

# QNAP NAS

資 安 防 禦 手 冊



QNAP SYSTEMS, INC.

誠摯感謝您對 QNAP 產品的愛用，將您的資料託付給 QNAP NAS 進行妥善保存。我們深知，使用者的信任是我們最珍貴的資產，我們亦時時精進產品資安設計，力求完善。

然而，面對網際網路上的各種攻擊與威脅，我們需要使用者和我們一起積極面對，以完善的資安觀念及良好使用習慣，共同抵禦惡意病毒的攻擊。透過這份手冊的指引，能夠極大程度地保護您的檔案安全。

威聯通科技

總經理 張明智

www.qnap.com

## 提升安全性的最佳實務

隨著駭客的攻擊手法日新月異，資料安全的防禦面向也隨之擴大。從 NAS 系統的密碼保護及系統權限、檔案層級的加密措施、作業系統及應用軟體的更新、網路連線的設定，到資料備份及災控防護的工具應用，皆是 NAS 使用者必須注意的防禦面向。QNAP 針對多面向資安防禦，健全產品資安功能。以下是 9 個資安防範要點，協助 QNAP NAS 使用者快速具備基本的資安防護觀念：

1. 移除未知或可疑使用者帳戶
2. 移除未知或鮮少使用的 NAS 應用程式
3. 在 myQNAPcloud 停用自動路由器設定
4. 設定裝置存取控制
5. 避免在網際網路公開預設埠號
6. 安裝並執行最新版本 Malware Remover
7. 變更所有帳號的密碼
8. 更新已安裝的應用程式至最新版本
9. 更新 NAS 作業系統至最新版本

後續我們將逐一說明 QNAP 各項資安防護設計，進一步建構完善的 NAS 防禦計畫。

# 使用高強度密碼

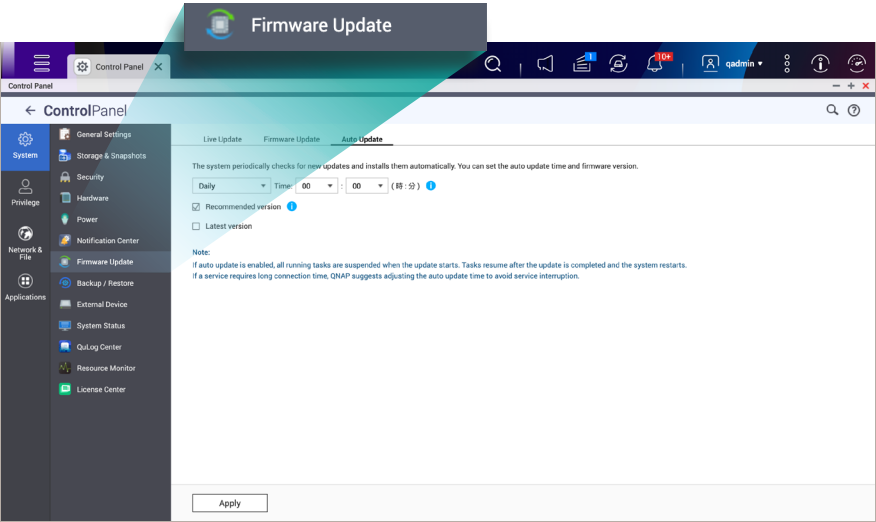
常見的資安事件中，攻擊者大多優先找尋採用弱密碼的帳號、或是系統預設管理員帳號 admin 加以破解。我們建議使用者停用系統預設的 admin 帳號，並且設定一組高強度密碼來保護您的管理員帳號。高強度密碼條件如下表，盡可能地符合以下條件，可大幅降低密碼破解機率。

條件	說明
英文字母	密碼至少具有一個大寫和一個小寫字母
數字	密碼必須至少有一個數字
特殊字元	密碼必須至少有一個特殊字元
避免重複	不允許重複字元。例如：AAA。
排除使用者名稱	密碼不可與使用者名稱相同，亦不可包含顛倒之使用者名稱。例如，使用者名稱為：user1 而密碼為：1resu。
最小長度	密碼長度必須大於或等於指定數量。密碼長度最多為 64 個字元。

除了使用高強度密碼外，使用者亦應定期更改密碼，您可與系統設定中指定使用者密碼的有效天數。

# 軟體更新很重要

使用舊的軟體版本非常容易使 NAS 置於風險中！QNAP 開發團隊全時關注資安資訊，一旦發現漏洞即刻予以修補，同時發送軟體及作業系統更新，獲得更新的軟體即可不受已知漏洞的危害。我們建議使用者於 QTS 系統中的「韌體更新」啟用自動更新，保持使用最新版本的軟體，並於 QNAP 官網的發行說明網頁查看軟體更新內容。

