ROYALTEC
Single Source For Your Needs
ROYALTEC INTERNATIONAL CO.,LTD.
350 Soi Ladprao 94, Ladprao Rd., Plubpla, Wangthonglang,
Bangkok 10310 Thailand. Tel : +66 2934 4790 Fax : +66 2539 4028
https://www.royaltec.com Email: info@royaltec.com

Cert No.SCUK002415Q

คู่มือการปฏิบัติงาน

ระบบสารสนเทศ

สารบัญ

เรื่อง หน้า

แนวทางการปฏิบัติงาน ในการตรวจสอบและแก้ไขปัญหาไวรัสคอมพิวเตอร์

1. ผู้ใช้งาน พบอาการผิดปกติ จากการใช้งานคอมพิวเตอร์ เช่น ข้อมูลหาย , Icon หน้าจอเปลี่ยน หรือคลิก Icon แล้วโปรแกรมไม่ทำงาน เป็นต้น

2. ผู้ใช้งาน แจ้งเจ้าหน้าที่สารสนเทศ ว่าพบปัญหาจากเครื่องคอมพิวเตอร์ อาการที่น่าสงสัย เช่น

2.1 เมื่อมีการ Boot ระบบแล้วระบบไม่สามารถ Boot ได้ตามปกติ มีข้อความเตือนเช่น "CMOS Check sum Error" (ข้อความเตือนนี้ สามารถเกิดได้จากเหตุอื่นด้วยเช่น Battery หมด)

2.2 เปิดเครื่องแล้วจอมืดเป็นเวลานาน (รีเซ็ตแล้วก็ไม่ทำงาน)

2.3 เมื่อมีการ Boot และเข้าสู่ระบบ ระหว่างที่รอวินโดว์ปรากฏข้อความที่ไม่คุ้นเคยปรากฏขึ้นมา

3. เจ้าหน้าที่สารสนเทศ จะดำเนินการตรวจสอบความผิดปกติตามที่ได้รับแจ้งจากผู้ใช้งาน (User) และดำเนินการกำจัดไวรัส โดยมีขั้นตอนการตรวจสอบ ดังนี้

3.1 ตรวจสอบ E-mail ทุกฉบับที่ส่งเข้ามา ว่ามาจากบุคคลที่รู้จักหรือไม่ ข้อมูลต้นทาง และปลายทางของ E-mail ถูกต้องมีหัวข้อเรื่องที่ติดต่อชัดเจน (หากไม่แน่ใจให้สงสัยไว้ก่อน)

3.2 หากมีไฟล์แนบมากับ e-mail จะต้องทำการ SCAN ตรวจหาไวรัสก่อนการใช้งานทุกครั้ง เอกสาร Word Excel อาจมีไวรัสประเภท Macro Virus แฝงมาได้

3.3 ไฟล์จำพวก .COM, .EXE, .ZIP หรืออื่นๆ อาจมีไวรัสประเภท Worm, Trojan หรืออื่นๆได้ ระวังไฟล์ Happyxxx.COM, .EXE, PICS4YOU.EXE หรืออื่นๆที่สงสัย

3.4 ตรวจสอบทุกครั้งเมื่อมีการนำเอาไฟล์ข้อมูลโปรแกรมต่างๆ จากเครื่องอื่น หรือแหล่งอื่นมาใช้งาน (การโหลดโปรแกรมจากอินเทอร์เน็ต, การแลกเปลี่ยนข้อมูลข้ามเครื่อง ข้ามฝ่าย)

3.6 Update Virus Definition อยู่เสมอ (ควรทำทุกสัปดาห์)

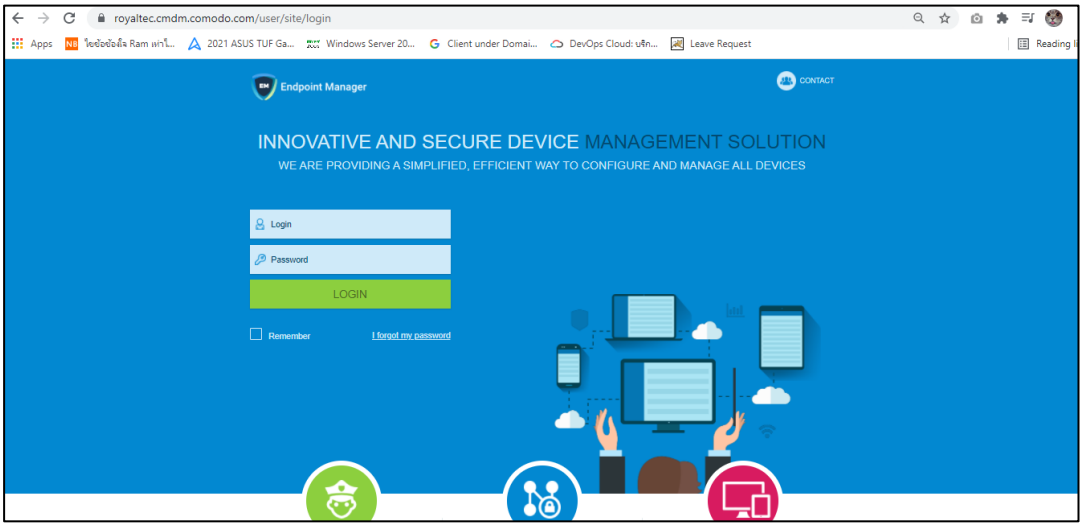
ขั้นตอนการปฏิบัติการ

เหตุการณ์	รายละเอียด
User แจ้งเหตุหรือตรวจพบภัยคุกคาม	จากการเฝ้าระวังตรวจสอบ Log จะช่วยให้ตรวจพบไวรัสคอมพิวเตอร์ก่อนที่จะสร้างเสียหายในวงกว้าง
ตรวจสอบภัยคุกคาม	ตรวจสอบถึงชนิดประเภท ความรุนแรงและ กระทบที่คาดว่าจะเกิดกับระบบ
การควบคุมภัยคุกคาม	ควบคุมไวรัส เพื่อบรรเทาความเสียหายที่เกิด ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลาม หรือ ขยายวงไปยังจุด อื่นๆ เช่น ปิดระบบ, ตัดการเชื่อมต่อ เป็น ต้น
ทำการแก้ไขปัญหา	แก้ไขหรือสามารถกำจัดภัยคุกคามได้ในเบื้องต้นให้ ทำการแก้ไขในทันที
เจ้าหน้าที่สารสนเทศแก้ไข	หากไม่สามารถแก้ไขได้ให้ติดต่อแผนกสารสนเทศ หรือบริษัท Partner เพื่อทำการแก้ไข หรือส่งซ่อม และเบิกเครื่องคอมพิวเตอร์สำรองไปใช้งาน
แก้ไขปัญหาสำเร็จและป้องกันไม่ให้เกิดความเสียหาย	เมื่อแก้ไขได้สำเร็จให้ตรวจหาช่องโหว่และ ทำการป้องกันเพื่อไม่ให้เกิดปัญหาในลักษณะเดิมซ้ำอีก
ทดสอบ	ตรวจสอบการใช้งานระบบว่าทำงานได้ปกติหรือมีข้อมูลสูญหายหรือไม่
กู้คืนระบบงานหรือ ข้อมูลที่สูญหายตามที่มีการ Backup ไว้	หากพบว่ามีความเสียหายให้กู้คืนข้อมูลหรือระบบตามที่มีการ Backup ไว้
ระบบสามารถใช้งานได้	ระบบอยู่ในสภาพการให้บริการตามปกติ
สรุปผลในการดำเนินการรับมือภัยคุกคามฯและจัดทำรายงาน	สรุปผลในการดำเนินงานรวมทั้ง แจ้งผลการดำเนินงานให้ผู้ที่เกี่ยวข้องรับทราบ และ บันทึกการดำเนินงาน

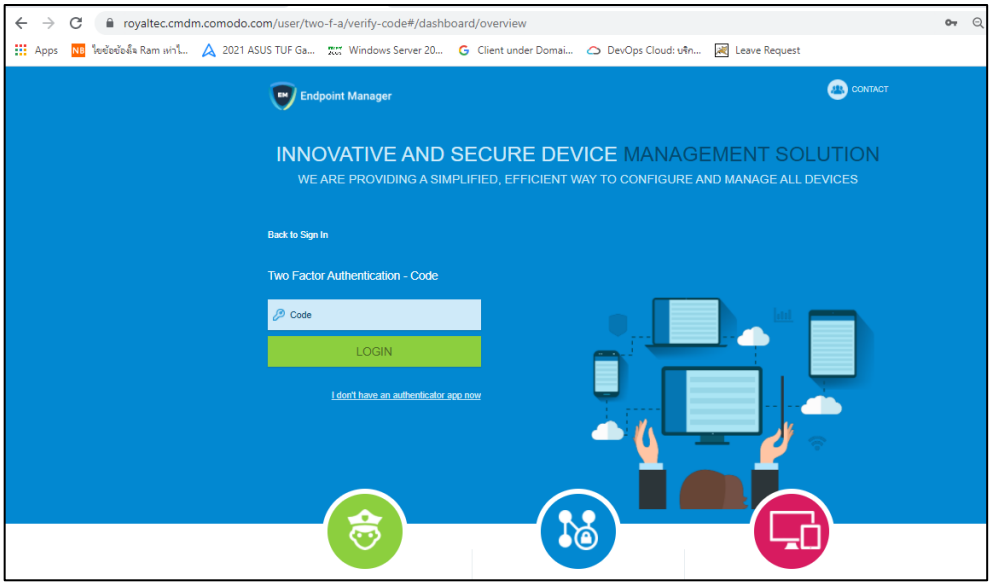
แนวทางการปฏิบัติงาน การตรวจเช็ค Antivirus Center

1. การเข้าตรวจเช็ค Antivirus Center สามารถล็อคอินได้ทั้ง Lan และ Internet เพราะ อยู่บน Cloud สามารถล็อคอินได้จากทุกที

วิธีเข้า ใช้งาน URL : https://royaltec.cmdm.comodo.com/user/site/login

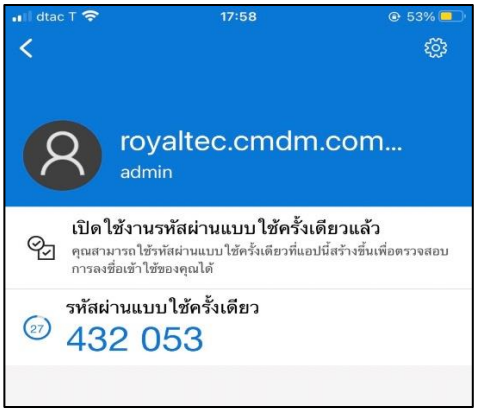


2. หลังจาก ล็อคอิน User password แล้ว ระบบจะถามหา Authentication – Code ต้องดาวโหลด app Authentication ก่อน

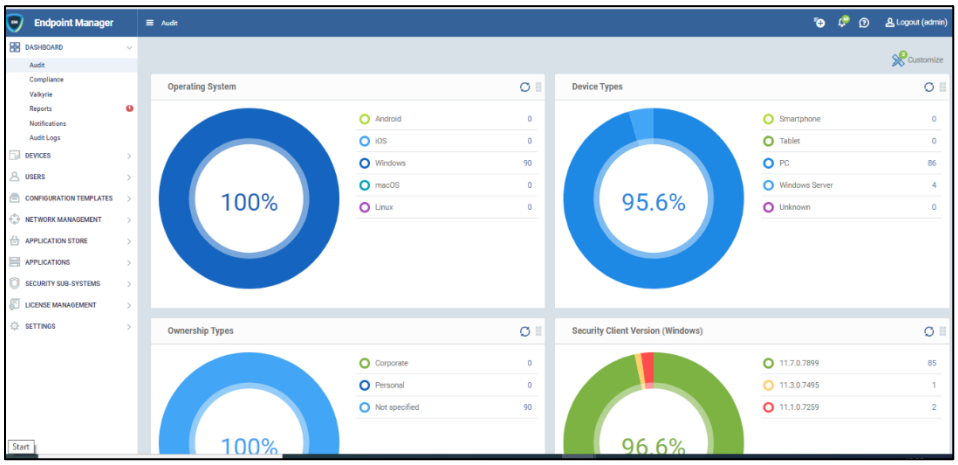


3. App Authentication - หลังจากลงทะเบียน App แล้วตัวโปรแกรมจะให้ทำการ Scan QR Code ของโปรแกรมที่จะให้มี Access เนื่องจาก Program Authentication จะมีการ Re Code ทุก 30 วินาที ทำให้มีความปลอดภัยป้องกันการ Hack User Pass

4. หลังจากลงทะเบียน App แล้ว ตัวโปรแกรมจะให้ทำการ Scan QR Code ของโปรแกรมที่จะให้มี Access เนื่องจาก Program Authentication จะมีการ Re Code ทุก 30 วินาที ทำให้มีความปลอดภัยป้องกันการ Hack User Pass



5. จะขึ้นหน้าจอการทำงานของ Antivirus Center

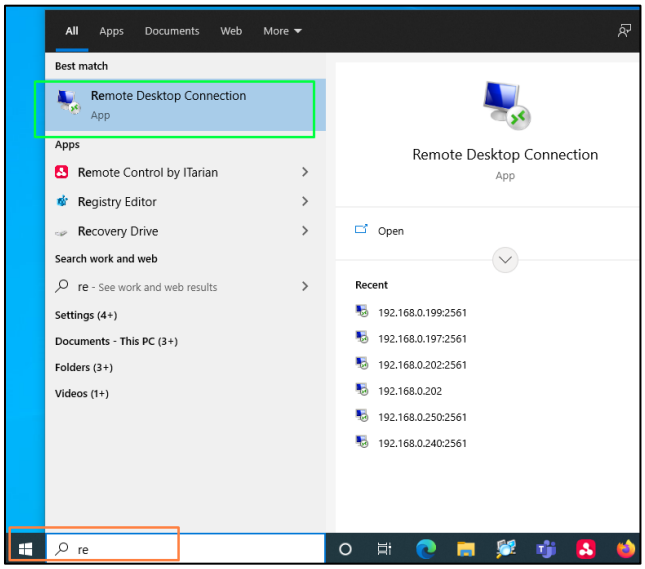


แนวทางการปฏิบัติงาน การตรวจเช็ค Server Main

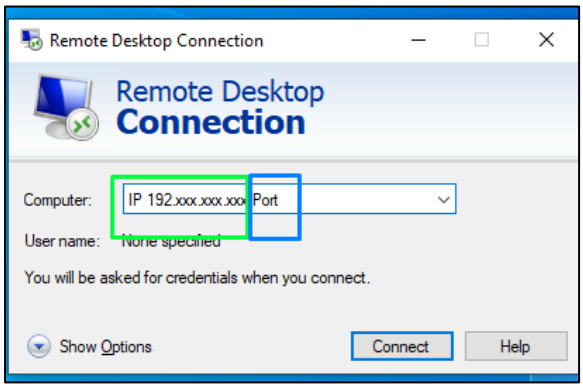
1. การตรวจเช็ค Server Main จะใช้ Program Remote Desktop

   ข้อควรระวัง : การ Remote ต้องตรวจสอบ เรื่อง port ที่ใช้ Remote Service Windows server Update ป้องกันการโดนเจาะข้อมูล

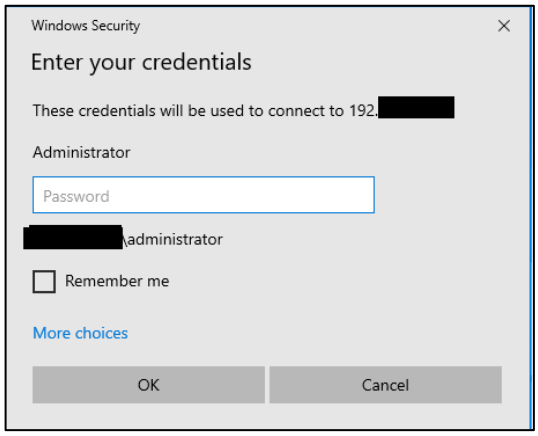
2. ไปที่ Start Windows -> RUN แล้วพิมพ์ข้อความในช่องว่าง (หากเป็น Windows ปัจจุบัน ดูจากรูปด้านล่าง คลิก แว่นขยาย ในการกรอบสีส้ม เมื่อพิมพ์ชื่อหรือ Subject ที่ใกล้เคียงกัน ระบบค้นหาจะดูโปรแกรมขึ้นมาให้เราเลือก เมื่อระบบดึงโปรแกรมขึ้นมาจะเห็นได้ในกรอบสีเขียว เป็นชื่อ Program Remote Desktop Connection ให้ทำการคลิก ที่ตัวโปรแกรมที่เราต้องใช้งาน



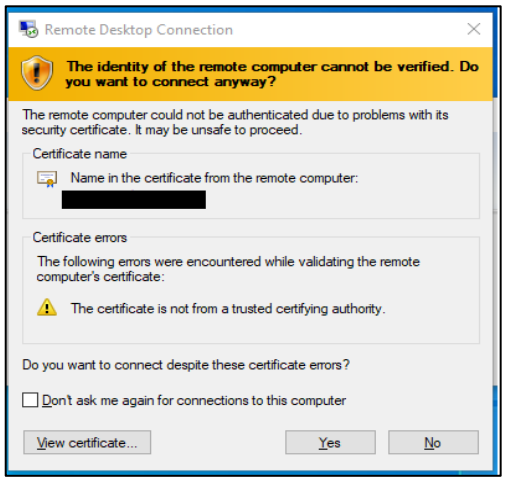
3. จากนั้นโปรแกรม Remote จะขึ้นป๊อบอัพ กรอบสีเขียว ให้เรา ใส่ ชื่อปลายทาง หรือ IP กรอบสีน้ำเงิน เป็นการระบุ Port การเชื่อมต่อ เมื่อเรารู้ IP , Port กด Connect ได้เลย



