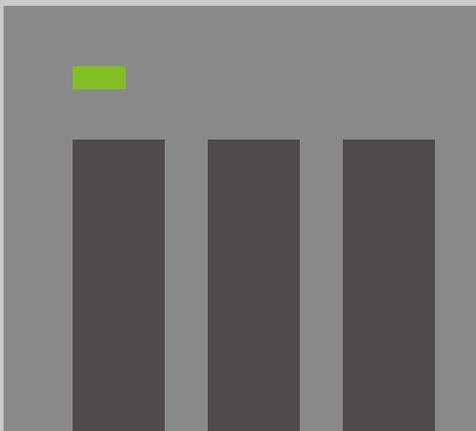


2 0 2 3

Security Guide



2 0 2 3

Security Guide

INDEX

- 1 序言
- 2 常見的攻擊手法
- 3 網路設備基本概念
- 4 從互聯網連線到 NAS 的各種方式

避免暴露 NAS 於互聯網

- 8 正確連接你的 NAS
- 9 檢查你的路由器設定
- 12 檢查 NAS 設定
- 15 網路相關設定檢查清單

NAS 安全設定

- 17 設定系統通知
- 24 啟用韌體 (QTS / QuTS hero) 自動更新功能
- 25 App 更新設定
- 27 停用或移除不必要功能
- 29 停用 Telnet / SSH 功能
- 30 強化系統帳戶安全性
- 34 設定密碼強度原則
- 35 啟用存取保護 (IP / 帳號)
- 36 啟用兩步驟驗證 (2SV)
- 39 修改預設通訊埠
- 40 查看存取紀錄
- 41 安裝及啟用安全性套件
- 42 Security Counselor
- 45 Malware Remover
- 46 QuFirewall
- 51 啟用排程快照 (Snapshot)
- 53 設定快照刪除原則
- 54 NAS 安全設定檢查清單

QNAP 極重視產品的安全性，在面臨日趨嚴重的駭客活動，QNAP 一直持續改善產品設計，為使用者提供兼顧安全及方便的解決方案。

QNAP 產品資安應變團隊 (PSIRT, Product Security Incident Response Team) 負責處理 QNAP 產品相關的安全性議題。PSIRT 除了處理資訊安全相關的事件外，亦管理各產品的弱點的通報、調查、修復和公告。

除此之外，QNAP 亦致力提高產品安全性，過去的產品設計比較重視方便，讓使用者能更簡易地設定及使用產品。隨著近年針對網路產品的網路攻擊愈來愈多，QNAP 的產品設計觀點也隨著改變，產品設計轉向以基於安全的設計 (Security by Design)，確保使用者可以應對相關威脅，為使用者把關。

要知道如何防禦，就必須知道攻擊者如何發動網路攻擊。就針對 NAS 的攻擊而言，大部分攻擊都是源自互聯網。而攻擊手法大多採用「破解密碼」及「弱點攻擊」兩種。其中「弱點攻擊」可分為「N-day」及「0-day」。

「N-day」意指濫用已修正的弱點發動攻擊，目前大部分活躍的攻擊活動都屬於這種。假如已安裝相關安全性修正的話，即可有效抵禦攻擊。

「0-day」意指濫用未知的弱點發動攻擊，廠商只能於事後發佈安全性修正。只有阻止攻擊者連線到裝置，才能有效抵禦攻擊。

下表整理出不同攻擊手法的應對方式，供使用者參考。

應對方式	攻擊手法		
	破解密碼	弱點攻擊 (N-day)	弱點攻擊 (0-day)
避免曝露外網	V	V	V
更新軟體 (系統及套件)	X	V	△
啟用自動更新功能 (系統及套件)	X	V	△
所有帳戶使用強密碼	V	X	X
停用預設「admin」帳戶	V	X	X
啟用兩步驟驗證	V	X	X
啟用存取保護功能	△	X	X
啟用防火牆	△	△	△
接收系統通知	△	△	△
修改預設通訊埠	△	△	△
停用 / 移除不必要功能	△	△	△

V: 有效 X: 無效 △: 可能有效 (代表可以緩解攻擊或降低被攻擊的機會)

「避免曝露外網」能有效阻擋攻擊者連線到你的裝置，讓攻擊者無法對你的裝置發動攻擊，本教學先以「避免曝露於互聯網」作為開始，然後會提供完整的「NAS 安全設定」教學，提高 NAS 防禦能力。

本教學旨在協助使用者正確設定 NAS 以提高安全性，
如對設定上或使用上有問題，歡迎聯絡我們的技術支援團隊取得協助：



而針對產品弱點及安全相關事件資訊，
可以參考及訂閱 QNAP 資安通報：

<https://www.qnap.com/go/security-advisories/>



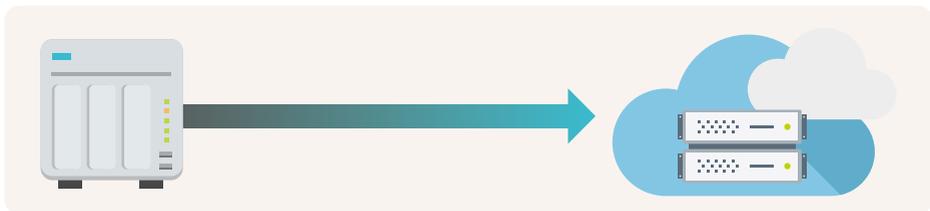
QNAP 客戶服務：

<https://service.qnap.com/>



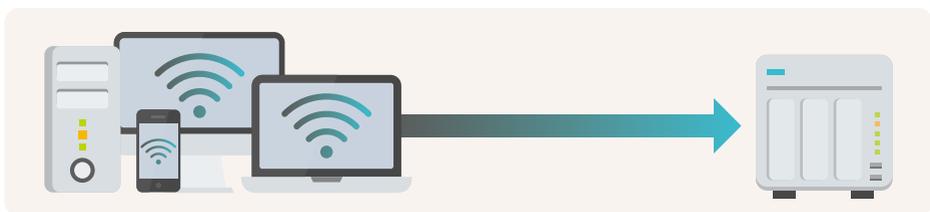
NAS 作為一台連接網路的裝置，其實具備兩個連接方向。

01 | NAS 對外連線



NAS 一般需要對外連線能力來讓所有功能正常運作。例如是自動更新、發送通知等基本系統功能。此外，如需要把 NAS 數據備份到公共雲端空間 (Public Cloud)，或使用 NAS 的備份套件備份其他裝置或公共雲端的數據，如備份虛擬機 (Virtual Machine)、SaaS 雲服務 (如 Google Workspace、Microsoft 365)、電腦或伺服器，都需要 NAS 具備往外面發起連線的能力。

02 | 其他裝置 (如電腦、手機或其他伺服器) 對 NAS 進行連線



假如你需要使用任何 NAS 提供的功能或服務，包括存取檔案、進入設定介面等等，都需要具備往 NAS 方向發起連線的能力。

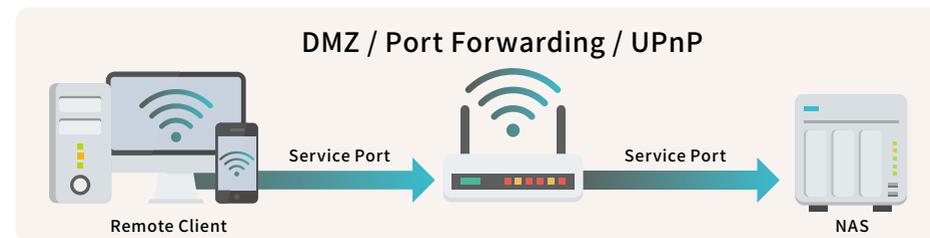
在路由器沒有開啟及設定 DMZ、Port Forwarding 或 UPnP 的情況下，路由器會阻擋來自互聯網的流量，即內聯網的設備可以連線到 NAS。

在路由器開啟及設定上述功能的狀態下，在互聯網內的所有人都可以連線到已開放的連接埠，再依路由器上的規則轉發到 NAS，然後可以正常登入並使用相關功能，但同時會讓不法份子嘗試以密碼攻擊或濫用軟體漏洞等方式嘗試攻擊及入侵，造成安全風險。

01 | 在路由器開啟及設定 DMZ、Port Forwarding 或 UPnP

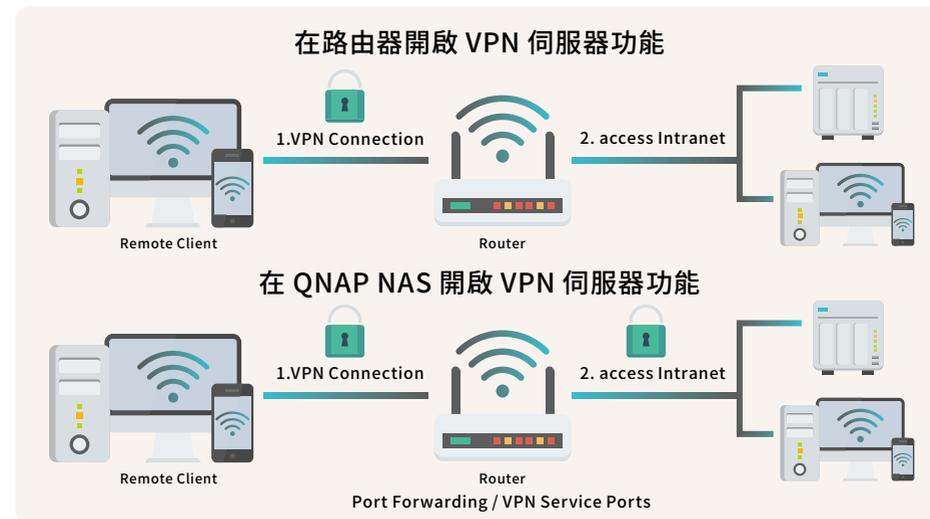
此方法具有安全風險，在現今攻擊者橫行的時代，如非必要，**QNAP 並不建議使用 ***。因路由器會放行通往內聯網裝置流量的關係，如在路由器及 NAS 之間沒有安裝防火牆阻擋惡意流量，攻擊者就可以輕易發動網路攻擊。然而，即使安裝防火牆，使用 NAS 內的基本防火牆或選購企業級的防火牆，也不能保證能 100% 阻擋攻擊。

* QNAP 僅建議開放相對低風險的 VPN 服務連接埠到互聯網，而其他較高風險的服務連接埠如系統管理、SMB、SSH 服務等，切勿輕易對互聯網開放。



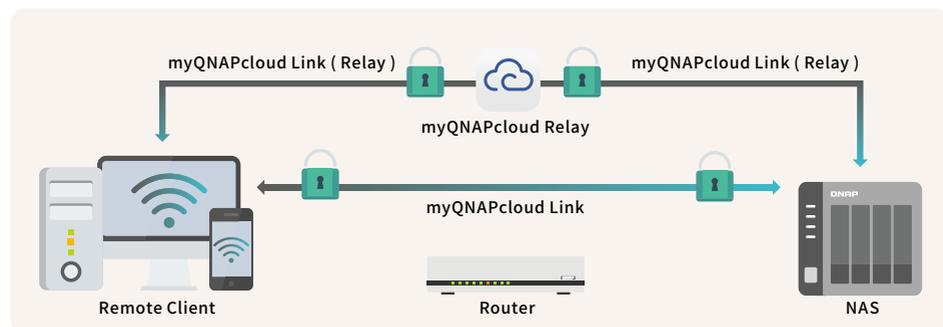
02 | 在路由器或 QNAP NAS 開啟 VPN 伺服器功能

部分路由器支援 VPN 伺服器功能 (如 QNAP QHora 及 QMiro 系列路由器)，而 QNAP NAS 同樣支援多種 VPN 伺服器。在開啟及正確設定此功能後，只要你從互聯網連線到 VPN 伺服器，即可在經 VPN 加密的連線環境下存取內聯網的各個裝置，透過此方式存取具有較高安全性。



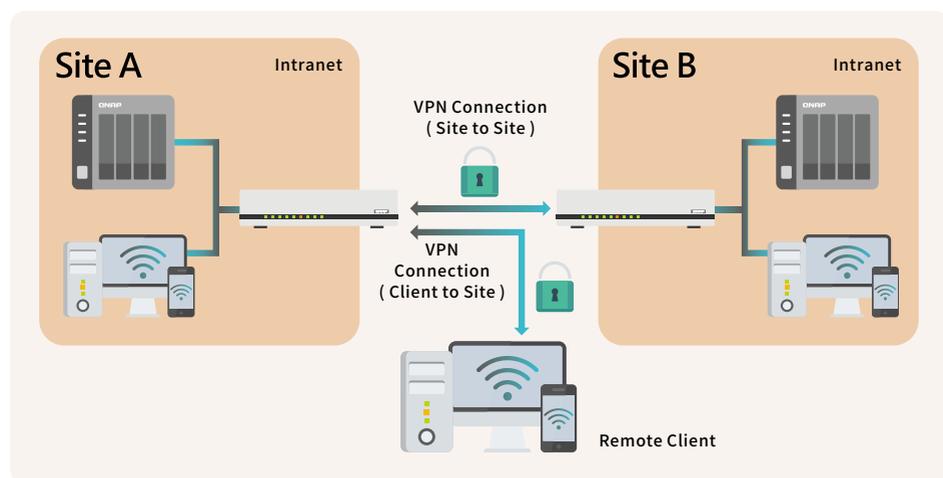
03 | 使用 myQNAPcloud Link 安全連線功能

使用 myQNAPcloud Link 連線到 NAS 並不需要設定路由器即可將 NAS 服務直接對互聯網開放。myQNAPcloud Link 是會依網路環境的狀況，透過中繼伺服器 (Relay Server) 或點對點技術 (Peer-to-Peer, P2P) 建立連線，整個連線會以加密的方式進行，確保安全。



04 | 使用 SD-WAN 或 Site-to-Site VPN 產品

有別於在前面提及的 VPN 伺服器功能 (Client-to-Site VPN)，SD-WAN 或 Site-to-Site VPN 是於兩台以上在不同地點的路由器建立 VPN 安全加密連線。簡單來說，在 Site-to-Site VPN 網路下的裝置都可以像在同一內聯網一樣，互相連通，適合擁有多個地點的使用者使用。配合 Client-to-Site VPN 使用，即可在任何地點存取 NAS。



你可依照以下比較表，挑選適合自己的連線方式。QNAP 提供多種安全連線解決方案，切合使用者所需。

連線方式	優點	缺點	適合的使用者
在路由器開啟及設定 DMZ/Port Forwarding of UPnP	<ul style="list-style-type: none"> 連線速度最快 	<ul style="list-style-type: none"> 容易受到網路攻擊 對 0-Day 弱點攻擊沒有防禦能力 	<ul style="list-style-type: none"> 清楚了解相關風險 對網路設定熟悉 已為重要數據建立多個備份 擁有災難復原檔案
在路由器開啟 VPN 伺服器功能 *	<ul style="list-style-type: none"> 設定相對簡單 	<ul style="list-style-type: none"> 欠缺登入失敗通知、自動封鎖及防火牆功能 支援的 VPN 協定較少 效能受限於路由器硬件 	<ul style="list-style-type: none"> 對網路設定不熟悉 對傳輸速度要求較低
在 QNAP NAS 開啟 VPN 伺服器功能 *	<ul style="list-style-type: none"> 支援多種 VPN 協定 可搭配 NAS 基本防火牆 (QuFirewall) 支援登入失敗通知及自動封鎖功能 	<ul style="list-style-type: none"> 設定略為複雜 	<ul style="list-style-type: none"> 對網路設定熟悉 經常需要從互聯網存取大量檔案
 使用 myQNAPcloud Link 全連線功能	<ul style="list-style-type: none"> 設定最簡單 支援存取控制功能 NAS 完全不需要曝露互聯網 	<ul style="list-style-type: none"> 連線速度較慢 	<ul style="list-style-type: none"> 對網路設定不熟悉 低頻率從互聯網存取 NAS 無法取得 WAN IP 地址的網路環境
使用 SD-WAN 或 Site to Site VPN 產品 *	<ul style="list-style-type: none"> 設定完後，內聯網使用者即可無感使用 同時支援 Client-to-Site VPN 	<ul style="list-style-type: none"> 需要增購額外設備 	<ul style="list-style-type: none"> 需要多點存取及遠端備份 需要加值應用

* QNAP NAS 產品支援：
myQNAPcloud Link / VPN Servers (L2TP/IPsec、OpenVPN、WireGuard、QBelt) / QuWAN SD-WAN

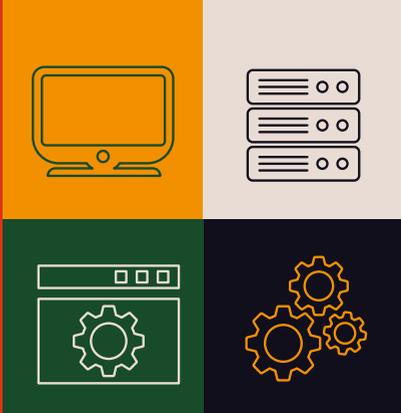
* QNAP Router 產品支援：
QuWAN SD-WAN / VPN Servers (L2TP/IPsec、OpenVPN、WireGuard、QBelt)

泛指一般家用路由器

01

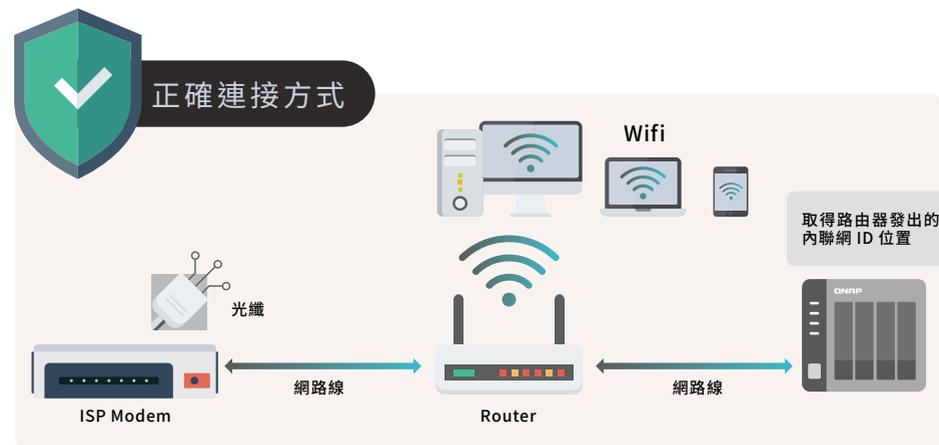
NAS 安全設定指南

避免曝露 NAS 於互聯網

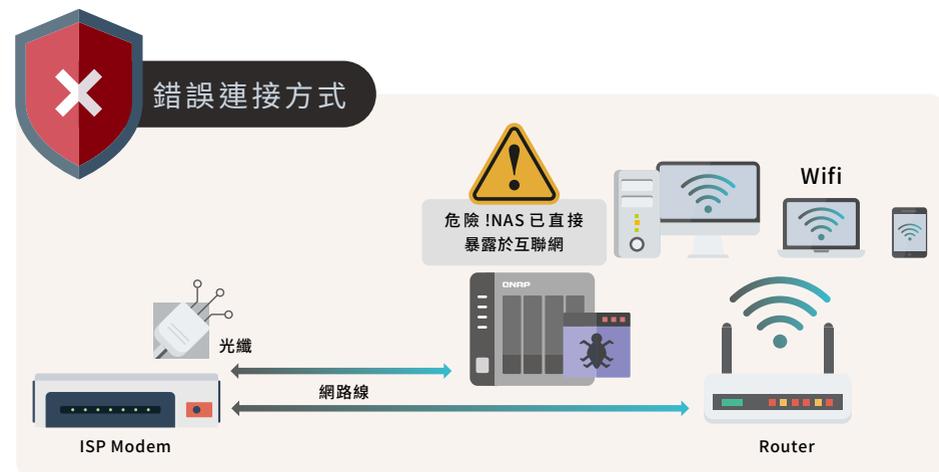


正確連接你的 NAS

請確保你的 NAS 是連接到路由器 (Router) 後。在正確的設定下，路由器可以為你阻擋來自互聯網的連線，讓你的 NAS 隱藏於互聯網，避免遭受網路攻擊。



如果把 NAS 連接到 ISP 提供的數據機下，你的 NAS 將直接取得 WAN IP 地址，在這情況下，任何人（包括攻擊者）都可以經由互聯網連線到你的 NAS，甚至是嘗試攻擊及入侵。

