



วิธีการใช้งาน

Synology® NAS

เนื้อหา



1

- NAS คืออะไร

2

- วัตถุประสงค์ของการนำ NAS มาใช้งานใน กพ.ทร.

3

- หลักการทำงานของระบบ NAS

4

- ความปลอดภัยระบบ NAS

5

- การใช้งานระบบจัดเก็บข้อมูลในระบบ Cloud

6

- การกำหนดสิทธิ์ในการเข้าถึงไฟล์เดออร์ในระบบ Cloud

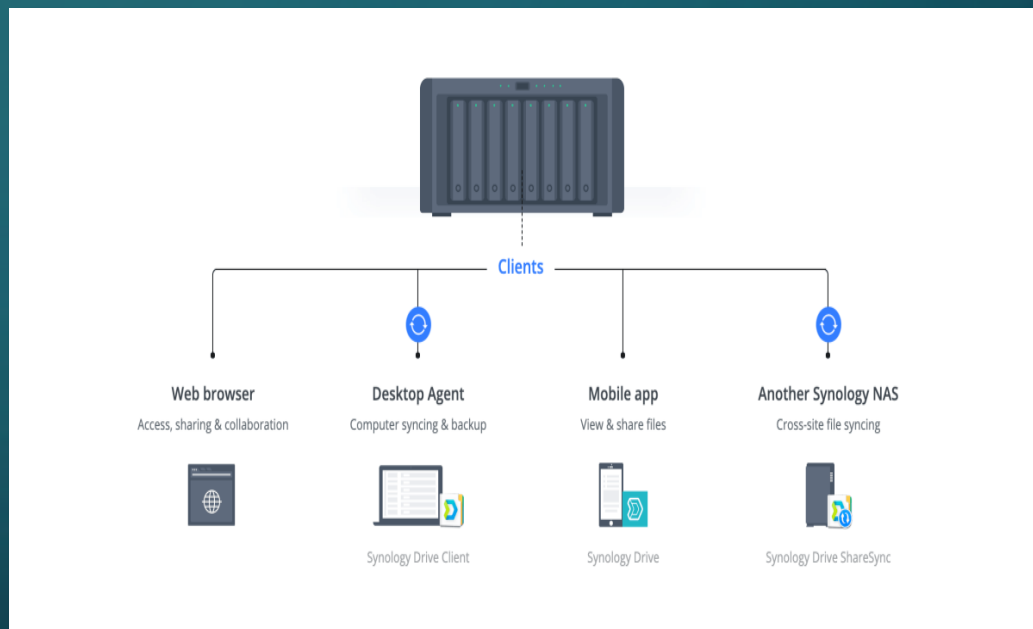
NAS คืออะไร



- พื้นที่เก็บข้อมูลที่เชื่อมต่อกับ
เครือข่าย



- ช่วยให้สามารถสร้างพื้นที่ส่วนตัว
เพื่อจัดเก็บ เข้าถึง สำรองข้อมูล และ
แชร์ไฟล์อย่างอิสระและปลอดภัย



วัตถุประสงค์ของการนำ NAS มาใช้งานใน กพ.ทร.

- เพื่อให้สามารถใช้ไฟล์อิเล็กทรอนิกส์ร่วมกัน เช่น MS WORD, MS EXCEL, MS Powerpoint หรือ pdf
- เพื่อให้สามารถใช้ไฟล์ดังกล่าวได้ทุกสถานที่ เช่น ที่ทำงาน หรือที่บ้าน
- เพื่อเป็นการป้องกันผู้ไม่หวังดีเข้าถึงไฟล์อิเล็กทรอนิกส์ ในกรณีที่ทำกร Share ไฟล์ในเครื่องคอมพิวเตอร์ ซึ่งเป็นไปตามที่ สสท.ทร. สแกนพบช่องโหว่ในระบบ เครือข่ายและรายงานให้แต่ละหน่วย ดำเนินการแก้ไข



EX ช่องโหว่



บันทึกข้อความ

ส่วนราชการ สสท.ท. (ศสท. โทร. ๕๓๗๕๕๕)

ที่ กท.๐๕๐๗.๕/๕๕๑ วันที่ ๒๕ ก.พ.๖๕


เรื่อง รายงานผลการตรวจสอบและวิเคราะห์จุดอ่อน/ช่องโหว่ในระบบสารสนเทศ

เสนอ กท.ท.

๑. สสท.ท. โดย ศสท.ท. ได้ดำเนินการตรวจสอบและวิเคราะห์จุดอ่อน/ช่องโหว่ในระบบสารสนเทศของ กท.ท. ในช่วงเดือน พ.ย.๖๔ ได้ตรวจพบช่องโหว่ในระบบฯ จำนวน ๓ ระดับ โดยเป็นช่องโหว่ประเภทความเสี่ยงสูงมาก (Critical) จำนวน ๕ รายการ ช่องโหว่ประเภทความเสี่ยงสูง (High) จำนวน ๒๒ รายการ และช่องโหว่ประเภทความเสี่ยงปานกลาง (Medium) จำนวน ๖๑ รายการ รายละเอียดตามแนบฯ ซึ่งช่องโหว่ดังกล่าว ทำให้เกิดความเสียหายที่ระบบสารสนเทศของ กท.ท.จะถูกโจมตีและได้รับผลกระทบ

๒. เพื่อให้การดำเนินการแก้ไขช่องโหว่ฯ ตามข้อ ๑ เป็นไปด้วยความเรียบร้อย สสท.ท. จึงขอส่งรายงานผลการตรวจสอบและวิเคราะห์จุดอ่อน/ช่องโหว่ในระบบสารสนเทศพร้อมข้อเสนอแนะให้ กท.ท. ทราบ เพื่อดำเนินการปรับปรุงแก้ไข และขอให้หน่วยงานผลการปรับปรุงแก้ไขให้ ศสท.ท. ทราบ เพื่อพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

จึงเสนอมาเพื่อโปรดพิจารณาดำเนินการต่อไป

พล.ร.ศ. 
 ผอ.ศสท.ท. ทำการแทน
 จก.สสท.ท.

ช.ศสท.ท.สท.ท. แบบฟอร์มบันทึกผลการตรวจประเมิน Audit Note

ตรวจสอบ : จ.อ.กิตติณัฐ นิลพงษ์ ส่วนที่รับการตรวจสอบ : กท.ท.

เครื่องมือที่ใช้ในการตรวจสอบ : Nessus Professional version 10.0.2 วันที่ : ๒๖ พ.ย.๖๔

รายละเอียด : ข้อเสนอแนะสำหรับการปรับปรุง/แก้ไขช่องโหว่ สามารถตรวจสอบได้จากเว็บไซต์ <https://www.tenable.com/plugins/nessus/PLUGIN-ID>

อย่างไร ช่องโหว่ PHP Unsupported Version Detection ให้ตรวจสอบจากเว็บไซต์ <https://www.tenable.com/plugins/nessus/58987>

ระดับความรุนแรง	IP address ที่ตรวจพบ	รายละเอียด	PLUGIN-ID
สูงมาก	10.106.6.x [70,101,111] 10.106.95.46	PHP Unsupported Version Detection	58987
สูงมาก	10.106.6.x [70,101] 10.106.95.46	Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow	57603

ช.ศสท.ท.สท.ท. แบบฟอร์มบันทึกผลการตรวจประเมิน Audit Note

ระดับความรุนแรง	IP address ที่ตรวจพบ	รายละเอียด	PLUGIN-ID
สูงมาก	10.106.6.x [70,101] 10.106.95.46	Apache 2.2.x < 2.2.15 Multiple Vulnerabilities	
สูงมาก	10.106.6.x [211,223,230] 10.106.95.29	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed)	
สูงมาก	10.106.6.x [79,83,131] 10.106.95.x [29,36,37]	Unsupported Windows OS (remote)	
สูง	10.106.6.111	PHP 5.6.x < 5.6.39 Multiple vulnerabilities	
สูง	10.106.6.x [70,101]	PHP 5 < 5.2.7 Multiple Vulnerabilities	

ช.ศสท.ท.สท.ท. แบบฟอร์มบันทึกผลการตรวจประเมิน Audit Note

ระดับความรุนแรง	IP address ที่ตรวจพบ	รายละเอียด	PLUGIN-ID
ปานกลาง	10.106.6.x [70,101,111] 10.106.95.x [46,216,217]	HTTP TRACE / TRACK Methods Allowed	
ปานกลาง	10.106.6.174	mDNS Detection (Remote Network)	
ปานกลาง	10.106.6.x [211,223,230] 10.106.95.x [216,217]	Terminal Services Encryption Level is Medium or Low	
ปานกลาง	10.106.95.x [216,217]	SSL Certificate Signed Using Weak Hashing Algorithm	
ปานกลาง	10.106.95.x [216,217]	SSL Certificate Cannot Be Trusted	
ปานกลาง	10.106.95.x [216,217]	SSL Self-Signed Certificate	
ปานกลาง	10.106.95.x [216,217]	SSL Certificate Expiry	
ปานกลาง	10.106.95.x [13,18,29,36,37,89]	SMB Signing not required	
ปานกลาง	10.106.95.29	Terminal Services Encryption Level is Medium or Low	57690
ปานกลาง	10.106.95.x [216,217]	TLS Version 1.0 Protocol Detection	104743
ปานกลาง	10.106.6.111	OpenSSL 1.0.2 < 1.0.2za Vulnerability	152780
ปานกลาง	10.106.6.111	OpenSSL 1.0.2 < 1.0.2u Procedure Overflow Vulnerability	132726
ปานกลาง	10.106.6.111	OpenSSL 1.0.x < 1.0.2m RSA/DSSA Unspecified Carry Issue	104408
ปานกลาง	10.106.6.111	OpenSSL 1.0.2 < 1.0.2k Multiple Vulnerabilities	96873

ช.ศสท.ท.สท.ท. แบบฟอร์มบันทึกผลการตรวจประเมิน Audit Note

ระดับความรุนแรง	IP address ที่ตรวจพบ	รายละเอียด	PLUGIN-ID
ปานกลาง	10.106.6.x [70,101] 10.106.95.46	Apache 2.2.x < 2.2.9 Multiple Vulnerabilities (DoS, XSS)	33477
ปานกลาง	10.106.6.111	Apache 2.4.x < 2.4.35 DoS	117807
ปานกลาง	10.106.6.x [70,101,111] 10.106.95.46	Apache < 2.4.49 Multiple Vulnerabilities	153583
ปานกลาง	10.106.6.111	Apache 2.4.x < 2.4.41 Multiple Vulnerabilities	128033
ปานกลาง	10.106.6.111	Apache 2.4.x < 2.4.42 Multiple Vulnerabilities	135290
ปานกลาง	10.106.6.111	Apache >= 2.4.17 < 2.4.49 mod_http2	153585
ปานกลาง	10.106.6.x [79,82,83,131,174,175,215]	SMB Signing not required	57608
ปานกลาง	10.106.6.111	OpenSSL 1.0.2 < 1.0.2n Multiple Vulnerabilities	105291
ปานกลาง	10.106.6.111	OpenSSL 1.0.2 < 1.0.2t Multiple Vulnerabilities	128115
ปานกลาง	10.106.6.111	OpenSSL 1.0.2 < 1.0.2w Information Disclosure	146374
ปานกลาง	10.106.6.111	OpenSSL 1.0.2 < 1.0.2x Null Pointer Dereference Vulnerability	144053
ปานกลาง	10.106.6.111	OpenSSL 1.0.2 < 1.0.2y Multiple Vulnerabilities	146591

หลักการทำงานของ NAS



บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน

- ข้อมูลมีการจัดเก็บในเครื่องคอมพิวเตอร์ของผู้ใช้งาน และมีการสำรองข้อมูลดังกล่าวไว้บน NAS เป็นการป้องกันความเสียหายของข้อมูล และเป็นสร้าง SnapShot และป้องกันความเสียหายจากไวรัส

บน NAS

- รับส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ของผู้ใช้งานกับ NAS มีการเข้ารหัส AES-256 ซึ่งสามารถป้องกันการแฮกข้อมูล