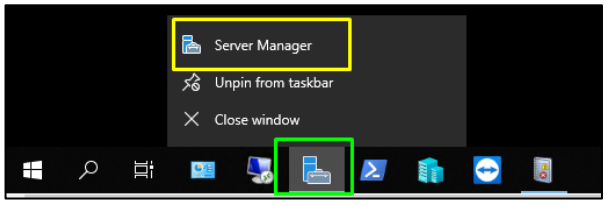
4. หลังจาก Connect แล้ว ขึ้นหน้าต่าง Login ทางระบบ แจ้งใส่ User Password



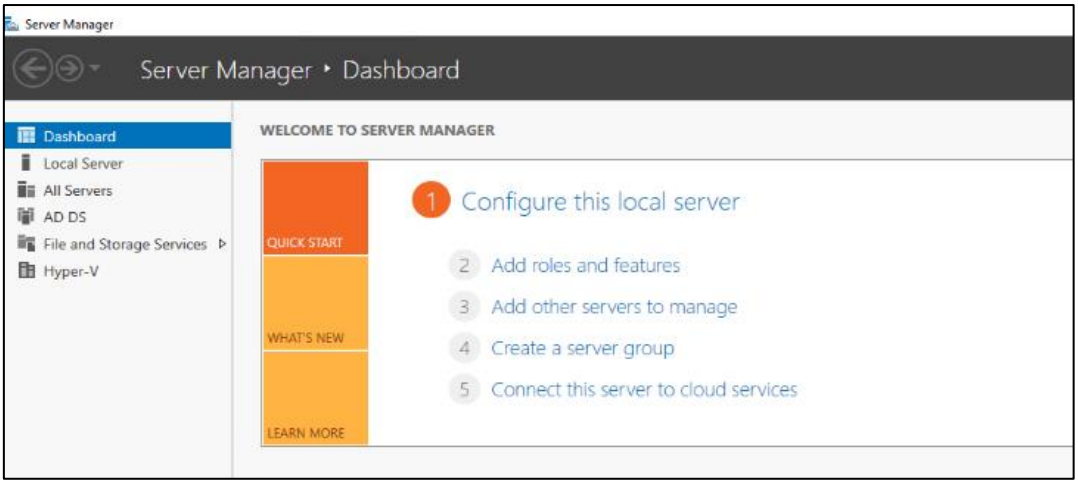
5. หลังจากใส่ User Password ถูก ระบบจะแจ้ง Certificate name เป็นชื่อเครื่องคอมพิวเตอร์ หรือ IP เครื่องที่เรากำลังรีโมทอยู่ ในส่วนนี้ให้คลิกที่ปุ่ม **Yes** (ปล. หากไม่ต้องการให้แสดงในครั้งถัดไป ให้ทำเครื่องหมายถูกที่ช่อง ☑ Don`t ask me again for Connection to this Computer)



6. ทำการ Login Server ด้วย Account (Admin) ไปที่ หน้าจอหลัก (Desktop) เช็คที่ ทาสก์บาร์ (Taskbar) จะ Icon ตามรูปด้านล่าง ของโปรแกรม Server Manager กรอบสีเขียว เป็น Icon (Server Manager) กรอบสีเหลือง ให้คลิกเข้าใช้งาน



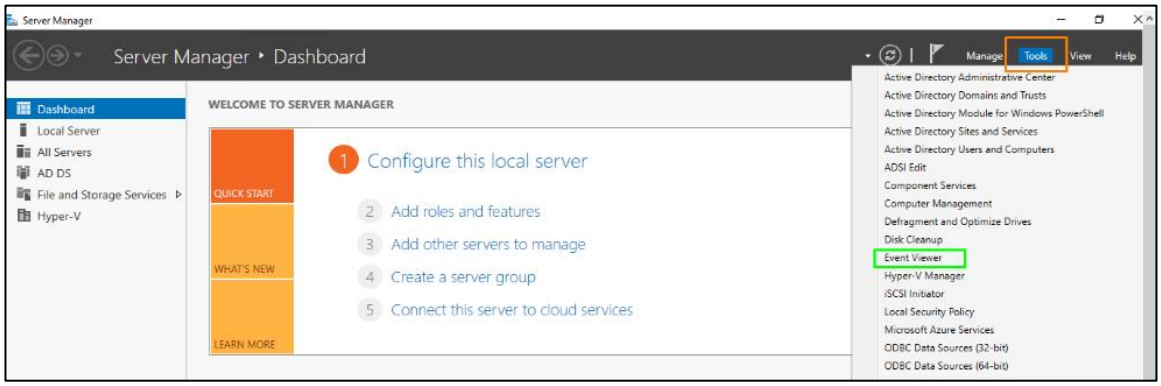
7. จะขึ้นหน้าจอ Server Manager



เป็นเครื่องมือที่ใช้ควบคุมงานทั้งหมดที่เซิร์ฟเวอร์ดำเนินการ เราสามารถทำอะไรกับตัวจัดการเซิร์ฟเวอร์หรือตัวจัดการเซิร์ฟเวอร์ใน Windows Server

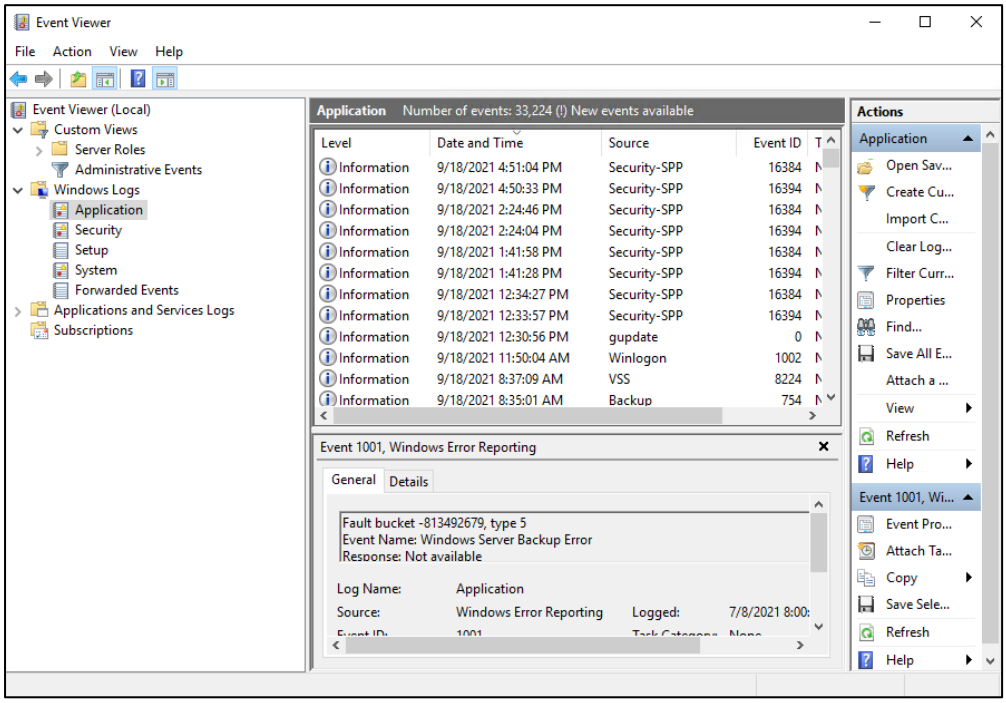
- วิเคราะห์และจัดการ บทบาทและคุณสมบัติที่ติดตั้งใน Windows Server
- เรียกใช้งานการดูแลระบบที่เกี่ยวข้องกับบริการที่ใช้งานบนเซิร์ฟเวอร์ เช่น การเริ่มหยุดหรือกำจัดบริการเหล่านี้
- วิเคราะห์พฤติกรรมของบทบาทและคุณสมบัติต่าง ๆ ของ Windows Server เพื่อให้การปฏิบัติที่ดีเป็นไปเพื่อประโยชน์สูงสุดของเซิร์ฟเวอร์
- ตรวจสอบสถานะการทำงานของเซิร์ฟเวอร์แบบเรียลไทม์
- เมื่อเปิด Server Manager ขึ้นมาแล้วไปแทบบาร์ด้านบนทางขวา

8. คลิก Tools เครื่องมือการจัดการจะเจอแถบบาร์



9. Windows Server บันทึก Log อยู่ 5 ประเภทดังนี้

1. Application คือ ล็อกไฟล์ที่เกิดขึ้นกับโปรแกรมที่ทำงานบน Windows และการเตือนหาข้อผิดพลาดอื่นๆ
2. Security คือ ล็อกไฟล์สำหรับการตั้งค่าเกี่ยวกับความปลอดภัย และการตั้งค่าบัญชีผู้ใช้คนอื่นๆ ที่ถูกบันทึกไว้
3. System จะบอกรายละเอียดของปัญหาระบบทั่วๆไป รวมถึงปัญหาที่เกิดขึ้นกับอุปกรณ์และการติดตั้งไดร์เวอร์ต่างๆ
4. Setup คือ ล็อกไฟล์ที่เกี่ยวกับการติดตั้งโปรแกรมก่อนหน้าที่จะเกิดปัญหาขึ้นมา
5. Forwarded events จะบอกถึงปัญหาที่เกิดจากเหตุการณ์ Remote ด้วยเครื่องคอมพิวเตอร์ระยะไกล เพื่อให้สามารถเข้ามาตั้งค่าเกี่ยวกับล็อกไฟล์และจะบันทึกเหตุการณ์ครั้งล่าสุดเก็บไว้ด้วย



10. วิธีการดู Log การเปิด Event Viewer แล้วทำตามขั้นตอนต่อไปนี้

- คลิกปุ่ม Start > Administrative Tools > Event Viewer
- ที่หน้าต่าง Event Viewer ให้คลิกเข้าไปที่หัวข้อ Windows Logs แล้วคลิกเลือกประเภทของ Log ที่ต้องการตรวจสอบ
- หากต้องการดูรายละเอียดต่างๆ ของ Log ให้ดับเบิ้ลคลิกที่รายการนั้นๆ

11. หัวข้อต่างๆ ของ Log จะบอกรายละเอียดและอธิบายถึงเหตุการณ์ต่างๆ ดังนี้

- Date : คือวันที่เกิดเหตุการณ์
- Time : คือเวลาที่เกิดเหตุการณ์
- Source : คือแหล่งที่มาของเหตุการณ์
- Category : คือประเภทของเหตุการณ์
- Type : คือชนิดของเหตุการณ์
- Event ID : คือหมายเลขประจำตัวของเหตุการณ์
- User : คือชื่อผู้ใช้ขณะเกิดเหตุการณ์
- Computer : คือชื่อเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์
- Description : คือรายละเอียดของเหตุการณ์

12. ประเภทของเหตุการณ์ (Level) Event Viewer แบ่งประเภทของเหตุการณ์ (Level) ได้เป็นหัวข้อดังนี้

- Information : เหตุการณ์ที่อธิบายการทำงานที่สำเร็จของงาน เช่น แอปพลิเคชัน ไดรเวอร์หรือเซอร์วิส ตัวอย่างเช่น บันทึกเหตุการณ์เมื่อ Server โหลดไดรเวอร์เครือข่ายสำเร็จ
- Warning : เหตุการณ์ที่ไม่สำคัญมาก อย่างไรก็ตาม อาจบอกถึงโอกาสในการเกิดของปัญหาในอนาคต ตัวอย่างเช่น แจ้งเตือนเมื่อพื้นที่ดิสก์ว่างเหลือน้อยลงมาก
- Error : เหตุการณ์ที่อธิบายปัญหาสำคัญ เช่น ความล้มเหลวของงานสำคัญ, เหตุการณ์ความผิดพลาดที่อาจเกี่ยวกับการสูญหายของข้อมูล หรือการสูญเสียฟังก์ชัน เช่น บันทึกเหตุการณ์ข้อผิดพลาดของเซอร์วิสที่ไม่สามารถโหลดเพื่อเริ่มต้นการทำงานได้
- Success Audit : บันทึกเหตุการณ์ของระบบรักษาความปลอดภัยที่ผ่านการตรวจสอบได้สำเร็จ ตัวอย่างเช่น เหตุการณ์เมื่อผู้ใช้ Log in เข้าสู่คอมพิวเตอร์หรือระบบ Domain ได้สำเร็จ
- Failure Audit : บันทึกเหตุการณ์ของระบบรักษาความปลอดภัยที่ไม่ผ่านการตรวจสอบ ตัวอย่างเช่น เมื่อผู้ใช้ไม่สามารถเข้าถึงแชร์ไดรฟ์ต่างๆ ในเครือข่ายได้

13. วิธีการค้นหา Log
    - ที่หน้าต่าง Event Viewer คลิกเลือกประเภทของ Log
    - ให้คลิกเลือกเมนู Action > Find
    - พิมพ์รายการของ Log ที่ต้องการค้นหาลงไป

14. วิธีการกรอง Log
    - ที่หน้าต่าง Event Viewer คลิกเลือกประเภทของ Log
    - ให้คลิกเลือกเมนู Action > Filter Current Log…
    - คลิกแท็บ Filter แล้วระบุข้อมูลที่ต้องการกรองลงไป

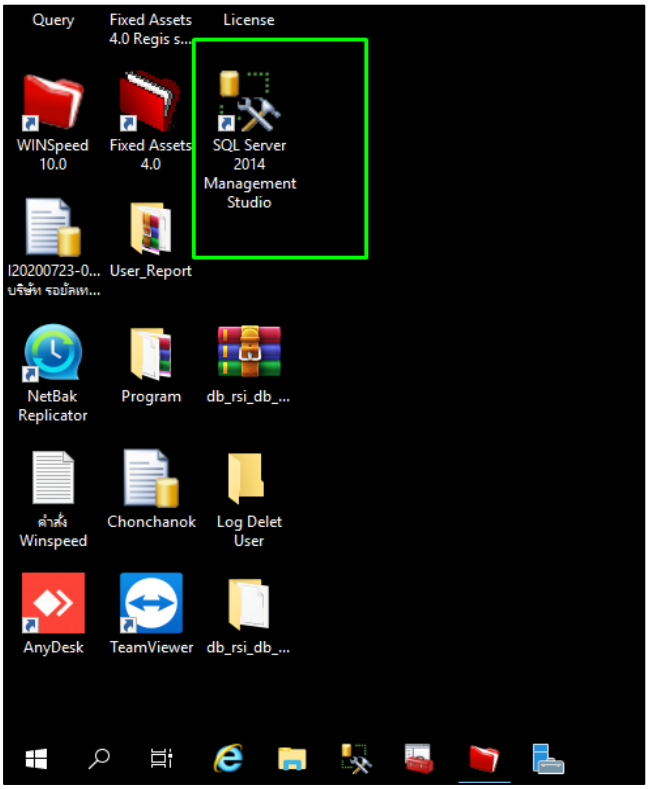
15. การบันทึกและกำหนดขนาดของ Log โดยค่าเริ่มต้น ขนาดสูงสุดของ Log จะได้รับการกำหนดเป็น 512 KB และเมื่อถูกใช้งานจนหมดแล้ว เหตุการณ์ใหม่ล่าสุดจะแทนที่เหตุการณ์เก่า เราสามารถเปลี่ยนแปลงแก้ไขค่าได้ โดยคลิกขวาที่ประเภทของ Log จากนั้นเลือกคำสั่ง Properties แล้วคลิกเลือกคำสั่งดังนี้
    - Maximum log size (KB) กำหนดขนาดของ Log Overwrite events as needed (oldest events first) สั่งบันทึกเหตุการณ์ใหม่ทับเหตุการณ์เก่า
    - Overwrite events as needed (oldest events first) สั่งบันทึกเหตุการณ์ใหม่ทับเหตุการณ์เก่า
    - Archive the log when full, do not overwrite events บันทึก Log ไว้ในพาธตามประเภทของ Log เช่น C:\windows\system32\winevt\logs\Security.evtx โดยไม่มีการบันทึกซ้ำของเก่า
    - Do not overwrite events ไม่ให้มีการบันทึกเหตุการณ์ซ้ำ ต้องสั่งเคลียร์ Log ด้วยตัวเองก่อน
    - และหากต้องการเซฟไฟล์ Log เก็บไว้ ให้คลิกขวาที่ประเภทของ Log นั้นๆ แล้วเลือกคำสั่ง Save All Event As
    - และถ้าต้องการเคลียร์บันทึกเหตุการณ์ทั้งหมด ให้คลิกขวาที่ประเภทของ Log นั้นๆ แล้วเลือกคำสั่ง Clear Log…

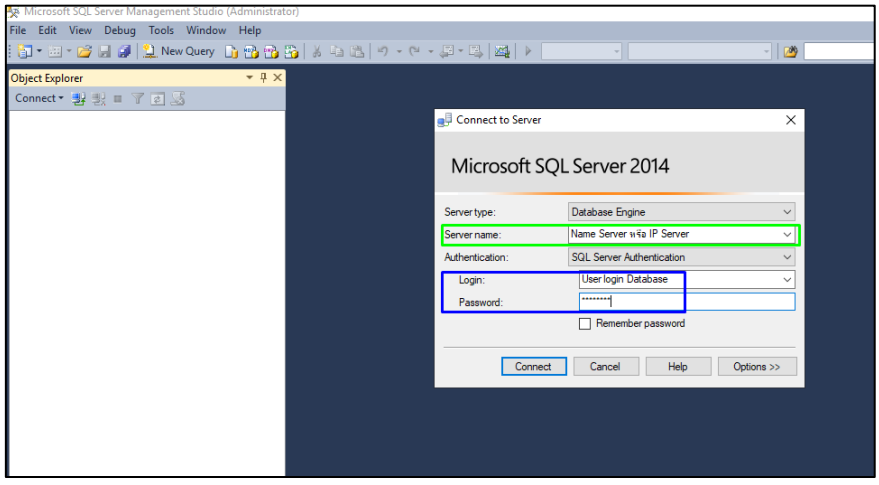
แนวทางการปฏิบัติงาน การตรวจเช็ค Server Winspeed