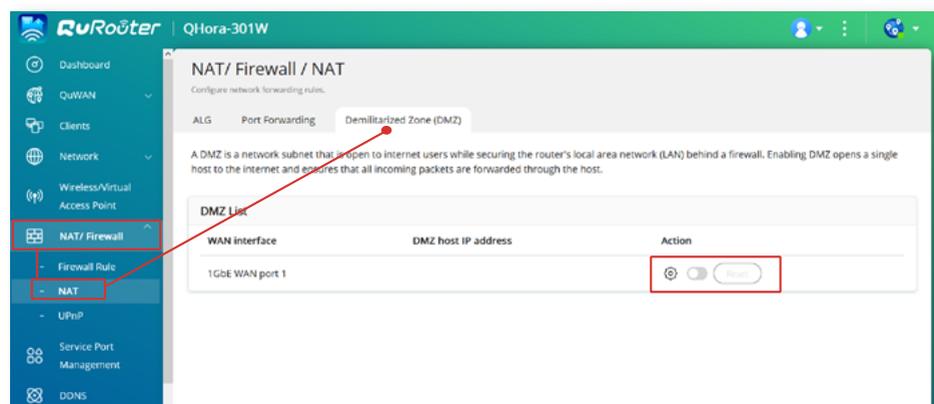
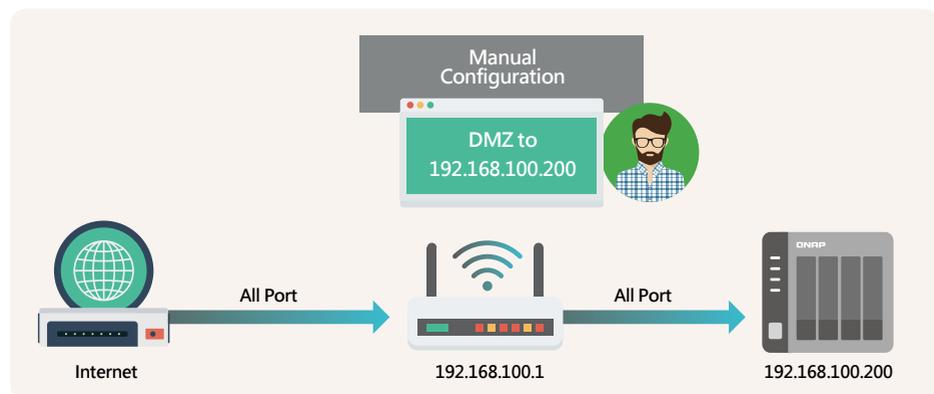


檢查你的路由器設定

在預設狀態下，理論上沒有人能從互聯網直接連線到你架設在路由器 (Router) 後的裝置，但如果你在路由器上開啟「DMZ (Demilitarized Zone 非軍事區域)」、「Port Forwarding (通訊埠轉發)」或「UPnP (Universal Plug and Play 通用隨插即用)」功能，你的路由器將會依你設定的規則轉發封包到你選定的裝置，讓你的裝置暴露在互聯網上。如無特殊需要，請檢查及確保以下功能處於**關閉狀態**。

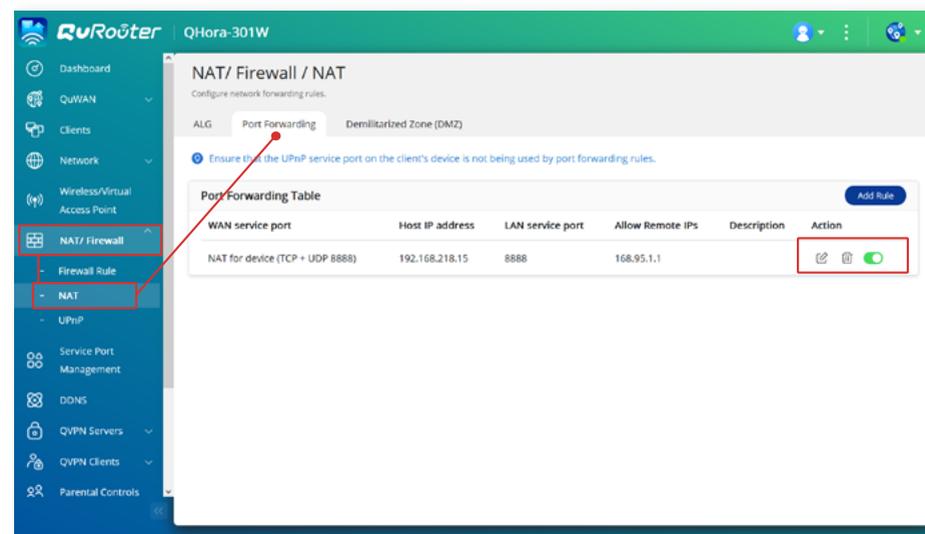
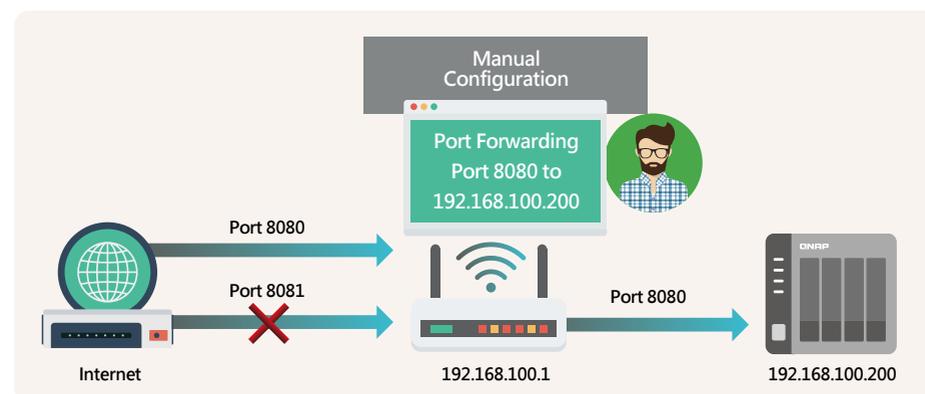
01 | 檢查 DMZ (Demilitarized Zone, 非軍事區域)

開啟這個功能後，你所選定的裝置的所有服務通訊埠將直接對互聯網開放，即完全暴露在互聯網上，為降低安全風險，請關閉這個功能。



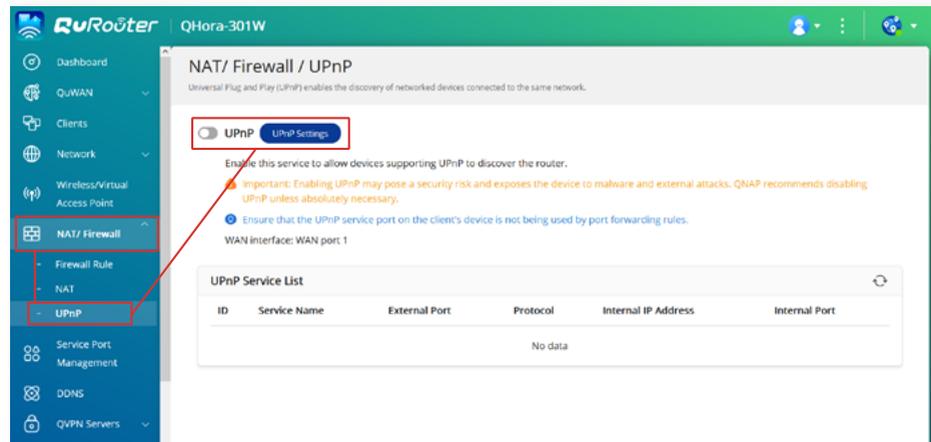
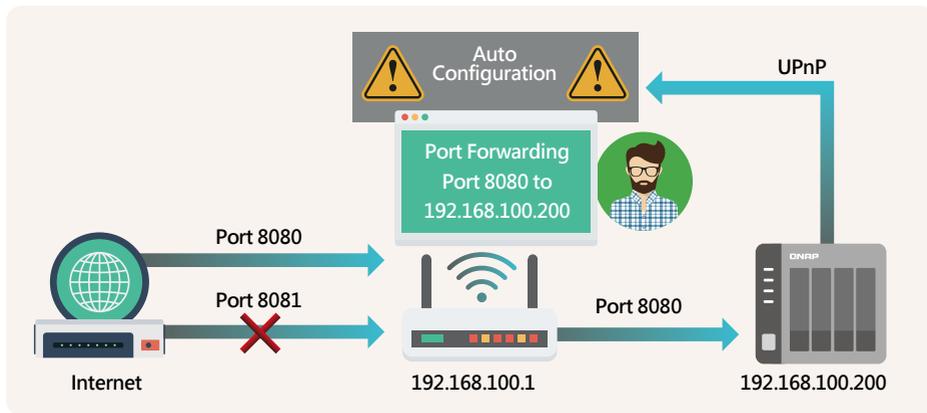
02 | 檢查 Port Forwarding (通訊埠轉發)

這個功能可以讓你把某裝置上的特定服務通訊埠對互聯網開放，讓任何人通過互聯網存取相關的服務。然而，駭客也可以從互聯網針對已開放的服務發動攻擊，造成安全風險，因此建議先關閉所有通訊埠轉發規則，在確保 NAS 已完成所有安全設定及定期備份重要數據後，再考慮使用這個功能開放部分必要服務到互聯網。



03 | 檢查 UPnP (Universal Plug and Play, 通用隨插即用)

此功能等同於自動化版本的通訊埠轉發。開啟這個功能後，你的裝置可以使用相關協定自動設定通訊埠轉發。這個功能有可能讓你在不知情的情況下把服務曝露到互聯網上，又或是被攻擊者利用此功能打開後門，造成嚴重安全風險，因此請關閉此功能，以提高安全性。



01 | 自動設定路由器,UPnP 通訊埠轉發

因部分路由器 (Router) 並不支援關閉 UPnP 功能，因此請同步檢查 NAS 上「自動設定路由器」設定，確保此功能已經關閉。

* 此功能在 QTS 4.5.0 / QuTS hero h4.5.3 後預設為關閉

停用「自動設定路由器」功能：

1. 使用具管理權限的使用者帳戶登入 QTS / QuTS hero 網頁管理介面
2. 打開管理介面左上角的選單，點選「myQNAPcloud」
3. QTS 5.0.0 / QuTS hero h5.0.0 或 以前版本：於左側選單點選「自動設定路由器 (Auto Router Configuration)」



QTS 5.0.1 / QuTS hero h5.0.1 或 以後版本：按右上角「☰」，點選「自動設定路由器 (Auto Router Configuration)」



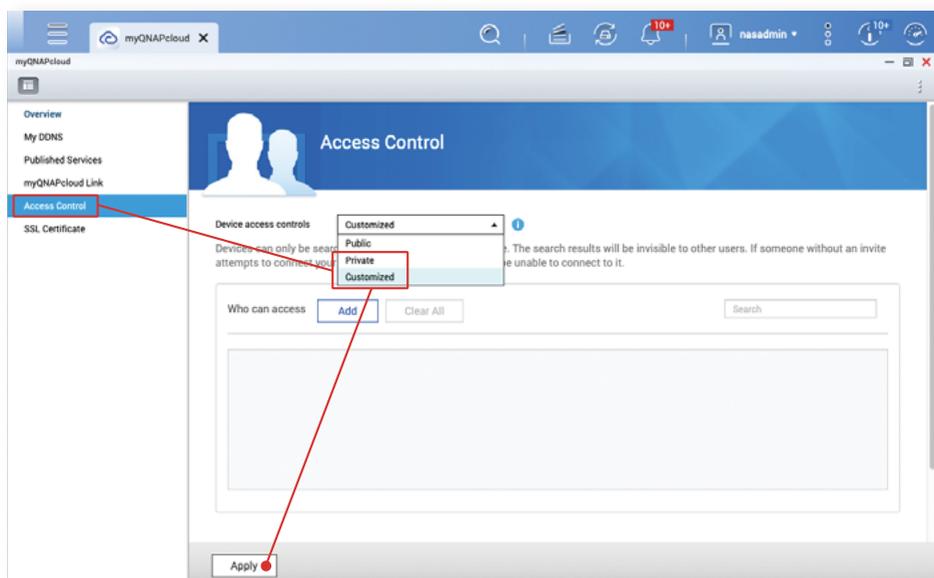
4. 於「自動設定路由器 (Auto Router Configuration)」設定頁面，取消勾選「啟用 UPnP 通訊埠轉送 (Enable UPnP Port Forwarding)」，然後按「套用」。

02 | myQNAPcloud Link 存取控制

在 myQNAPcloud Link 是 QNAP 提供的安全連線雲服務，使用者可以透過自行設定的 myQNAPcloud 裝置名稱連線到對應的 QNAP NAS。myQNAPcloudLink 有提供存取控制設定，當存取控制設定為「公開 (Public)」時，任何知道你的裝置名稱的人員都可以使用 myQNAPcloud Link 連線到你的 NAS。因此，我們建議把存取控制設定成「私人 (Private)」或「自訂 (Customized)」，在這兩個模式下，使用者需要先登入在「允許存取清單」內的 QNAP ID 帳戶才可以使用 myQNAPcloud Link 安全連線雲服務。

* 此設定在 Q TS 4.5.0 / Qu TS her o h4.5.3 或之後版本，預設為「自訂 (C ustomized)」

1. 使用具管理權限的使用者帳戶登入 QTS / QuTS hero 網頁管理介面
2. 點選管理介面左上角的選單，點選「myQNAPcloud」
3. 於左側選單點選「存取控制 (Access Control)」
4. 於「存取控制 (Access Control)」設定頁面，於「裝置存取控制 (Device access controls)」設定為「私人 (Private)」或「自訂 (Customized)」，然後按「套用」。



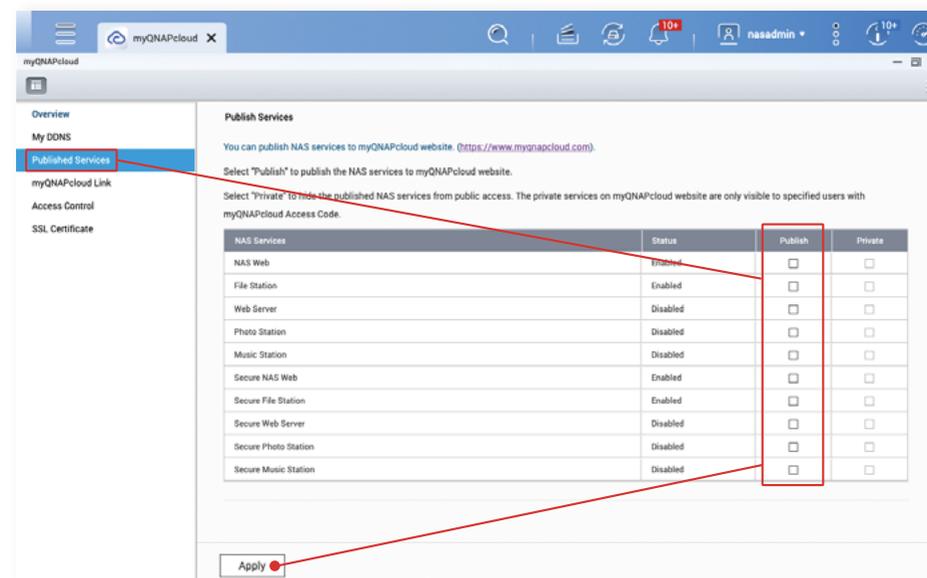
03 | 公開服務

公開服務能讓使用者在 myQNAPcloud 網站更方便地使用相關功能，但相對會提高安全風險。如沒有需要使用此功能，建議將其關閉，以提高安全性。

* 此功能在 QTS 4.5.0 / QuTS hero h4.5.3 後預設為關閉

「公開服務」功能：

1. 使用具管理權限的使用者帳戶登入 QTS / QuTS hero 網頁管理介面
2. 點選管理介面左上角的選單，點選「myQNAPcloud」
3. 於左側選單點選「公開服務 (Published Services)」
4. 於「公開」欄位，全部取消勾選，然後按「套用」。



網路相關設定檢查清單

硬體相關

- NAS 連接在路由器 (Router) 後
- NAS 取得內聯網 IP 地址

路由器

- 停用路由器「DMZ」功能
- 停用路由器「Port Forwarding」規則
- 停用路由器「UPnP」功能

NAS

- 停用 NAS「自動設定路由器 UPnP 通訊埠轉送」功能
- 設定 NAS「myQNAPcloud Link 存取控制」成「私人 (Private)」或「自訂 (Customized)」
- 停用「公開服務」功能

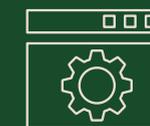
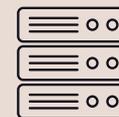
在完成檢查及套用以上設定後，你的 QNAP NAS 並不會曝露在互聯網上，被駭客攻擊的機會已經大幅降低。請繼續閱讀及檢查其餘的設定，以強化 QNAP NAS 防禦能力。

如需要於互聯網存取 NAS，可以考慮以下三個較安全的替代方案：

		
myQNAPcloud Link	QVPN Service	QuWAN SD-WAN
		
了解更多	了解更多	了解更多

02

NAS 安全設定指南



NAS 安全設定



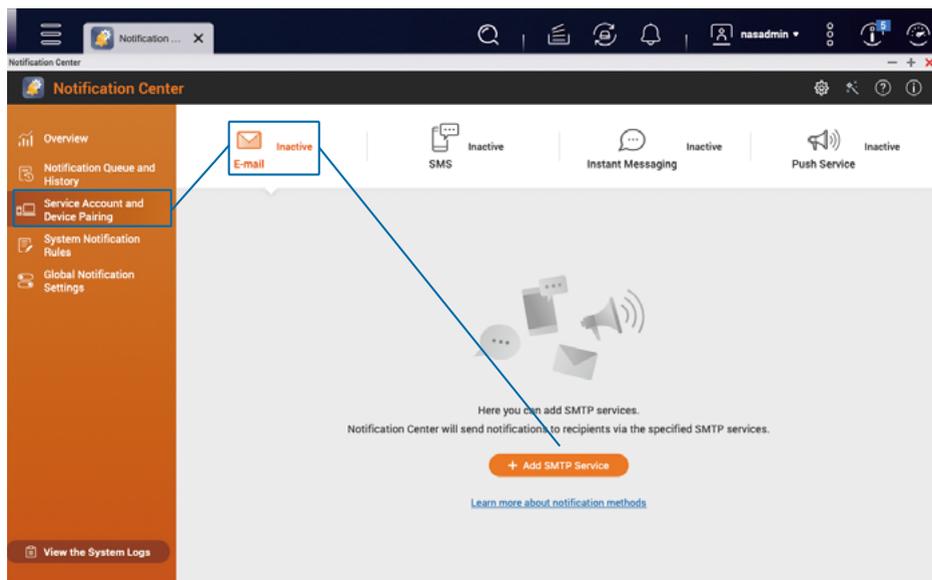
設定系統通知

QNAP QTS / QuTS hero 系統內建的通知中心 (Notification Center) 可依照你設定的條件推送通知，讓使用者隨時掌握 NAS 的狀況，在出現異常時能及早反應及處理。