ระบบจัดเก็บข้อมูลบนระบบ CLOUD ในภาพรวม ทร

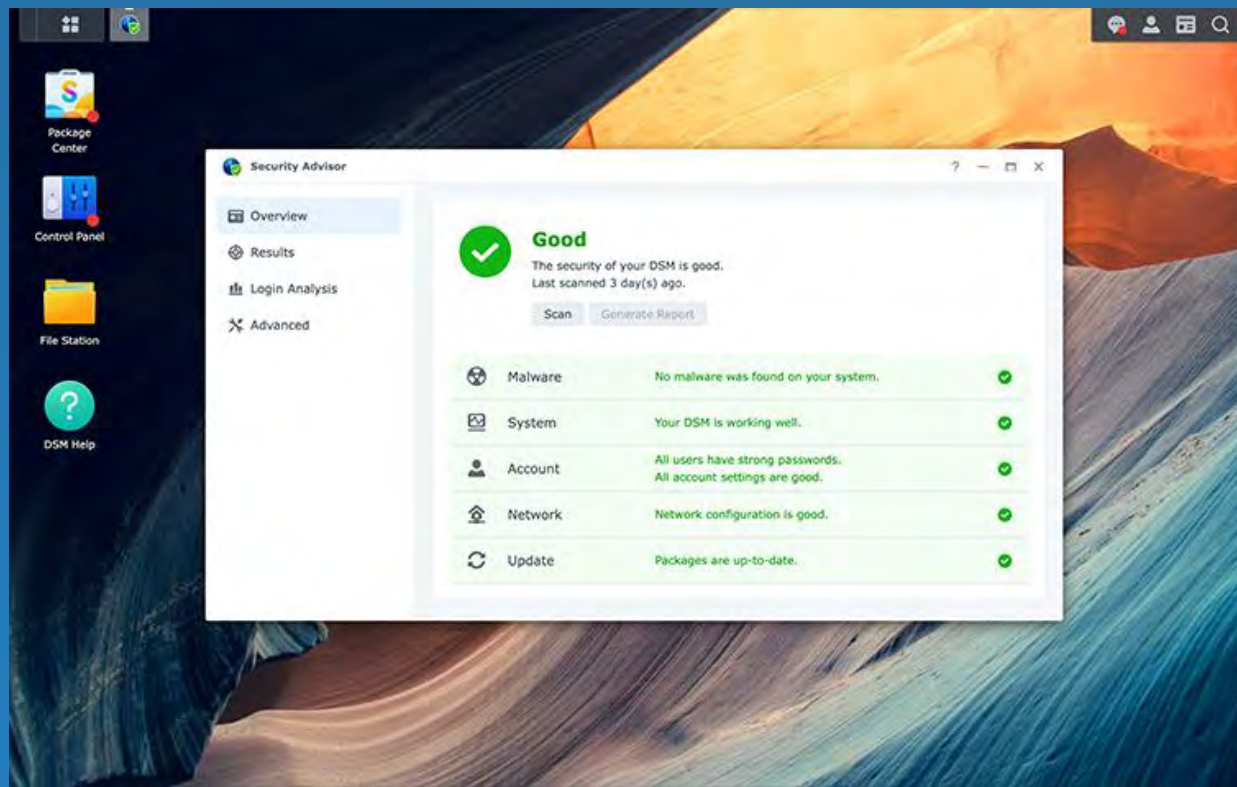


- เป็นระบบ Synology NAS
- มี log ที่สามารถติดตามการ ลบ แก้ไข ไฟล์
- สามารถกำหนดขนาดพื้นที่จัดเก็บข้อมูลของแต่ละผู้ใช้งาน
- ผู้ใช้งานสามารถกำหนดสิทธิ์ให้ผู้ใช้งานรายอื่นเข้าถึงข้อมูลของตนเอง

ความปลอดภัยระบบ NAS

VIRUS

- ป้องกันจากแรนซัมแวร์ ด้วยการสแกนไฟล์ใน Server ด้วย Antivirus

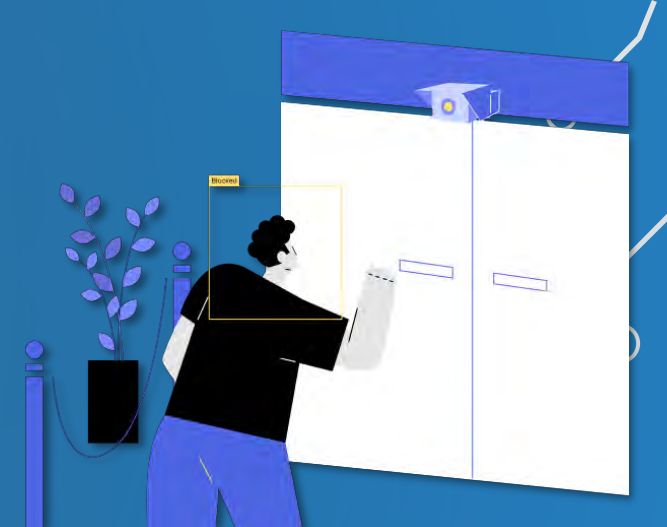


ความปลอดภัยระบบ NAS

- มีการอัปเดตด้านความปลอดภัยของ Synology nas



Advisory	Severity	Status	Last Updated
Synology-SA-23:08 SRM	Moderate	Ongoing	2023-06-13 15:24:48 UTC+8
Synology-SA-23:07 DSM	Moderate	Resolved	2023-06-13 15:24:31 UTC+8
Synology-SA-23:06 SRM	Moderate	Ongoing	2023-06-13 15:36:46 UTC+8
Synology-SA-23:05 DSM	Moderate	Resolved	2023-06-13 15:36:32 UTC+8
Synology-SA-23:04 VPN Plus Server	Moderate	Ongoing	2023-05-04 15:09:58 UTC+8
Synology-SA-23:03 Netatalk	Not affected	Resolved	2023-03-30 16:37:45 UTC+8
Synology-SA-23:02 Sudo	Low	Ongoing	2023-03-30 16:17:07 UTC+8
Synology-SA-23:01 ClamAV	Critical	Resolved	2023-03-16 09:55:19 UTC+8
Synology-SA-22:26 VPN Plus Server	Critical	Resolved	2023-01-03 13:27:44 UTC+8
Synology-SA-22:25 SRM	Critical	Resolved	2023-05-16 16:15:13 UTC+8
Synology-SA-22:24 Samba AD DC	Important	Resolved	2023-05-22 15:34:54 UTC+8
Synology-SA-22:23 PWN2OWN TORONTO 2022	Important	Resolved	2023-06-09 11:29:19 UTC+8
Synology-SA-22:22 Samba	Not affected	Resolved	2022-12-26 10:11:19 UTC+8
Synology-SA-22:21 OpenSSL	Not affected	Resolved	2022-11-02 10:46:49 UTC+8
Synology-SA-22:20 Samba	Moderate	Resolved	2023-05-22 15:32:29 UTC+8
Synology-SA-22:19 Presto File Server	Moderate	Resolved	2022-10-26 18:04:54 UTC+8
Synology-SA-22:18 DSM	Moderate	Resolved	2022-10-25 10:56:21 UTC+8



ป้องกันความเสี่ยงด้านความปลอดภัยของระบบ NAS



การป้องกันระดับระบบ

- สร้างกฎไฟร์วอลล์ บล็อก IP แอดเดรสโดยอัตโนมัติเมื่อมีความพยายามลงชื่อเข้าใช้ที่ล้มเหลวมากเกินไป และเปิดใช้งานการปกป้องบัญชีเพื่อลดภัยคุกคามของการโจมตีแบบ Brute-Force จากไคลเอนต์ที่ไม่ได้รับความเชื่อถือ



การป้องกันระดับผู้ใช้

- เพิ่มการรักษาความปลอดภัยอีกชั้นหนึ่ง หลีกเลี่ยงการรั่วไหลของข้อมูลยืนยันตัวตน การตั้งค่าสิทธิ์ระดับผู้ใช้สามารถนำไปใช้กับการจำกัดการเข้าถึงไฟล์และพีเจอร์ในแต่ละโฟลเดอร์หรือแอปพลิเคชัน

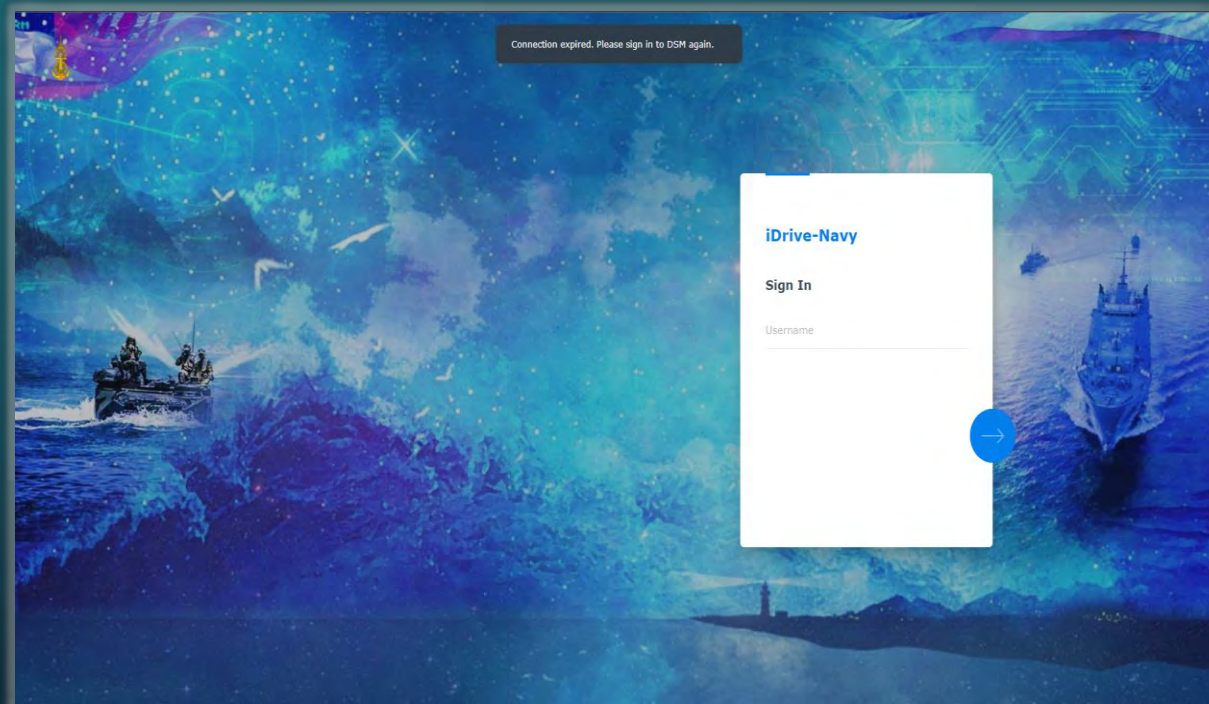


การเข้ารหัสที่ผ่านการรับรองและเชื่อถือได้

- การเข้ารหัส AES-256 ที่ฝังไคลเอนต์

การใช้งานระบบจัดเก็บข้อมูลในระบบ CLOUD

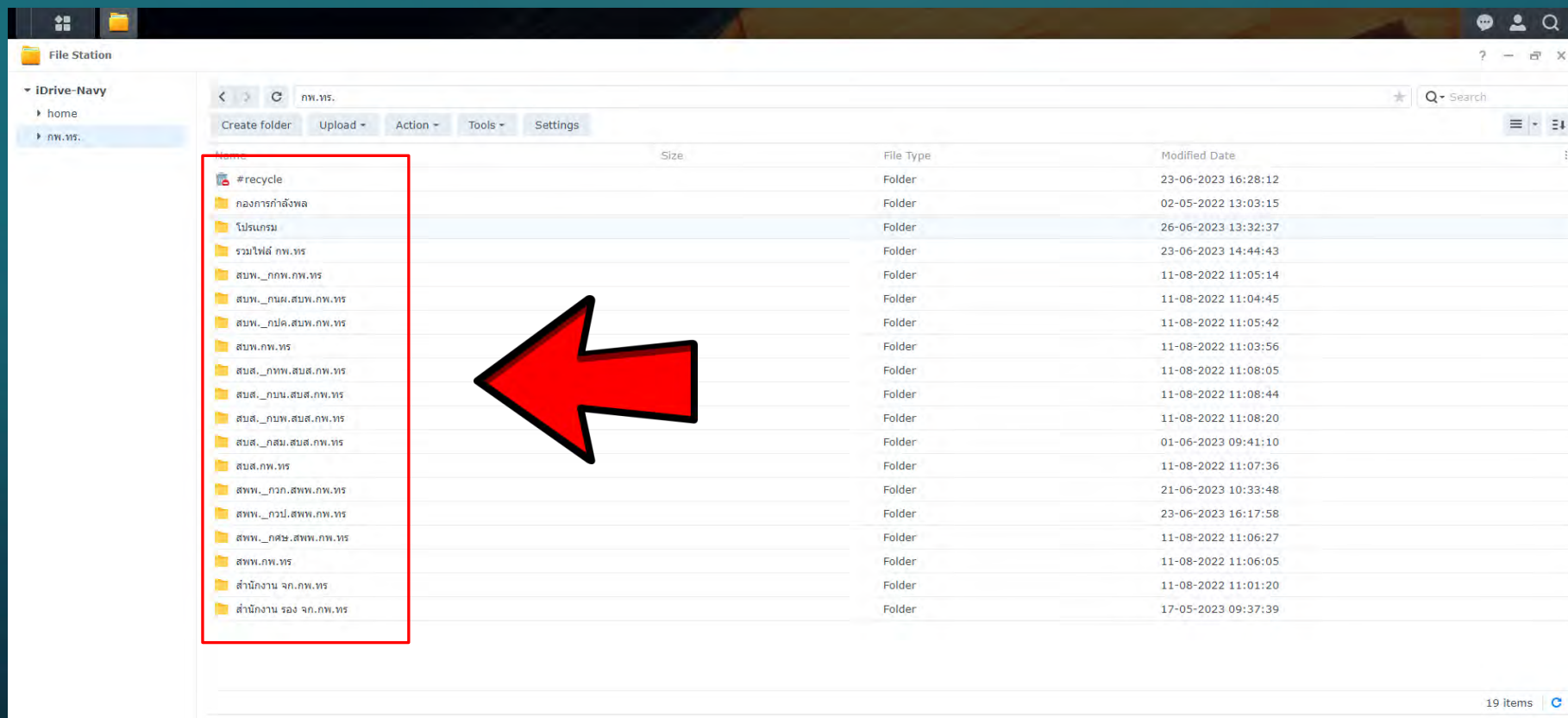
- เข้าไปที่ URL: drive.navy.mi.th ล็อกอินด้วย Username และ Password ที่ได้รับจัดสรรให้



ดับเบิลคลิกเข้าที่ “FILE STATION”