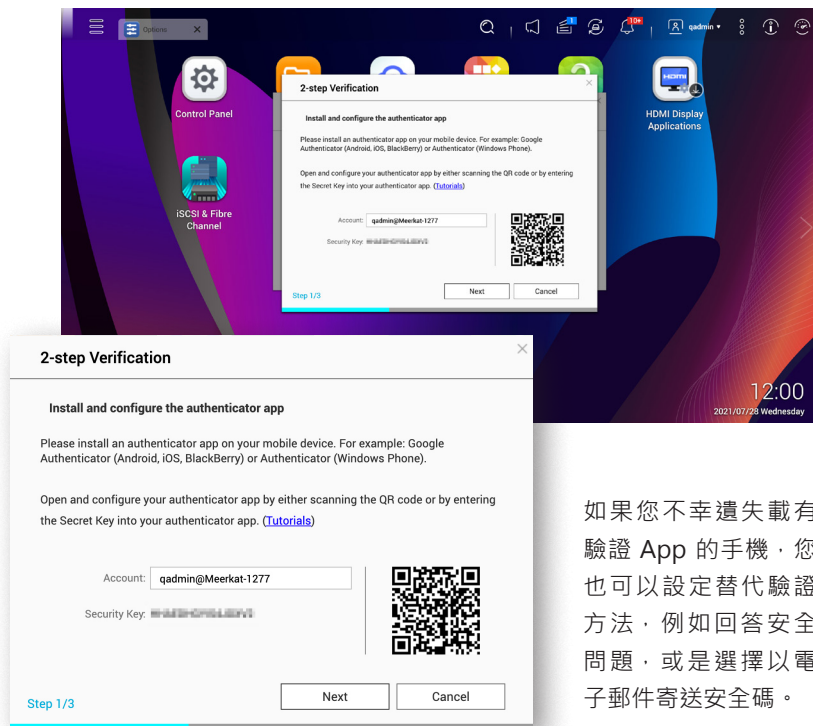


於 QTS 4.5.3 之後，App Center 預設自動安裝必要的更新。較舊的機種需要至控制台介面設定為自動更新。若您的 NAS 沒有與外網連線，則可透過 QNAP 官網的下載中心取得最新版本軟體，並進入 QTS 控制台的韌體更新功能，完成更新。

## 啟用兩步驟驗證

兩步驟驗證能夠加強使用者帳號安全。啟用此功能後，除登入所需的帳號認證資料外，系統還會要求使用者於行動裝置上輸入安全碼。多一道程序把關您的帳號安全，如此一來駭客將會更難攻破您的帳號資訊。

若要使用兩步驟驗證，您必須在行動裝置安裝驗證應用程式。此應用程式必須使用基於時間的一次性密碼 (TOTP) 演算法建置驗證服務。QTS 支援 Google Authenticator (Android、iOS 及 BlackBerry) 和 Authenticator (Windows Phone)。



如果您不幸遺失載有驗證 App 的手機，您也可以設定替代驗證方法，例如回答安全問題，或是選擇以電子郵件寄送安全碼。

## 讓我們為您評估安全性

網際網路上的資安風險不盡其數，QNAP 獨特的安全評估中心 (Security Counselor) 應用程式可稽核 NAS 上的資安弱點，並提供系統設定調整建議，避免您的 NAS 受到多種攻擊手段的危害。

在 Security Counselor 中，您可以依據 NAS 使用需求，指定不同的安全性等級建議，選擇單次或排程安全性掃描。亦可調整更多設定，例如：IP 封鎖、安全憑證、密碼原則等等。



## 即時掃除威脅

可定時掃描您的 NAS 是否受到惡意軟體影響，並在 NAS 受到已知病毒感染時即刻進行清除。加密勒索軟體不斷被改良、變種，防不勝防。Malware Remover 會自動下載最新惡意軟體定義檔，搭配自動掃描，給您零時差的資安防護。



除了提供病毒掃除威脅之外，您亦可設定將 Malware Remover 掃描結果傳送給 QNAP，讓 QNAP 快速更新惡意軟體定義檔，共同強化 NAS 資安防護。

## 為 NAS 加裝安全防火牆

網路上的資安威脅不分內外網，單靠設置在區網邊緣的網路型 (Network-Based) 防火牆設備 (邊界)，不足以保障全方位的安全。隨著當前主流的零信任網路 (Zero Trust Networks) 概念崛起，您可在 QNAP 設備上安裝並啟用 QuFirewall，打造主機型 (Host-Based) 防火牆 (微邊界) 來保護您的重要資料及服務。



QuFirewall 這款免費 QNAP NAS 應用程式可供您設定傳入方向的網路流量規則，來允許或拒絕連線，提高 NAS 在網際網路上的安全性。同時，QuFirewall 也支援 GeoIP，能依照特定區域作為連線與否的判斷條件，完全阻絕陌生區域的連線請求。如果需要更強大的保護，您亦可從 Virtualization Station 內的虛擬機市集安裝熱門的開源防火牆 pfSense。