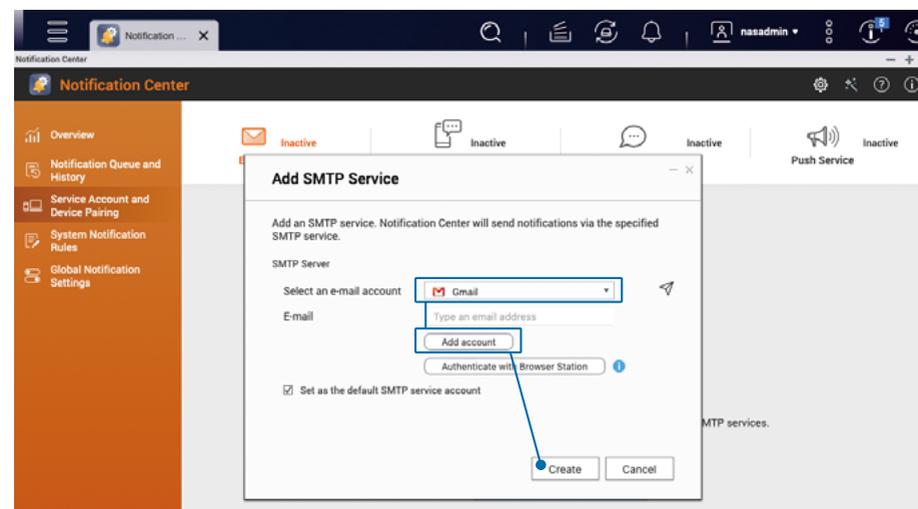
以下教學會教你建立以「電子郵件」傳送「警示通知」及「韌體更新」這兩條基礎的規則，如有需要，可自行再加入更多規則。

01 | 加入「電子郵件」通知方式

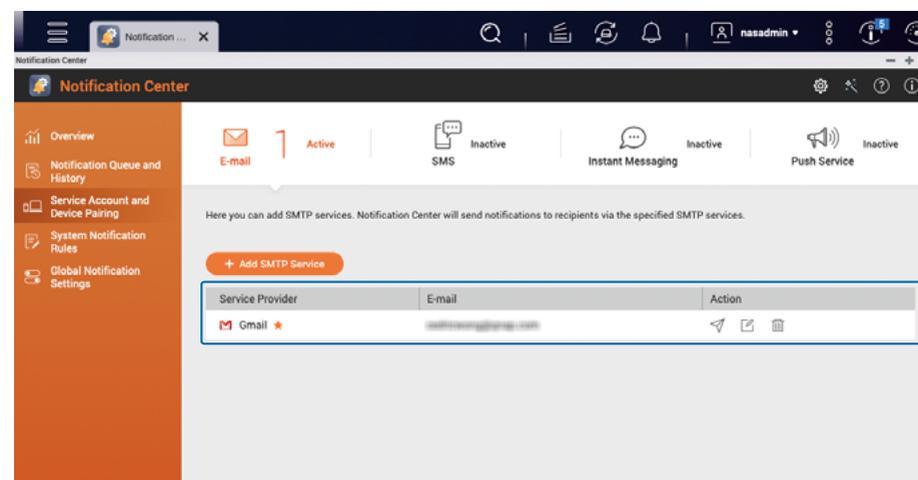
打開「通知中心」，左方選單點選「服務帳號與裝置配對」，選擇「電子郵件」，再點選「新增 SMTP 服務」



先選擇電子郵件帳號，以下會使用 Gmail 作為示範，點選「新增帳號」，按指示完成 Gmail 的認證過程，認證完成後按「建立」。

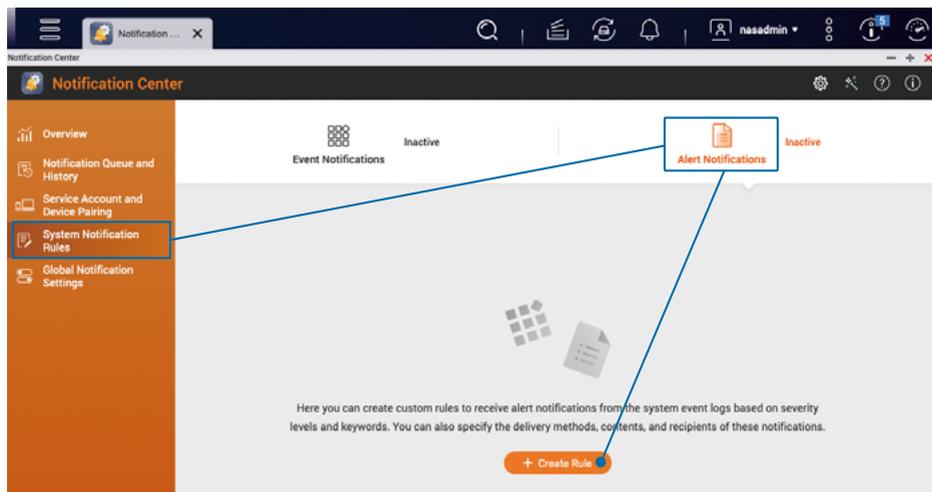


↓↓建立完成後，即可在列表中看到你已加入的電子郵件帳號。

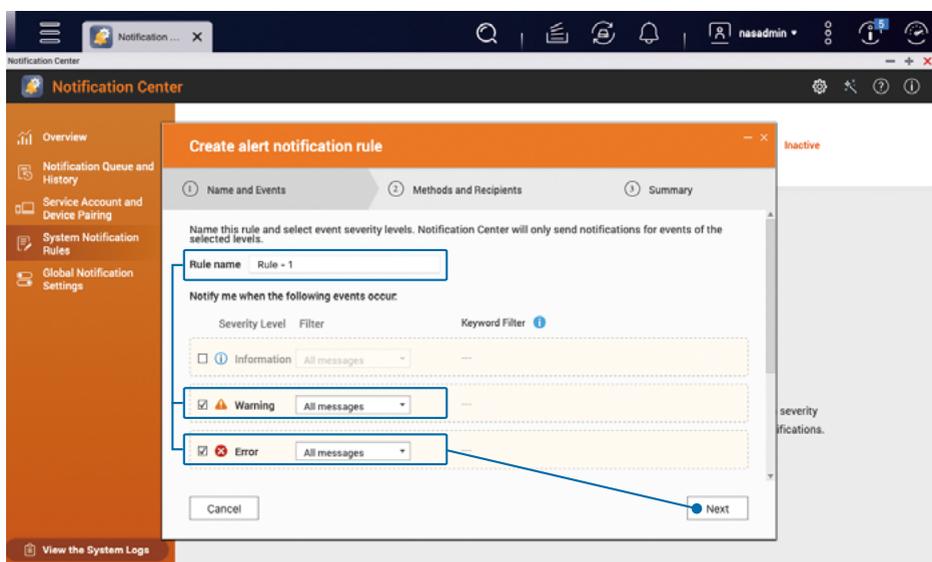


02 | 設定「警示通知」

於「通知中心」左方選單點選「系統通知規則」，選擇「警示通知」，再點選「建立規則」。

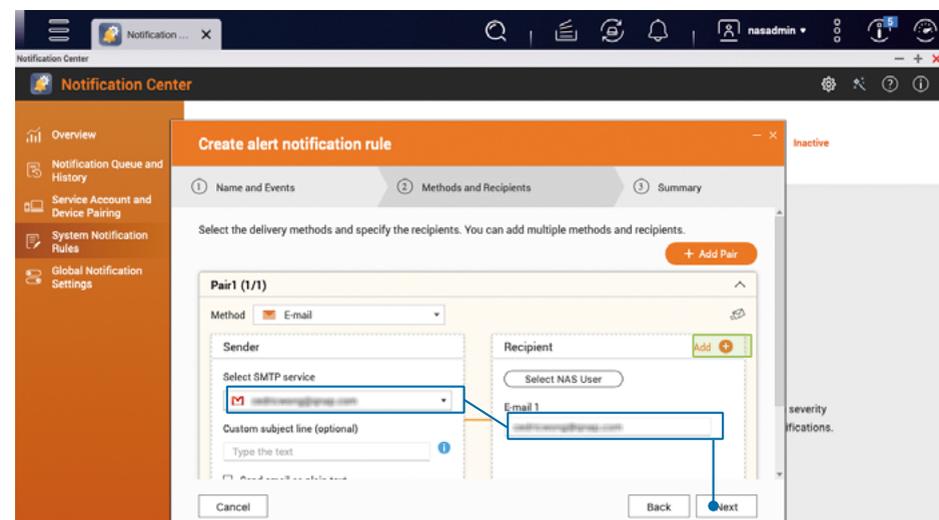


按自己的需要修改「規則名稱」，勾選「警告」及「錯誤」兩個嚴重性層級，然後按「下一步」。

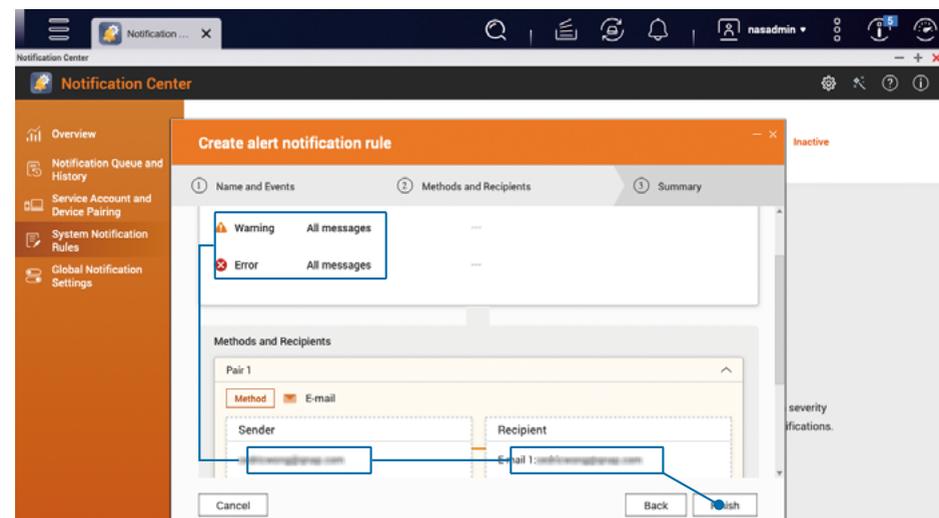


設定傳送方式及設定收件者，於配對中選擇剛剛加入的電子郵件帳號作為「寄件者」，再填入「收件者」的「電子郵件地址」，然後按「下一步」。

如有需要，你可以按「收件者」旁邊的「新增 +」填入多個收件者。另外也可「新增配對」以多種方式同時傳送通知。

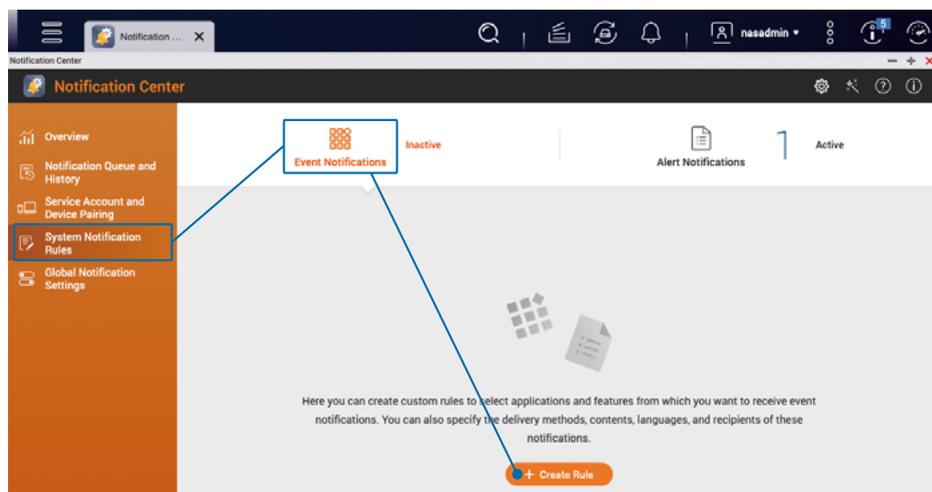


確認設定正確後，按「完成」套用設定，即可完成設定「警示通知」。

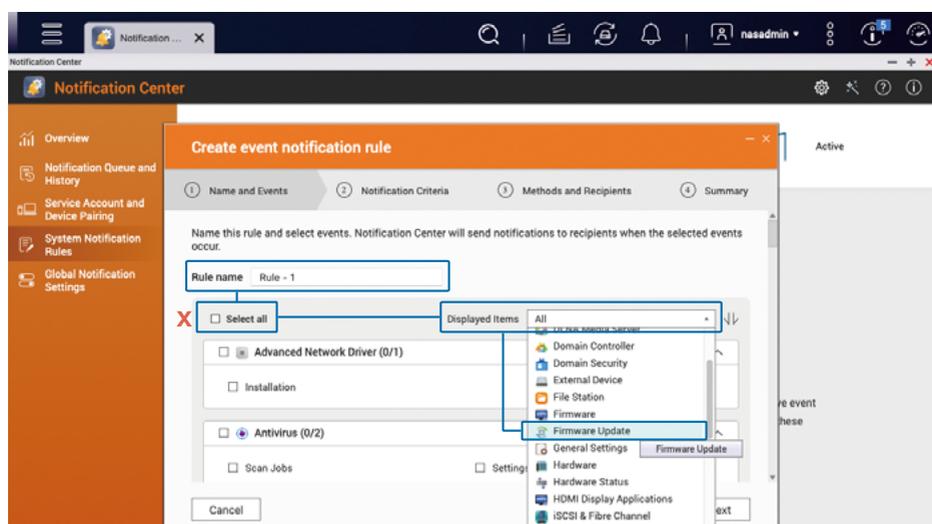


03 | 設定「韌體更新」通知

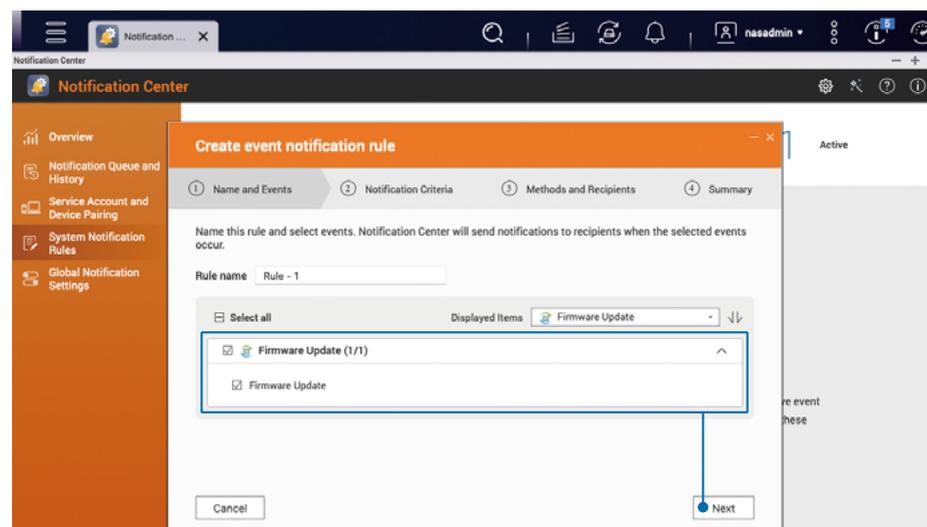
於「通知中心」左方選單點選「系統通知規則」，選擇「事件通知」，再點選「建立規則」。



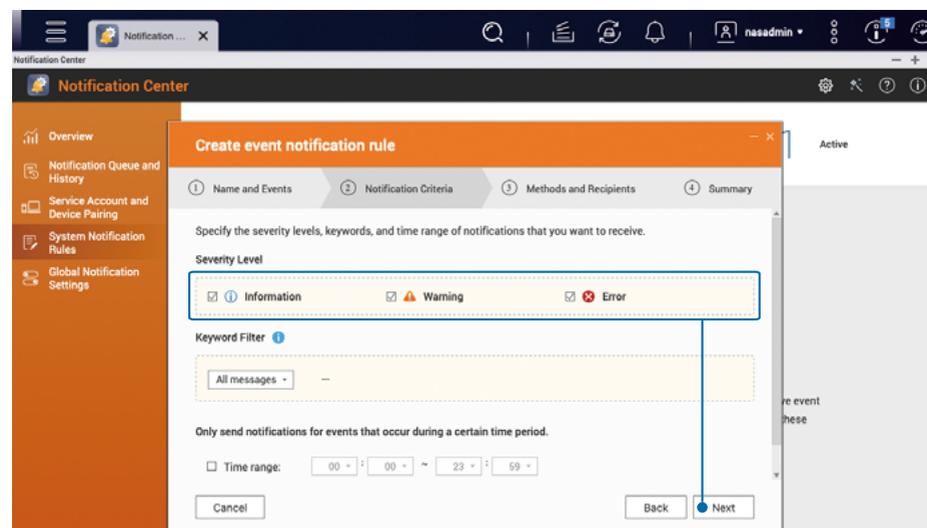
按自己的需要修改「規則名稱」，取消勾選「全選」，再於左側「顯示項目」選擇「韌體更新」，然後選下方勾選「韌體更新」選項。



於下方勾選「韌體更新」選項，按「下一步」。



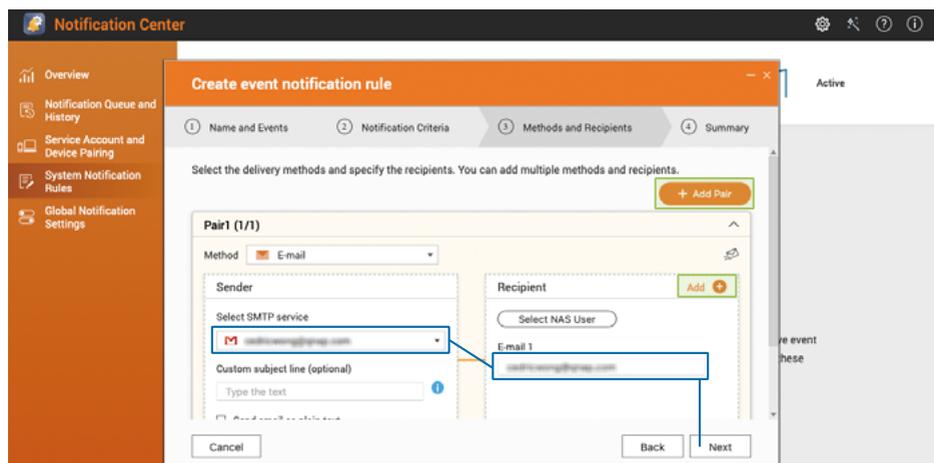
勾選所有嚴重性層級，包括「資訊」、「警告」及「錯誤」，按「下一步」。



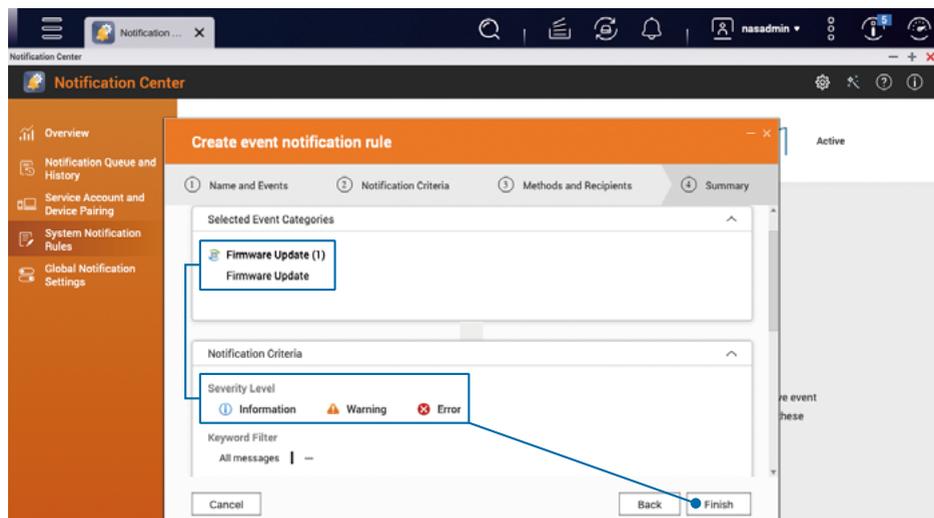
啟用韌體 (QTS / QuTS hero) 自動更新功能

設定傳送方式及設定收件者，因目前只設定了「電子郵件」通知，於配對中選擇剛剛加入的電子郵件帳號作為「寄件者」，再填入「收件者」的「電子郵件地址」，然後按「下一步」。