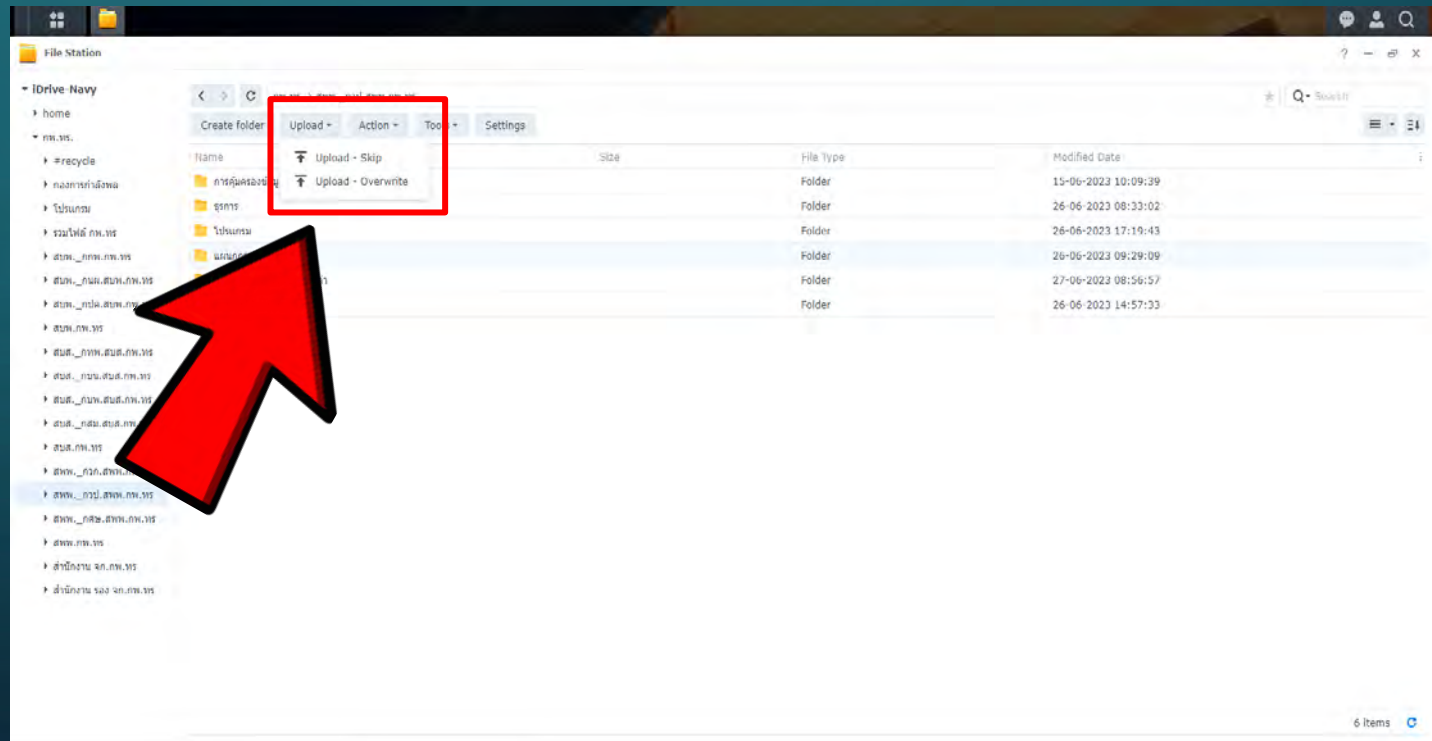


โพลเดอร์ แต่ละกอง ในหน่วย กพ.ทร.

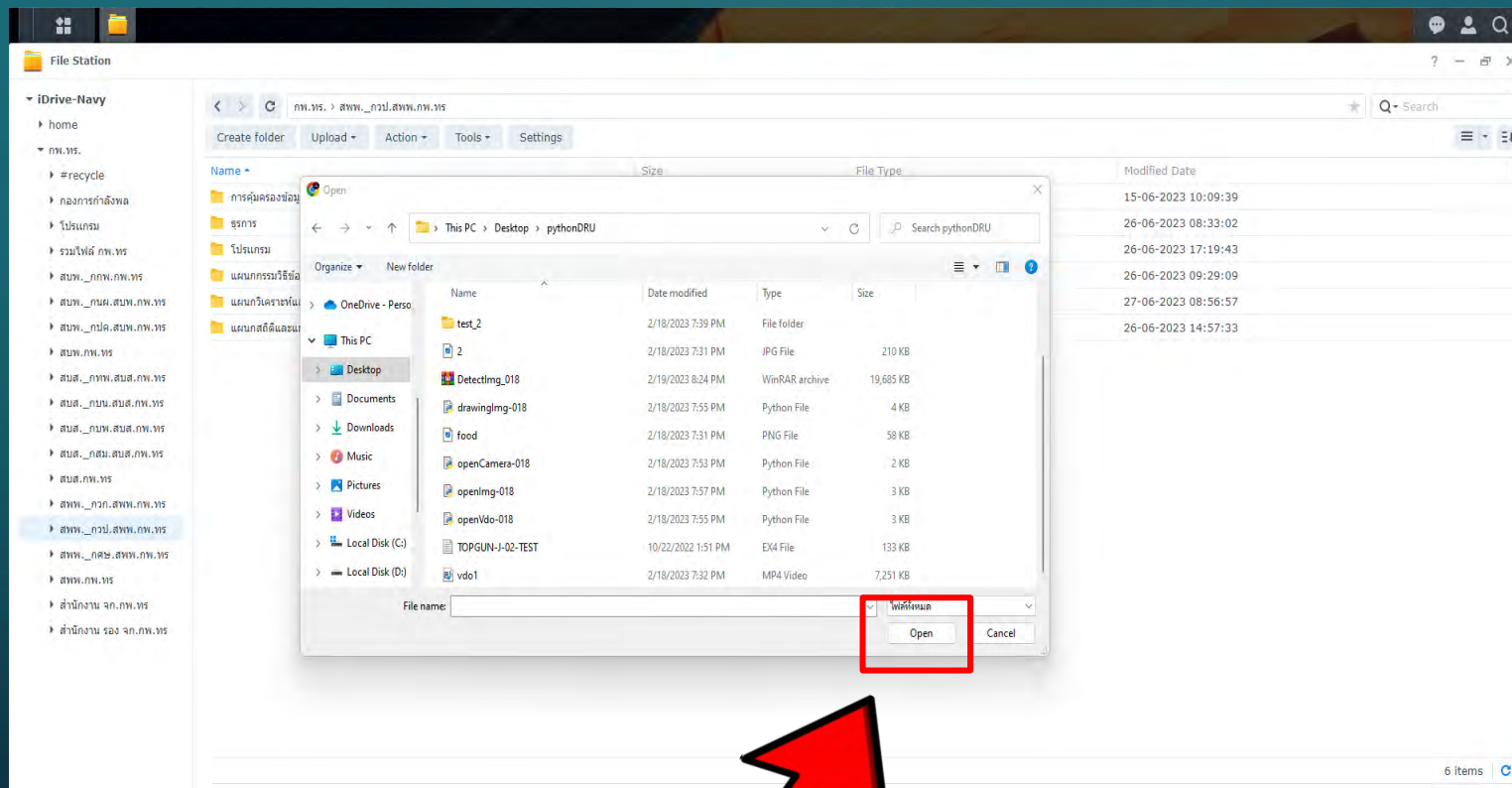


การ UPLOAD FILE

- ดับเบิ้ลคลิกเข้าไปยังโฟลเดอร์ที่ต้องการอัปโหลดไฟล์ จากนั้นกดที่เมนู “Upload” เลือก “Upload - Skip” หรือ “Upload - Overwrite”

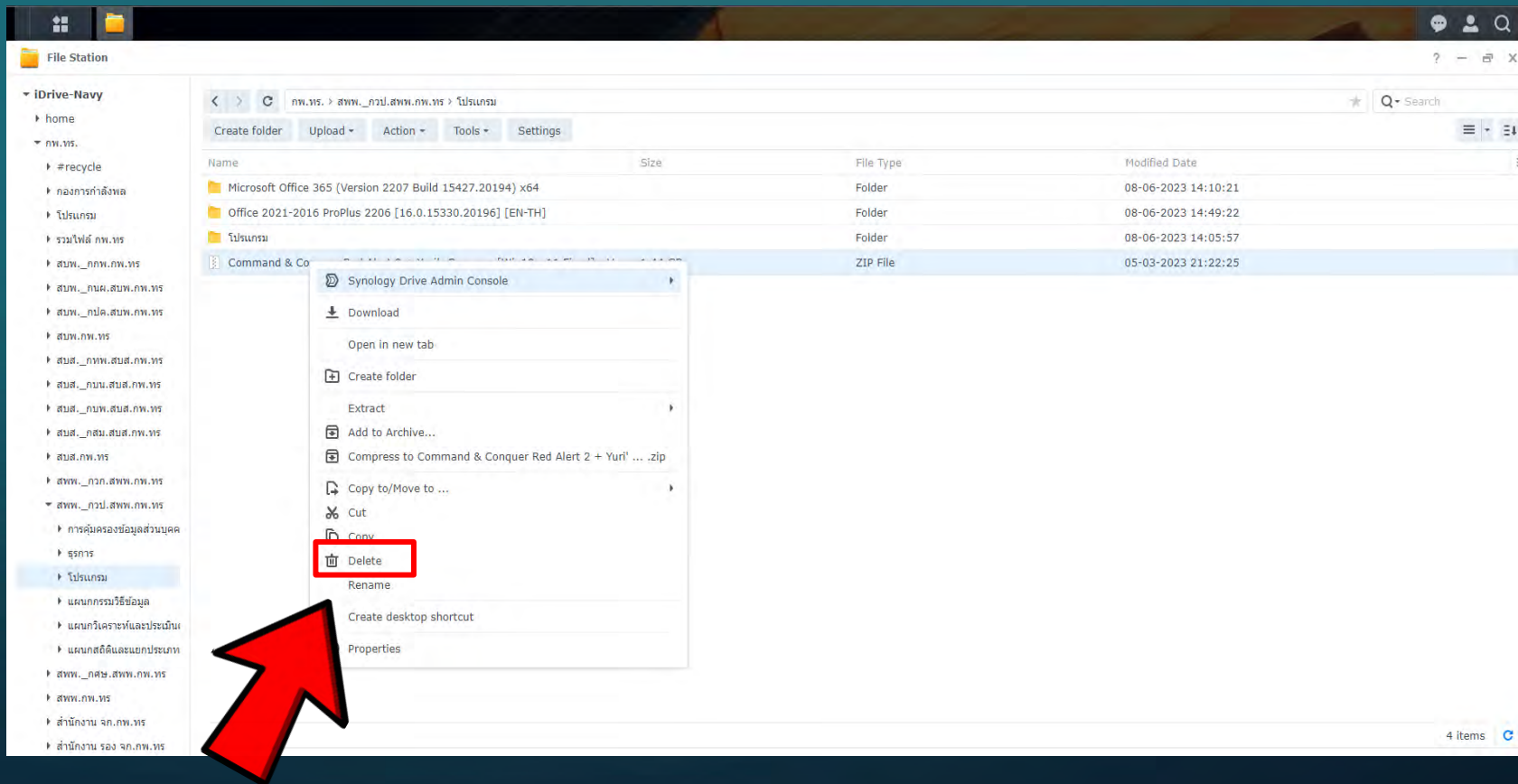


เลือกไฟล์ที่ต้องการอัปโหลดแล้วกด “OPEN”



การลบไฟล์

- การลบไฟล์สามารถทำได้โดยเลือกไฟล์ที่ต้องการ คลิกขวา กดปุ่ม “Delete”



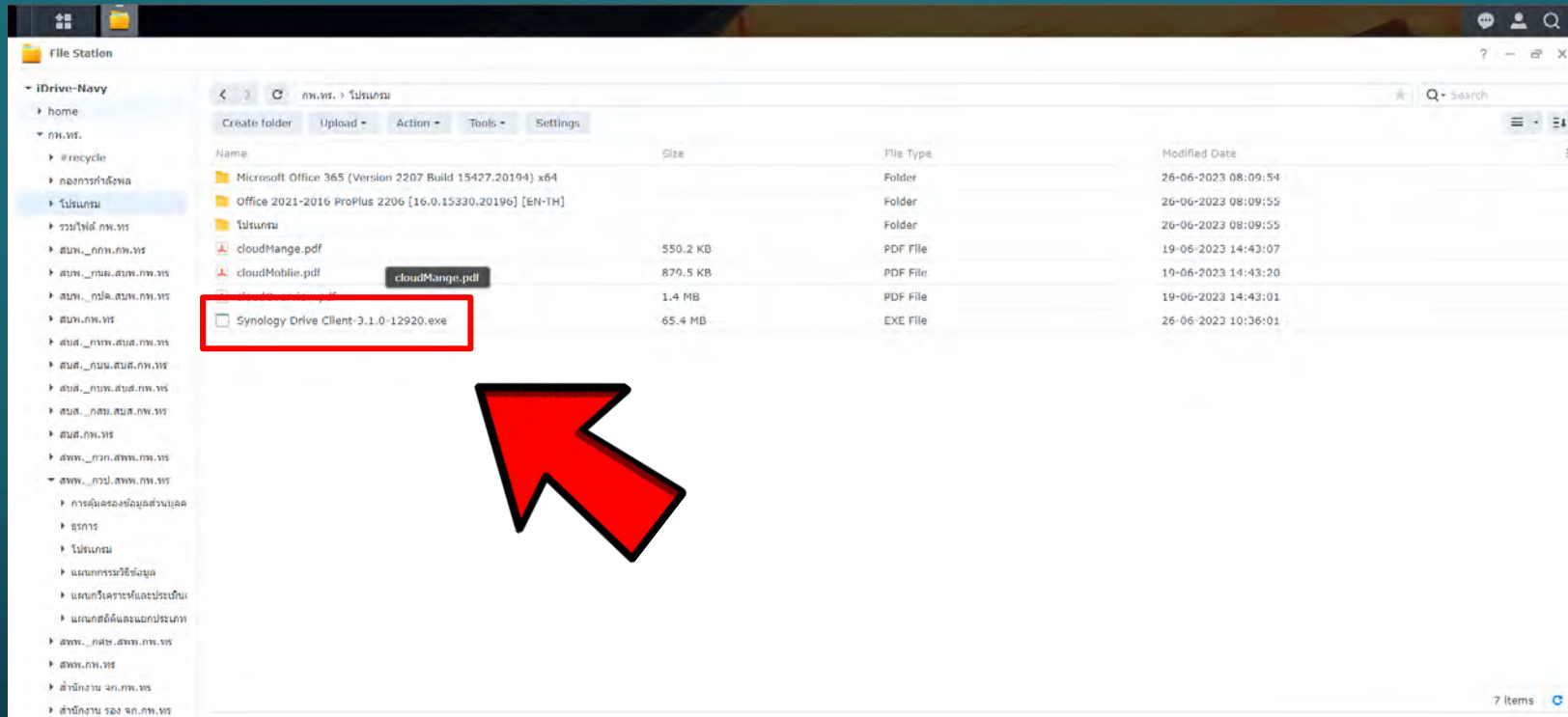
การใช้งานระบบ CLOUD ผ่านโปรแกรม SYNOLOGY DRIVE CLIENT บน อุปกรณ์คอมพิวเตอร์