1. การตรวจเช็ค Server Winspeed จะใช้ Program Remote Desktop

   ข้อควรระวัง : การ Remote ต้องตรวจสอบ เรื่อง port ที่ใช้ Remote Service Windows server Update ป้องกันการโดนเจาะข้อมูล

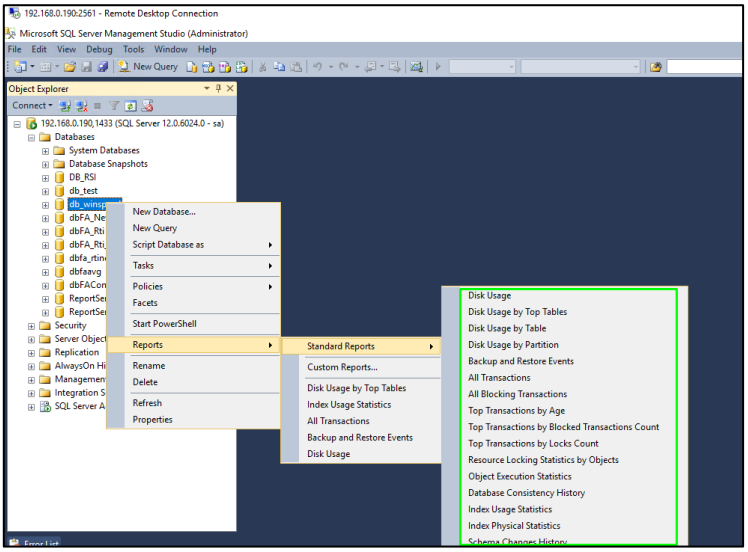
2. การตรวจเช็ค Database กลับมาที่หน้าจอหลัก Server Winspeed ให้คลิก Icon SQL Server 2014 ตามรูปด้านล่าง



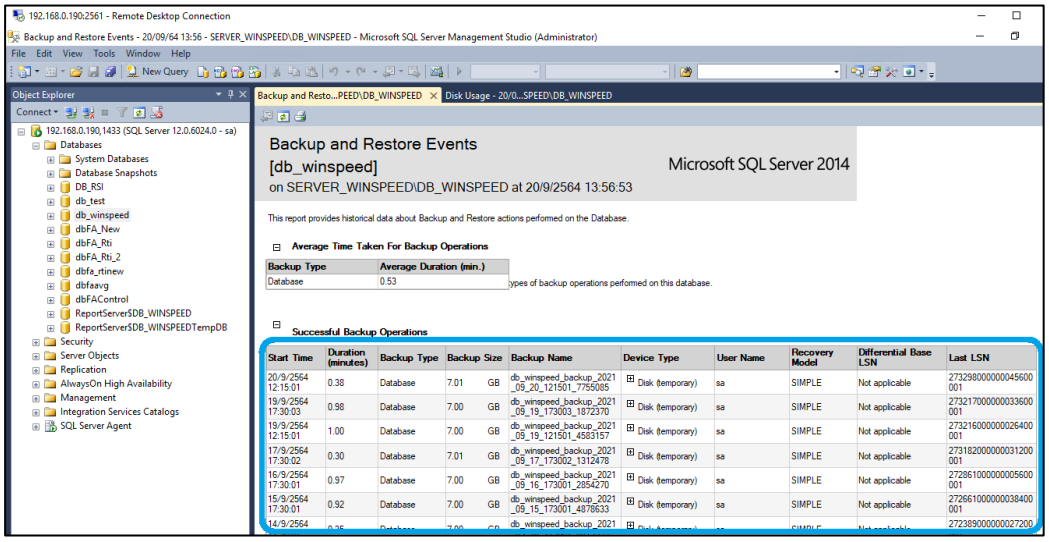


3. เลือก Database (DB) ที่ใช้งาน จากทาง Object Explorer -> คลิกขวาที่ DB

4. เลือก Report -> Standard Report (กรอบสีเขียว ตามรูปด้านล่าง) สามารถ เลือกดู Report แบบต่างๆ



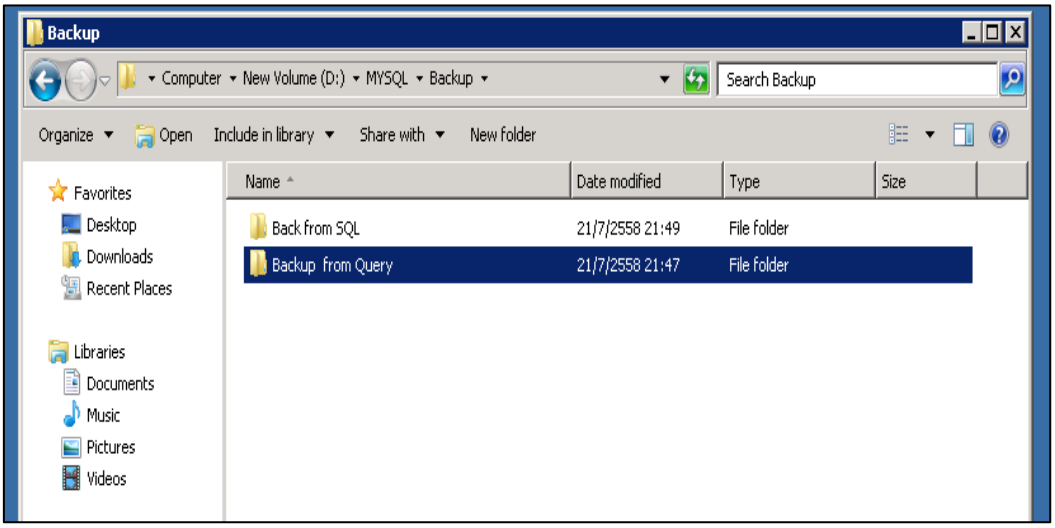
5. ตัวอย่าง การ Backup and Restore



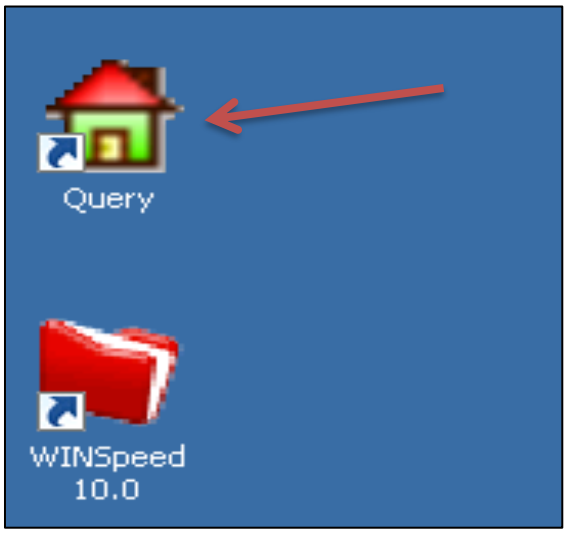
การ Backup Winspeed

การ Backup มีหลายแบบ แต่เลือกใช้ Winspeed ทำ Backup ด้วยตัวของโปรแกรมเอง แบบ Manual

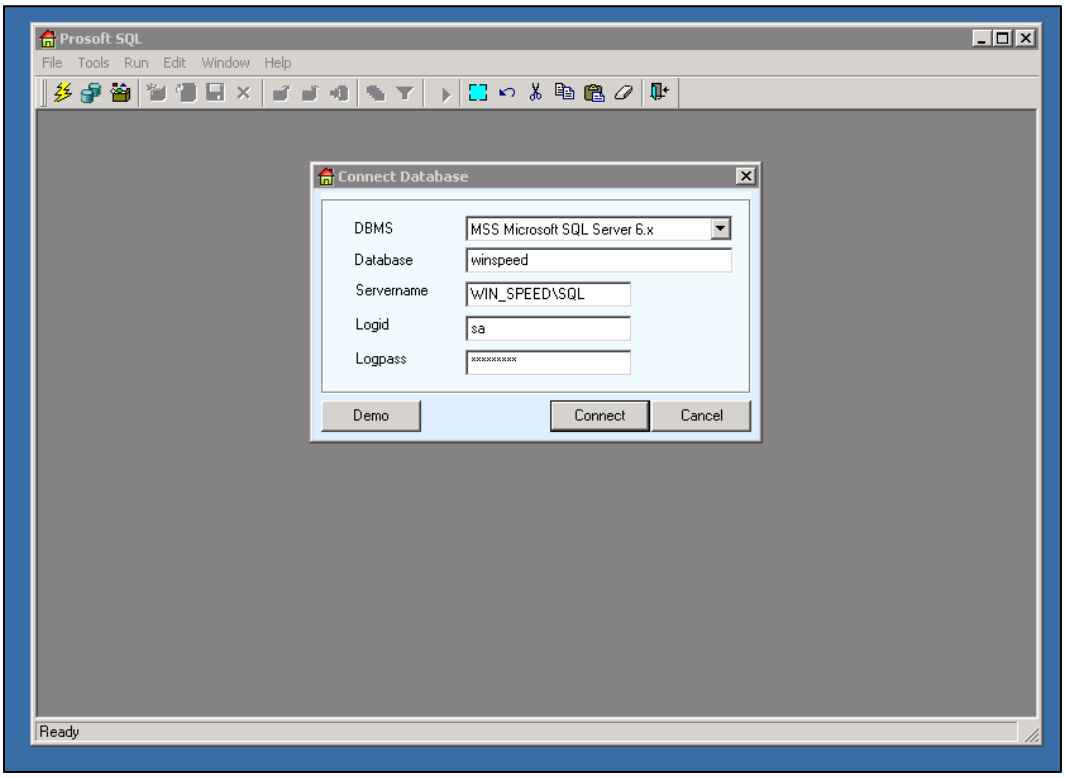
1. เริ่มสร้าง Folder ใช้สำหรับ Backup ในที่นี้ใช้ชื่อ Backup from Query เนื่องจากเป็น backup จากตัว Winspeed เอง



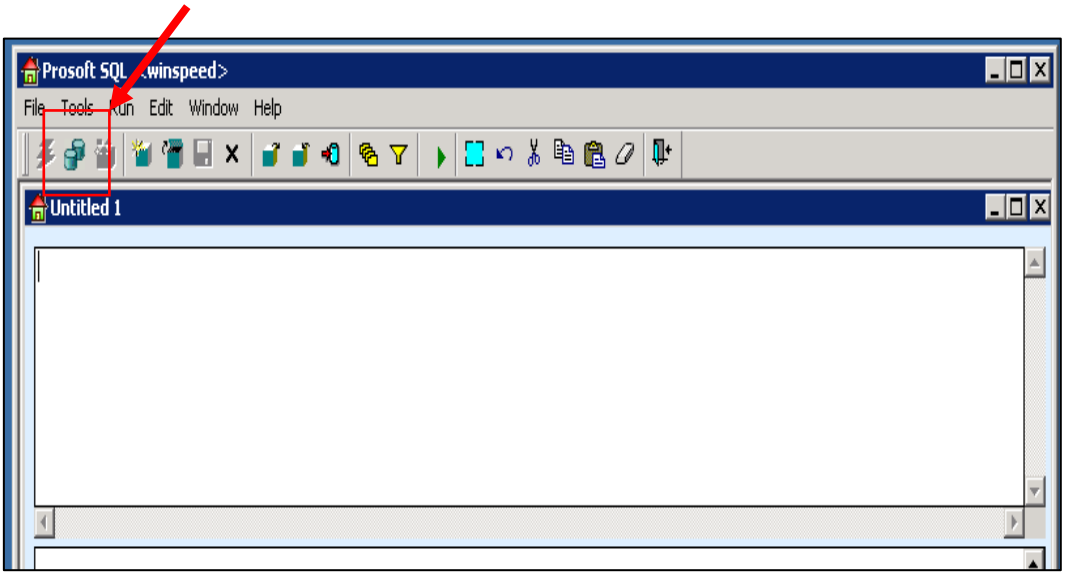
2. เริ่มต้น Backup ให้ไปที่เครื่อง Server (Winspeed) ในหน้า Desktop จะมี Icon ชื่อ Query ตามรูปด้านล่างแต่ถ้าไม่มีให้ไปที่ Start ->All Programs แล้วหา Folder ชื่อ Prosoft ให้คลิกซ้าย 1 ครั้ง จะพบ Sub ย่อย และไฟล์ Query



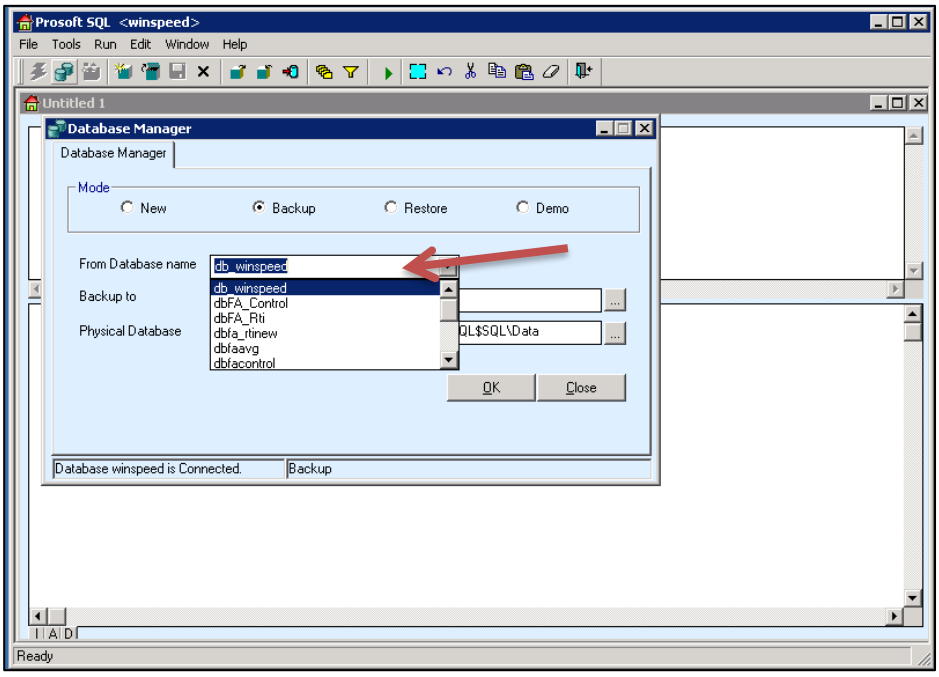
3. หลังจากนั้น จะขึ้นหน้าโปรแกรมตามรูปด้านล่าง ให้ใส่ข้อมูลของฐานข้อมูลที่ใช้งานอยู่ แล้วคลิก Connect



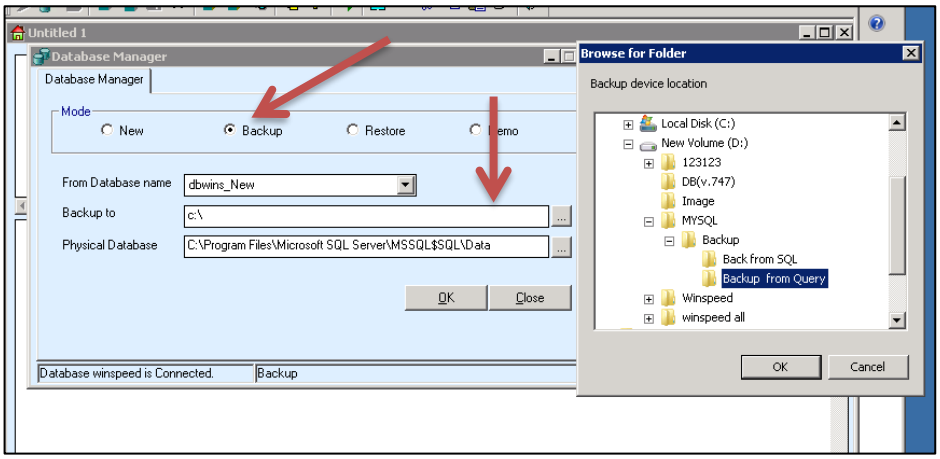
4. หลังจาก Connect เข้าฐานข้อมูลแล้ว ไปที่แทบเครื่องมือ คลิกรูปตามลูกศรที่ชี้ (กล่องสีเขียว 2 กล่องติดกัน = Database Manager)



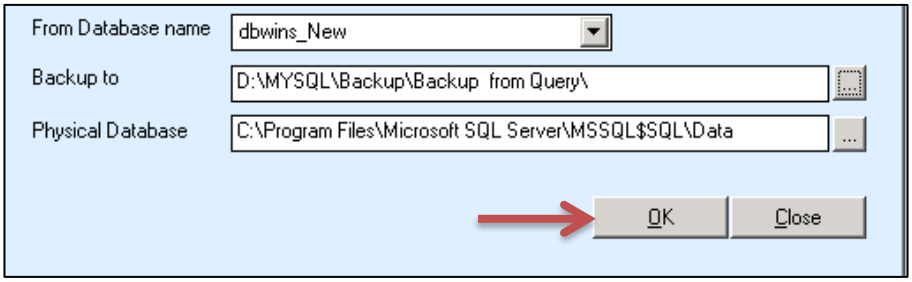
5. เมื่อคลิกจะเป็นหน้าต่าง (Database Manager) ตามรูปด้านล่าง ให้เลือก Backup แล้ว
6. Mode เลือก____(Backup)____
7. From Database name เลือก___(db_winspeed)___