如有需要，你可以按「收件者」旁邊的「新增 +」填入多個收件者。另外也可「新增配對」以多種方式同時傳送通知。

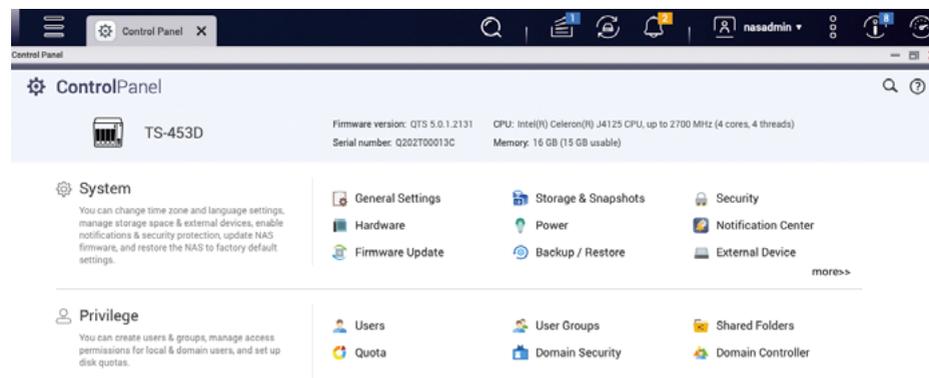


確認設定正確後，按「完成」套用設定，即可完成設定「韌體更新」通知。



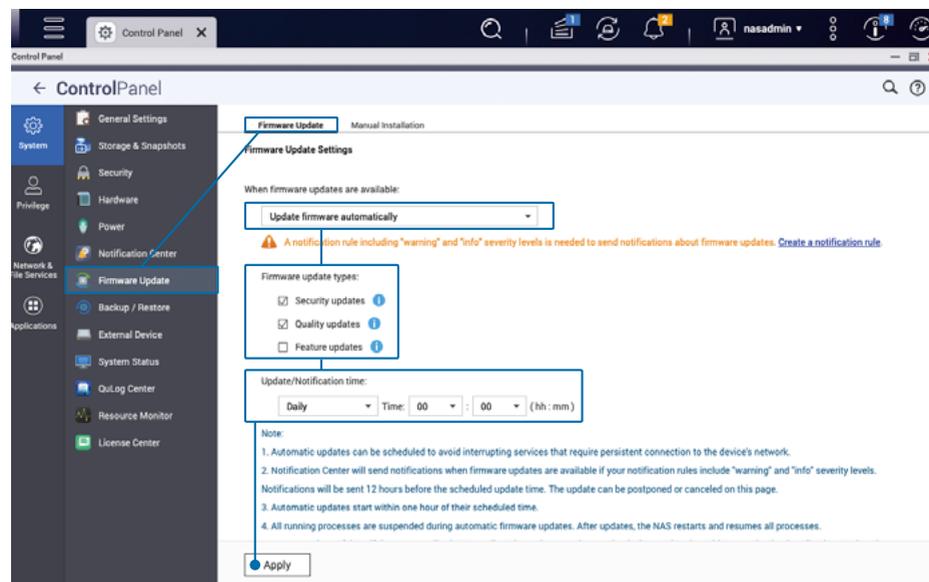
自動更新功能可以助你更輕鬆地安裝更新檔，以取得新功能、修正問題及弱點。

打開「控制台」，點選「韌體更新」。



於「韌體更新設定」，選擇「自動安裝韌體」，並勾選「安全更新」及「品質更新」；「更新 / 通知時間」建議設定為「每日」的非使用時段，如「00:00」，然後按套用。

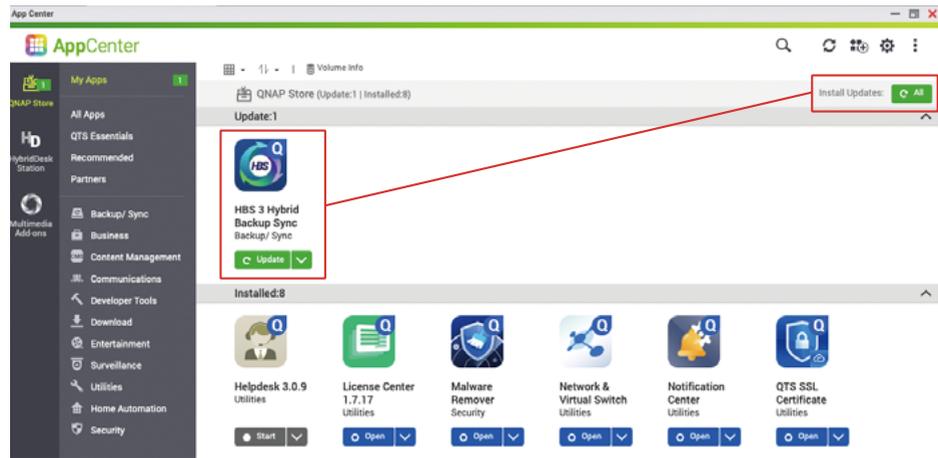
★ QTS 5.0.0 / QuTS hero h5.0.0 或更舊版本請於「自動更新」頁面勾選「建議版本」



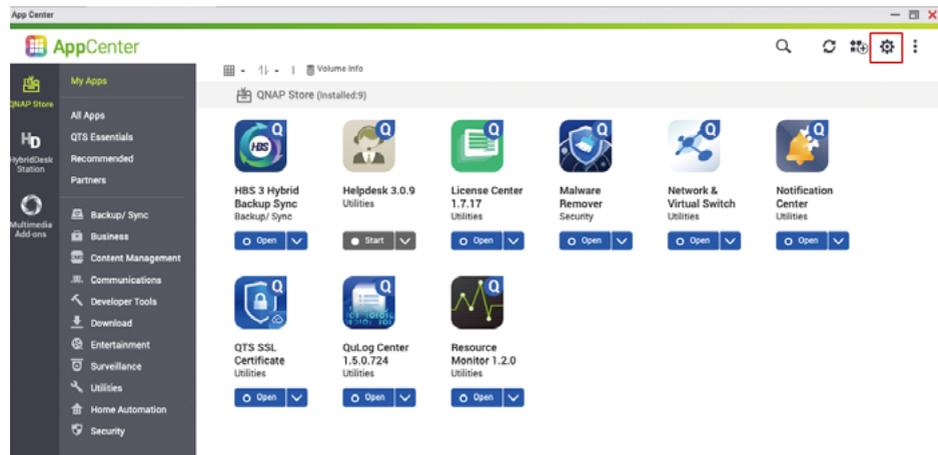
App 更新設定

App Center 提供多個套件為你的 QNAP NAS 加入更多功能，但套件同樣是需要保持更新的，以強化套件功能及修正問題與弱點，改善使用體驗。

打開「App Center」，即可看到有沒有需要更新的套件，如有的話，請按右上方的「全部 All」按鍵，以更新所有套件。

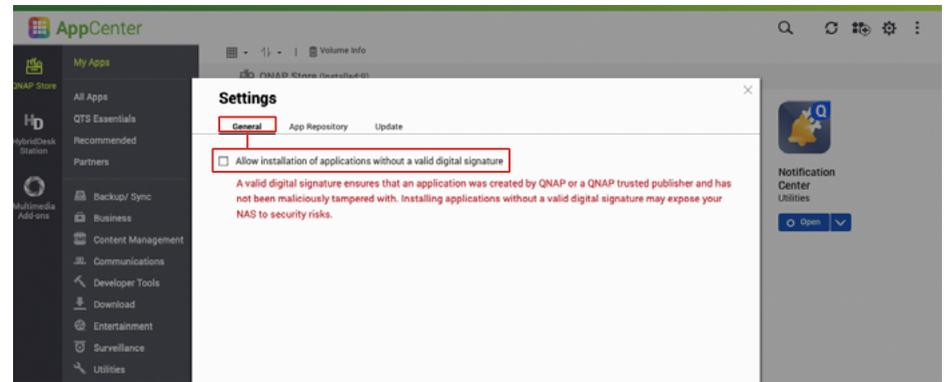


更新完成後，可以點選右上角的「設定 」圖示，即可進入 App Center 的設定頁面。



QNAP 或 QNAP 信任的開發者會為套件加入數位簽章，以確保套件沒有被惡意竄改。建議取消勾選「允許安裝不具有有效數位簽章的應用程式」，以增強安全性。

★ 預設值為沒有勾選；即禁止安裝不具有有效數位簽章的應用程式

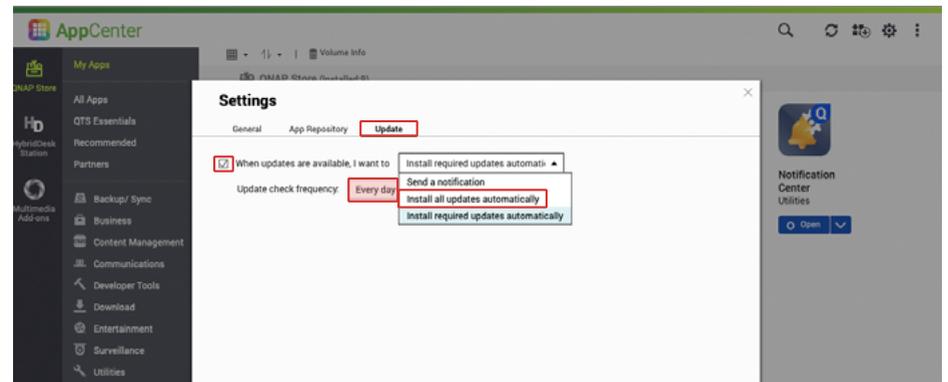


點選更新頁面，如無特殊的需要，建議選擇「自動安裝所有更新」，頻率設定為「每天」，按套用完成設定。

⇒「必要更新」主要用於滿足套件與韌體的相依性，另外會包括「重大的弱點更新」。

⇒「所有更新」包含所有功能改善、問題修正及所有弱點修正，更新頻率會較高。

★ 預設值為「自動安裝必要更新」

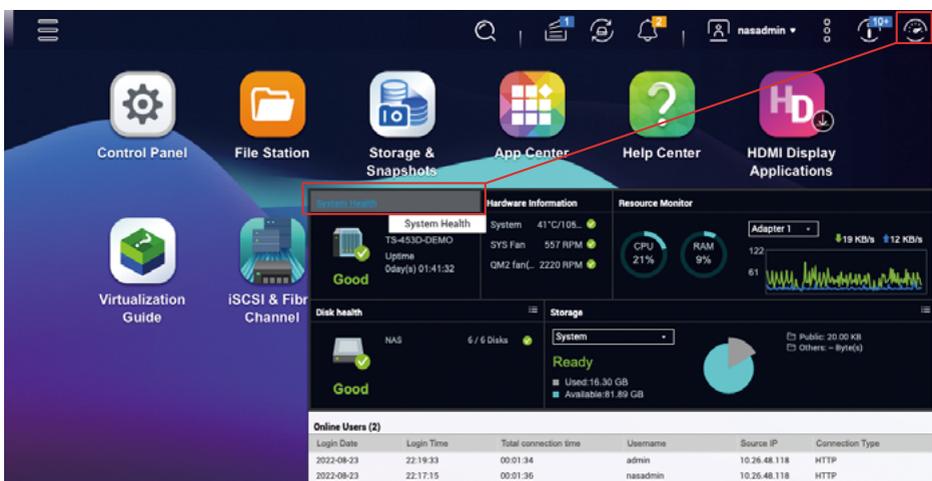


停用或移除不必要功能

QNAP NAS 提供了各式各樣的功能及套件，但功能啟用得愈多，也代表可能潛在的攻擊表面 (Attack Surface) 愈多，因此需要定期檢查及停用（或移除）不必要的功能，以提高安全性，也能讓系統運作更暢順。

★ 為增強產品安全性，自 QTS 5.0.0 / QuTS hero h5.0.0 版本後初始化系統，所有非必要功能已預設關閉，App Center 也不會預設安裝任何非必要套件。如系統於 QTS 5.0.0 / QuTS hero h5.0.0 以前的版本初始化，請務必認真檢查。

點選右上角「🔍」按鍵，打開系統「Dashboard」，點選「系統健康」，即可打開「系統狀態」視窗。



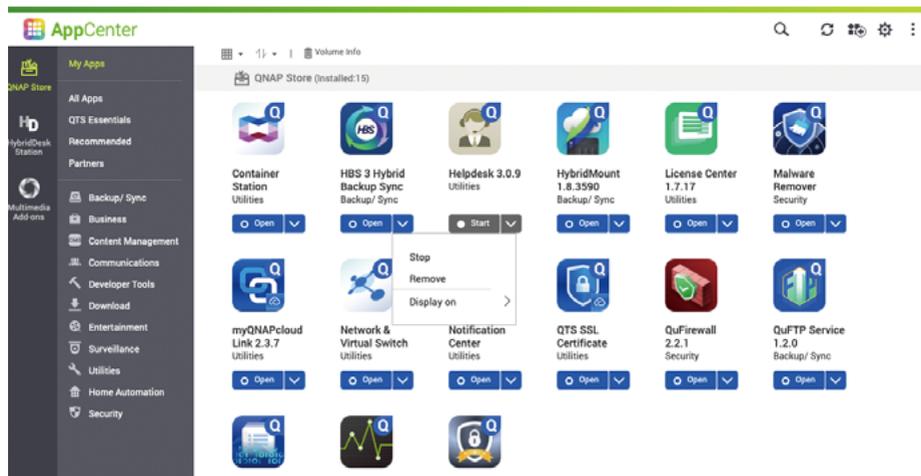
點選「系統服務資訊」查看已啟用的系統功能，你可以到控制台停用不需要使用的系統功能。

System Status

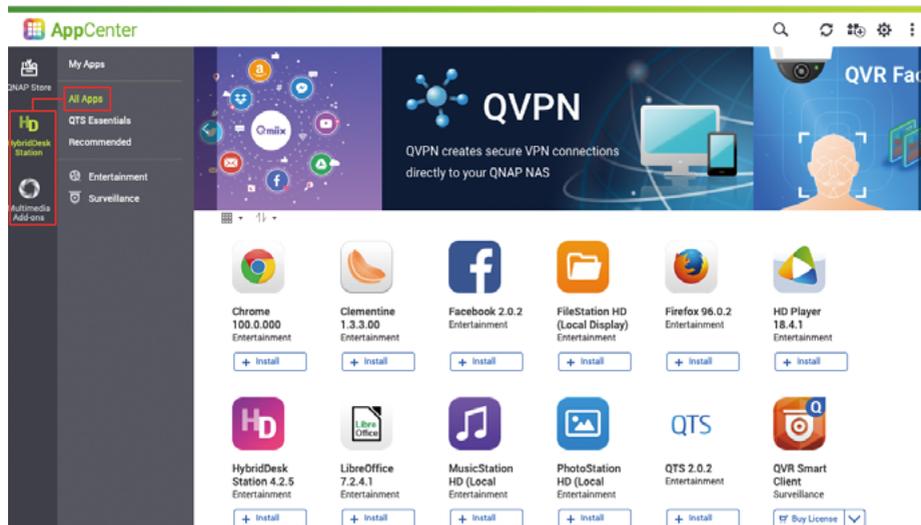
System Information Network Status **System Service** Hardware Information

Service	Status	Port	Description
Antivirus	Disabled	-	
Apple Networking	Disabled	-	
DONS Service	Disabled	-	
Disk Management	Disabled	3260	
Domain Controller	Disabled	-	
FTP Service	Disabled	21	Maximum connections:30
LDAP Server	Disabled	-	
Microsoft Networking	Enabled	-	Server type :Standalone server Workgroup:WORKGROUP Enable WINS server:Disabled

除了系統內建的功能外，你還需要檢查 App Center 已安裝的功能。



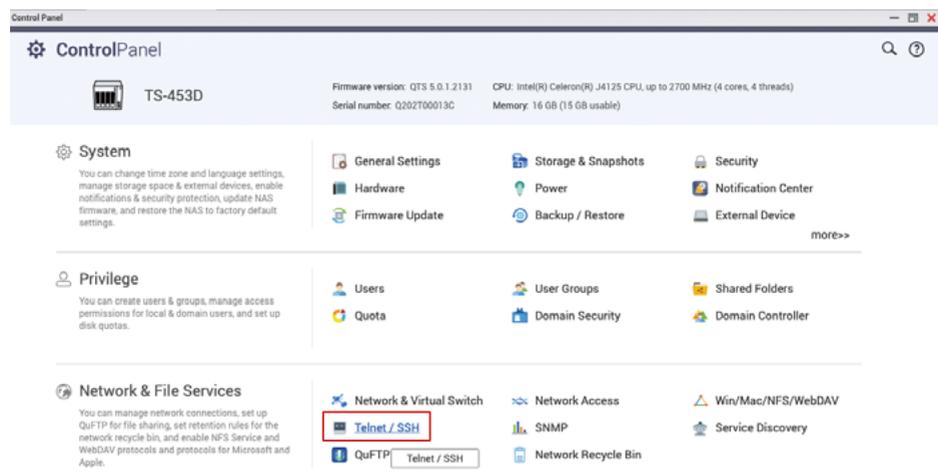
查看最左側，你可以點選「HybridDesk Station」及「多媒體附加元件」，查看對應的套件狀態。



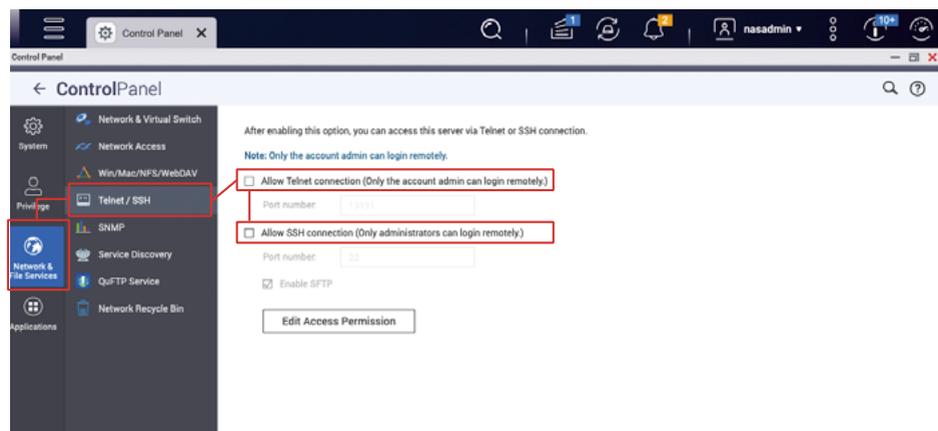
停用 Telnet / SSH 功能

如非專業人員，強烈建議關閉「Telnet」及「SSH」功能。這兩個功能一般是供 QNAP 客服或專業 IT 人員維護系統使用，一般的用戶並不需要使用這個功能，因此建議保持在關閉狀態。