โปรแกรม Synology Drive Client จะแบ่งฟังก์ชันการใช้งานออกเป็น ๒ ฟังก์ชันหลักคือ Sync Task และ Backup Task

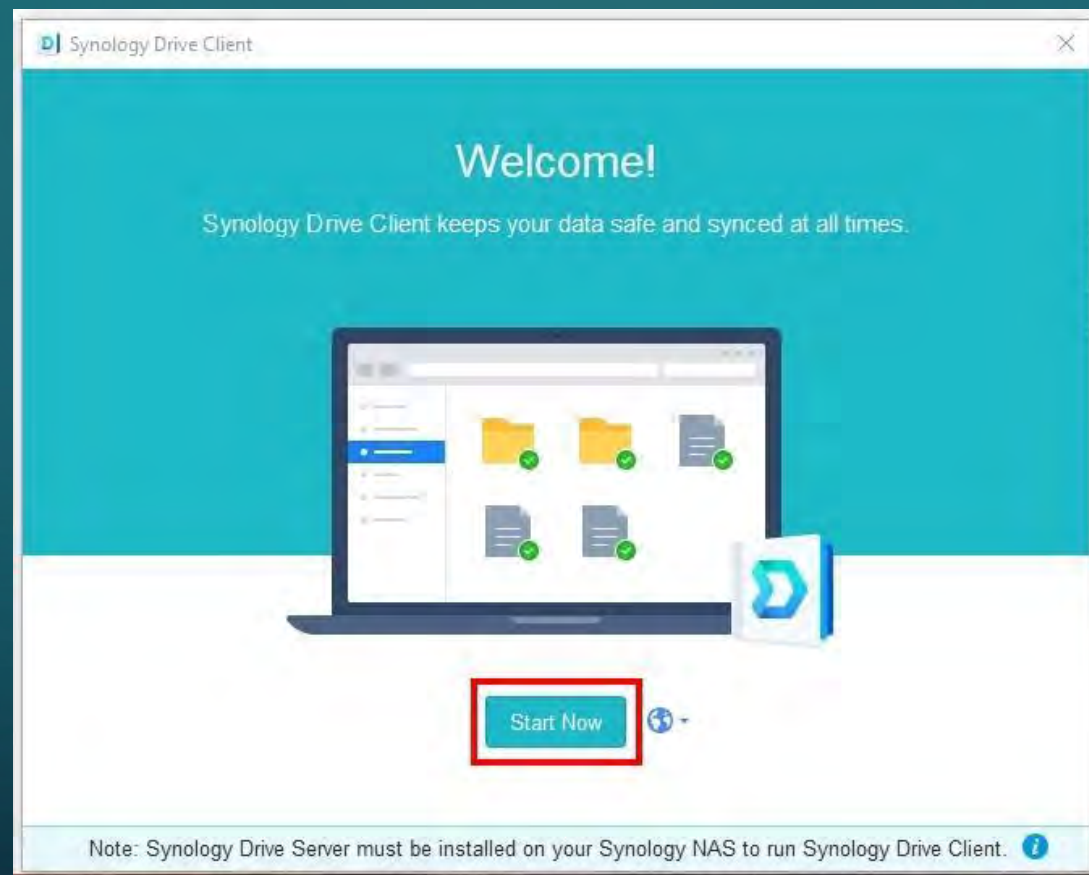
๑. Sync Task จะเป็นการอัปเดตไฟล์ขึ้นไปบนคลาวด์แบบ real time
๒. Backup Task จะเป็นการสำรองไฟล์โดยอัปเดตไฟล์ขึ้นไปบนคลาวด์ สามารถเลือกให้อัปเดตเมื่อมีการเปลี่ยนแปลงข้อมูลไฟล์จากเครื่องต้นทางหรือกำหนดช่วงเวลาไว้



ดาวน์โหลดไฟล์ SYNOLGY DRIVE CLIENT-3.1.0-12920 จากระบบ CLOUD และติดตั้งบนเครื่องคอมพิวเตอร์



เลือกภาษาที่ต้องการโดยกดที่รูปโลก จากนั้น กด “START NOW”



กรอกข้อมูลดังกล่าว SYNOLGY NAS จะต้องเป็น “ROYALTHAINAVY” หรือ “DRIVE.NAVY.MI.TH” โดยใช้ USERNAME และ PASSWORD ตามที่ได้รับจัดสรร จากนั้นกด “NEXT”

Synology Drive Client

Connect to your Synology NAS

Synology NAS: royalnavy01

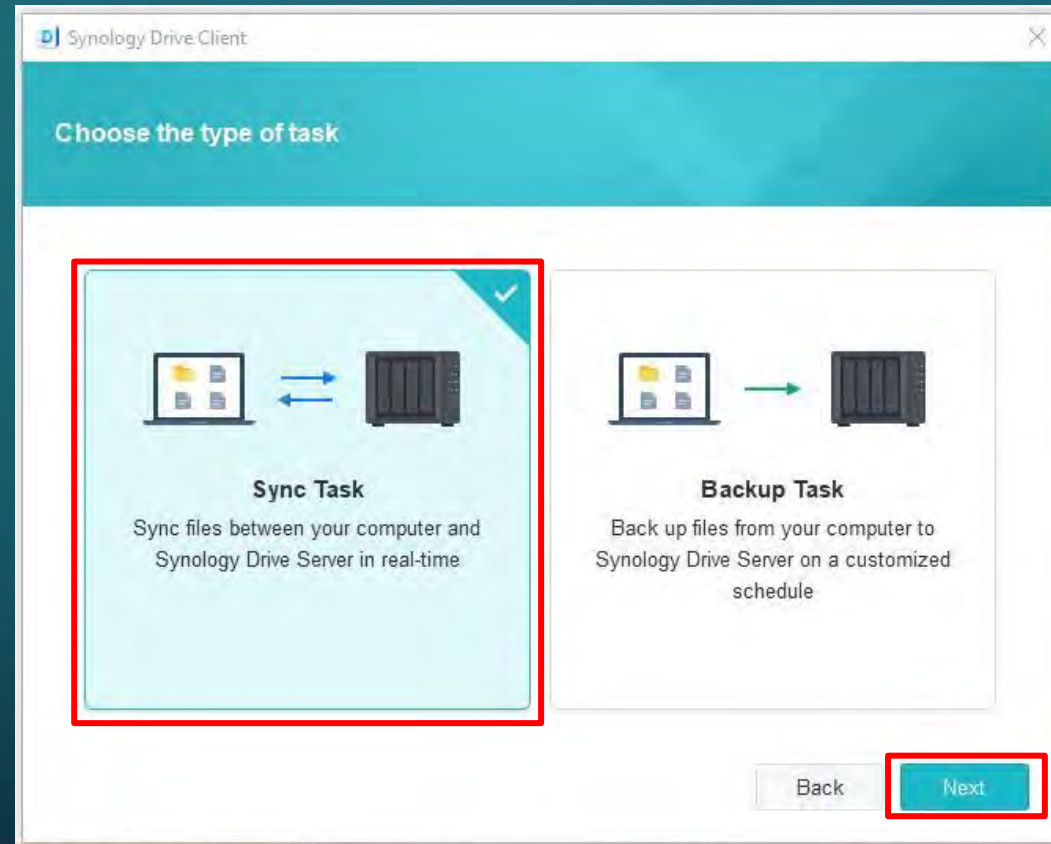
Username:

Password:

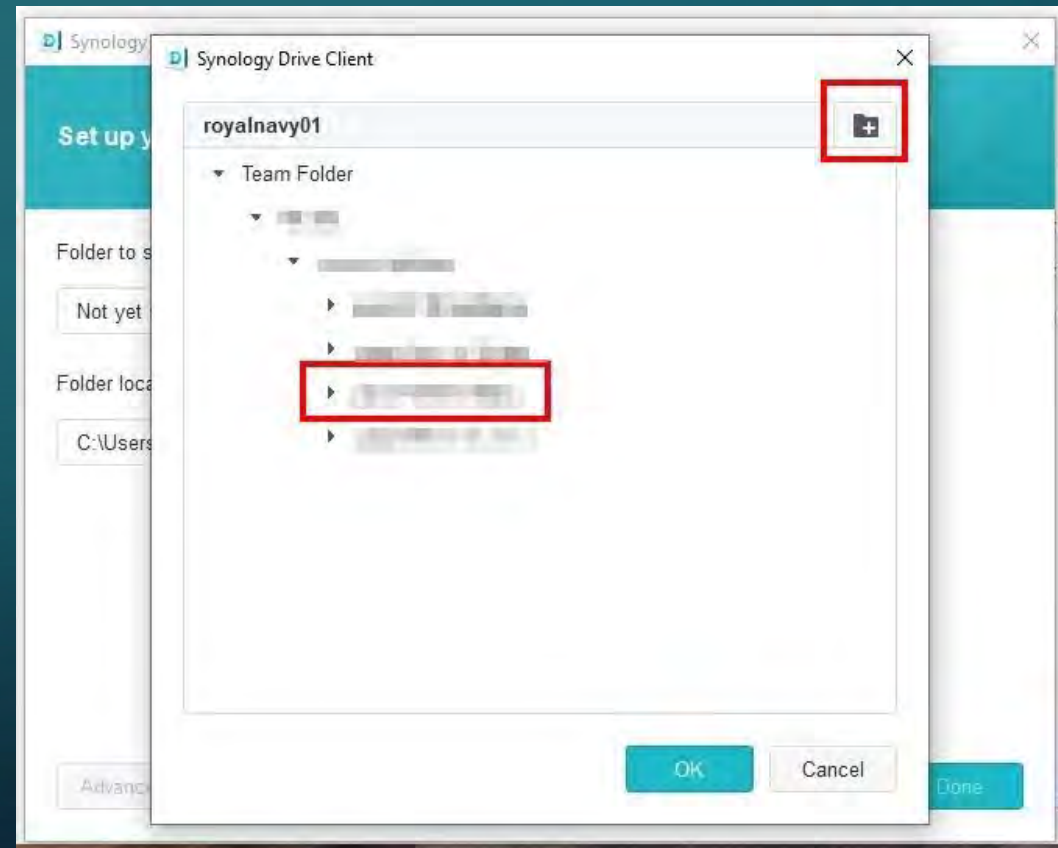
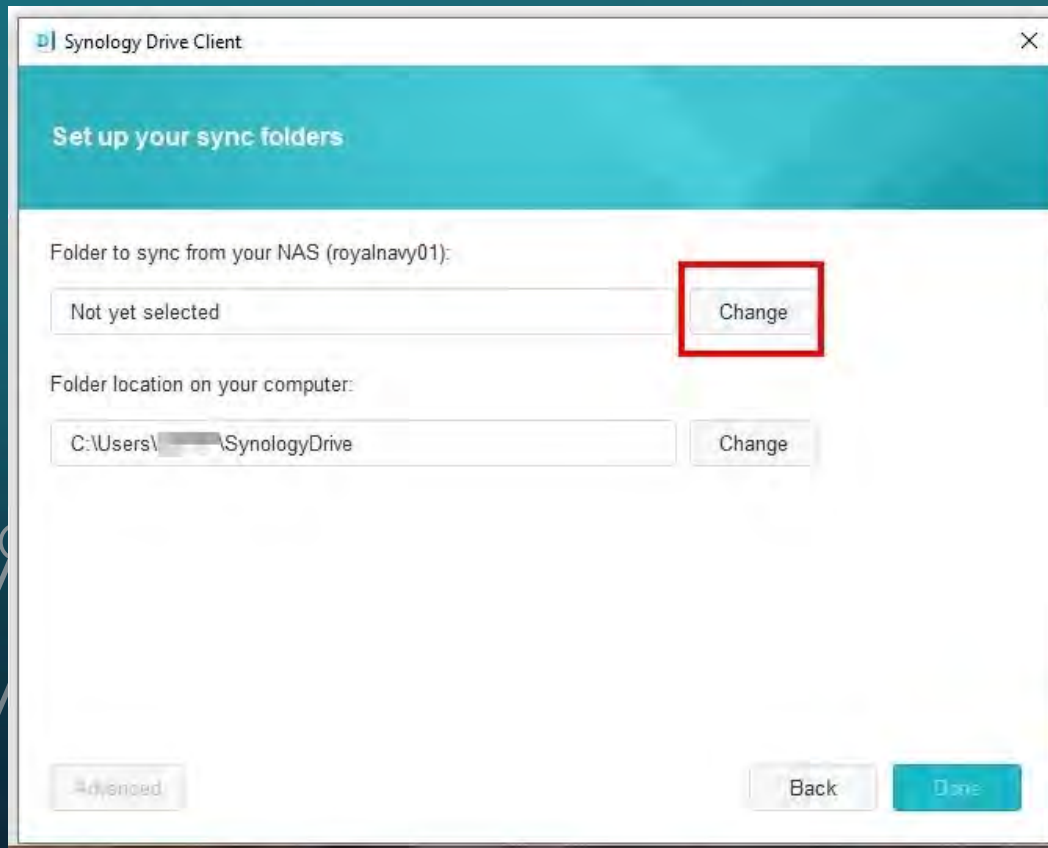
Enable SSL data transmission encryption