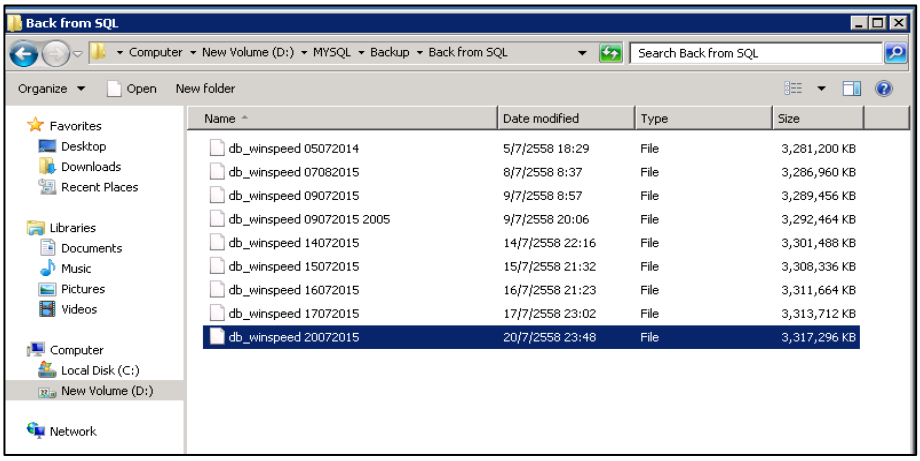
8. Backup to ให้ คลิก ตามรูป___(ปลายทางที่กำหนดให้เก็บ Backup)___



9. หลังจากกำหนดครบแล้วจะได้ข้อมูลตามด้านล่าง แล้วคลิก OK เป็นอันเสร็จสิ้น



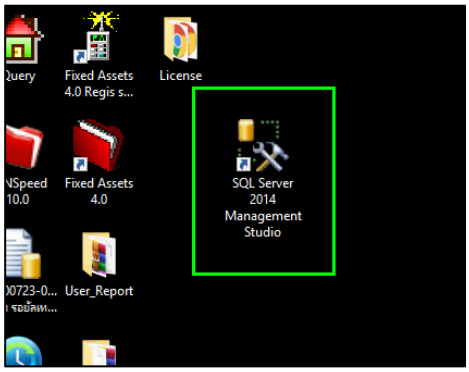
10. เลือกข้อมูลที่เก็บปลายทางที่กำหนดตามข้อ 6.1.8 สั่ง Backup การ Backup นั้นจะเร็วหรือช้าขึ้นอยู่กับขนาดของ Database (ในตัวอย่าง เป็นข้อมูลหลายปีซึ่งมีขนาดใหญ่ จึงใช้เวลา 5 -7 นาที)



แนวทางการปฏิบัติงาน การทำ Auto backup SQL

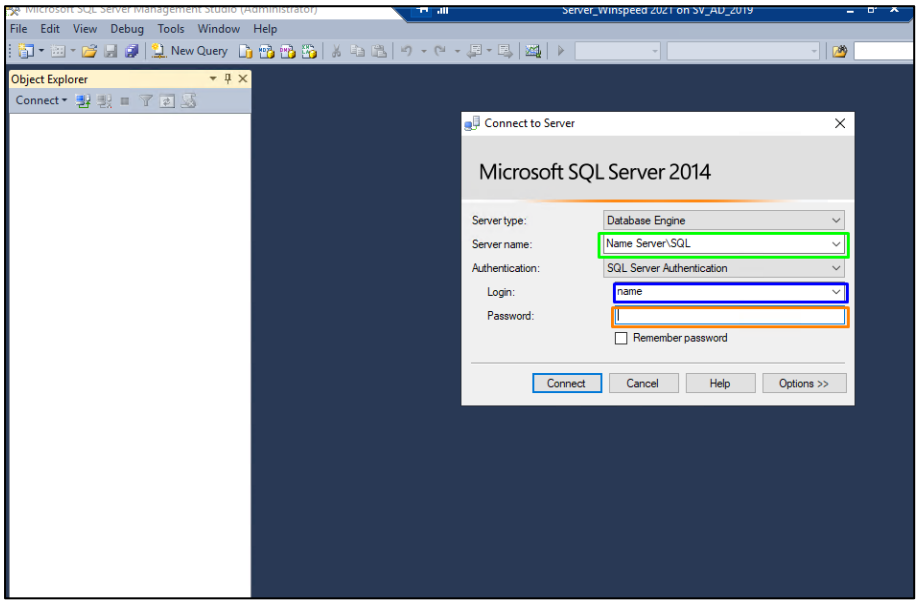
1. การทำ Auto backup เป็นการทำ Backup โดยที่ผู้ดูแลไม่ต้องทำการ Backup ด้วยตัวเองแต่เป็นการตั้งค่าที่ตัวโปรแกรม

2. ไปที่ Server Database ไปที่ Icon บนหน้าจอหลัก ชื่อว่า SQL Server 2014 ตามรูปด้านล่าง



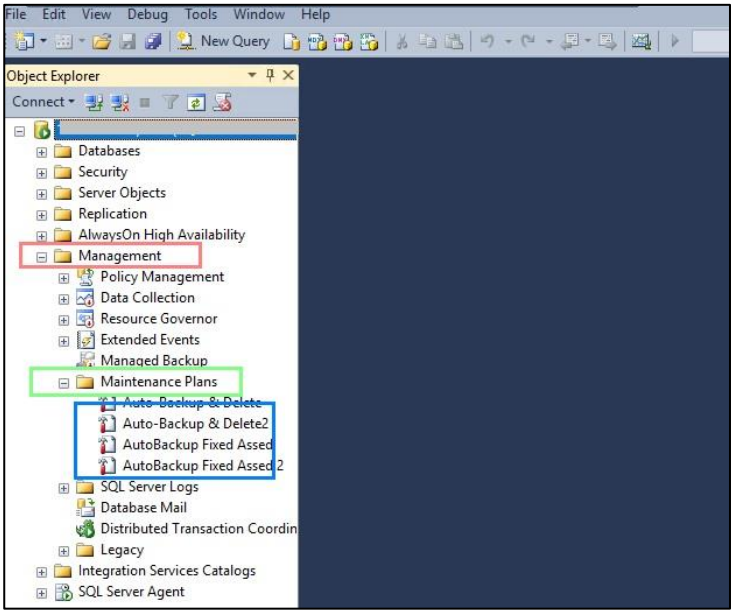
3. เมื่อเรารันโปรแกรมขึ้นมาทางตัวโปรแกรม จะให้เราใส่ค่าของการ ล็อคอินให้ถูกต้องตามรูป

- กรอบสีเขียว Server Name = ชื่อ Server ที่เราตัดตั้งตัว Database เอาไว้
- กรอบสีน้ำเงิน Login = ถูกสร้างเมื่อตอนกำหนด Database ครั้งแรก
- กรอบสีส้ม Password = แบบเดียวกับ Login

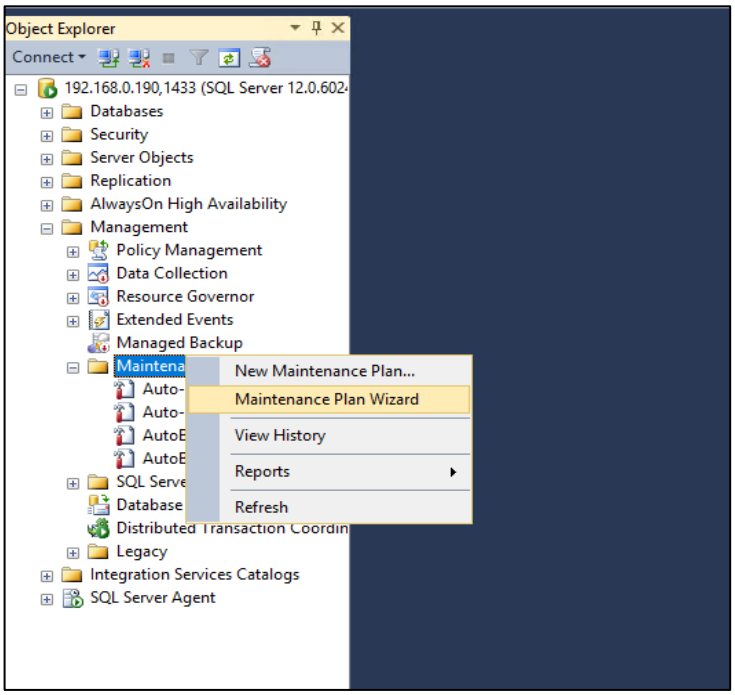


4. เมื่อ Login ผ่านแล้วจะเข้ามาที่หน้าโปรแกรม SQL Server ทางซ้ายมือ คือ Profile Database

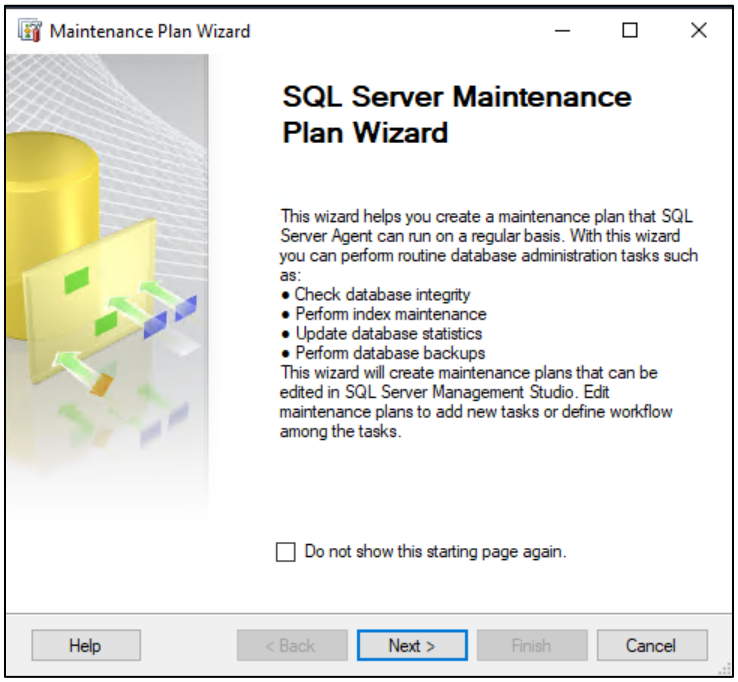
   - ของเราไปที่ Management > Maintenance Plan > Maintenance plan wizard >
   - กรอบสีน้ำเงิน คือ ไฟล์ Auto Backup ที่สร้างไว้แล้ว



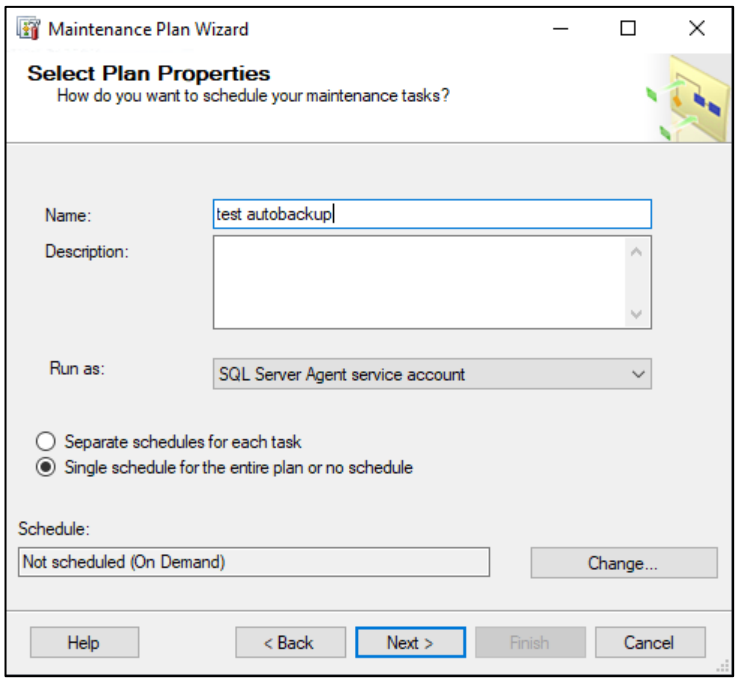
5. เริ่มด้วยการสร้าง Plan Backup คลิกไปที่ Maintenance Plan → Maintenance Plan Wizard



6. หน้าแรกของการสร้าง Maintenance Plan Wizard กด Next



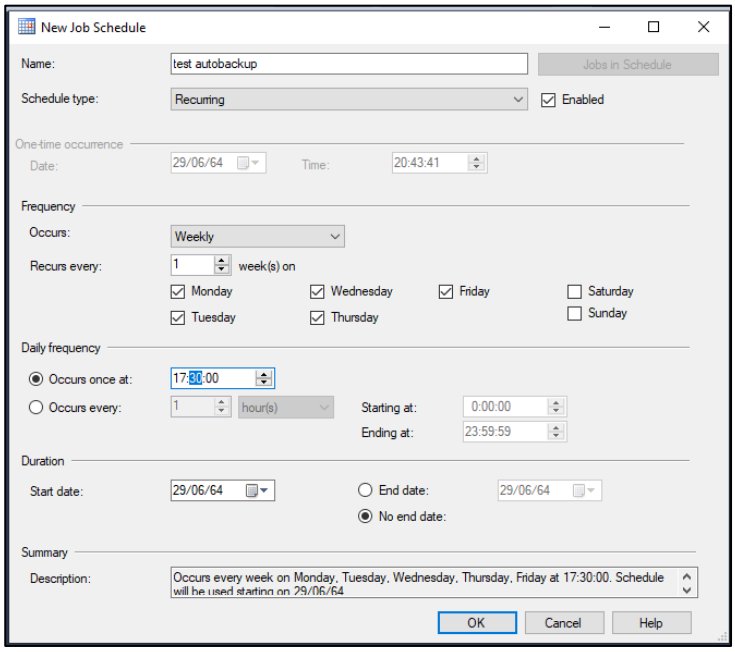
7. Plan Properties ค่าชื่อ ตามรูป ยกตัวอย่าง ใช้ test auto backup ให้เลือก Chang (เป็นการตั้งค่า)



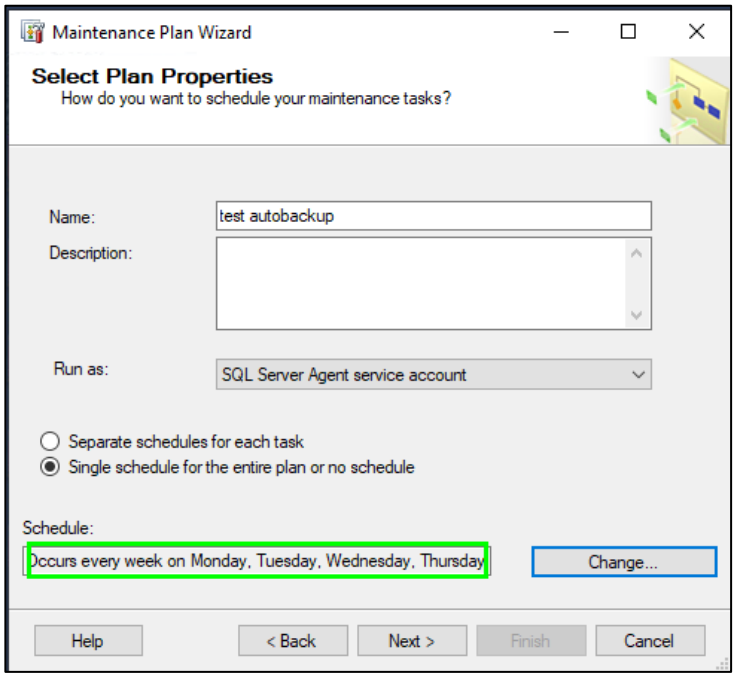
8. การตั้งค่า New Job Schedule

- Frequency การกำหนดความถี่ในการทำ Backup มากน้อยแค่ไหน ใช้ตั้งค่าแบบรายสัปดาห์ เลือก วันจันทร์ ถึง วันศุกร์

- Daily frequency กำหนดช่วงเวลาต่อครั้ง กด OK

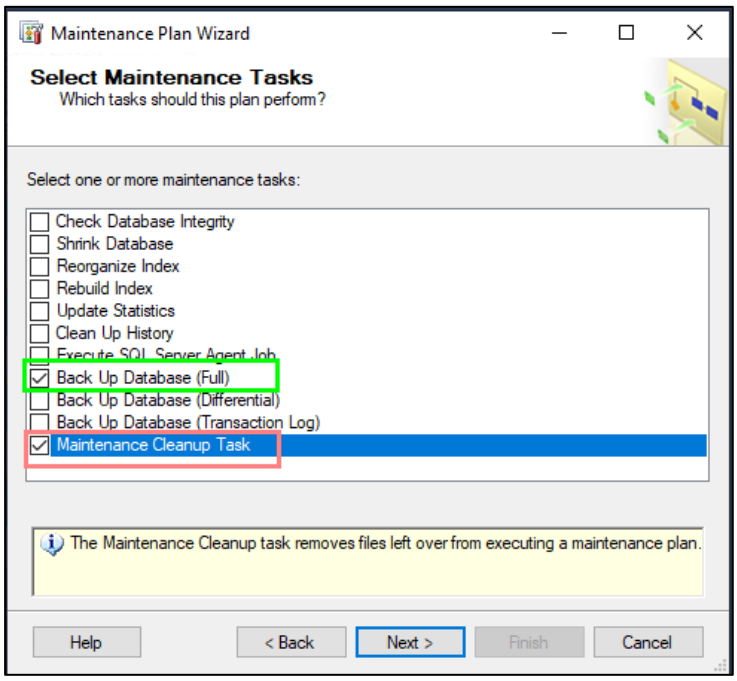


9. จากหน้าที่แล้ว หลังจากกด OK จะกลับมาหน้า Wizard Plan ในกรอบสีเขียว จะมีค่าที่ตั้งไว้ขึ้นมา กด OK