打開「控制台」，點選「Telnet / SSH」



取消勾選「允許 Telnet 連線」及「允許 SSH 連線」，然後按「套用」完成設定。

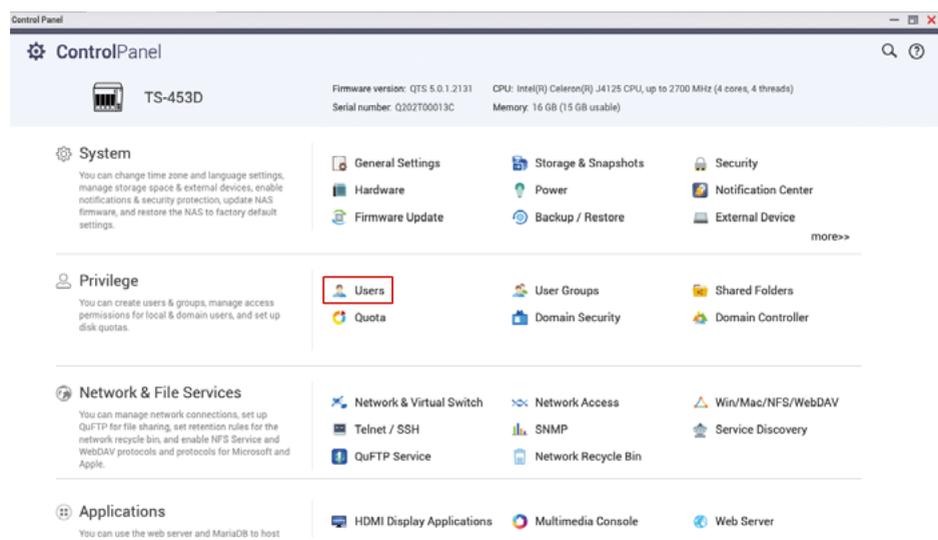


強化系統帳戶安全性

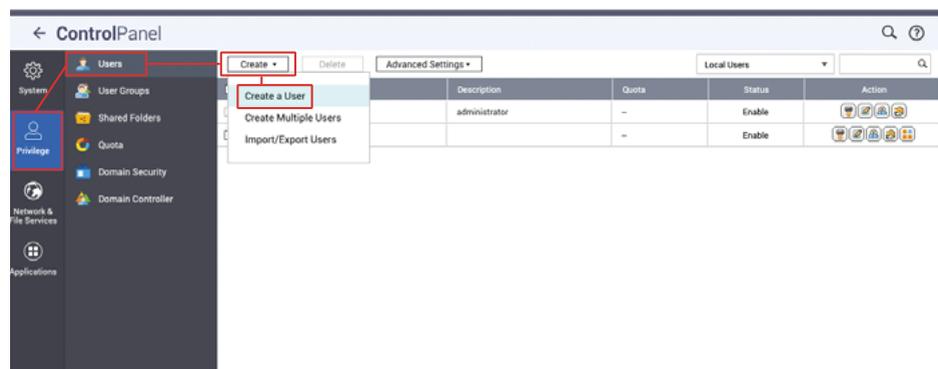
停用預設管理員帳戶「admin」

採用暴力破解密碼的攻擊者一般會針對性攻擊預設的管理員帳戶「admin」，如系統於 QTS 4.5.4 / QuTS hero h4.5.4 或以前的版本初始化，預設的管理員帳戶「admin」將處於啟用狀態，請依照以下步驟建立一個新的管理員帳戶及停用「admin」帳戶。

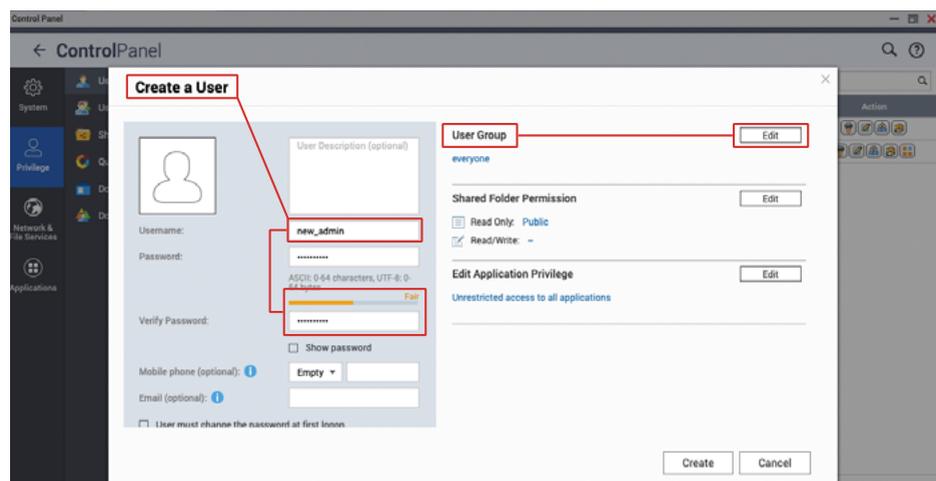
打開「控制台」，點選「使用者」



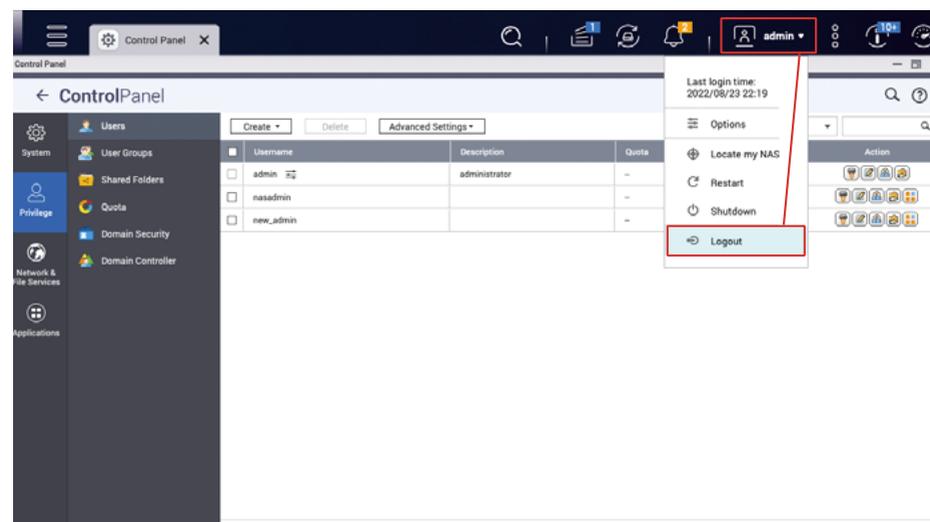
點選「建立」，再點選「建立使用者」



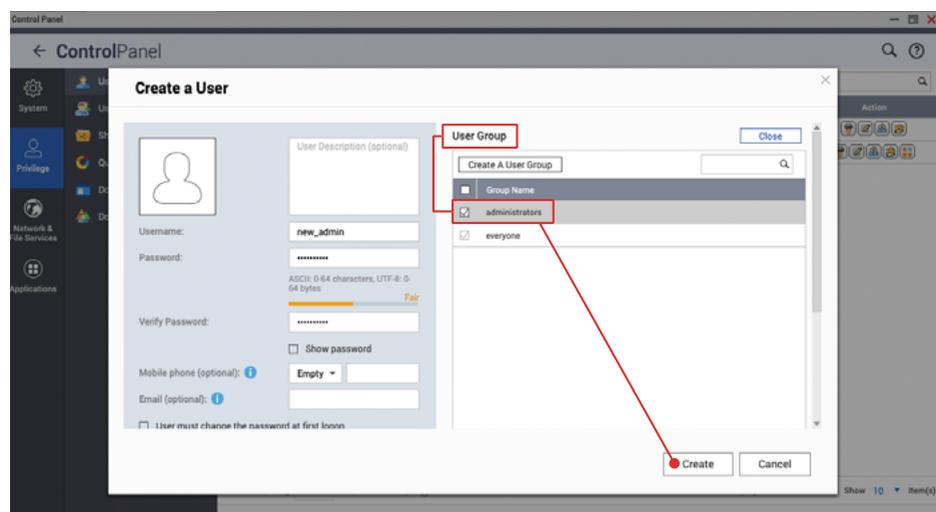
輸入希望用作管理員帳戶的「使用者名稱」，如「new_admin」，以及設定一個「強密碼」。



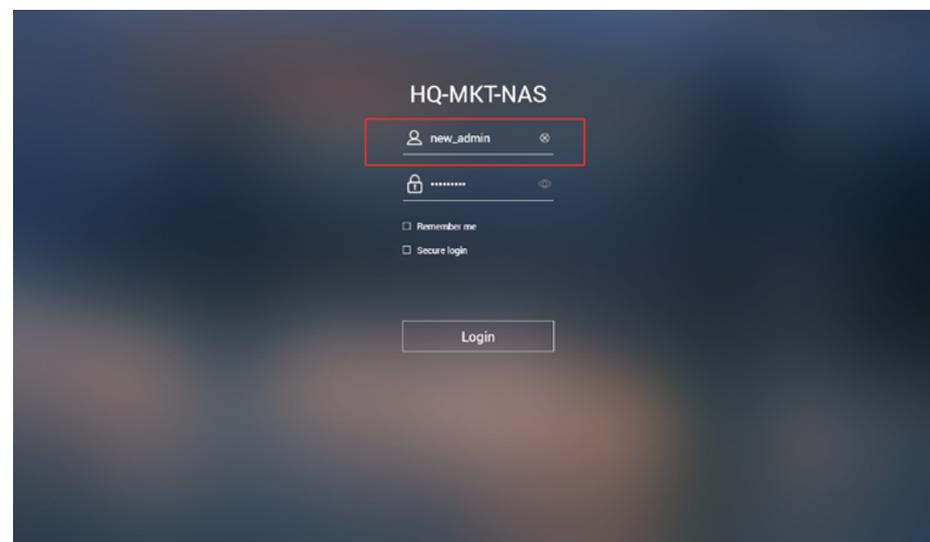
點選最上方的「admin」，打開選單，按「登出」來登出 QTS 網頁管理介面。



於「使用者群組」部分，點選「編輯」，勾選「administrators」群組，按「建立」新增使用者。

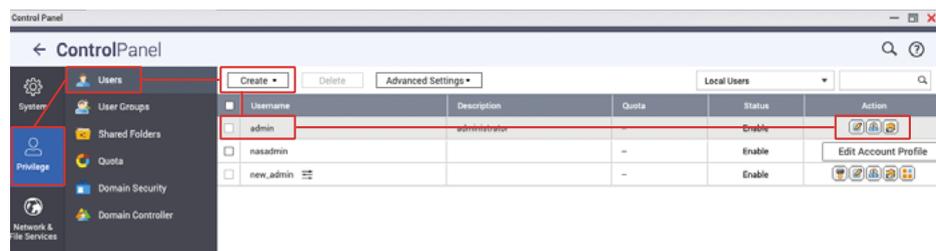


使用剛才建立的「管理員帳戶」登入 QTS 網頁管理介面。

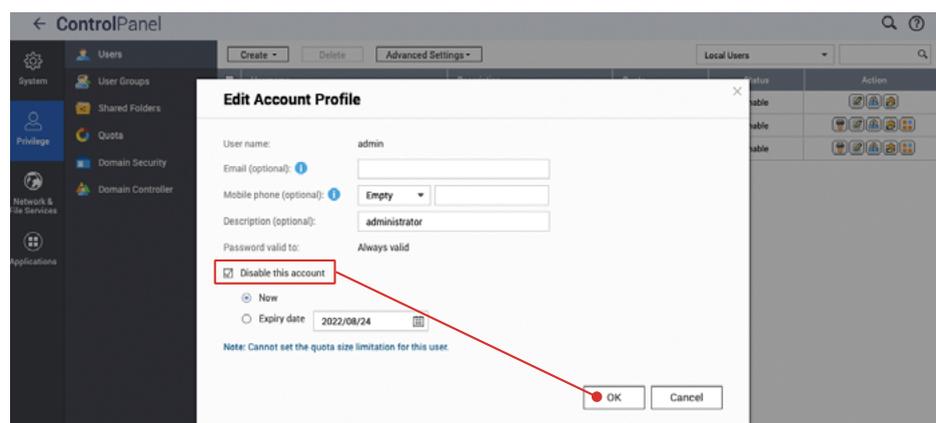


設定密碼強度原則

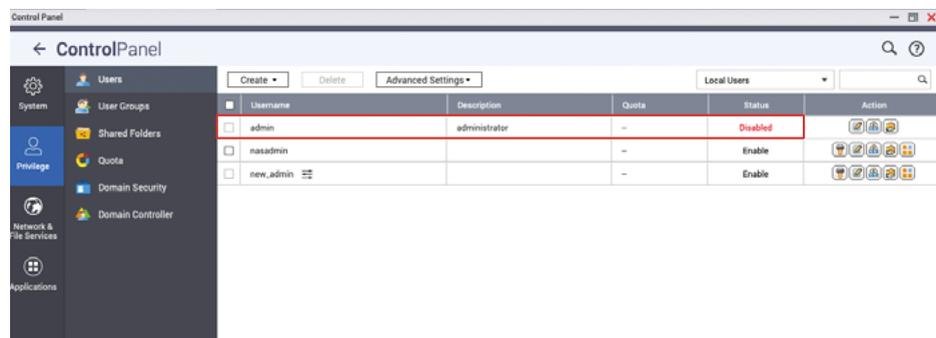
再次打開「控制台」，點選「使用者」，於「admin」那行，點選「編輯帳號資料」



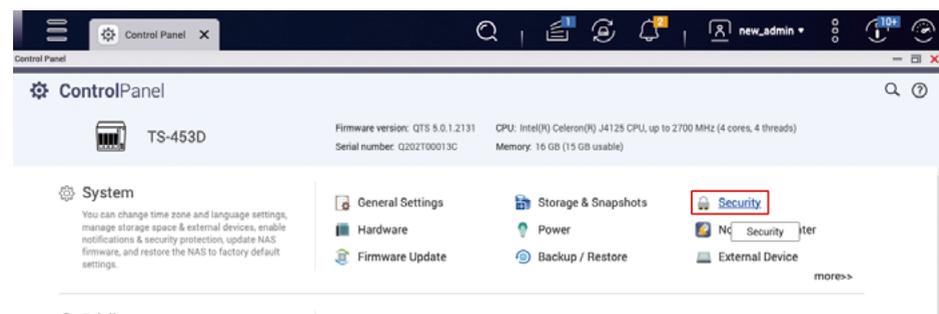
勾選「停用此帳號」，再按「確定完成」



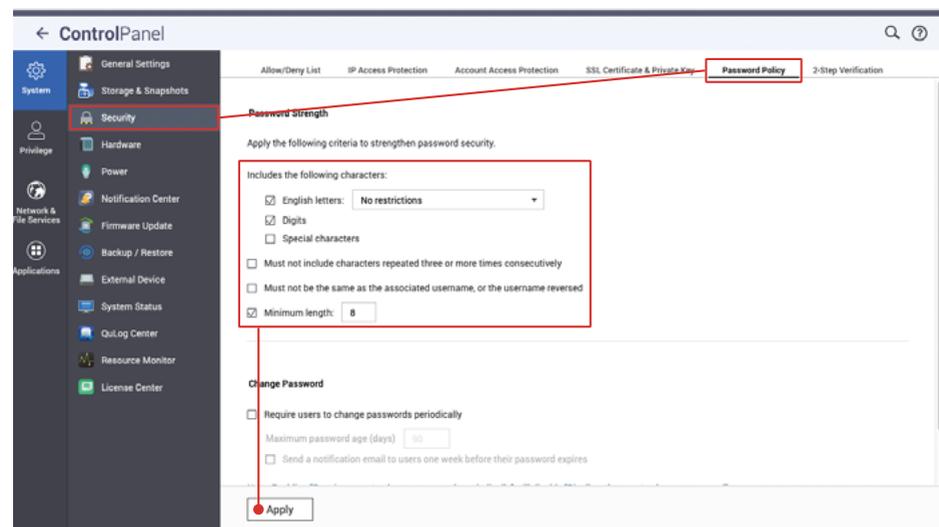
完成後可以看到「admin」狀態為「停用」



除了停用預設的管理員帳戶「admin」外，還需要確保所有帳戶都有採用強密碼。配合「存取保護」，可助你阻止惡意的登入嘗試。如希望擁有更高安全性，可以為所有帳戶強制啟用「兩步驟驗證 (2SV)」，防止被破解密碼及惡意登入。



點選「密碼原則」進入設定頁面，如系統於 QTS 5.0.0 / QuTS hero h5.0.0 或以後的版本初始化，預設已啟用基本的密碼強度條件，你可以按需要設定加強條件，一般建議最少要求密碼包含「大小寫英文字母」、「數字」，而密碼長度建議最少需要「10位」，完成後按「套用」。



啟用存取保護 (IP / 帳號)

「IP 存取保護」及「帳號存取保護」可以防止密碼被暴力破解，當特定 IP 或帳號登入失敗次數過多即會觸發 IP 封鎖或帳號停用，阻止攻擊者嘗試密碼。

點選「IP 存取保護」進入設定頁面，勾選所有服務，你可以按自己的需求去設定「時間間隔」、「失敗次數」及「IP 封鎖時間」，按「套用」完成設定。

Allow/Deny List **IP Access Protection** Account Access Protection SSL Certificate & Private Key Password Policy 2-Step Verification

Automatically block client IP addresses after too many failed login attempts within the specified time period. You can view blocked IP addresses in [QuFirewall](#).

Service	Time interval	Failed login attempts	IP block length
<input checked="" type="checkbox"/> SSH	1 minute(s)	5	5 minutes
<input checked="" type="checkbox"/> Telnet	1 minute(s)	5	
<input checked="" type="checkbox"/> HTTP(S)	1 minute(s)	5	IP
<input checked="" type="checkbox"/> FTP	1 minute(s)	5	IP
<input checked="" type="checkbox"/> SAMBA	1 minute(s)	5	IP
<input checked="" type="checkbox"/> AFP	1 minute(s)	5	IP
<input checked="" type="checkbox"/> RTTR	1 minute(s)	5	IP
<input checked="" type="checkbox"/> Rsync	1 minute(s)	5	IP

*** 為如錯誤地封鎖了正常使用者的 IP 地址可透過以下方式調整封鎖清單：**

1. 在另一台電腦登入 QTS / QuTS hero 管理介面
2. 更換 IP 地址再登入 QTS / QuTS hero 管理介面
3. 以手機瀏覽器登入 QTS / QuTS hero 管理介面
4. 使用 QManager 應用程式

點選「帳號存取保護」進入設定頁面，按自己需要啟用相關的服務及設定「時間間隔」、「失敗次數」按「套用」完成設定。

Allow/Deny List IP Access Protection **Account Access Protection** SSL Certificate & Private Key Password Policy 2-Step Verification

Disable accounts automatically when they fail too many login attempts within a specified time period. You can view the disabled accounts in [Users](#).

Users: All users not in the administrators group

Service	Time interval	Failed login attempts
<input checked="" type="checkbox"/> SSH	5 minute(s)	5
<input checked="" type="checkbox"/> Telnet	5 minute(s)	5
<input checked="" type="checkbox"/> HTTP(S)	5 minute(s)	5
<input checked="" type="checkbox"/> FTP	5 minute(s)	5
<input checked="" type="checkbox"/> SAMBA	5 minute(s)	5
<input checked="" type="checkbox"/> AFP	5 minute(s)	5
<input checked="" type="checkbox"/> RTTR	5 minute(s)	5
<input checked="" type="checkbox"/> Rsync	5 minute(s)	5

*** 如為管理員帳戶開啟「帳號存取保護」，有機會因密碼破解攻擊而讓所有管理員帳戶被停用，屆時只能透過重設功能重新啟用「admin」帳戶，而「admin」帳戶密碼也會被重設，請務必記得在重設後修改密碼。**

啟用兩步驟驗證 (2SV)

點選「兩步驟驗證」進入設定頁面，你可以針對「使用者」或「使用者群組」來強制要求使用「兩步驟驗證 (2SV)」。一般情況下，可以考慮為「系統管理員群組」的帳號啟用這個功能。而其他帳戶，請自行評估風險再套用合適的設定。

點選「本機使用者」開啟選單，選擇「本機群組」。

ControlPanel

← ControlPanel

Allow/Deny List IP Access Protection Account Access Protection SSL Certificate & Private Key Password Policy **2-Step Verification**

2-Step Verification

2-Step Verification (2SV) adds an extra layer of protection to a user's account by requiring an additional one-time security code whenever a user signs in to your NAS. You can enforce 2-step verification for specific users and groups.