Proxy Back Next

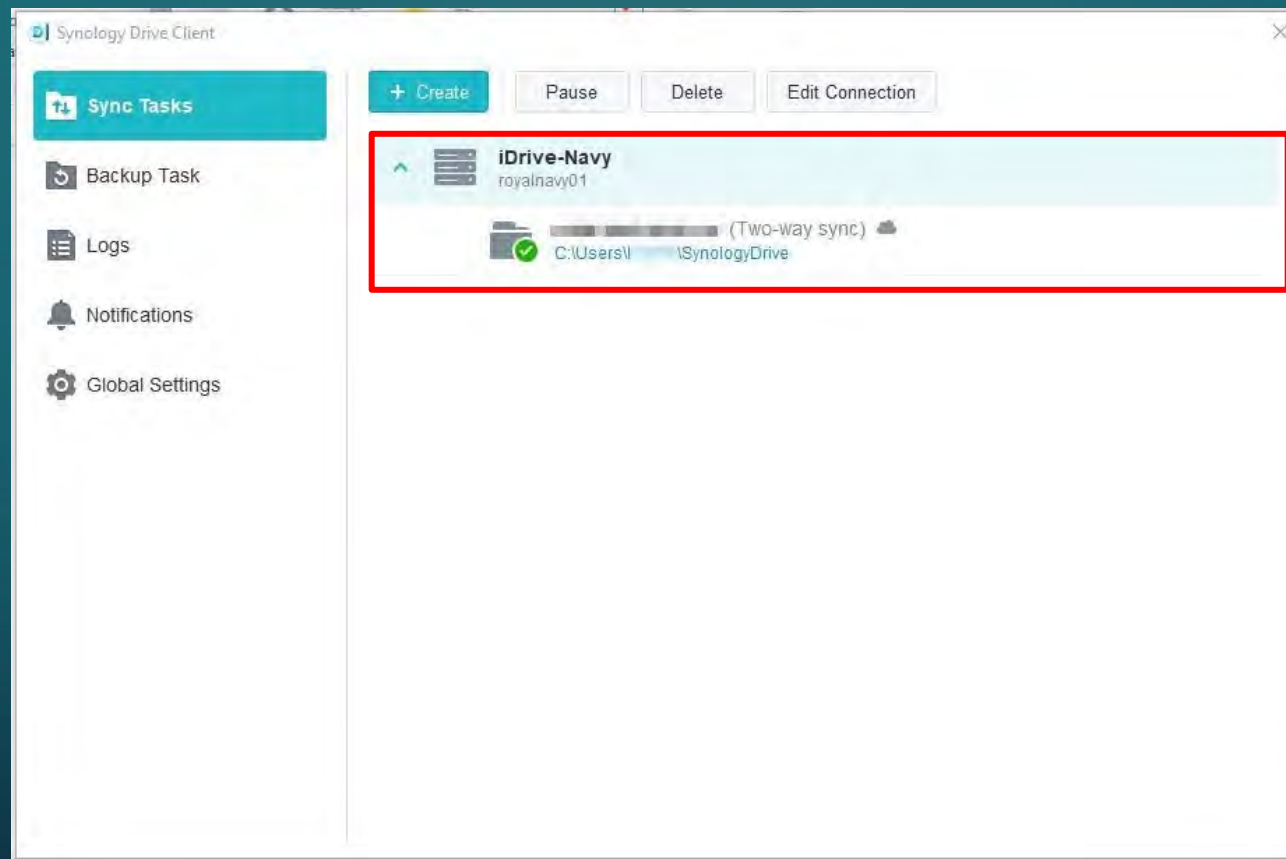
การเลือกรูปแบบในการจัดเก็บข้อมูล ทั้งนี้เพื่อให้ง่ายต่อการใช้งานและสามารถจัดเก็บข้อมูลได้แบบ REAL TIME ให้เลือก เป็นแบบ SYNC TASK จากนั้นกด “NEXT”



- เลือกโฟลเดอร์ที่ใช้จัดเก็บข้อมูลในระบบ Cloud โดยกด Change ตามภาพ
- เลือกโฟลเดอร์ที่ต้องการหรือหากต้องการสร้างโฟลเดอร์ใหม่ ให้กดไอคอนที่มุมขวาด้านบนตามภาพ จากนั้นกด “OK” และกด “Done”



เมื่อเสร็จสิ้นจะปรากฏชื่อโพลเดอร์ที่ใช้สำหรับการซิงค์



การกำหนดสิทธิ์ในการเข้าไฟล์เดออร์ในระบบ CLOUD



The screenshot displays a File Station interface with a file list and a Properties dialog box. The file list includes:

Name	Modified Date
Microsoft Office 365 (Version 2207 Build 1542)	26-06-2023 08:09:54
Office 2021-2016 ProPlus 2206 [16.0.15330.2]	26-06-2023 08:09:55
โปรแกรม	26-06-2023 08:09:55
cloudMange.pdf	19-06-2023 14:43:07
cloudMobile.pdf	19-06-2023 14:43:20
cloudOverview.pdf	19-06-2023 14:43:01
Synology Drive Client-3.1.0-12920.exe	26-06-2023 10:36:01

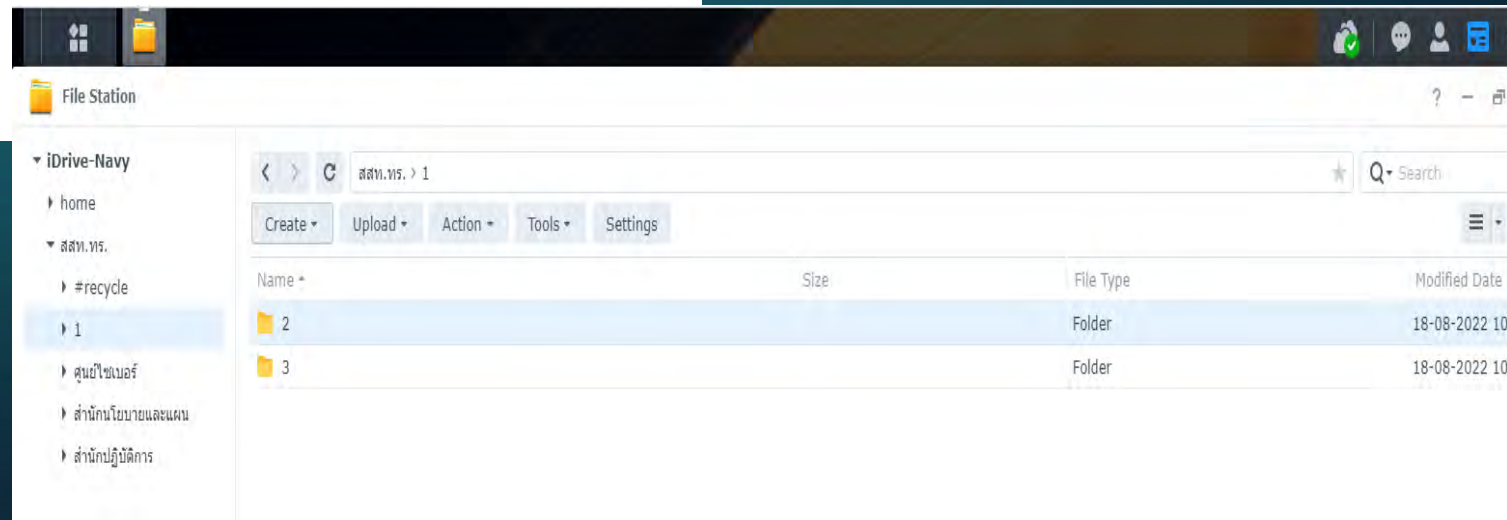
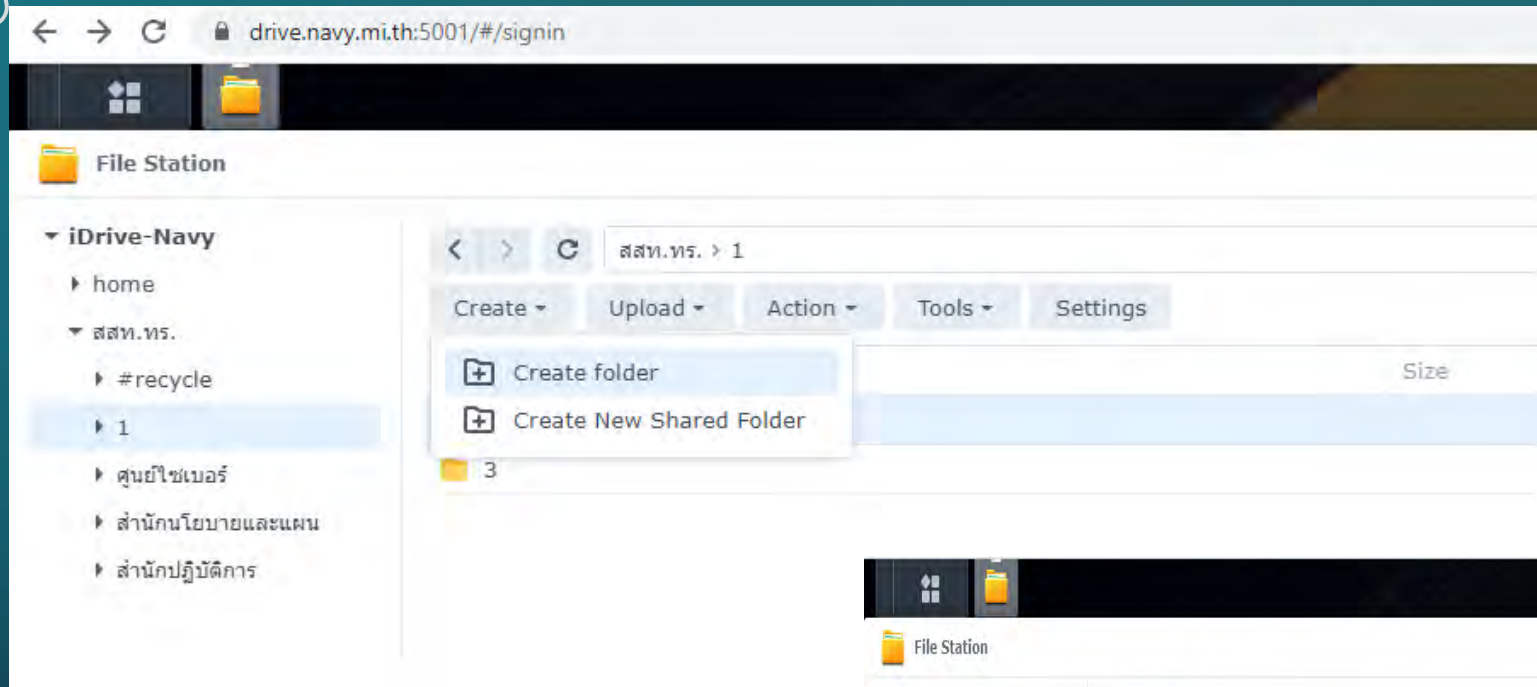
The Properties dialog box shows the Permission tab with the following table:

User or group	Type	Permission
SCTR001	Deny	Full Control
SCTR002	Deny	Full Control
kawincoet	Deny	Full Control
wichayakul.p	Deny	Full Control
no.vrs.	Deny	Full Control
nu.vrs.	Deny	Full Control
nvs.vrs.	Deny	Full Control
ns.	Deny	Full Control
nas.member	Deny	Full Control
on.vrs.	Deny	Full Control
os.vrs.	Deny	Full Control
os.vrs.	Deny	Full Control

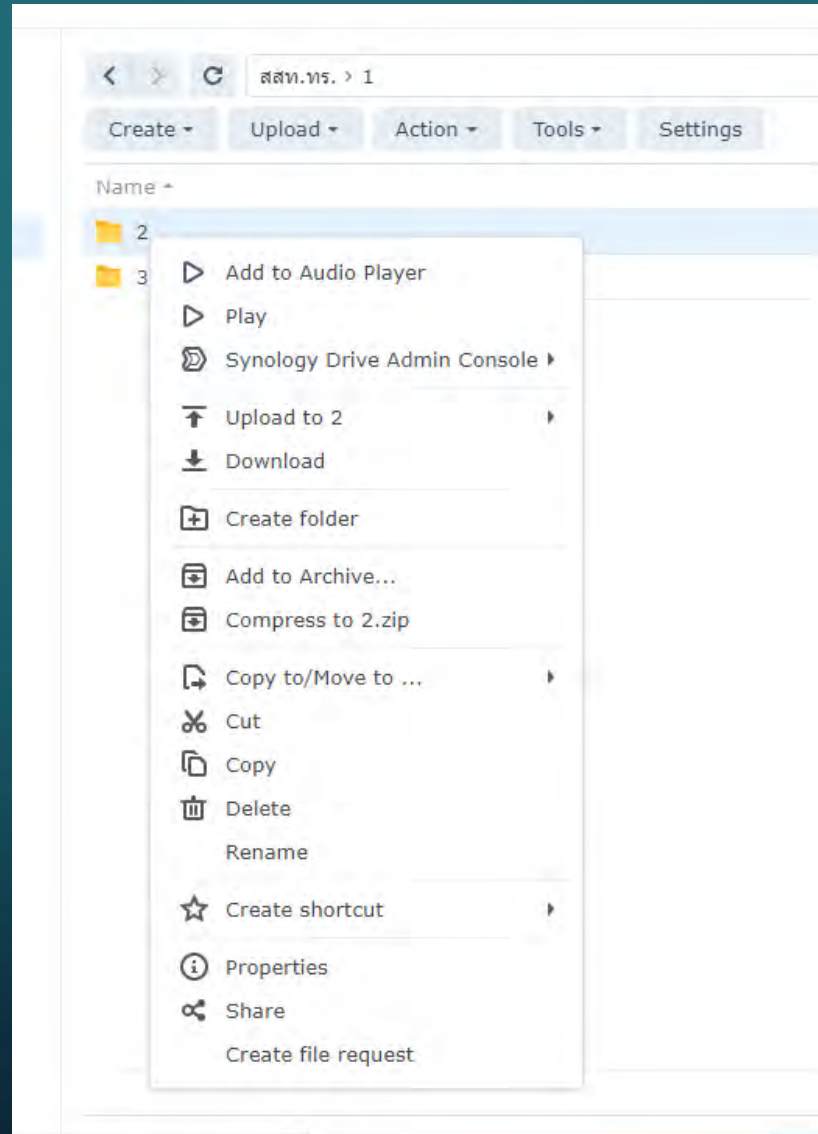
The dialog box also includes a checkbox for "Apply to this folder, sub-folders and files" and "Cancel" and "Save" buttons.