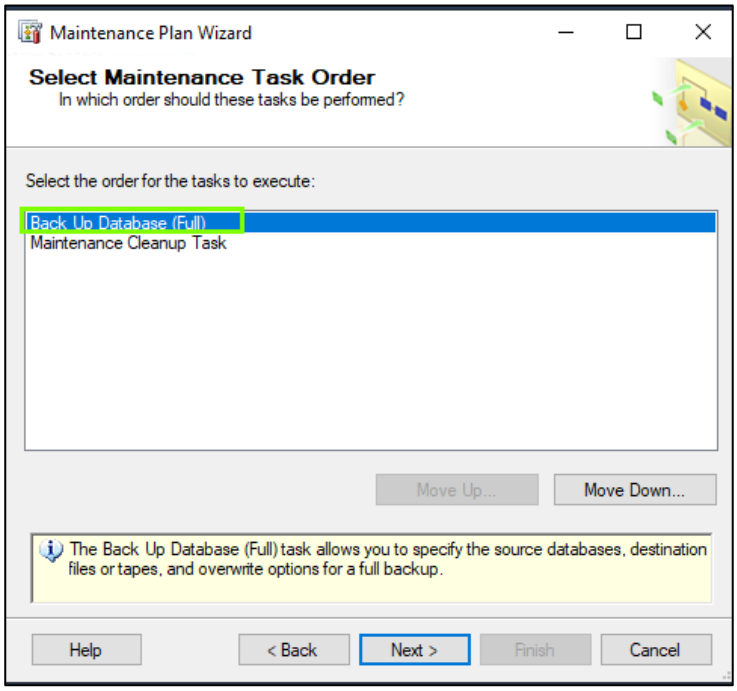


10. ถัดหน้าที่ 2 Select Maintenance Task

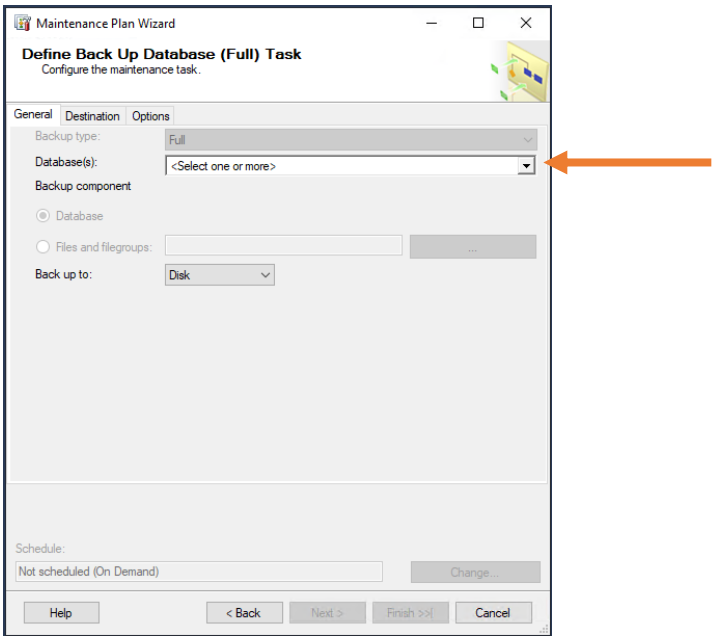
- เลือกว่าจะเอาอะไรเข้ามาใช้ในการทำ Backup กด Next
- ในกรอบสีเขียว เป็น Database ที่เราต้อง Backup
- ในกรอบสีชมพู เป็นการตั้ง clean up หรือ delete ข้อมูลที่ไม่ได้ใช้



11. เลือกข้อแรก เป็น Backup Database (Full) กด Next

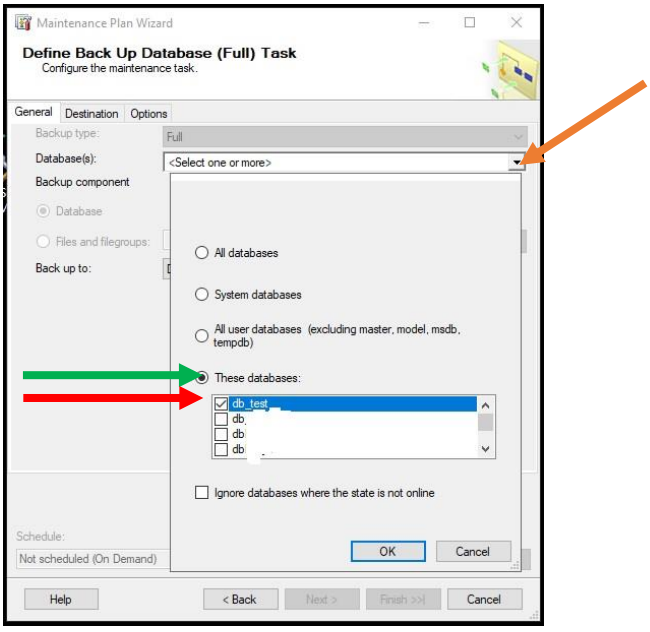


12. หน้านี้เป็นการเริ่มตั้งค่า Backup ในหัวข้อ General ให้ทำการตั้งค่าโดยเลือก Database (ในช่องสีขาว ให้กดที่ลูกศร)



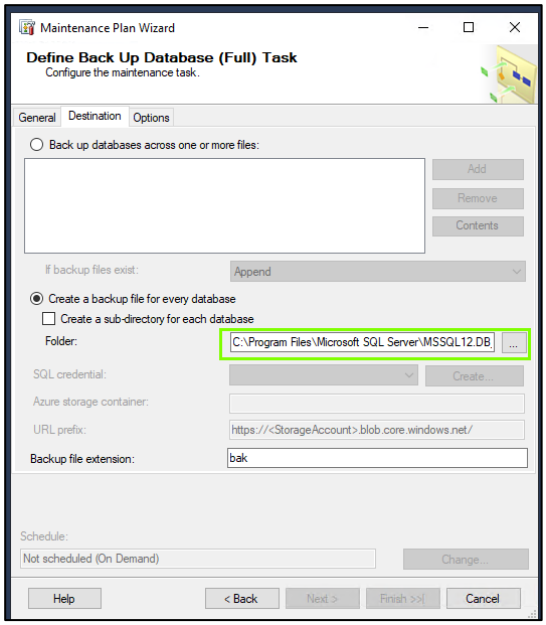
13. Define Backup Database (Full) Task กด OK

- เมื่อกดที่ลูกศรสีเขียว These database เป็นการเลือก
- ลูกศรสีแดง ให้เราเลือกไฟล์ Database ที่จะ Backup ในตัวอย่าง (db_test)

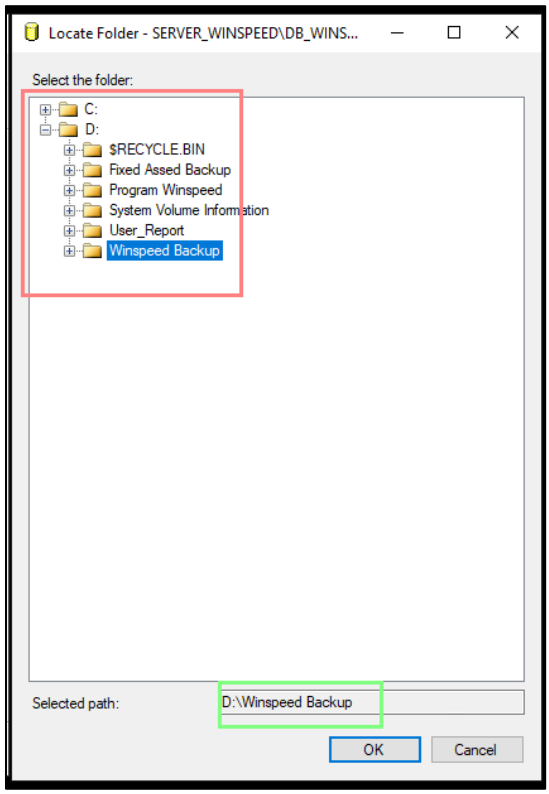


14. กลับมาที่ หน้า Main Plan Backup ให้เลือกหัวข้อด้านบน (Destination)

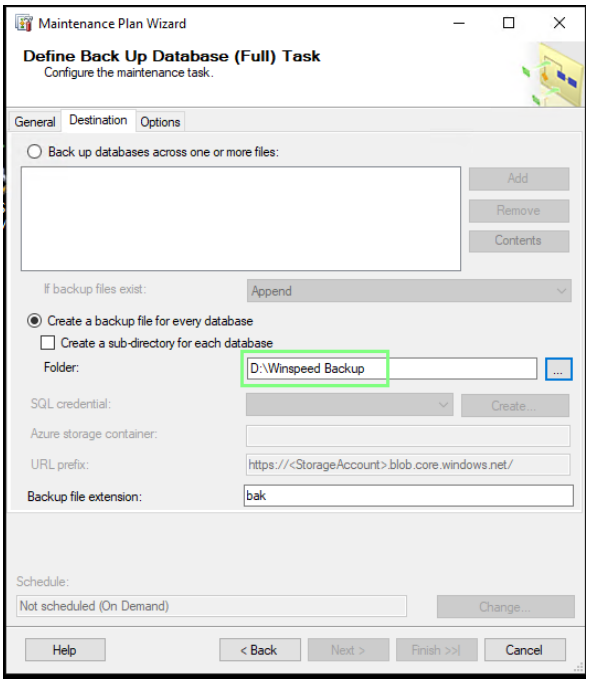
- ให้เลือก Create a backup ในกรอบสีเขียว
- ส่วน Backup file extension คือเลือกนามสกุลไฟล์ ที่จะให้ save เป็นอะไร



15. ให้เรากำหนดปลายทางที่จะเก็บไฟล์ Backup ในที่นี้เลือกเป็น Drive (D) กด OK

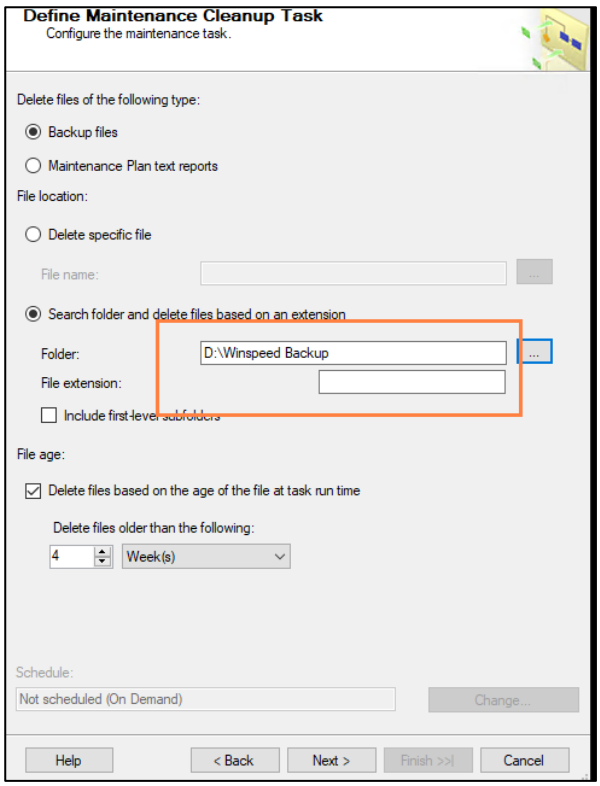


16. กลับมาที่หน้า Destination ในกรอบสีเขียว มีการเปลี่ยนแปลงที่เก็บไฟล์ Backup

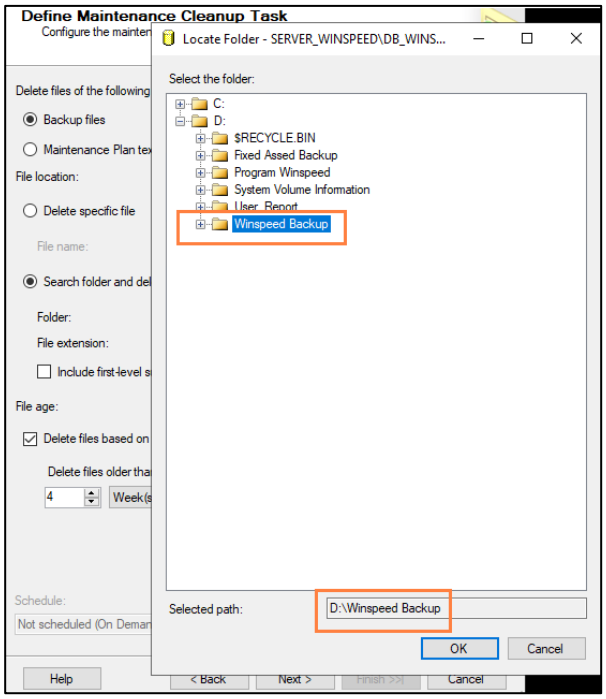


17. หน้านี้เป็นหน้า Option ทางซ้ายบน

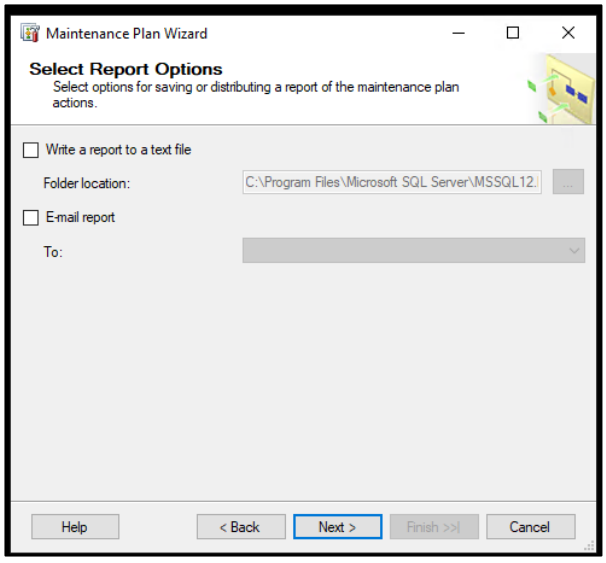
- เมื่อมีการ Backup แล้วจะมีการตั้งค่าลบ ไฟล์ให้ เพื่อป้องกันพื้นที่เต็ม
- ในกรอบสีส้มเป็นการเลือกไฟล์ที่จะลบ (ให้กดจุด.... ด้านหลัง)



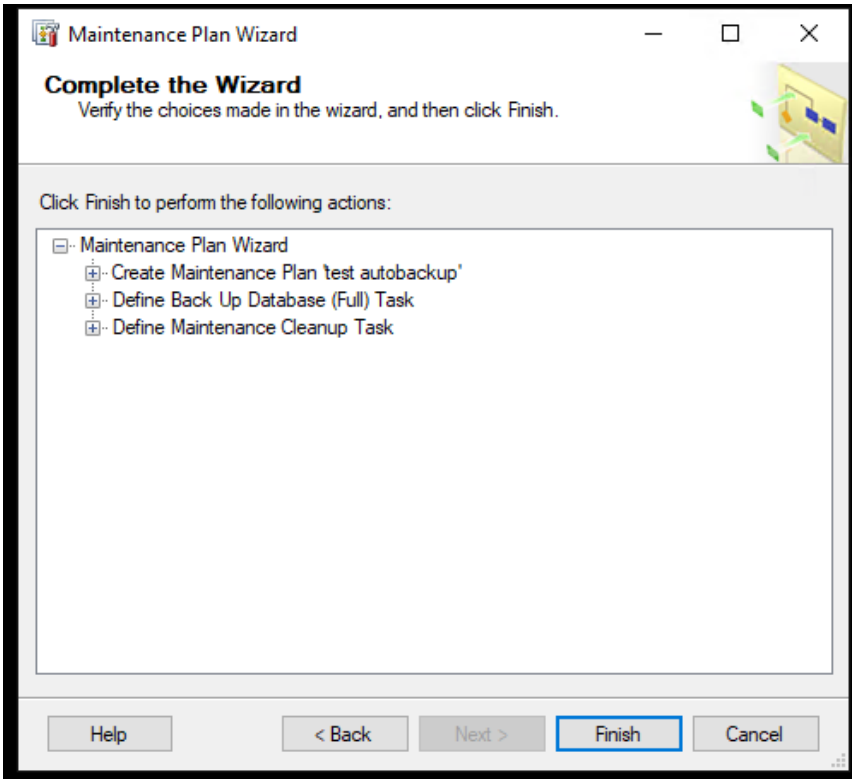
18. จะมีหน้า Popup ให้เราเลือกไฟล์ที่เก็บไว้



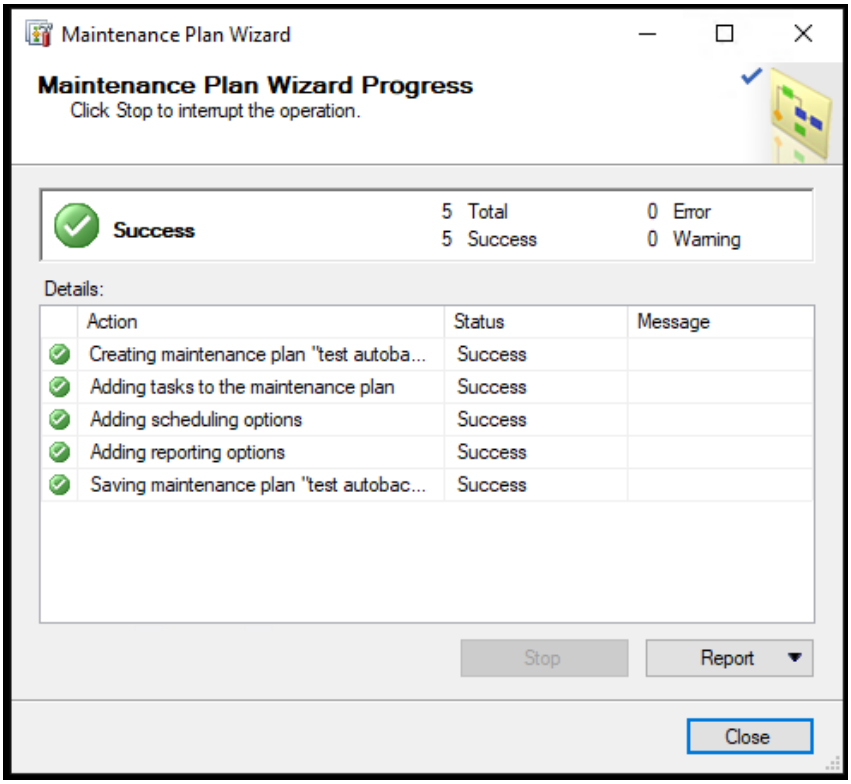
19. หน้านี้เป็นหน้า แจ้งเตือนหรือ Log ให้เรารู้ว่าการทำงานของ Auto backup มีปัญหา ตรงจุดไหน สามารถให้ส่งไปยังเมล ให้กับผู้ดูแลได้รับทราบ