Note: The configuration of "Enforce 2SV" between the group and users in the group may not be consistent. See "Status" to check the final 2SV status of users.

Enforce 2SV	Username	Description	Status
<input type="checkbox"/>	admin	administrator	Disabled
<input type="checkbox"/>	masadmin		
<input type="checkbox"/>	new_admin		

Local Users

於「administrators」勾選「強制使用 2SV」，按「套用」完成設定。

← ControlPanel

Allow/Deny List IP Access Protection Account Access Protection SSL Certificate & Private Key Password Policy **2-Step Verification**

2-Step Verification

2-Step Verification (2SV) adds an extra layer of protection to a user's account by requiring an additional one-time security code whenever a user signs in to your NAS. You can enforce 2-step verification for specific users and groups.

Note: The configuration of "Enforce 2SV" between the group and users in the group may not be consistent. See "Status" to check the final 2SV status of users.

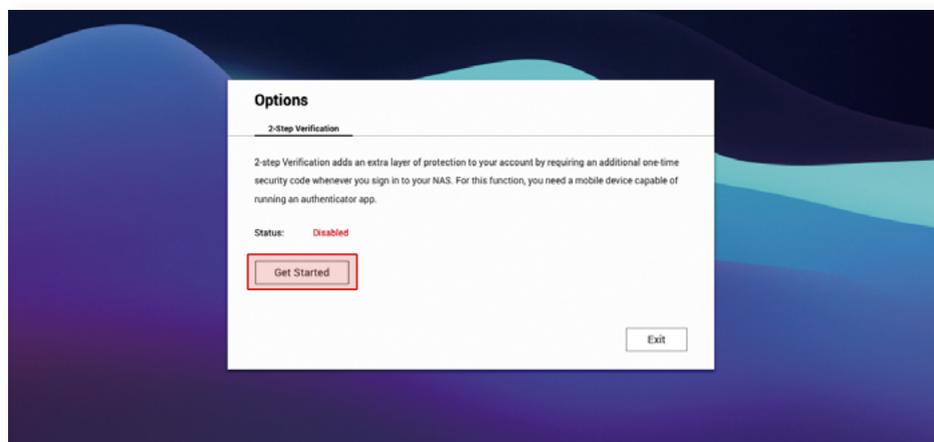
Enforce 2SV	Group Name	Description	Status
<input checked="" type="checkbox"/>	administrators		
<input type="checkbox"/>	everyone		

Page 1 / 1

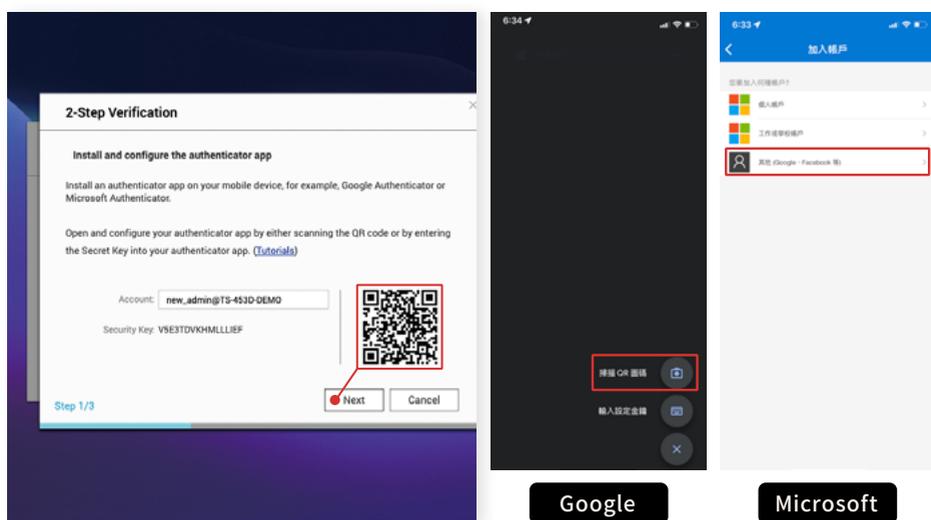
Display item: 1-2, Total: 2 | Show 10 | Item(s)

啟用「強制使用 2SV」後，假如「系統管理員」帳號未設定「兩步驟驗證 (2SV)」，下次登入時會被強制引導到設定該帳號的「兩步驟驗證 (2SV)」設定頁面。

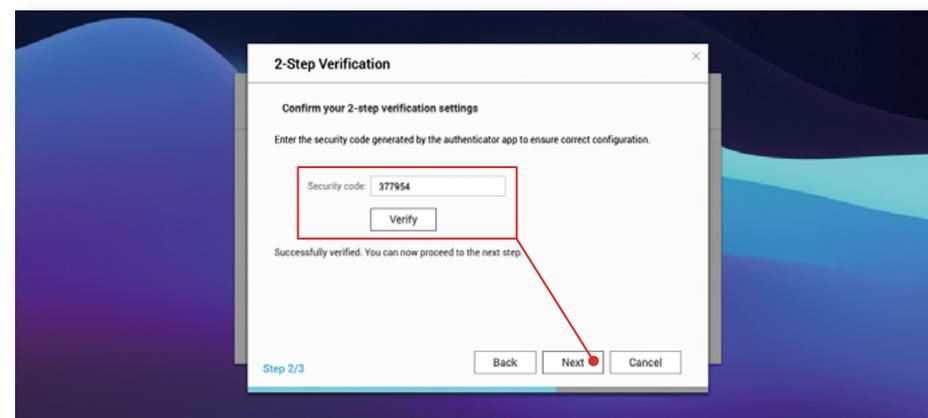
重新登入「系統管理員」帳號，按「開始使用」開始設定。



在行動裝置先安裝「Google Authenticator」或「Microsoft Authenticator」，在該程式掃描 QR 碼加入裝置，然後按「下一步」。

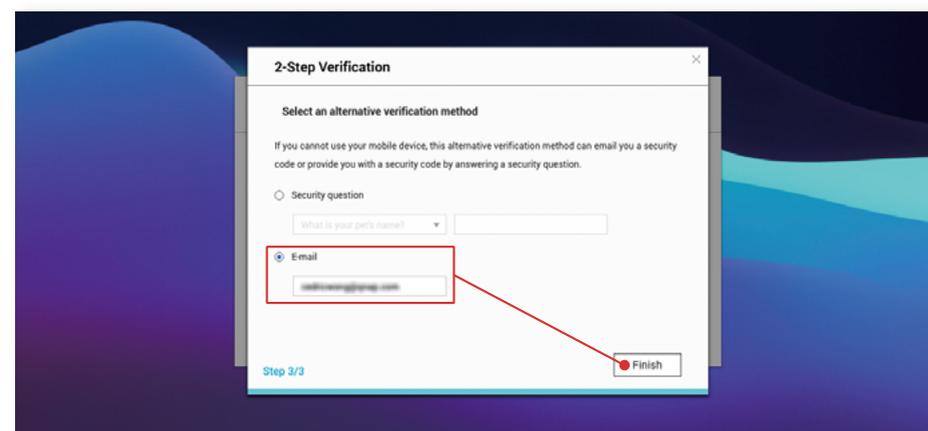


輸入「Google Authenticator」或「Microsoft Authenticator」所產生的六位數字「安全碼」，然後按「驗證」，通過驗證後按下一步繼續。



設定替代的驗證方式*，你可以選擇「安全問題」**或「電子郵件」***，填寫後按「完成」即可啟用「兩步驟驗證 (2SV)」。

- * 如果無法由驗證程式取得「安全碼」，你可以使用回答「安全問題」或使用「電子郵件」接收「安全碼」。
- ** 正確回答「安全問題」即可通過兩步驟驗證，請勿使用過於簡單或容易猜中的問題及答案。
- *** 你必須在「通知中心」加入「電子郵件」通知方式才可正常使用此功能。



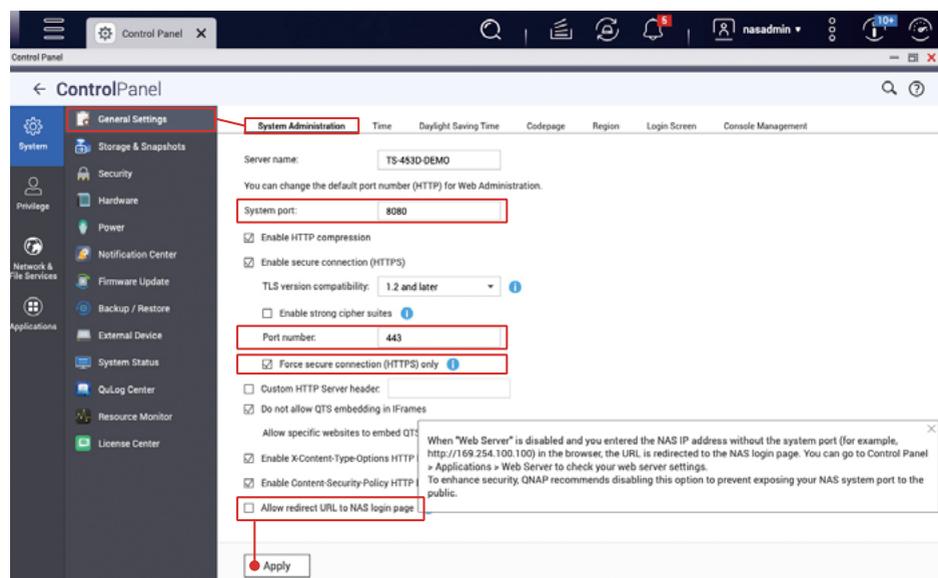
修改預設通訊埠

每個在 NAS 上運行的服務都有對應的通訊埠，除了一些標準化的服務通訊埠無法修改外，其餘的都可以讓使用者自行定義。

攻擊者在尋找攻擊目標時，又或是常被攻擊者利用的物聯網搜尋引擎，一般會優先嘗試預設的通訊埠，為降低被攻擊的機會，修改常用服務的預設通訊埠是十分重要的。以針對 NAS 的攻擊而言，最常見是針對「系統通訊埠」，以下將示範如何修改「系統通訊埠」，而其他功能的通訊埠，可以在對應的設定頁面修改，在啟用相關服務前請務必修改，以保安全。

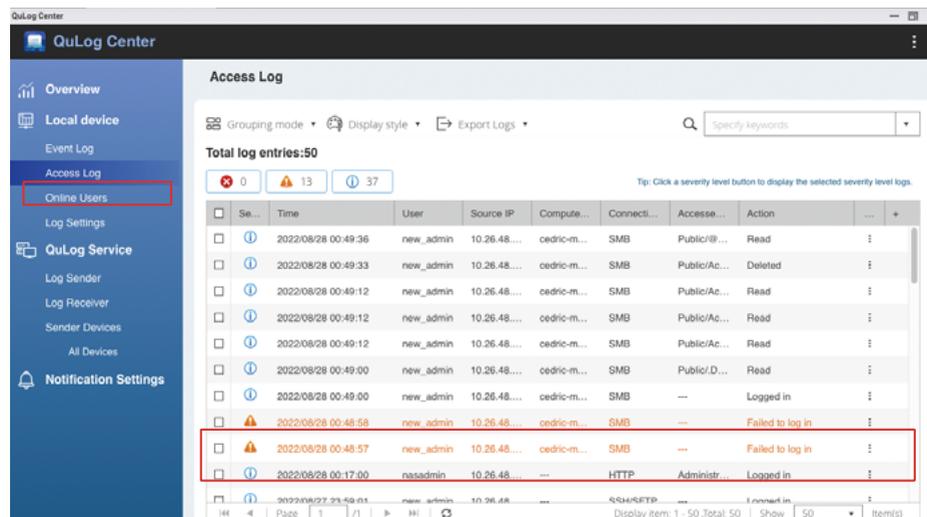
打開「控制台」，點選「一般設定」，「系統通訊埠 (HTTP)」預設為「8080」，你可以輸入介於 1 到 65535 的埠號作為通訊埠，如「56789」；而「系統通訊埠 (HTTPS)」，即開啟了「安全連線」功能的系統通訊埠 (預設為「443」)，也建議修改。同時也建議勾選「強制只使用安全連線 (HTTPS)」，確保所有使用者都是以 HTTPS 安全加密連線傳輸數據，避免攻擊者從中截取帳號密碼等敏感資訊。

另外，也建議取消勾選「允許將 URL 重新導向到 NAS 登入頁面」，避免「系統通訊埠」因自動重新導向而被公開。修改完成後，按「套用」完成設定。

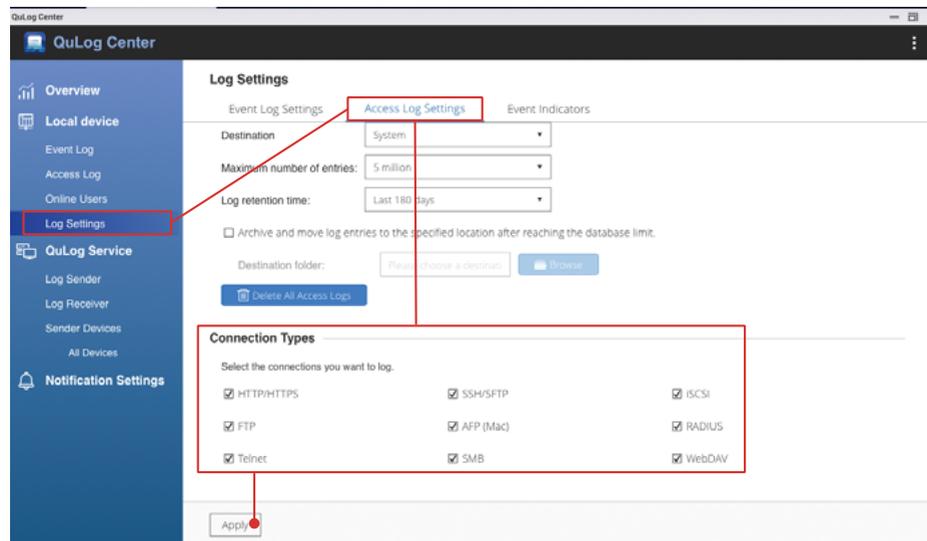


查看存取記錄

存取記錄可以幫助您查看使用者的檔案存取記錄、操作記錄及登入記錄等。當發生問題時，存取記錄可以助您分析問題及作出相應的處理。



打開「QuLog Center」，於左方選單點選「記錄設定」，切換到「存取記錄設定」頁面，於「連線類型」，勾選所有連線服務，然後按「套用」完成設定。



安裝及啟用安全性套件

QNAP 提供多個安全性套件以提高 NAS 安全性。正確設定相關套件可以提高 NAS 安全性，讓使用者用得更安心。



Security Counselor 可助你定期檢查 NAS 設定是否安全，並提示相關的風險。



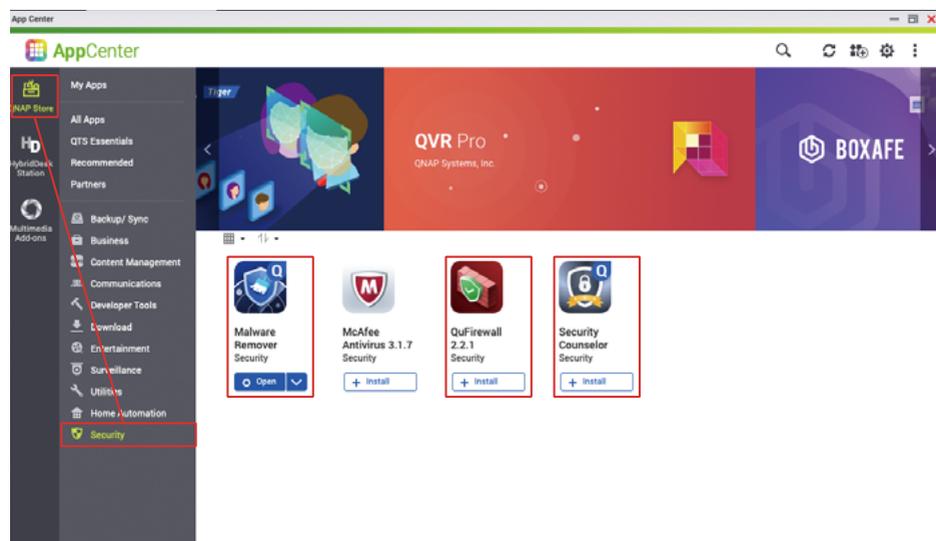
Malware Remover 可助你檢查 NAS 是否存在惡意程式並加以移除。



QuFirewall 能為 QNAP NAS 提供基本防火牆功能，盡可能阻擋攻擊者連線到你的 NAS。

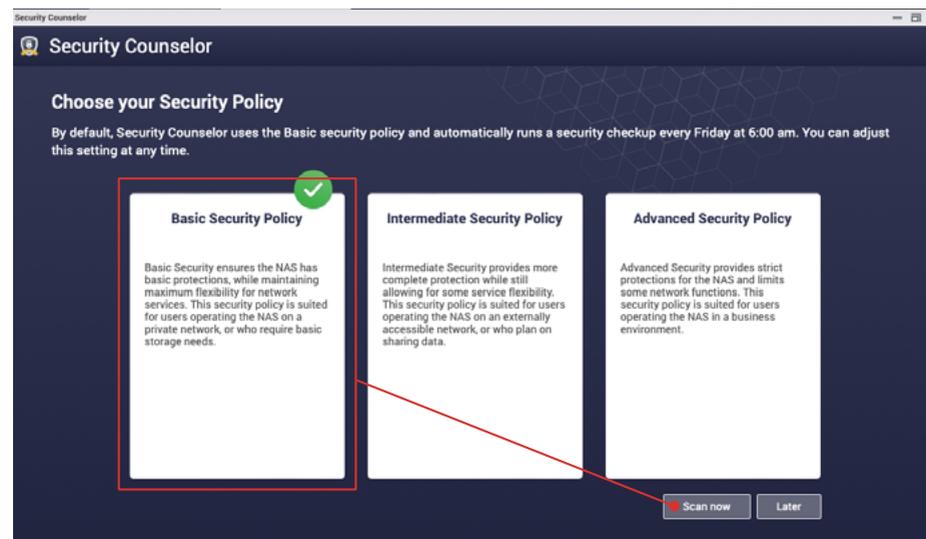
打開「App Center」，於左側點選「安全性」，安裝「Security Counselor」、「Malware Remover」* 及「QuFirewall」。

* QTS 4.4.3 或之後版本及 QuTS hero 已預載 Malware Remover

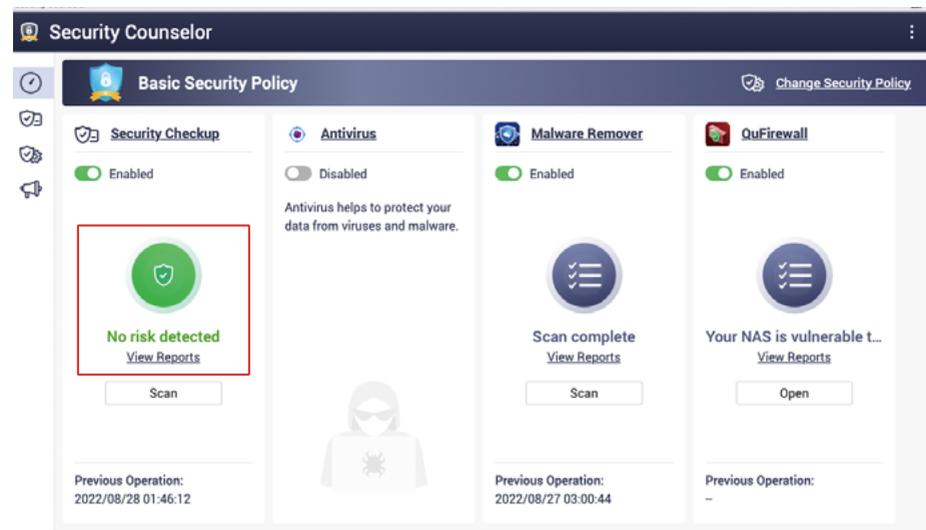


Security Counselor

打開「Security Counselor」，選擇「基本安全性等級」，按「立即掃描」。



請等待掃描完成，正常情況下結果應該是「未偵測到風險」，如有被偵測到風險，請點選「查看報告」了解詳情及按指示修改設定。



以下為故意修改成錯誤的設定而產生的「高風險」掃描結果，你可以按「建議設定小幫手」協助你調整設定。

Security Counselor Basic Security Policy

At High Risk Last scan status: Finished Last scan time: 2022/08/28 01:53:30 Scan schedule: Friday 06:00

Overview **1** High **1** Medium **0** Low **0** Scan

Category	Status	Risk	Result	Action
Account	❌	High	Either this setting is deselected in the Password Policy screen or the current required mini...	⋮
Update	✅	High	Do the current settings in the Password Policy screen include requiring the use of passwords with a minimum of 8 characters?	⋮
Account	✅	High	Either this setting is deselected in the Password Policy screen or the current required minimum length for passwords is below 8 characters.	⋮
Network	✅	High	The web server on your device cannot be directly accessed from the internet using the foll...	⋮
Network	✅	High	The NAS doesn't allow Telnet connections.	⋮
System	✅	High	Run user defined processes during startup is disabled.	⋮

「建議設定小幫手」會列出相關的建議，閱讀及確認後，點選「套用建議」，系統即會自動為你套用相關的設定；而部分設定必須手動修改，請查看左邊的「手動」分頁，依建議調整設定。套用完成後會自動重新掃描，你可以再次檢查掃描結果，確保 NAS 沒有被偵測出安全風險。

Security Counselor Suggested Settings Assistant

The Suggested Settings Assistant offers suggestions that help improve NAS security.