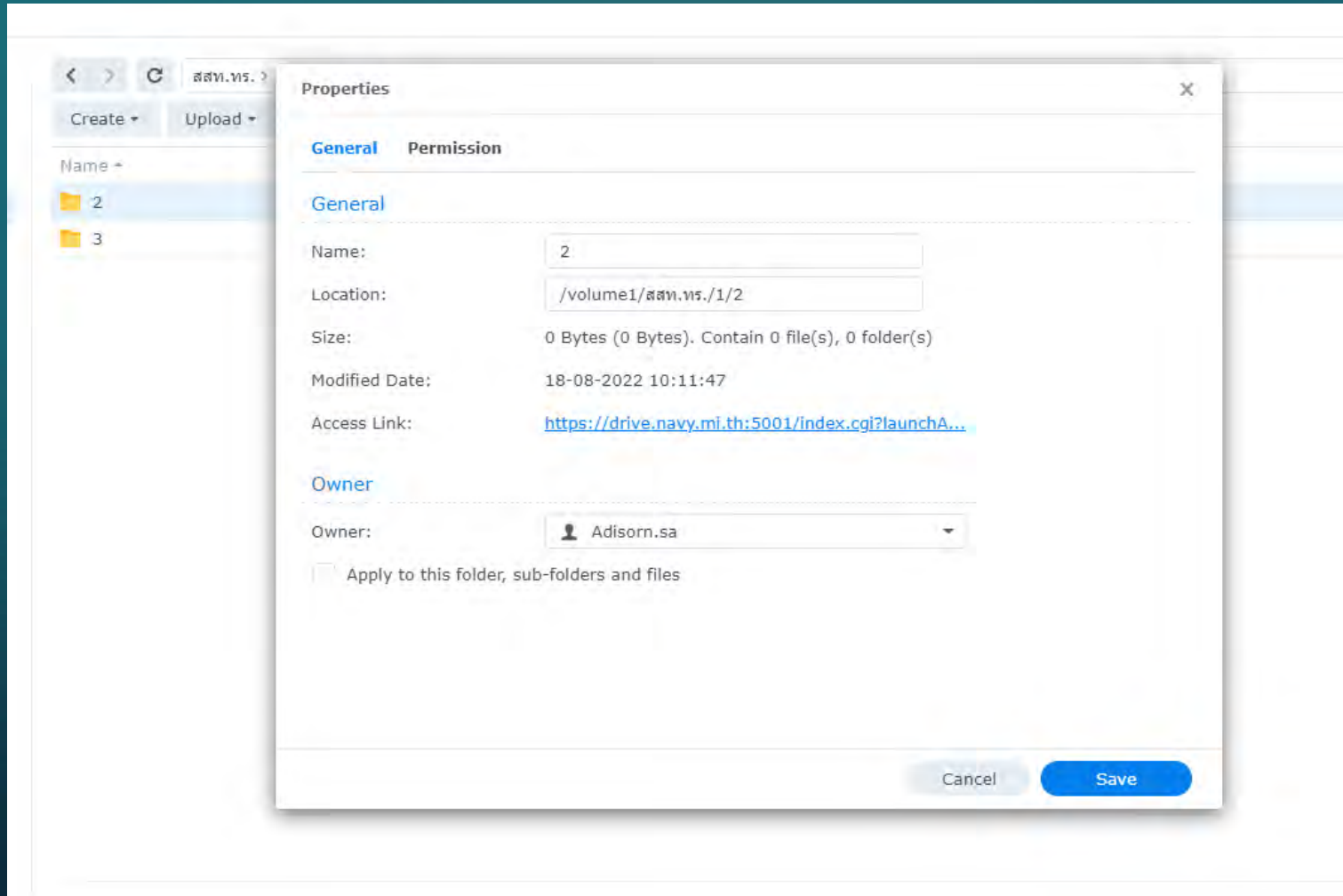
ทำการสร้าง FOLDER ที่ต้องการการเข้าถึง



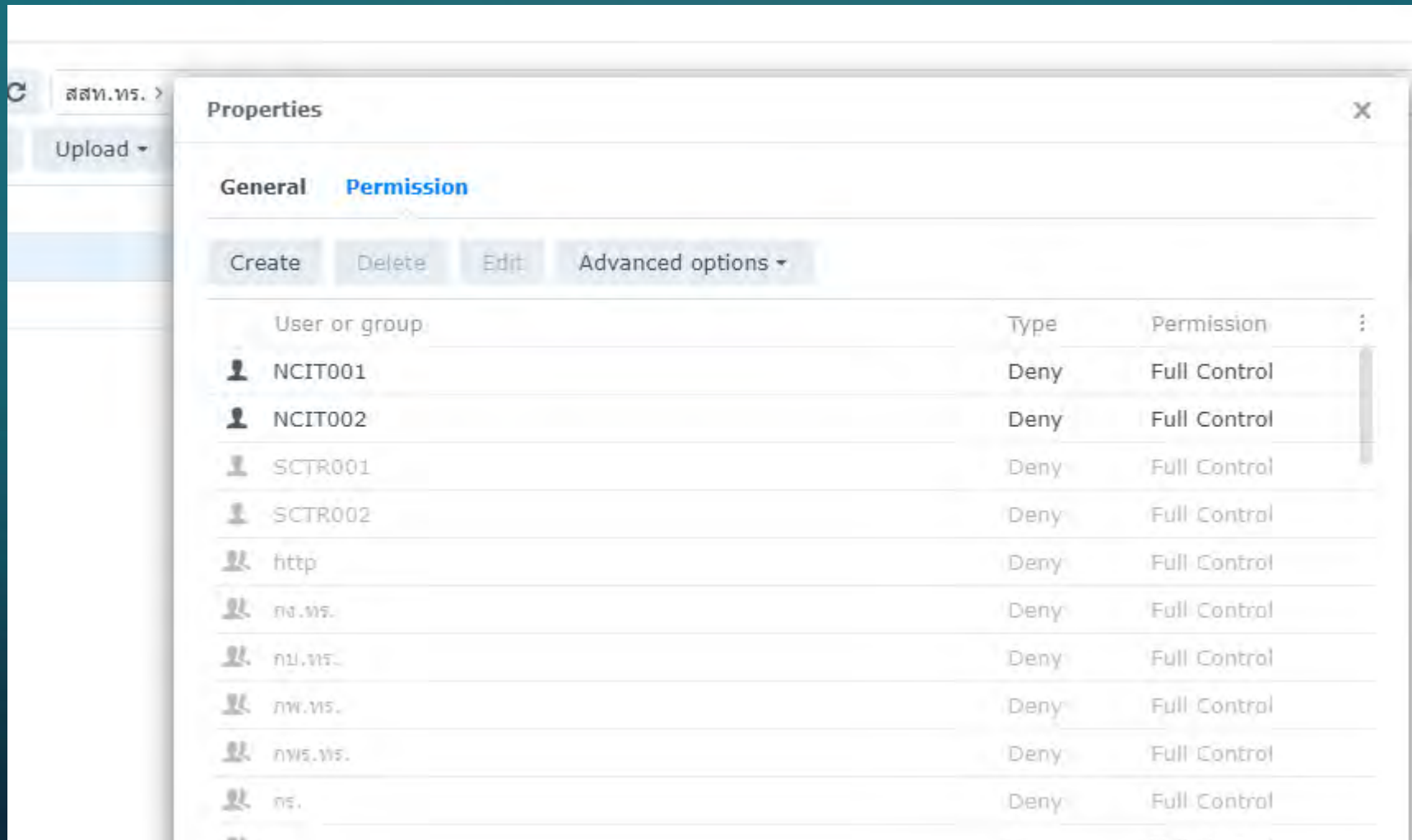
- เมื่อได้ FOLDER ที่ต้องการจากนั้นทำการกำหนด USER ที่ไม่ต้องการให้เข้าถึงโฟลเดอร์ดังกล่าวโดยทำการคลิกขวา
- เลือกเมนู PROPERTIES



