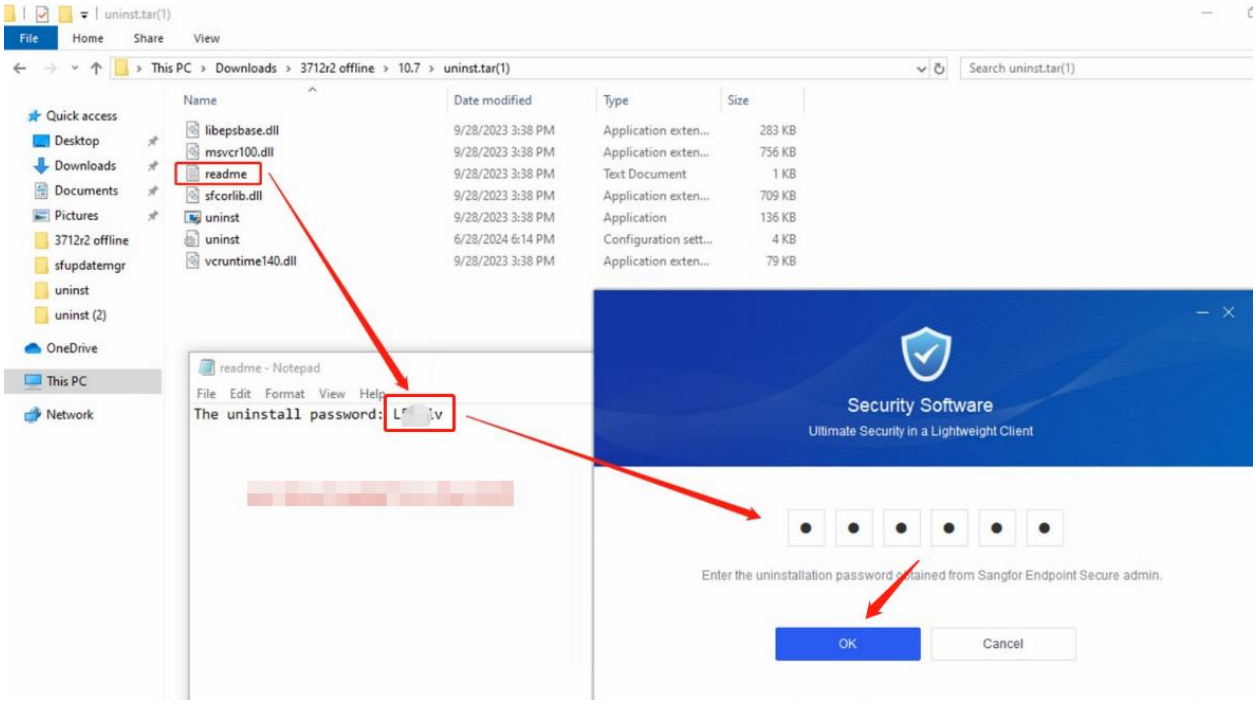


4. หากหน้า UI Uninstaller ไม่ปรากฏขึ้น ให้ทำการกด Uninstall จาก Windows ตามปกติ



5. หากมีขึ้นให้กรอก Password ให้เปิดไฟล์ readme และกรอก Uninstall Password ลงไป และกด OK

(การ Run uninstal.exe จะทำการ overwrite uninstall password เป็นข้อมูลชุดใหม่)



6. ระบบจะทำการถอนตัวเองได้ตามปกติ