Automatic Adjustment: There are **1** at-risk settings. Select the risk items below to automatically adjust the related settings.

At-risk User Settings	Suggestion
<input checked="" type="checkbox"/> Either this setting is deselected in the Password Policy screen or the current required minimum length for passwords is below 8 characters.	<input checked="" type="checkbox"/> Configure the settings in the Password Policy screen and require the use of passwords with a minimum of 8 characters.

Apply suggestion

Last scan time 2022/08/28 01:53:30

點選左側的「安全檢查」，進去檢查結果畫面，再點選右方的「掃描排程」 打開掃描排程設定畫面。

Security Counselor Basic Security Policy

No risk detected Last scan status: Finished Last scan time: 2022/08/28 02:08:53 Scan schedule: Friday 06:00

Overview **0** High **0** Medium **0** Low **0** Scan

Category	Status	Risk	Result	Action
Update	✅	High	The NAS is using the most up-to-date version of firmware.	⋮
Account	✅	High	The current settings in the Password Policy screen include requiring passwords to have a ...	⋮
Account	✅	High	The default administrator password is not the default password.	⋮
Network	✅	High	The system administration service on your device cannot be directly accessed from the int...	⋮
Network	✅	High	The web server on your device cannot be directly accessed from the internet using the foll...	⋮
Network	✅	High	The NAS doesn't allow Telnet connections.	⋮
System	✅	High	Run user defined processes during startup is disabled.	⋮

「掃描排程」建議設定成**最少一個月一次**，讓系統定期檢查設定及系統狀況。如果有偵測到風險，而通知中心又有正確設定的話，你將會接收到相關的通知以便及早處理。

Security Counselor Basic Security Policy

No risk detected Last scan status: Finished Last scan time: 2022/08/28 02:08:53 Scan schedule: Friday 06:00

Overview **0** High **0** Medium **0** Low **0** Scan

Scan schedule

Disable schedule

Enable schedule

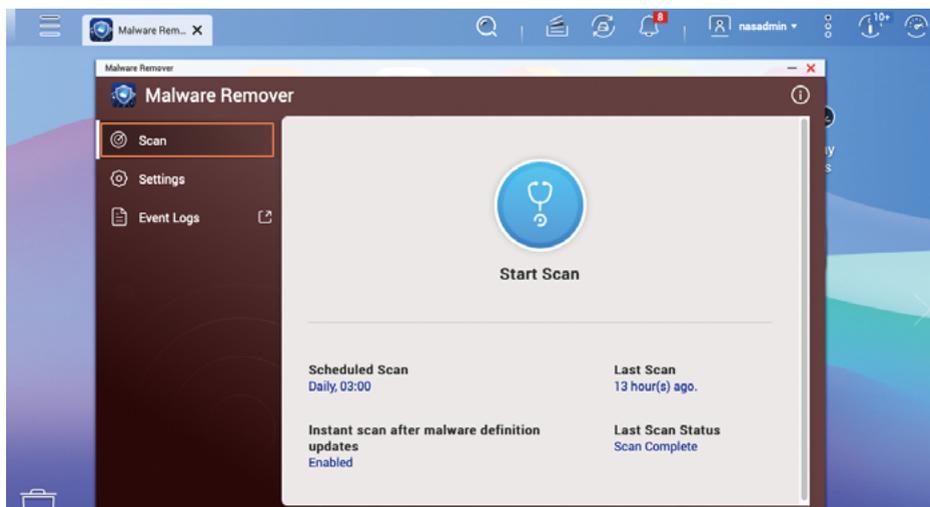
Run on the following days: Friday

Run at the following time: 06:00

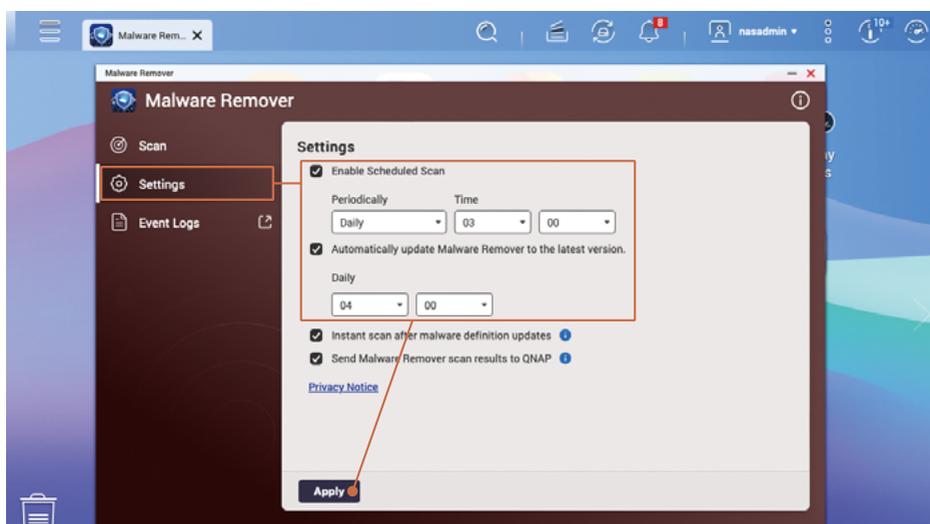
Apply Cancel

Malware Remover

打開「Malware Remover」，可以查看到上一次掃描的狀況，點選左側的「設定」進入設定畫面。

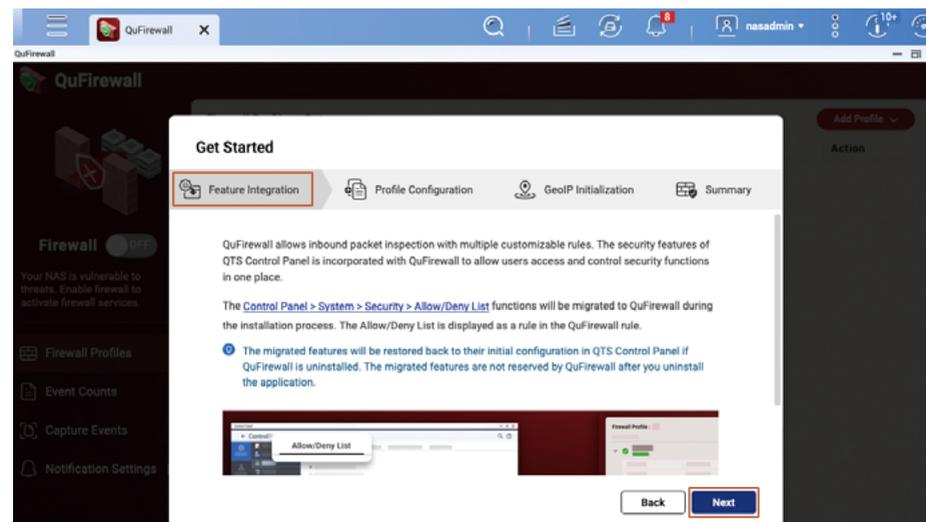


「掃描排程」建議設定成**每天一次**，讓「Malware Remover」定期檢查系統狀況。另外請確保「Malware Remover」自動更新功能保持打開。

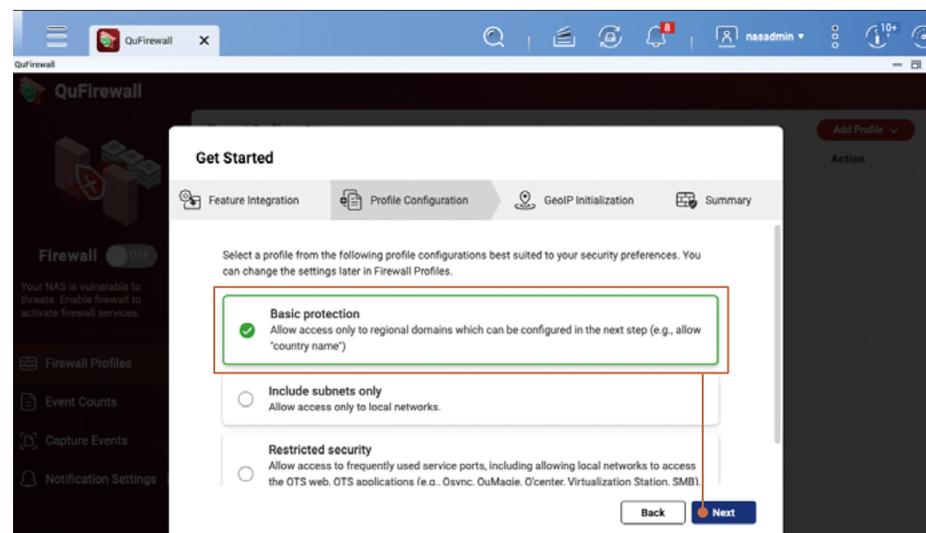


QuFirewall

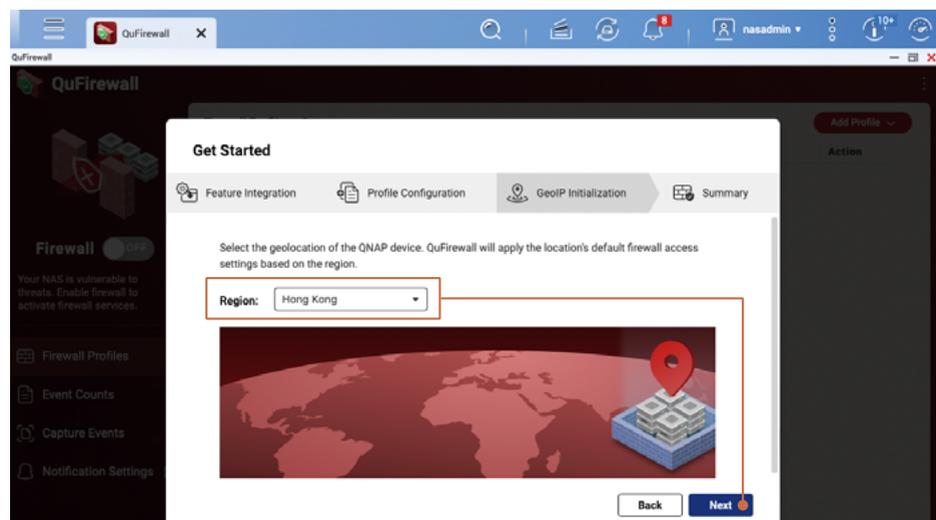
打開「QuFirewall」，在初次打開會進入初始化畫面。閱讀後按「下一步」繼續。



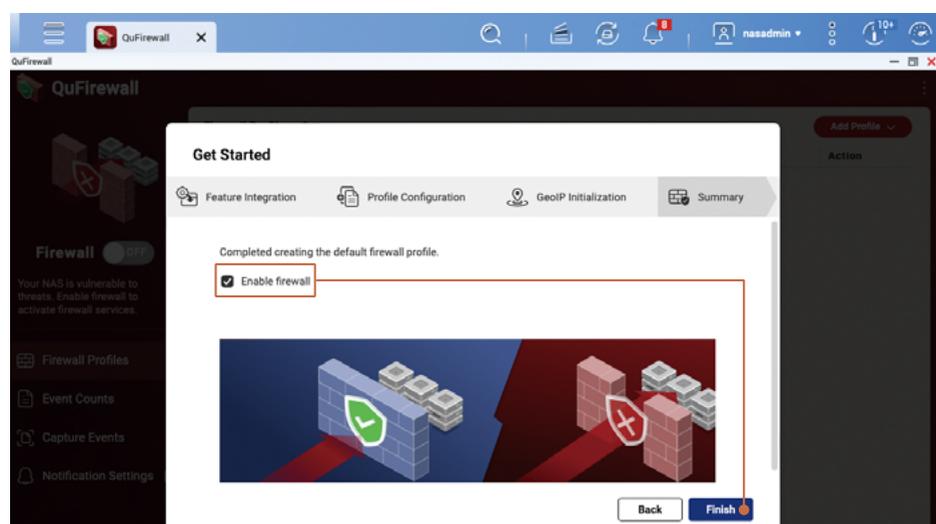
如無特殊的需要，建議選擇「基本防護」，然後按「下一步」繼續。



依你的所在地，設定一個地區。如你在台灣，請選擇「Taiwan」；如你在香港，請選擇「Hong Kong」；如你在澳門，請選擇「Macao」。你可以稍後新增更多地區，完成選擇後按「下一步」繼續。

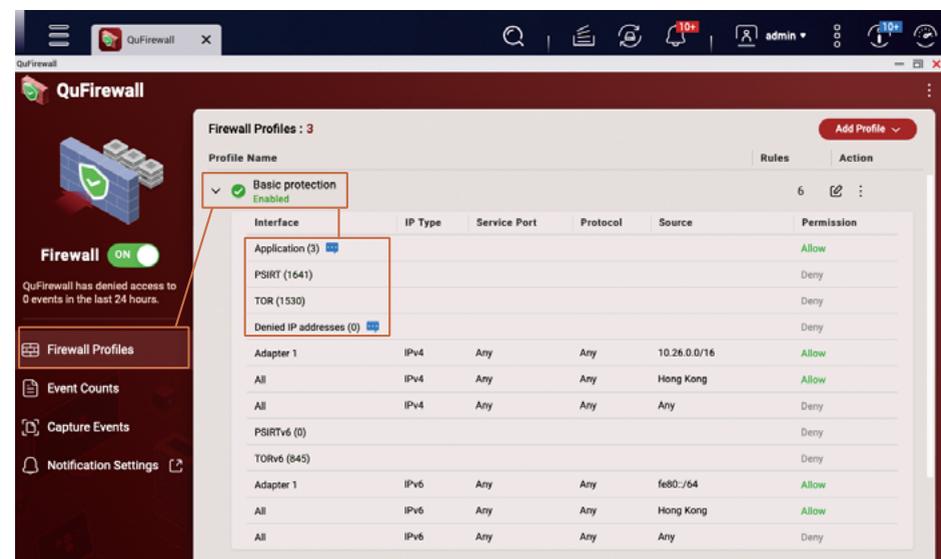


勾選「啟用防火牆」，按「完成」套用設定及啟用防火牆。



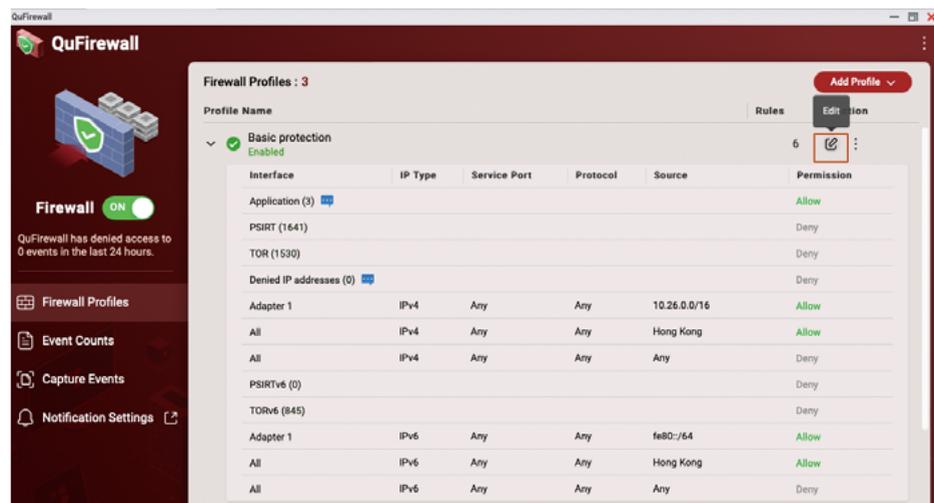
進入 QuFirewall 的管理頁面，可以看到「Basic protection」已經啟用。按下「Basic protection」，即可展開及查看對應的防火牆規則，規則是依據傳入的封包的資訊作檢查，並依防火牆規則允許通過或阻擋。防火牆規則會依次序執行，如不符合條件，即會檢查下一行規則，如全不符合，即會落入最入一條「全部拒絕」規則，防火牆會阻擋相關的連線。

- 「應用程式」規則為系統用來確保系統功能能正常執行而建立的。
- 「PSIRT」規則是 QNAP PSIRT 整理出來的黑名單，當中包含針對 QNAPNAS 進行 攻擊或掃描的 IP 位址。
- 「TOR」規則是用來阻擋來自 TOR Network 的連線，TOR Network 因其匿名的特性而廣泛被不法份子利用，阻擋後可以降低被攻擊的機會。
- 「拒絕的 IP 位址」是被「IP 存取防護」功能封鎖的 IP 位址或使用者手動加入的黑名單。

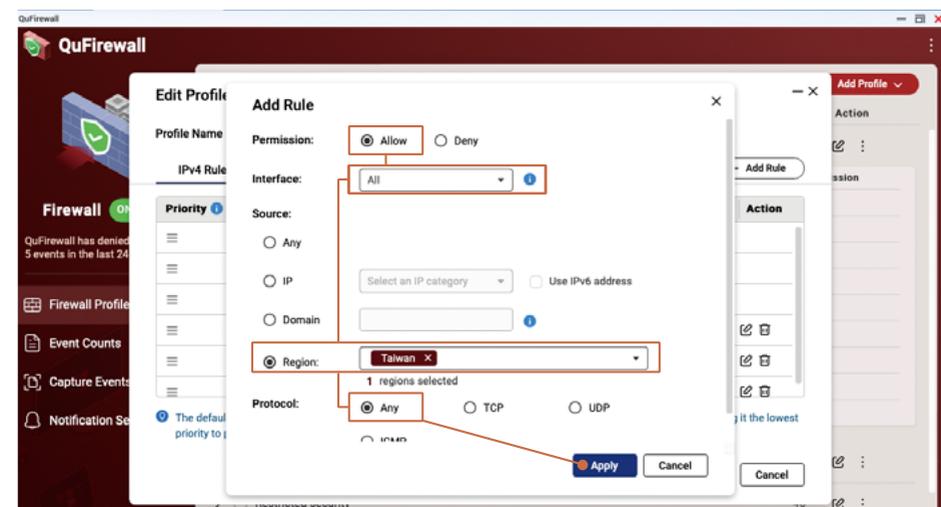


餘下的規則可以讓使用者自訂，在基本防護設定下，只有來自同一內聯網及來自相同地區的互聯網連線才會被「允許」通過。QNAP 建議以「白名單」的概念去管理你自訂的規則，以嚴格限制可以連線到 NAS 的 IP 位址。