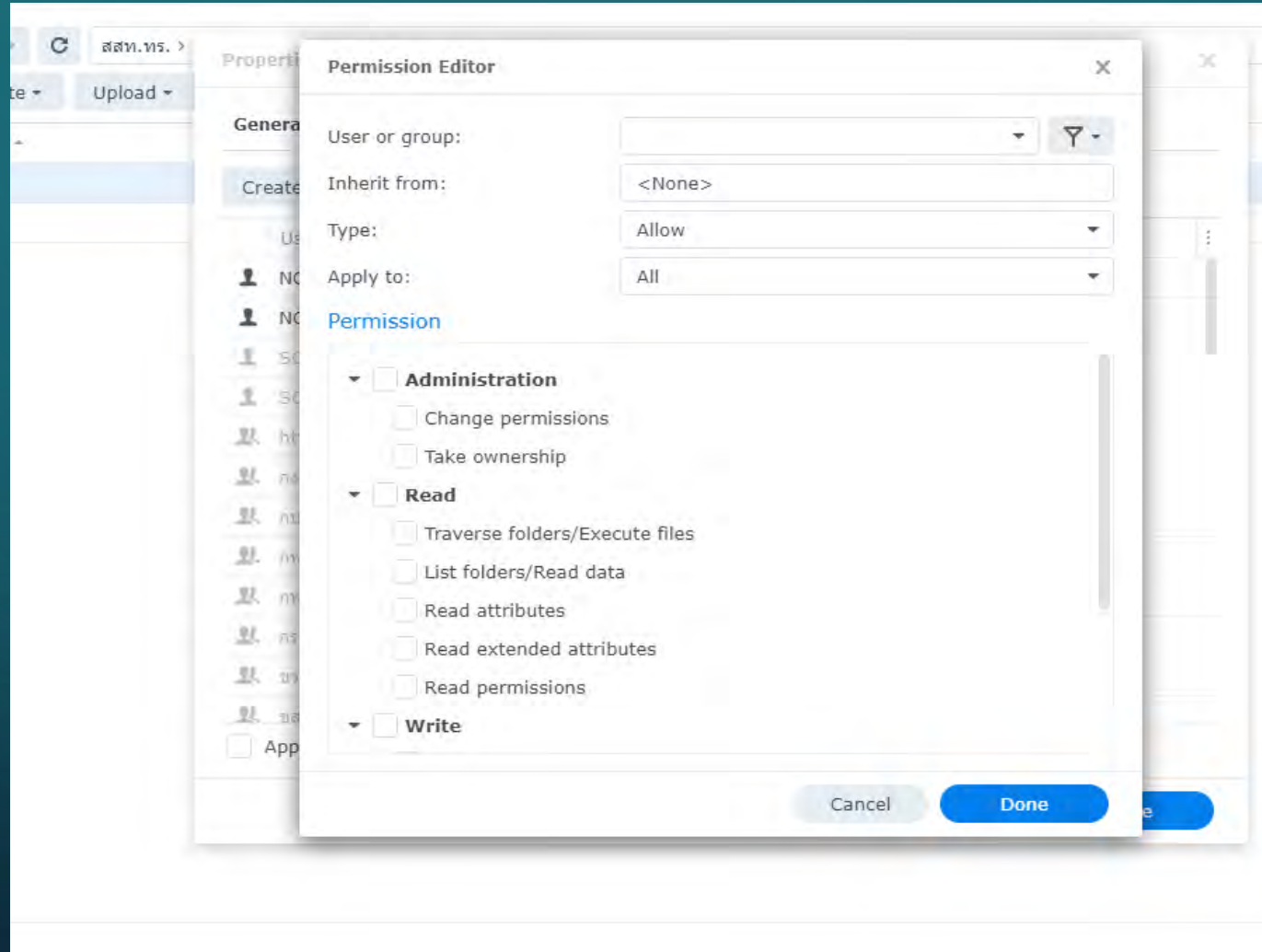
เลือกหัวข้อแถบ PERMISSION



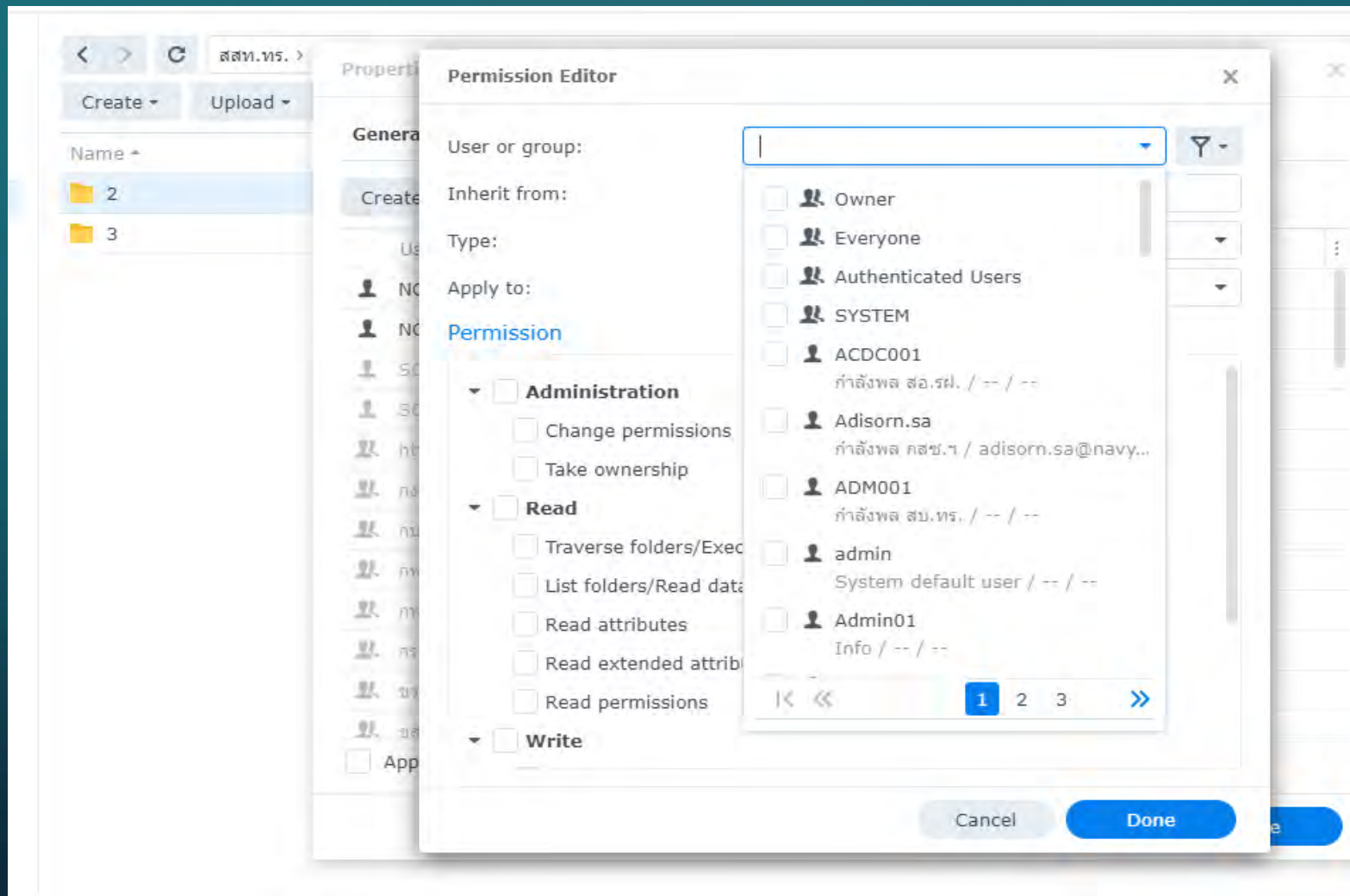
กดปุ่ม CREATE



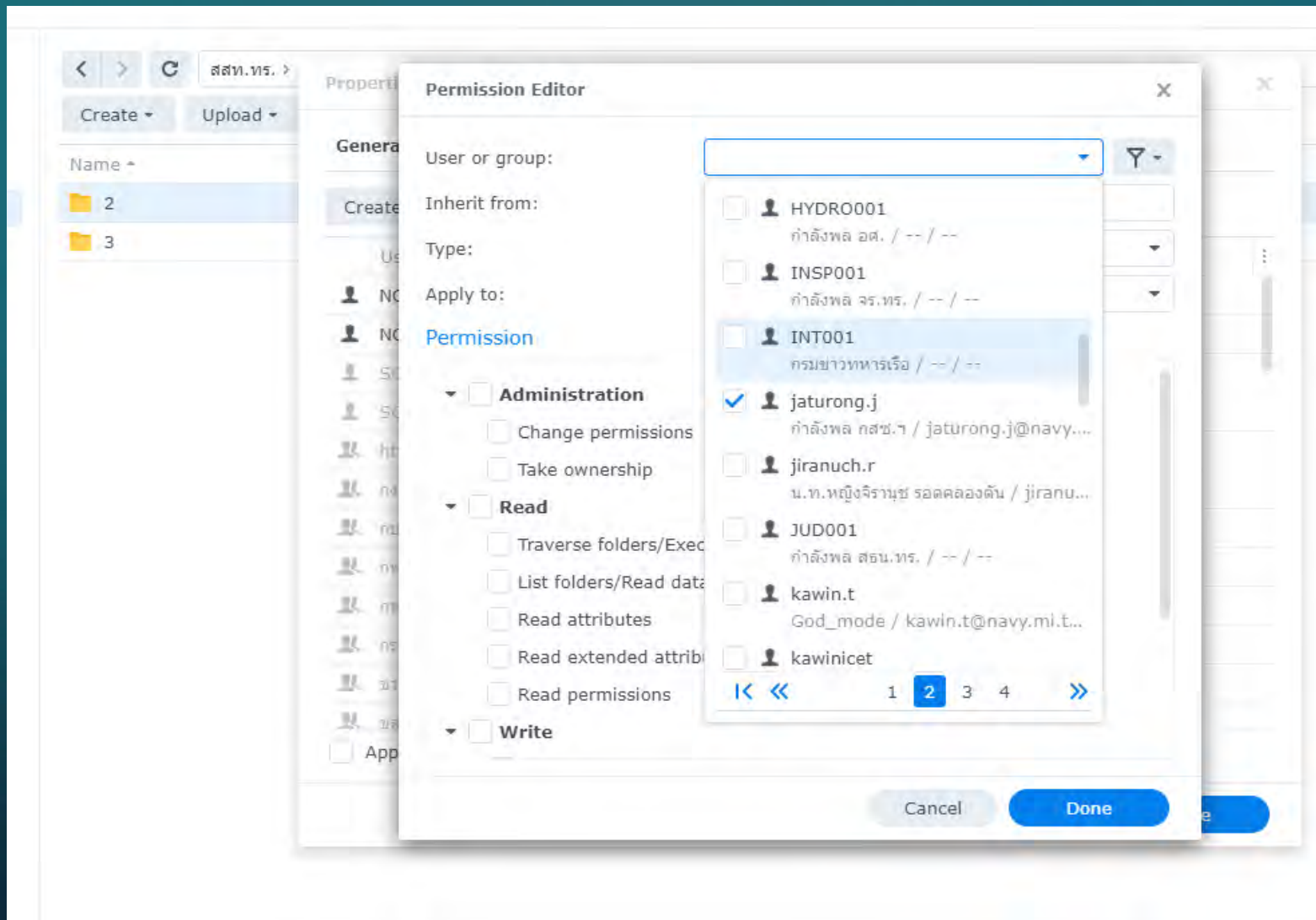
คลิกที่ลูกศร ในหัวข้อ **USER OR GROUP :**



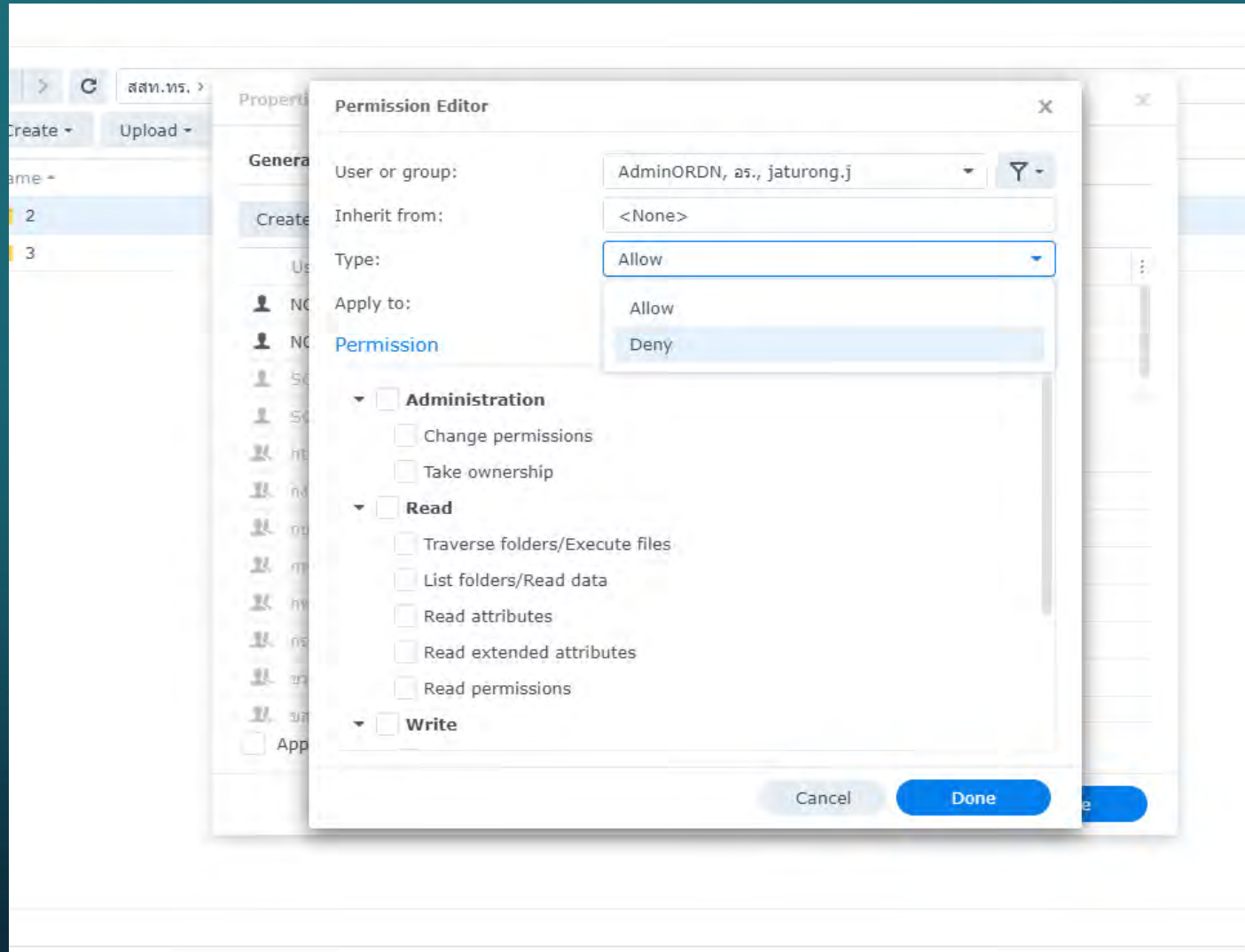
เลือกหน่วยหรือบุคคลที่ไม่ต้องการให้สิทธิ์เข้าถึงโดยเลือกที่ CHECK BOX ซึ่งสามารถเลือกได้ตามจำนวนที่ต้องการ