20. เมื่อเราตั้งค่าครบทุกอย่างเสร็จแล้วตัวโปรแกรมจะแสดงให้เห็นว่าเราได้กำหนดอะไรไว้บ้าง

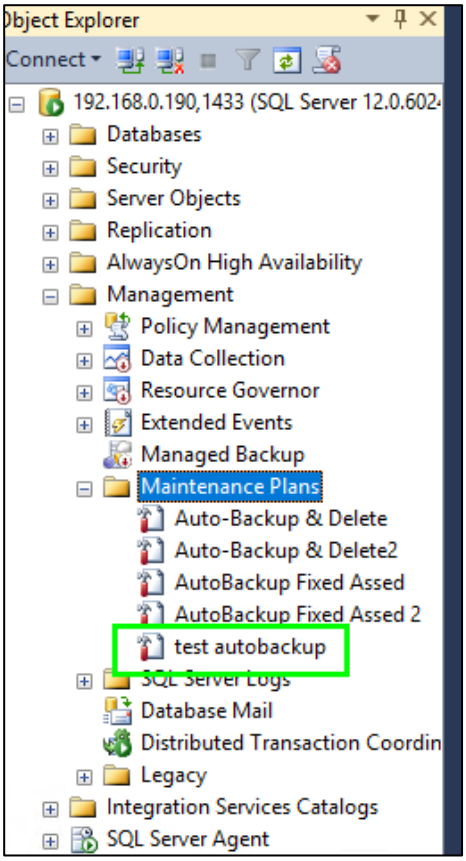


21. หน้านี้เป็นการรีเช็ค ว่ากระบวนการที่เราทำไม่มีอะไรผิดพลาด



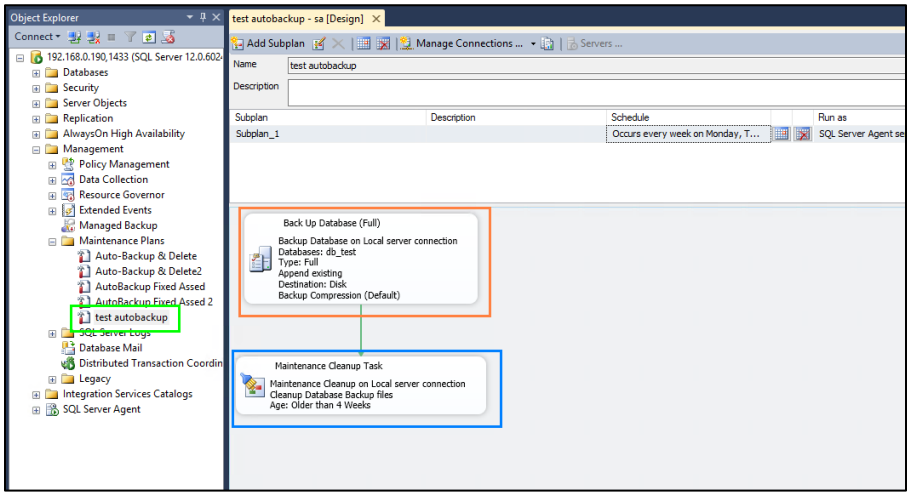
22. เมื่อเสร็จสิ้นการตั้งค่า Auto backup จะกลับมาหน้าโปรไฟล์ Database หลัก

- ในกรอบสีเขียว เป็นการโชว์ Plan ที่เราทำ Auto backup ขึ้นมา



23. เมื่อเราดับเบิ้ลคลิกที่ Plan ที่เราสร้างขึ้นมา จะเห็น Flowchart

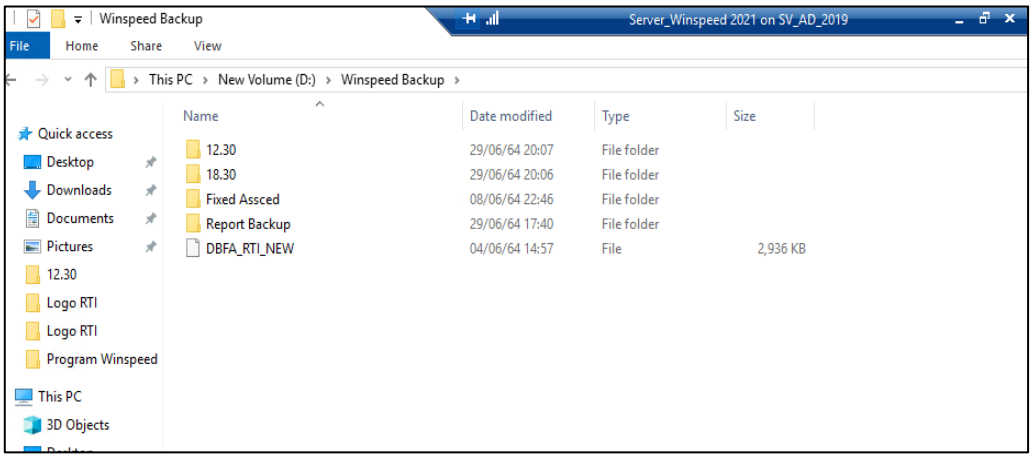
- ในกรอบสี ส้ม คือ Plan Auto backup ที่เราทำเอาไว้
- ในกรอบสีฟ้า คือ Plan Auto Delete ที่เรากำหนดไวเช่นกัน



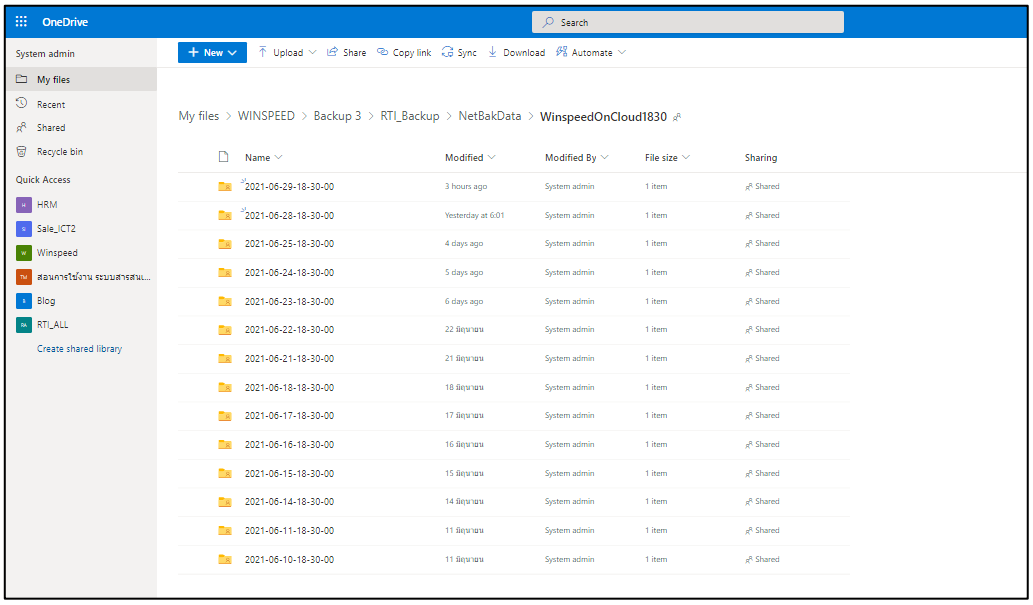
การ Backup มีการสำรองข้อมูล

1. สำรองตามระบบภายใน คือ ไม่ว่าจะทำการ Backup แบบ Manual และ Auto backup จะมีการจัดเก็บข้อมูลไว้ที่ตัว Server และจะ Backup ขึ้น NAS หรืออุปกรณ์ Hard Disk External ที่อยู่ภายใน ออฟฟิศ
2. สำรองตามระบบภายในแต่จัดเก็บไว้นอก Location ของออฟฟิศ เช่น ฝากไว้บน Cloud เช่น Dropbox, Google Drive และ OneDrive

การ Backup แบบเก็บไว้ภายในเครื่อง Server Drive (D)



การ Backup on Cloud

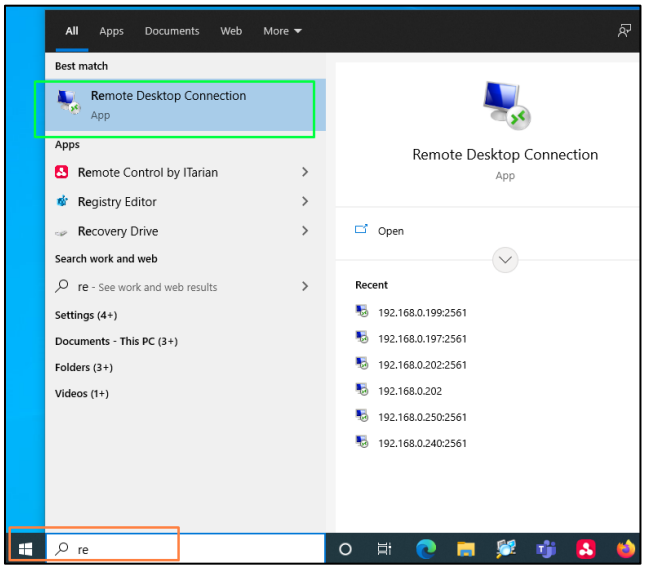


แนวทางการปฏิบัติงาน การเข้า Server Remote

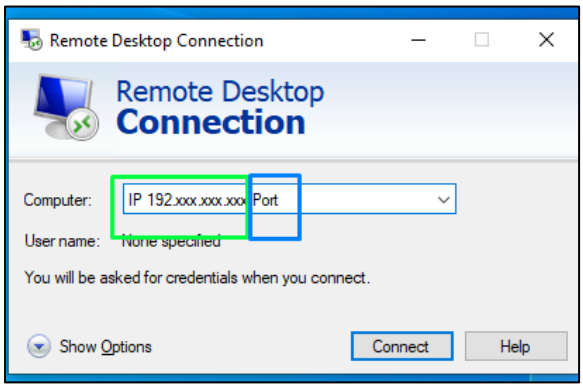
1. การตรวจเช็ค Server Remote จะใช้ Program Remote Desktop

   ข้อควรระวัง : การ Remote ต้องตรวจสอบเรื่อง port ที่ใช้ Remote Service Windows server Update ป้องกันการโดนเจาะข้อมูล

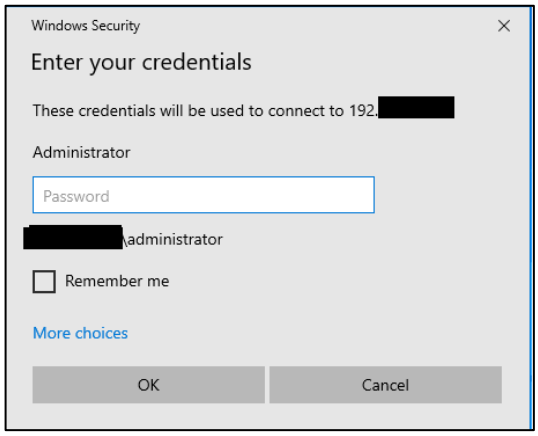
2. ไปที่ Start Windows -> RUN แล้วพิมพ์ข้อความในช่องว่าง (หากเป็น Windows ปัจจุบัน ดูจากรูปด้านล่าง คลิก แว่นขยาย ในการกรอบสีส้ม เมื่อพิมพ์ชื่อหรือ Subject ที่ใกล้เคียงกัน ระบบค้นหาจะดูโปรแกรมขึ้นมาให้เราเลือก เมื่อระบบดึงโปรแกรมขึ้นมาจะเห็นได้ในกรอบสีเขียวเป็นชื่อ Program Remote Desktop Connection ให้ทำการคลิก ที่ตัวโปรแกรมที่เราต้องใช้งาน



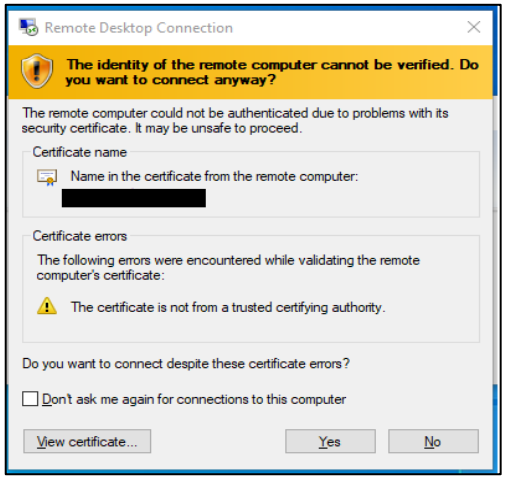
3. จากนั้นโปรแกรม Remote จะขึ้นป๊อบอัพ กรอบสีเขียว ให้เราใส่ชื่อปลายทาง หรือ IP กรอบสีน้ำเงิน เป็นการระบุ Port การเชื่อมต่อ เมื่อเรารู้ IP , Port กด Connect ได้เลย



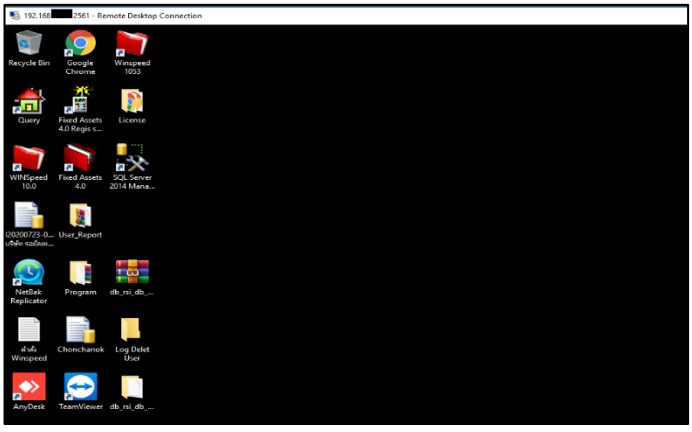
4. หลังจาก Connect แล้ว จะขึ้นหน้าต่าง Login ทางระบบแจ้งใส่ User Password



5. หลังจากใส่ User Password ถูกต้อง ระบบจะแจ้ง Certificate name เป็นชื่อเครื่องคอมพิวเตอร์ หรือ IP เครื่องที่เรากำลังรีโมทอยู่ ในส่วนนี้ให้คลิกที่ปุ่ม **Yes**
(ปล. หากไม่ต้องการให้แสดงในครั้งถัดไป ให้ทำเครื่องหมายถูกที่ช่อง Don`t ask me again for Connection to this Computer)

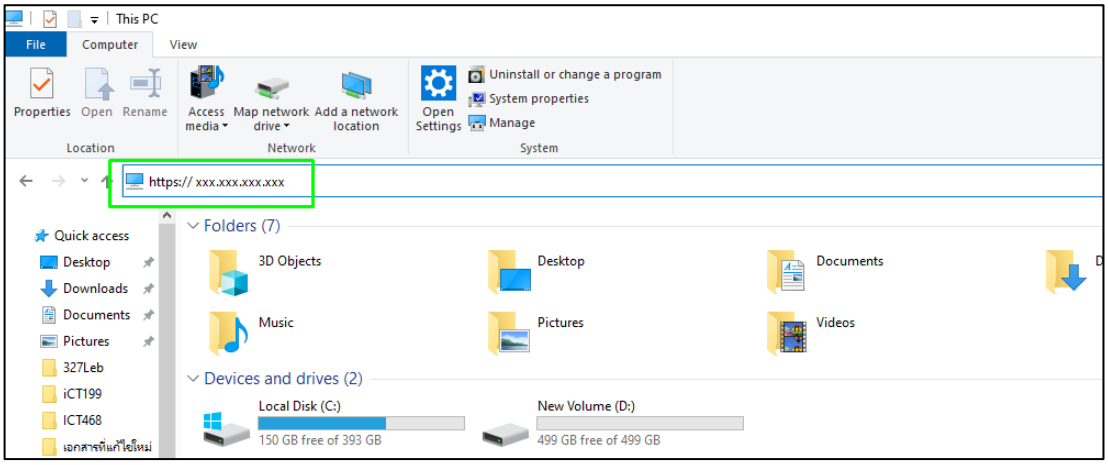


6. จะเข้าสู่หน้าจอ Server Remote

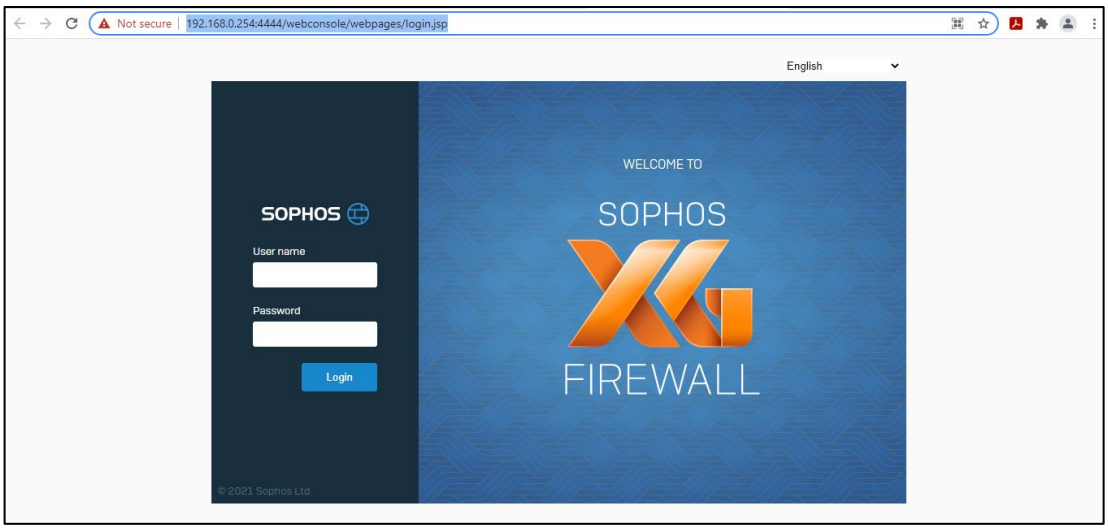


แนวทางการปฏิบัติงาน การตรวจเช็ค Firewall

1. การเข้าตรวจเช็ค Firewall ใส่หมายเลข IP ของ Firewall หรือ IP WAN (กรอบสีเขียว)