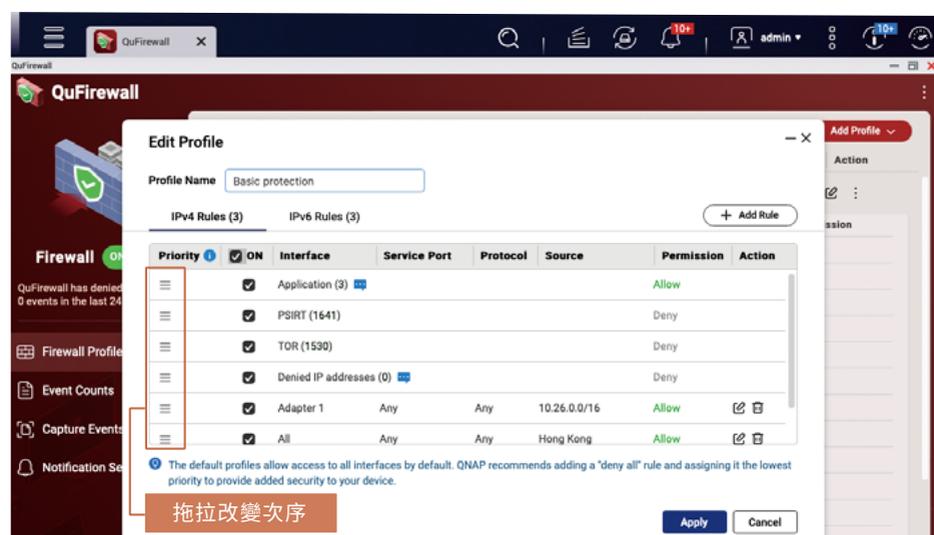
以下示範如何編輯防火牆規則，按下「編輯」按鍵，即可進行編輯防火牆設定檔畫面。



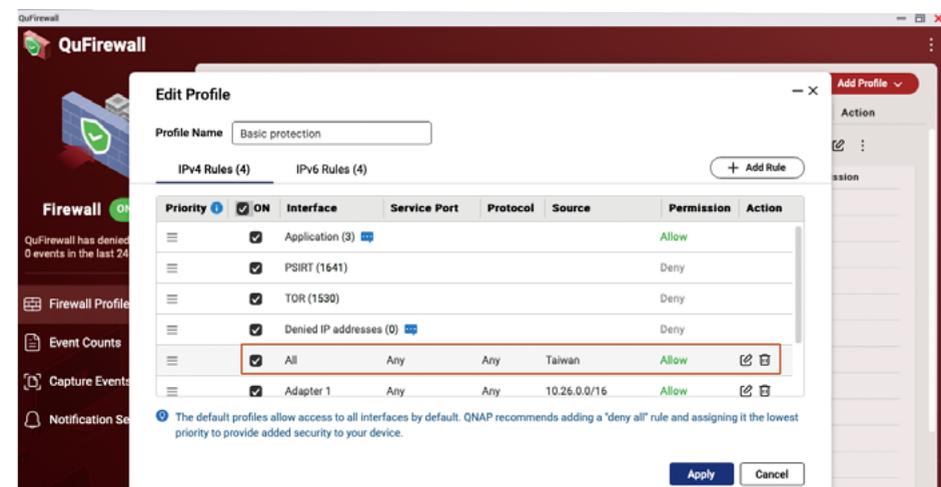
例如我需要允許來自台灣的連線，「權限」需要設定成「允許」；「介面」則設定成「All」；「來源」點選「地區」，再選擇「Taiwan」；「通訊協定」選擇「Any」，完成後按「套用」加入規則。



在編輯設定檔頁面，你可以改動規則的次序或加入新的規則。以下示範加入多一個允許連線的地區，按下「新增規則」，進入設定畫面。



在「編輯設定檔」頁面，即可看到剛剛已新增的規則，如有需要可以調整規則次序，確認正確後，按「套用」生效防火牆設定。



啟用排程快照 (Snapshot)

快照功能可以藉由建立多版本還原點來保護你的重要數據。你可以在 QNAP NAS 設定快照排程，讓系統依排程自動建立快照作為基本的數據保護。

- * QTS 5.0.0 建立的「完整 / 精簡磁碟區」會預設啟用排程快照
- * QTS 5.0.1 或以上版本僅「精簡磁碟區」會預設啟用排程快照
- * QuTS hero h5.0.1 或以上版本建立的「共用資料夾」會預設啟用排程快照

打開「儲存與快照總管」，於左側點選「儲存空間 / 快照」，先確認「儲存空間」是「儲存池」架構，且「儲存池」有足夠的可用空間供快照功能運作。如你的磁碟區類型為「完整磁碟區」，可以考慮透過「調整磁碟區大小 *」和「轉換為精簡磁碟區 *」來釋放「儲存池」空間供快照功能使用。

- * 執行前請先備份數據 - 避免發生意外導致損失。

Storage & Snapshots

Storage Space Storage Pool: 1, Volume: 3, LUN: 0

Name/Alias	Status	Type	Snapshot Re...	Snapshot	Capacity	Percent Used
Storage Pool 1	Ready				5.83 TB	
Data	Ready	Thin volume			2.97 TB	
System (System)	Ready	Thin volume		to 9	98.20 GB	
Thick	Ready	Thick volume			494.54 GB	

Thick Management

Name/Alias: Thick

Capacity: 494.54 GB

Free Size: 494.47 GB

Thin: No

SSD cache: --

Status: Ready

Utilization: 100% / 75% / 50% / 25%

Actions:

- Remove
- Resize Volume
- Set Threshold
- Set Caching Storage
- Check File System
- Rename Volume Alias
- Format
- Convert to Thin Volume

* 打開磁碟區管理即可進行相關調整，以釋放「儲存池」空間

在 NAS 確認「儲存池」有足夠空間後，先點選「磁碟區」，再按上方的「快照」，於選單中點選「快照管理員」。

Storage & Snapshots

Storage Space Storage Pool: 1, Volume: 2, LUN: 0

Name/Alias	Status	Type	Snapshot Rep...	Snapshot	Cap...
Storage Pool 1	Ready				
Data	Ready	Thin volume			
System (System)	Ready	Thin volume		to 9	

Snapshot -

- Take a Snapshot
- Snapshot Replica
- Snapshot Manager
- Import Snapshot
- Global Settings

進入「磁碟區」的「快照管理員」設定頁面，點選右上方的「排程快照」。

Snapshot Manager

Pool Guaranteed Snapshot Space

Data Ready

Schedule Snapshot

Take Snapshot

Daily 01:00

Name (0/0)	Replicated	Capacity	Retention Policy	Taken	Taken By	Status

將「啟動排程」切換到「啟用」狀態，再依自己的需要，修改排程。建議設定成「每日」或「每週」。

Snapshot Settings

Schedule Snapshot Snapshot Retention Pool Guaranteed Snapshot Space

Enable schedule:

Repeat: Daily Time: 01:00 (hh:mm)

Snapshot retention policy: Smart Versioning

The snapshot will be stored in Storage Pool 1 (5.65 TB available).

- Enable smart snapshot
- Description

Note: The performance of a volume or LUN may be affected after taking a snapshot, due to data structure change.

Note: Snapshots will be automatically recycled when available storage pool space is low. [Change policy.](#)

你可以設定快照保留原則來限制快照數量，避免快照佔用過多空間。建議設定「智慧型版本控制」，即三代輪換保留規則 (Grandfather-Father-Son, GFS)，以保留足夠的版本作數據保護，設定完成後按「確定」套用設定。

Snapshot Settings

Schedule Snapshot Snapshot Retention Pool Guaranteed Snapshot Space

How many Snapshot can I have?

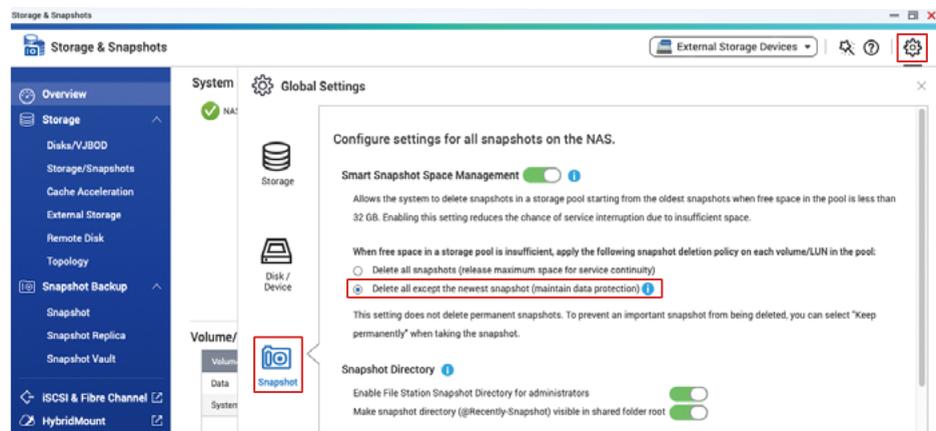
The snapshot retention policy determines how long to keep a snapshot or how many total snapshots to keep. When the specified value is exceeded, the system deletes the expired snapshot or the oldest snapshot automatically.

- Maximum amount of time to keep: 12 Months
- Maximum number of snapshots to keep: 4 Snapshots
- Smart Versioning
 - Hourly snapshots: 24
 - Daily snapshots: 7
 - Weekly snapshots: 4
 - Monthly snapshots: 12

設定快照刪除原則

當儲存池空間不足時，系統會依設定刪除快照以維持系統正常服務，避免因快照佔用太多空間而造成服務中斷。

於「儲存與快照總管」點選右上角的「設定」按鍵，打開「全域設定」，點選「快照」，建議設定成「除了最新快照外全部刪除」，避免全部快照被回收而失去保護。

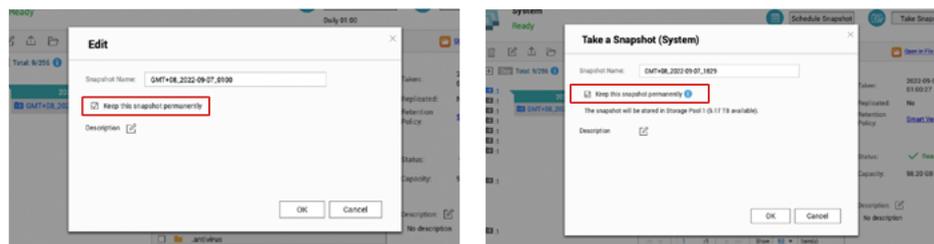


如希望系統在「儲存池」空間不足時仍然保留所有快照，請關閉「智能快照空間管理」。但請注意，這樣在「儲存池」空間不足時將造成「儲存池」進入「唯讀 / 刪除」狀態，需要手動刪除快照方可恢復「儲存池」正常運作。停用此功能後請務必定期留意空間使用量。



為避免因快照刪除原則造成保護失效，建議當存入大量資料後，將全部快照或部分快照設定為「永久保留」*，避免快照被系統回收。

* 需手動刪除才能釋放空間，建議定期手動建立及刪除



NAS 安全設定檢查清單

設定系統通知 (Notification Center, 通知中心)

- 設定最少一個通知方式
- 建立「警示通知」通知規則
- 建立「韌體更新」通知規則

啟用韌體 (QTS / QuTS hero) 自動更新功能

設定 App Center

- 更新所有套件到最新版本
- 禁止安裝不具有有效數位簽章的應用程式
- 啟用自動更新功能

停用或移除不必要功能

- 檢查已啟用的服務是否必要
- 檢查已啟用的 App Center 套件是否必要
- 停用 SSH 服務
- 停用 Telnet 服務

強化系統帳戶安全性

- 停用預設「admin」帳戶
- 設定密碼強度原則
- 啟用 IP 存取保護
- 啟用兩步驟驗證 (2SV)

修改預設系統通訊埠

啟用存取記錄

安裝及啟用安全性套件

- Security Counselor
 - 啟動排程掃描
- Malware Remover
 - 啟動排程掃描
- QuFirewall
 - 啟用防火牆
 - 設定 Geo-IP 地區
 - 啟用 PSIRT 規則
 - 啟用 TOR 規則

啟用排程快照

- 定期設定「永久保留快照」

常見問題

Q NAS「斷網」是否會比較安全？

A 不是。NAS「斷網」一般是指切斷 NAS 對外發起連線的能力。雖然有部分惡意軟件需要對外連線才能執行，但仍然有不需要對外連線也能執行的惡意軟件能成功進行惡意行為。因此，此舉不但無法阻止攻擊者進行不法行為，更會讓部分系統功能無法正常運作，例如是軟體自動更新功能及通知功能。正確的做法是限制連向 NAS 的流量，如避免曝露在互聯網上，方能提高安全性。

Q 我的硬碟設定了 RAID，是否不需要備份？

A 不是。RAID 只能避免資料因硬碟故障而造成損失，所以他並不是一種備份方式。對於資料被刪除、誤改或被加密，是完全沒有保護能力的。因此**建議以備份 3-2-1 原則**去妥善備份數據。

Q 我已經設定了「快照」，是不是不需要備份？

A 不是。因「快照」是跟你的數據儲存在同一組硬碟上，因此假如出現 RAID 故障等情況，數據依然是會丟失的。此外，如攻擊者能取得足夠的權限（如攻擊者成功破解管理員帳戶），「快照」也有被刪除的可能性。因此建議以備份 3-2-1 原則去妥善備份快照檔案。

Q 我的 NAS 沒有曝露於互聯網，是不是不可能受到攻擊？

A 不是。雖然大部分網路攻擊是來自互聯網，但是 NAS 在內聯網仍然存在被攻擊的風險。例如你內聯網的電腦或其他裝置被入侵或安裝惡意軟體，受感染的裝置也有機會攻擊內聯網的其他裝置，於內聯網擴散。在電腦上安裝防毒軟體及部署網路安全產品能有助你應對相關威脅。例如是 QNAP ADRA NDR，具備偵測內聯網可疑活動能力及自動隔離功能。同時也建議以備份 3-2-1 原則去妥善備份數據。

Q 我的 NAS 已經使用了一段長時間，我應該如何檢查有沒有被安裝惡意程式？

A 如發現處理器負載異常升高，軟體更新功能失效或 App Center 存在不明套件等情況，都有可能是被安裝了惡意程式。建議先手動安裝新最版本 Malware Remover 進行掃描。如仍然無法解決，請即聯絡 QNAP 技術支援團隊取得協助。

Q 如果我有必要開放部分服務到互聯網，我應該如何設定才能保障安全？

A 請先確保 NAS 已安裝最新版本的韌體及套件。你可以啟用 QuFirewall 以提供基本的防火牆防護，當中的「PSIRT」及「TOR」規則能助你阻擋部分攻擊者連線。如需強化防禦能力，建議採購專業的防火牆設備。另外，如儲存池空間許可，可建立「快照」作基本的資料保護；也建議以備份 3-2-1 原則去妥善備份數據，為最壞的情況作準備，避免損失。

Q 我的 NAS 已經 EOL 及無法取得最新版本 QTS，還可以安全地使用嗎？

A 已經 EOL 的機種只能獲得有限度的支援，因此只建議限制於內聯網使用及妥善備份，以保安全。

Q 為什麼我會一直收到 NAS 登入失敗的警告？

A 如登入失敗的 IP 地址來自互聯網，代表你的 NAS 正遭受暴力破解密碼攻擊，請避免曝露 NAS 在互聯網上，及依照本教學提高 NAS 防護能力。如登入失敗的 IP 地址來自內聯網，請檢查該 IP 地址的裝置是否被安裝惡意軟體。

Q 為什麼我的檔案都變成奇怪的附檔名？

A 這通常是已經不幸感染了勒索病毒。你可以透過檢查 NAS 存取記錄去判斷加密動作是來自其他電腦還是 NAS 本機，再作適當的處理。如有需要，請聯絡 QNAP 技術支援團隊取得協助。

Q 如果我的 NAS 感染了勒索病毒，應該如何處理？

A 因勒索病毒大多採用無法破解的加密方式，如沒有正確的金鑰是無法解鎖檔案，因此只能用備份或快照還原檔案。

請立即依本教學修改路由器設定，避免曝露 NAS 在互聯網上，避免被二次攻擊。其次，應立即暫停所有同步任務以及將快照設定成永久保留，避免失去備份檔。如你的數據有備份或有可供還原的快照，你可以在更新 NAS 韌體和套件後及完成 Malware Remover 掃描後，再還原檔案。如果數據沒有備份的話，請先備份勒索病毒留下的勒索信及支付贖金的方法，再嘗試使用數據救援 (Data Recovery) 等方式嘗試救回部分數據。如有需要，請聯絡 QNAP 技術支援團隊取得協助。

Q 我不斷看到有媒體報導 QNAP 產品修正弱點的新聞，是不是代表 QNAP 產品並不安全？

A 世上沒有完美的軟體和硬體，不論是各廠商自行開發的軟體或開源軟體，甚至是硬體，都一直被發現弱點，再由廠商修補。QNAP 跟各大科技同業一樣持續修正已知的弱點，再盡快發佈更新檔供使用者更新，以保障使用者的裝置及數據安全。QNAP PSIRT 並會在合適的時間發出資安通報對外披露，讓使用者可以有所行動。QNAP 認為公開透明處理弱點，能保障使用者的知情權及有助改善產品安全性，也建議使用者訂閱 QNAP 資安通報，搶先在媒體報導前取得相關、正確及完整的資訊。

QNAP 資安通報：

<https://www.qnap.com/go/security-advisories/>



Q 什麼是備份 3-2-1 原則？

A 備份 3-2-1 原則是資訊科技業界公認的備份原則，為最壞的情況做好準備，一旦災難發生時，也有備份檔可以恢復數據，避免損失，保障安全。

備份 3-2-1 中的「3」是指備份最少要有三份；「2」是指最少兩種儲存媒介；而「1」是指最少一份是異地備份 (Offsite Backup)。

基於備份 3-2-1 原則，不論是誤改、誤刪、硬件損壞、中毒、災難如火災、水災等，都會有備份檔可以還原。

要達到這個原則，可以利用 QNAP 提供的 Hybrid Backup Sync 3 (HBS3) 套件、Snapshot Replica 或 SnapSync (僅 QuTS hero 支援) 等功能，將 NAS 上的重要數據備份到異地 NAS、公有雲端、外置儲存裝置、其他檔案伺服器，確保萬無一失。

Hybrid Backup Sync 3 (HBS3) 相關教學：

<https://www.qnap.com/go/how-to/tutorial/article/hybrid-backup-sync>



Snapshot Replica 相關教學：

<https://www.qnap.com/go/how-to/tutorial/article/save-snapshots-to-other-qnap-nas-with-snapshot-replica>



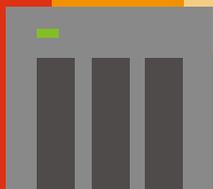
SnapSync 相關教學：

<https://www.qnap.com/go/how-to/tutorial/article/best-practices-for-the-configuration-of-realtime-snapync>



如希望再提高安全性，可以加入離線備份 (Offline Backup) 或備份到 QuTS hero 一寫多讀 (WORM, Write Once Read Many) 儲存空間，防止資料被竄改，達到更安全的境界。

MEMO



2 0 2 3

Security Guide

QNAP



QNAP SYSTEMS, INC.

TEL : +886-2-2641-2000 FAX: +886-2-2641-0555 Email: qnapsales@qnap.com

Address : 3F, No.22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221, Taiwan

QNAP may make changes to specification and product descriptions at any time, without notice.

Copyright © 2023 QNAP Systems, Inc. All rights reserved.

QNAP® and other names of QNAP Products are proprietary marks or registered trademarks of QNAP Systems, Inc. Other products and company names mentioned herein are trademarks of their respective holders.