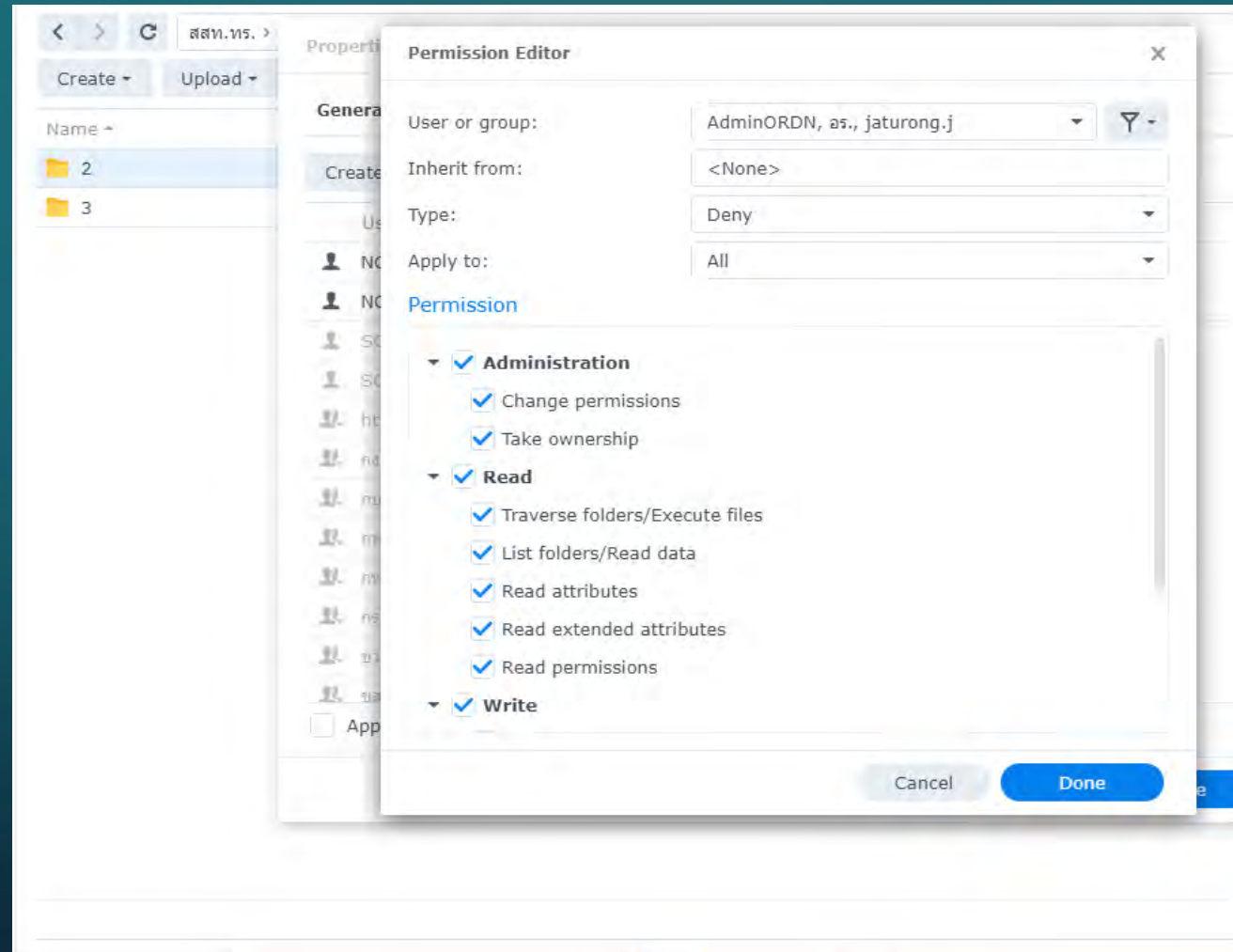
เมื่อได้แล้ว เลือก DONE



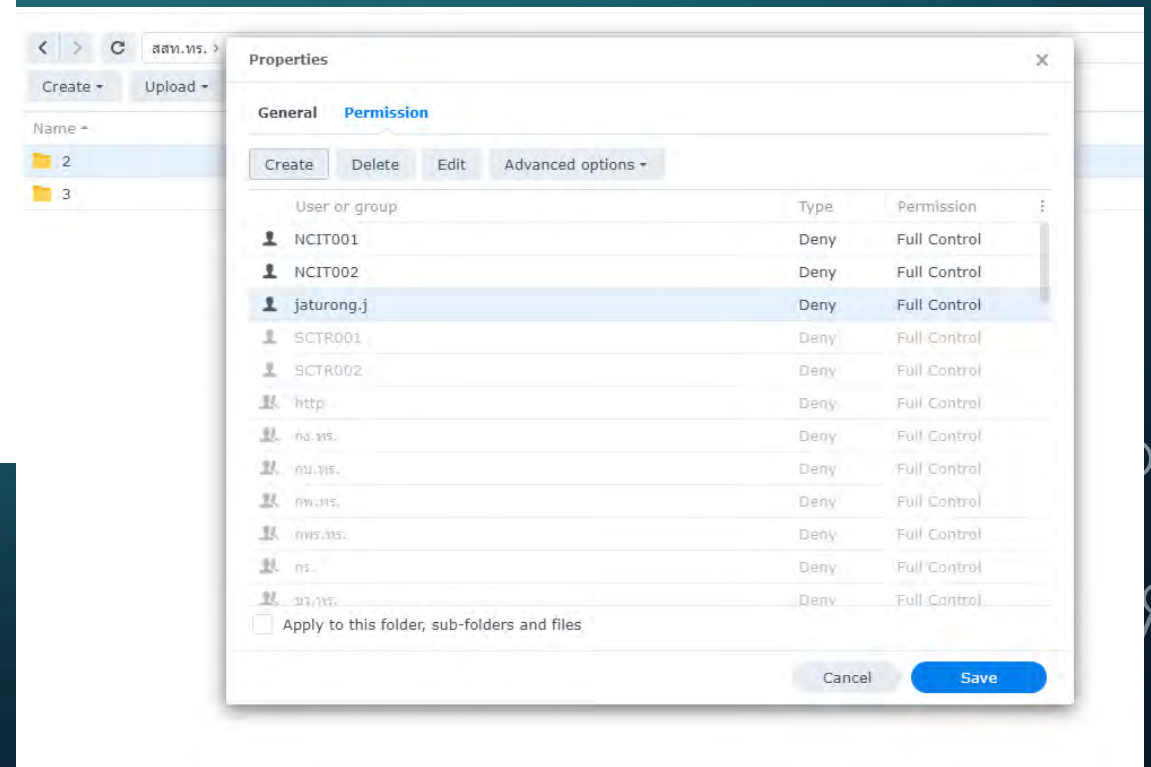
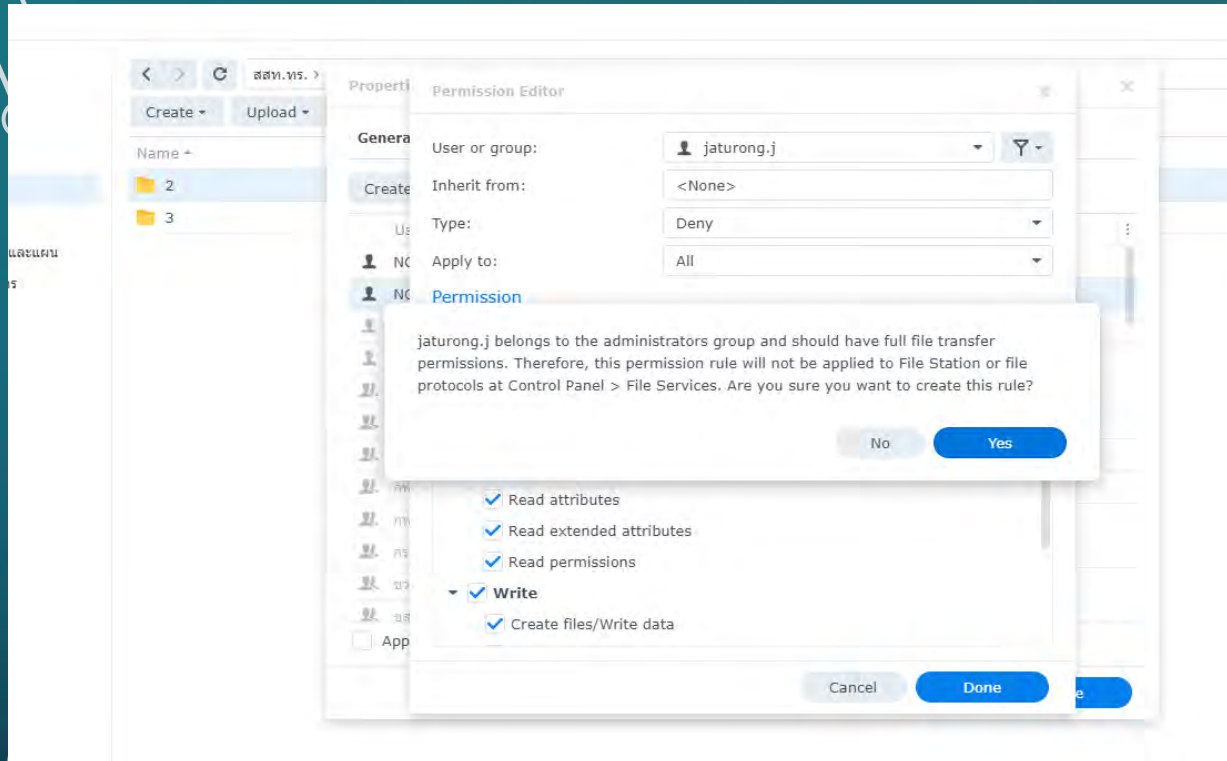
ชื่อแสดงบนแถบ USER OR GROUP



ในหัวข้อ TYPE : เลือก DENY เพื่อปฏิเสธการเข้าถึง เลือกเสร็จคลิกที่ DONE

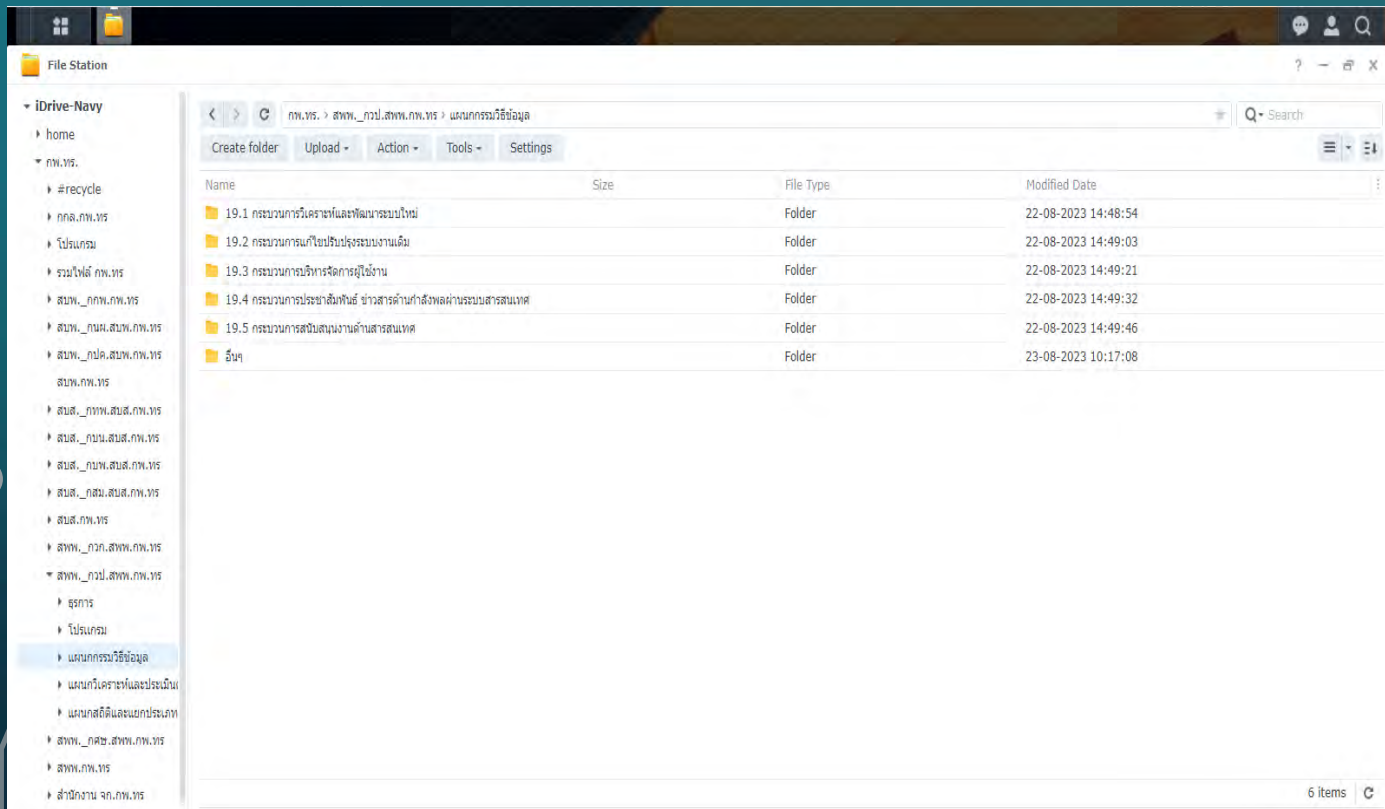


คลิก YES เพื่อยืนยันการเข้าถึงสิทธิ์ใน FOLDER
คลิก SAVE เสร็จสิ้น กระบวนการ



แนวทางการจัด FOLDER

- จัดตามกระบวนการหลัก (Core Process) ของแต่ละแผนก ที่ได้จาก สพพ.กวก.สปพ.กพ.ทร.



CP 17 กระบวนการประเมินค่ากำลังพล

CP 17.1 กระบวนการวิเคราะห์และประเมินผลการปฏิบัติงานของกำลังพล

CP 17.2 กระบวนการประเมินเพื่อสรรหาผู้ที่มีความสามารถได้เป็นยศเป็นนายทหารชั้นนายพลเรือ

น.อ.พิเศษ และ น.อ.

CP 17.3 กระบวนการรายงานผลการปฏิบัติงานที่ของนายทหารสัญญาบัตรที่บรรจุในตำแหน่ง สรท. และ
ประจำหน่วย

CP 17.4 กระบวนการสนับสนุนการประเมินความภาคภูมิใจและความพึงพอใจของกำลังพล

CP 18 กระบวนการควบคุมและแยกประเภทกำลังพล

CP 18.1 กระบวนการเสนอ ยกเลิก แก้ไขตำแหน่งที่กำหนดให้ได้รับเงินประจำตำแหน่ง

CP 18.2 กระบวนการจัดทำคำขอเงินเพิ่มประจำตำแหน่งที่มีพฤกษิเศษ

CP 18.3 กระบวนการเสนอรายงานสถานภาพกำลังพล

CP 18.4 กระบวนการเสนอรายงานสถานภาพกำลังพล

CP 19 กระบวนการจัดการข้อมูลกำลังพล

CP 19.1 กระบวนการวิเคราะห์และพัฒนาระบบใหม่

CP 19.2 กระบวนการแก้ไขข้อบกพร่องระบบงานเดิม

CP 19.3 กระบวนการบริหารจัดการผู้ใช้งาน

CP 19.4 กระบวนการประชาสัมพันธ์ ข่าวสารด้านกำลังพลผ่านระบบสารสนเทศ

CP 19.5 กระบวนการสนับสนุนงานด้านสารสนเทศ