2. เมื่อเข้า Firewall ได้แล้ว



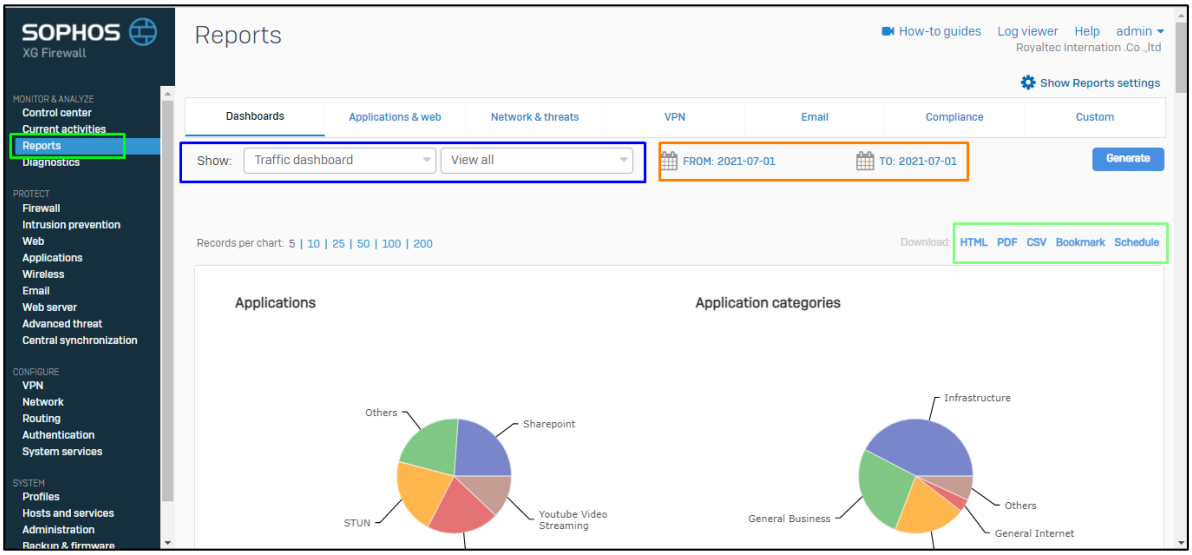
3. เลือก Report แสดงการทำงานของการเชื่อมต่อ เช็คจากต้นทางผู้ใช้, Port ต่างๆ ที่มีการเปิดให้เข้าใช้ ดูเรื่องของ WEB / Program / Port ที่มีการตั้งค่า Policy Allow / Block สามารถดูย้อนหลังจากวันที่ย้อนหลังได้ไม่เกิน 3-5 เดือน ตามมาตรฐานของ Brand

4. เลือก Show สามารถเลือกดู Traffic dashboard หมวดหมู่ของการรับส่งข้อมูลเครือข่าย เช่น แอพพลิเคชัน หมวดหมู่เว็บ และผู้ใช้

5. Security dashboard การทำงานของเครือข่าย และรับส่งข้อมูล ข้อมูลเดี่ยวกับมัลแวร์ สแปมจากผู้ส่งและผู้รับปลายทาง

6. Executive report ข้อมูลที่ใช้งานบ่อยเกี่ยวกับ Firewall ปริมาณข้อมูล และ ภัยคุกคาม

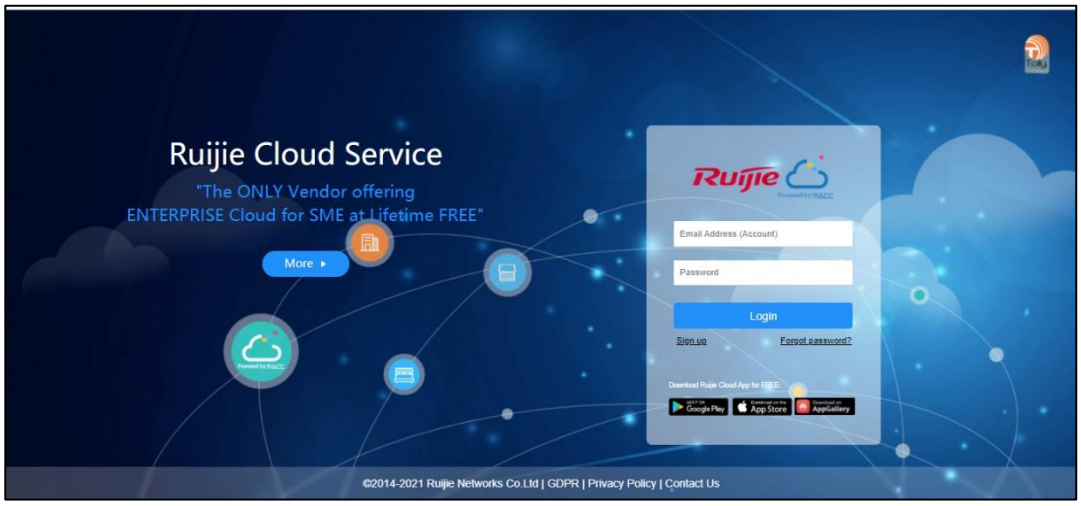
7. User threat quotient (UTQ) จัดอันดับผู้ใช้งานและภัยคุกคาม



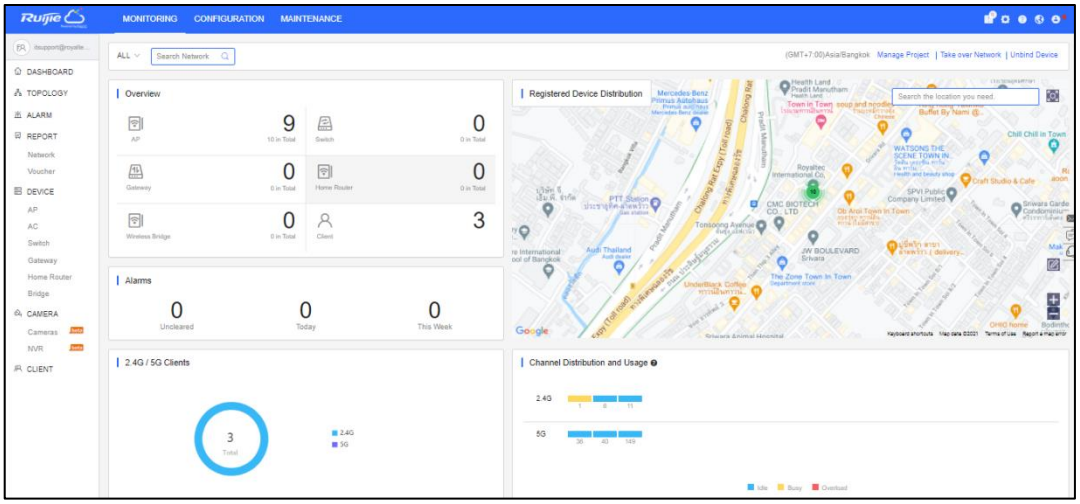
แนวทางการปฏิบัติงาน การตรวจเช็ค Access Control Wi-Fi

1. การเข้าตรวจเช็ค Access Control Wi-Fi สามารถล็อกอินได้ทั้ง Lan และ Internet เพราะอยู่บน Cloud สามารถล็อคอินได้จากทุกที่

วิธีเข้า ใช้งาน URL : https://cloud-as.ruijienetworks.com/sso/login?service=https%3A%2F%2Fcloud-as.ruijienetworks.com%2Fadmin3%2F



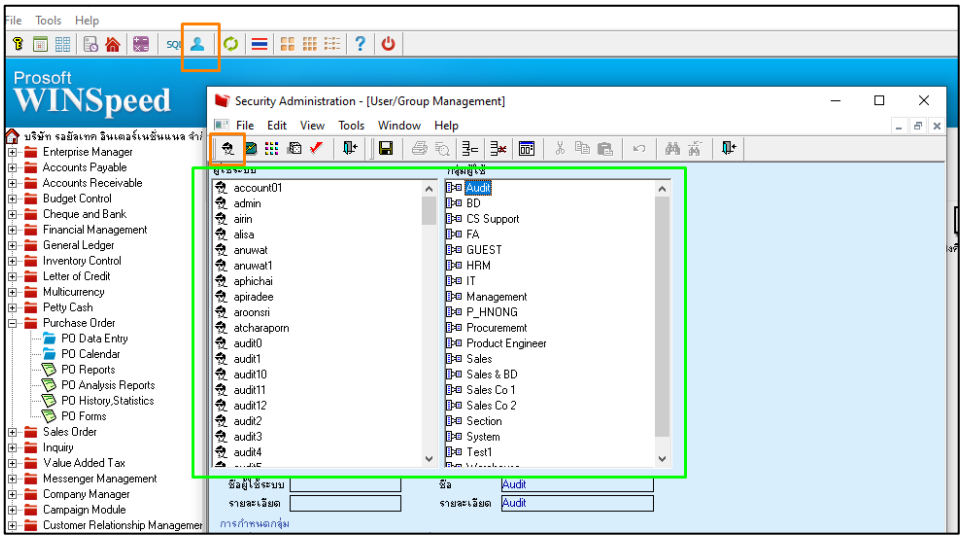
2. ล็อกอินเรียบร้อย หน้าตาของ Dashboard สามารถตรวจสอบ Access Control Wi-Fi ได้เลย



การสร้างกลุ่ม การเปิดและปิด เมนูการใช้งาน WINSPEED

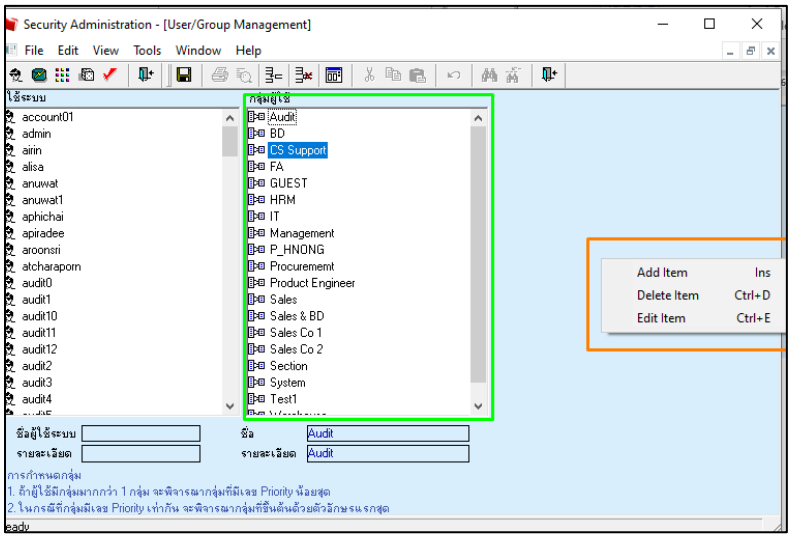
1. การกำหนด Group

- Login user Admin คลิกที่รูปคนสีฟ้า
- จากนั้นจะขึ้นกรอบของ (Security Administrator) คลิกรูปคนอยู่ใกล้กรอบสีเขียว
- รูปคน (ผู้ใช้งานระบบ / กลุ่มผู้ใช้ระบบ) จะแบ่งด้านซ้าย ผู้ใช้งาน ด้านขวา กลุ่มผู้ใช้งาน

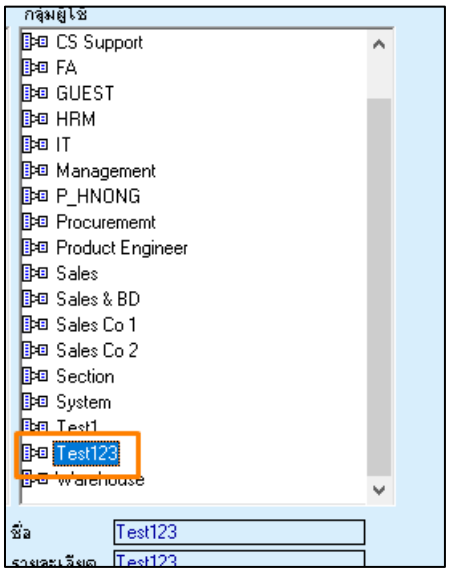


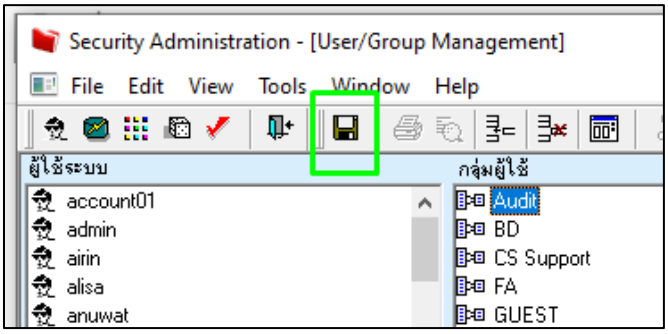
2. สร้างกลุ่มผู้ใช้งาน

- คลิกขวา พื้นที่ขาวๆ ในกรอบสีเขียว จากนั้นจะขึ้นข้อความในกรอบสีส้ม
- Add item (สร้างกลุ่มใหม่)
- Delete item (ลบกลุ่ม)
- Edit Item (แก้ไขกลุ่ม)

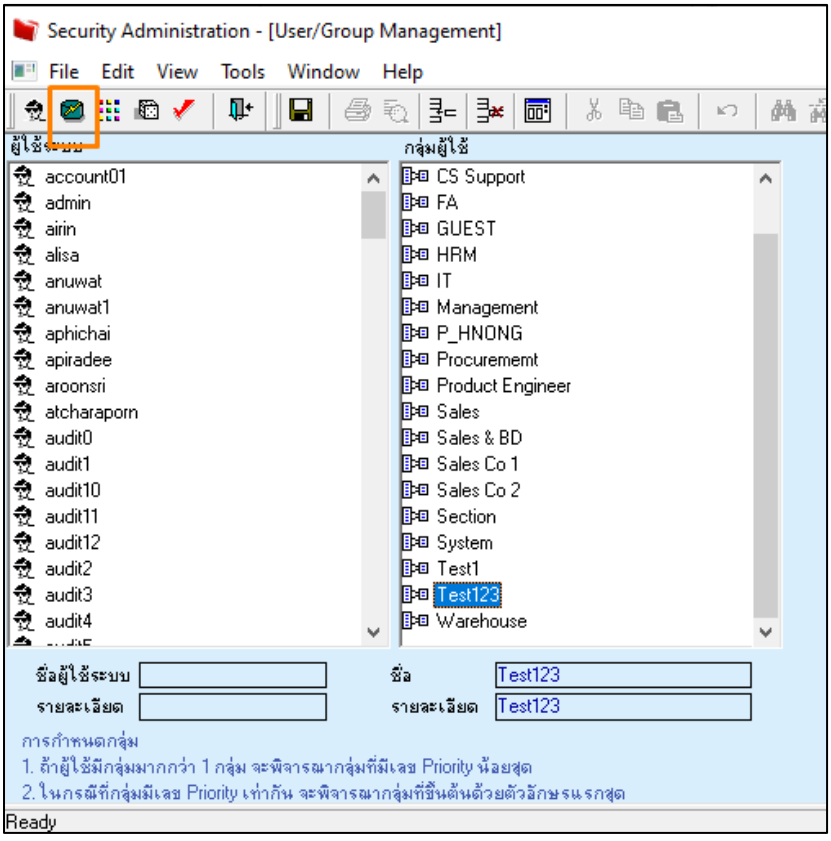


- สร้าง กลุ่ม ชื่อ (Test123) จากนั้น กด Save



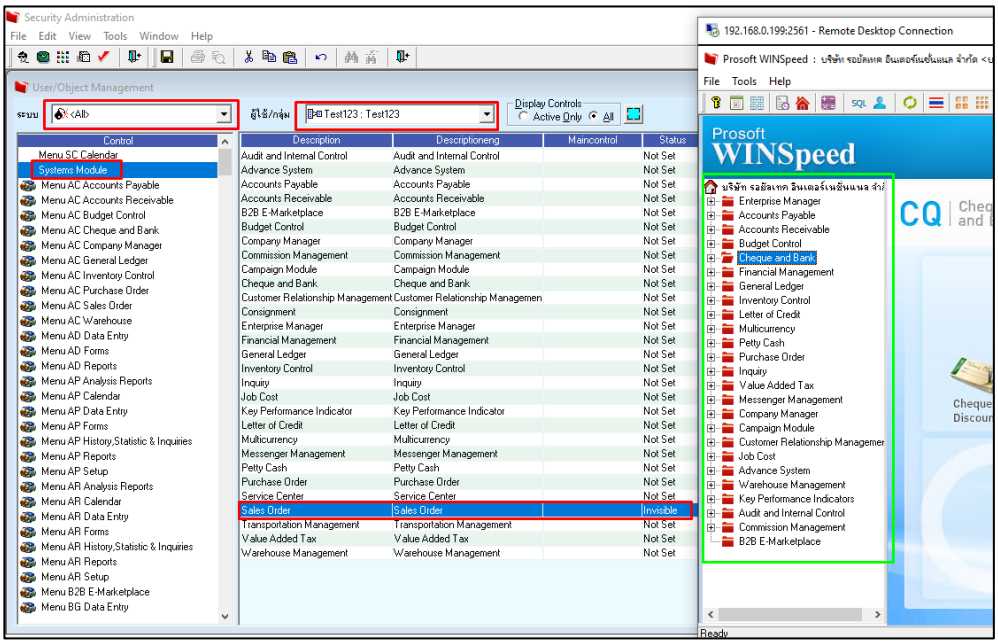


- เมื่อสร้างชื่อกลุ่มเสร็จแล้ว ให้คลิกรูปฐานข้อมูลในกรอบสีส้ม (User/Object)



3. ในหน้าต่าง User/Object

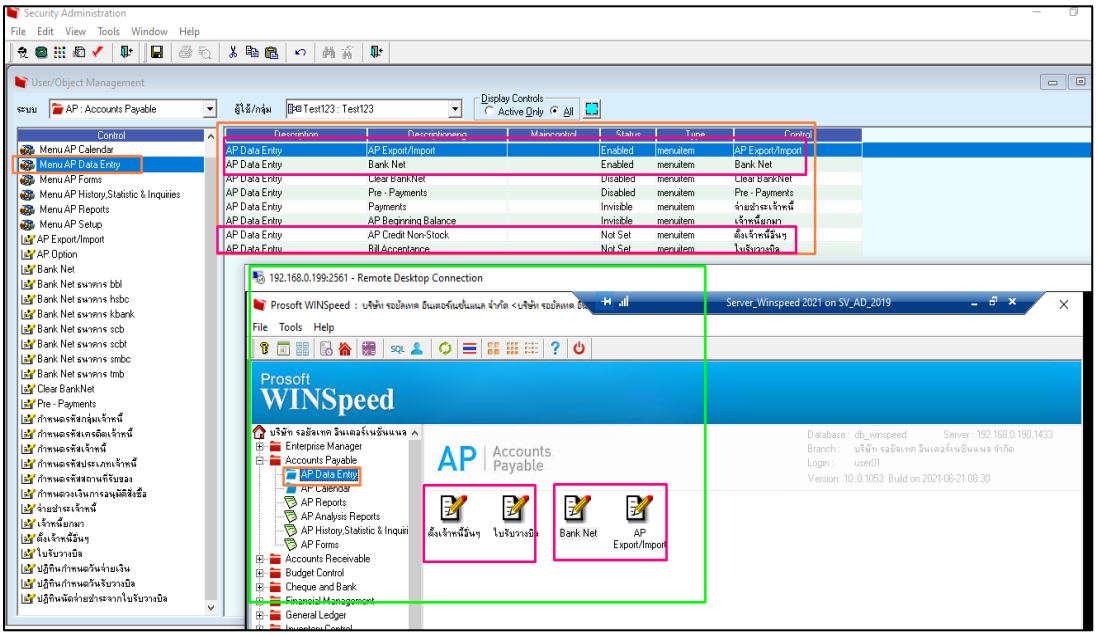
- ด้านซ้าย (ระบบ) คือ เมนูหลัก
- ในหน้าหลัก เลือก System Module
- ด้านขวา (ผู้ใช้/ กลุ่ม) คือ กลุ่มผู้ใช้งาน
- ให้เลือกเมนูที่เกี่ยวข้องกับกลุ่มในตัวอย่างด้านล่างจะเลือกปิด Sales Order (Invisible = ไม่แสดง)
- ในกรอบสีเขียว เป็นกลุ่ม Test123 จะมองไม่เห็น Sales Order



4. รูปของการปิด Module ภายใน

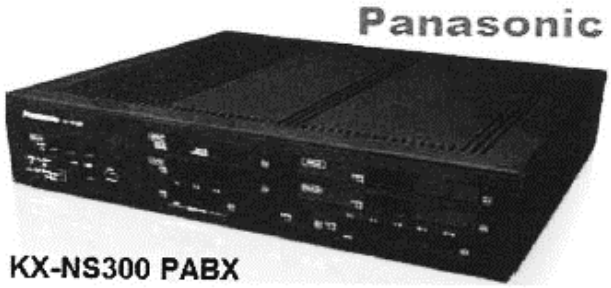
- ยกตัวอย่าง ทางซ้ายในส่วนของ AP : Accounts Payable กรอบสีส้ม เลือกหูข้อ AP Data Entry
- ทางขวากรอบสี ส้ม / สีชมพู ทำการตั้งค่าในส่วน Status
- Not set = ไม่มีการตั้งค่า
- Enable = เปิด
- Disable = ปิดไม่ให้ใช้งาน
- Invisible = มองไม่เห็น
- กรอบสีเขียว คือหน้าต่างผู้ใช้งาน
- เมน AP Accounts Payable (AP Data Entry)
- กรอบสีชมพู หลังจากการตั้งค่า ของฝั่ง admin ในส่วนของกลุ่มผู้ใช้งาน

ตัวอย่างการตั้งค่า ตั้งเจ้าหนี้ / ใบรับวางบิล / Bank Net (AP Export/Import)



แนวทางการปฏิบัติงาน การใช้งานระบบโทรศัพท์ IP PBX

ยี่ห้อ Panasonic รุ่น KX-NS300



ขนาดระบบ

- 12 เบอร์ภายนอก
- 2 เครื่องดิจิตอล
- 16 เบอร์ภายใน
- 86 SIP EXT

- NS300-Built - in

- 2-ch DISA : Recording time 20 min. (ระบบตอบรับอัตโนมัติ)
- Digital PT 2-port (Port สำหรับต่อเครื่องโทรศัพท์แบบดิจิตอลหรือเครื่อง DSS)
- SLT 16-port with caller ID (Port สำหรับต่อเครื่องโทรศัพท์แบบ Analog ธรรมดาทั่วไป)
- Analog CO 6-port with caller ID (Port สำหรับต่อสายนอกแบบ Analog ธรรมดาทั่วไป)
- LAN port (10/100 Base TX) (Port สำหรับต่อเข้าอินเตอร์เน็ตหรือสำหรับเข้าโปรแกรมระบบ)

LAN
1-RJ45

Analog CO
3-RJ45 for 6-ch

DPT
1-RJ45 for 2-DPT

SLT 5-RJ45
SLT 1-2 / SLT 3-4
SLT 5-8 / SLT 9-12
SLT 13-16

Power failure transfer for 2 ch (CO-1/2 to SLT1/2)

- IP ตู้ PABX / เข้า Log-in

IP : 192.168.30.253

Username : INSTALLER
Password : 12345678

- รายละเอียด IP

LAN Setting

IP Address : 192.168.30.~~230~~ 253

MAC Address : 255.255.255.0

Default Gateway : 192.168.30.254

DSP IP Setting

DSP1 : 192.168.30.251

DSP2 :192.168.30.252

NAT - External IP Address / FQDN : 110.170.188.66

UDP Port No. for SIP Extension Server : 36060

NAT - SIP Proxy Server Port No. : 36060

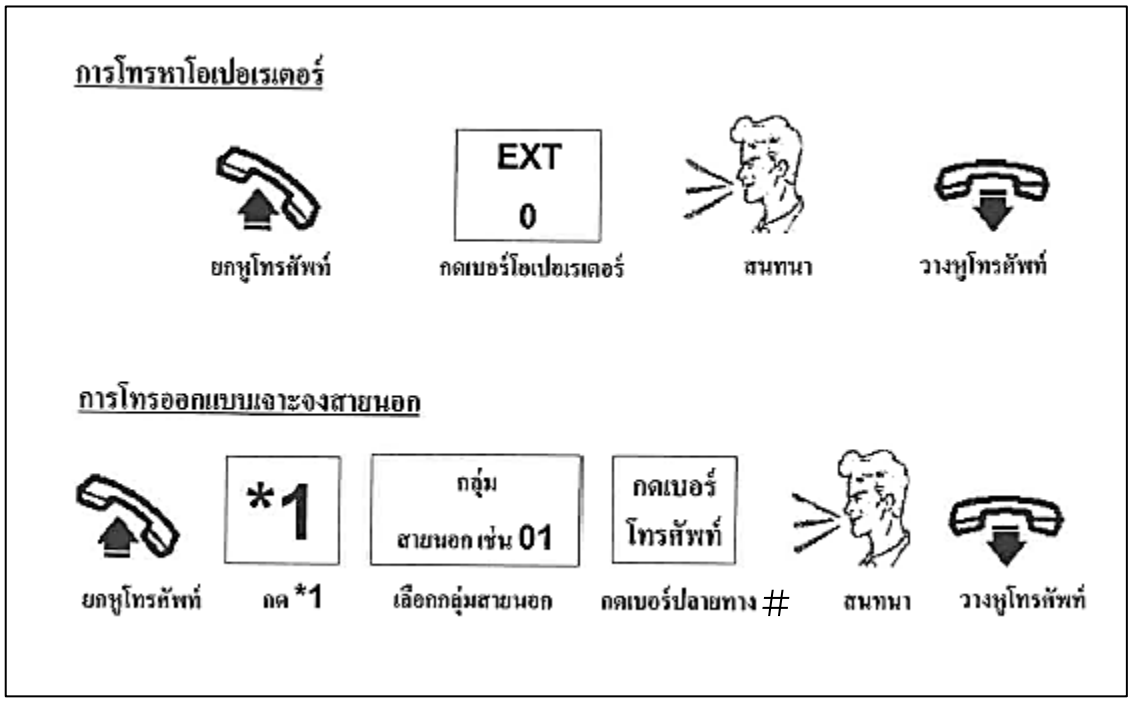
Forwarding Port

Port 36060 : 192.168.30.253 / UTP

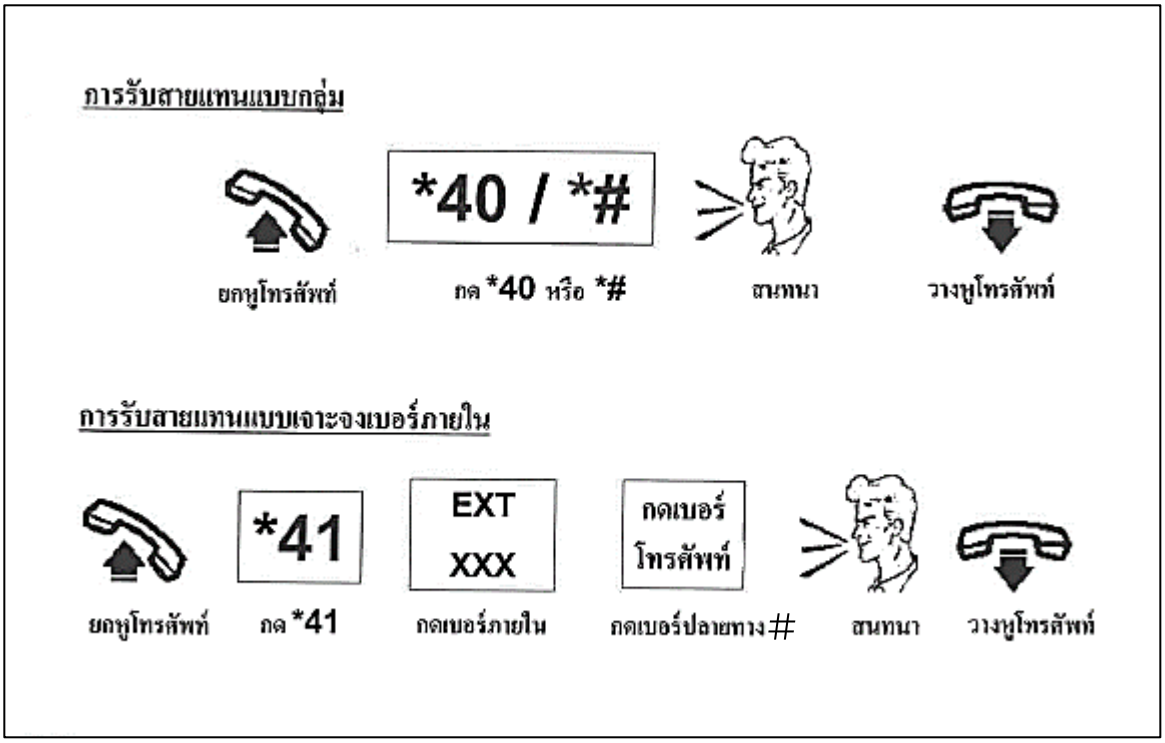
Port 16000 – 16511 : 192.168.30.251 / UTP

- การใช้งานทั่วไป

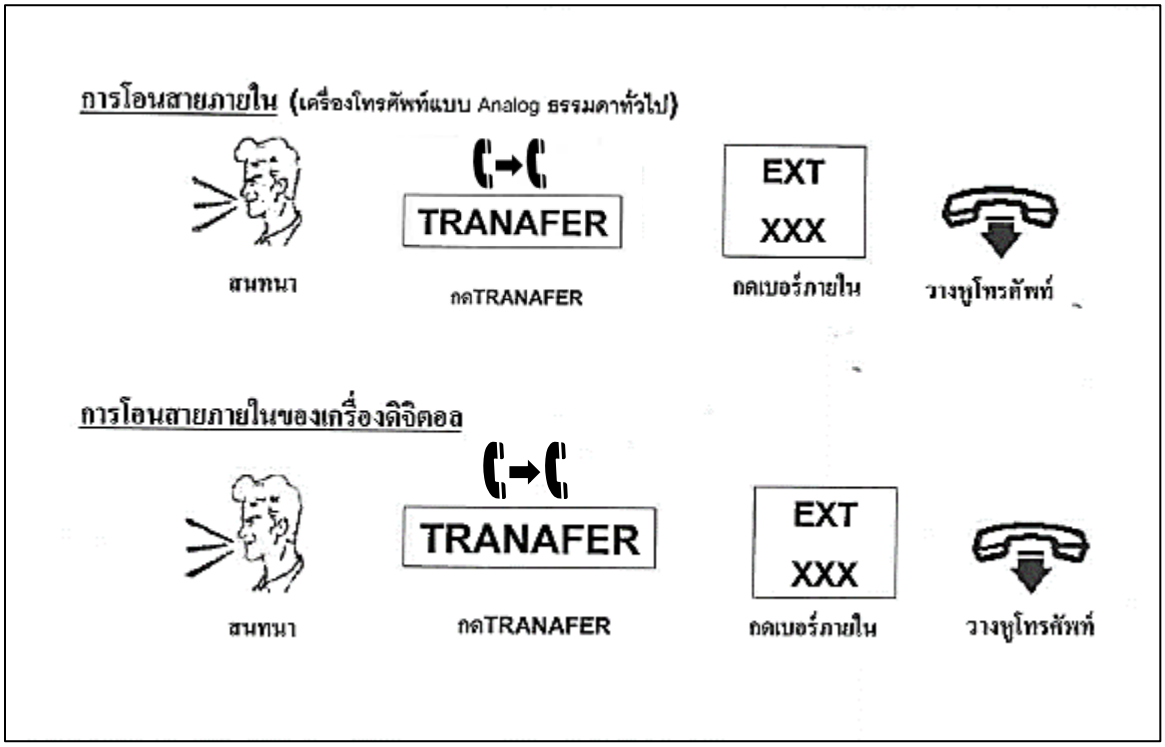
1. การโทรออก



2. การรับสายแทน/การดึงสาย



3.การโอนสาย



แนวทางการปฏิบัติงาน ในการใช้แบบฟอร์มขอแก้ไขเปลี่ยนแปลงแก้ไขเพิ่มเติมโปรแกรม

1. ผู้ใช้งาน ต้องการแก้ไขแบบฟอร์มสั่งปริ้นบน Winspeed

2. ผู้ใช้งานแจ้งเจ้าหน้าที่สารสนเทศ เพื่อขอดำเนินการตรวจสอบข้อมูลตามคำร้องขอ แจ้งจากผู้ใช้งาน (User) โดยมีขั้นตอนการตรวจสอบ ดังนี้

3. เจ้าหน้าที่สารสนเทศแจ้งให้หัวหน้าฝ่าย และผู้เกี่ยวข้องรับทราบข้อมูล

4. หัวหน้าฝ่ายและผู้เกี่ยวข้องหารือ และ รออนุมัติ

5. หัวหน้าฝ่ายและผู้เกี่ยวข้องหารือ แล้วไม่ อนุมัติ

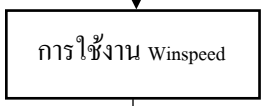
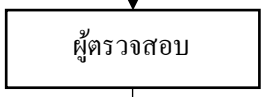
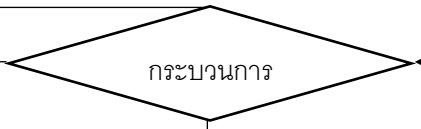
6. หัวหน้าฝ่ายและผู้เกี่ยวข้องหารือ แล้วให้ทางฝ่ายสารสนเทศดำเนินการแก้ไข

    6.1 ฝ่ายสารสนเทศ แก้ไขได้ ทำการทดสอบ แล้ว ใช้งานจริง

    6.2 ฝ่ายสารสนเทศ แก้ไขเองไม่ได้ ต้องแจ้งให้หัวหน้าฝ่ายรับทราบและให้ บริษัทตัวแทนจำหน่ายแก้ไข

7. บริษัทตัวแทนจำหน่าย แก้ไขข้อมูล

ขั้นตอนการปฏิบัติการ

เหตุการณ์	รายละเอียด
	-ผู้ใช้งานใช้งานพบปัญหาในการใช้งาน
	-การใช้งานโปรแกรมมีการพบข้อแก้ไข
	-ผู้แลระบบ ตรวจสอบตามที่ผู้ใช้งานร้องขอ
	-แจ้งหัวหน้าฝ่ายที่เกี่ยวข้องรับทราบ -รอหัวหน้าฝ่ายตัดสินใจอนุมัติให้ทำตามคำขอของผู้ใช้งาน
	-หัวหน้าฝ่ายไม่อนุมัติ
	-ฝ่ายสารสนเทศตรวจแก้ไข -ออกเอกสารแบบฟอร์มขอแก้ไขเปลี่ยนแปลงให้ผู้ใช้งานกรอกรายละเอียด
	-จ้างบริษัทตัวแทนจำหน่ายแก้ไข้
	-ตรวจสอบความถูกต้องก่อนใช้งาน