## 不要在網路上暴露 NAS

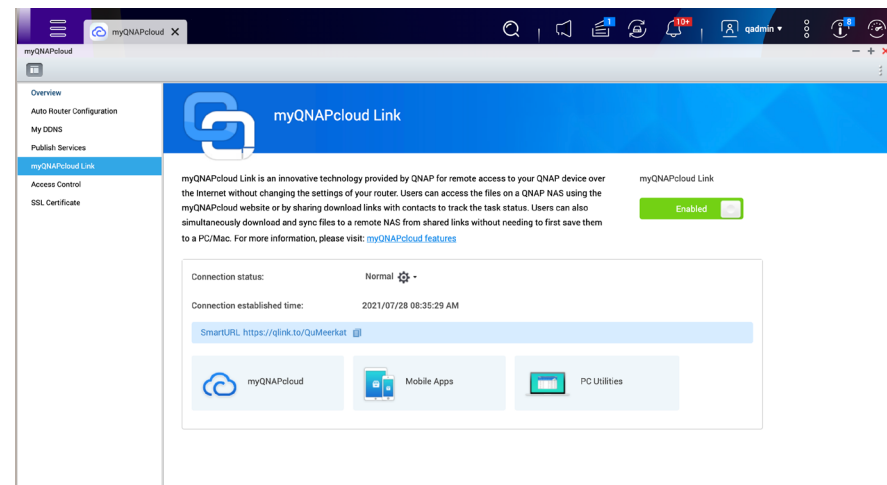
您的 QNAP NAS 如果毫無防護、直接連線上網際網路，便存在被窺探的潛在風險。攻擊者通過利用 Shodan 等特定網站或殭屍網路，可以輕易地鎖定裝置並發起攻擊。這個狀況發生於分享器、路由器及數據機的連接埠轉發 (Port Forwarding) 設定，若你啟用了手動轉發、自動連接埠轉發 (UPnP；通用隨插即用) 或非軍事區 (DMZ)，那麼您的 QNAP NAS 即為直接連線到網際網路。此外，直接連線到網際網路的狀況還發生於讓 QNAP NAS 直接取得公有 IP 位址 (靜態 /PPPoE/DHCP)。

當您需要遠端連線 NAS，最安全的做法是建立 VPN 安全連線或是使用 myQNAPcloud Link 應用程式。如果您不採用以上兩種連線方式，則請務必將 QNAP NAS 安裝於路由器及防火牆後方後面。若 NAS 位於路由器後方，但透過連接埠轉址連接至網際網路，則應在路由器指定新的埠號，勿使用 22、443、80、8080 或 8081 等埠號。

## 遠端連線的安全秘訣

我們知道 NAS 的價值即是隨時隨地的連線存取。為了增進遠端連線的便利性及安全性，我們開發了 myQNAPcloud Link 應用程式，透過 p2p 的連線模式連回到 NAS，所以可以不用設定防火牆的開埠即可達到連線 NAS，避免直接在網際網路上暴露 NAS，實現更高的安全性。

在過去，您必須透過 DDNS 服務，經過繁瑣的設定程序，才能進行遠端連線。現在，myQNAPcloud Link 提供化繁為簡的遠端連線方式，讓您不論身在何處都能隨時連線至 QNAP NAS，就如同隨身攜帶著 NAS 一般。

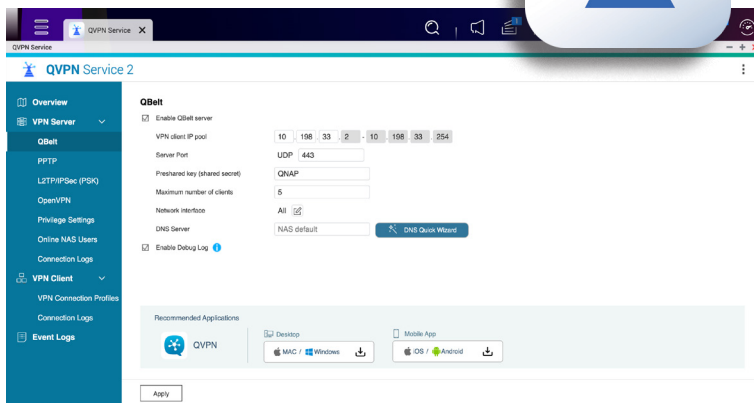


## 建立 VPN 安全連線

除了 myQNAPcloud Link 遠端連線之外，使用 QVPN Service 在 QNAP NAS 上設置您專屬的虛擬私人網路 (VPN) 伺服器則是更高層級的安全連線方式，讓保障您的裝置間與 NAS 之間進行更安全的通訊。此外，您還可將 QNAP NAS 連接到其他 VPN 伺服器。

只有在 QVPN Service 中才能使用的 QNAP 獨家 VPN 通訊協定 QBelt，可以更高程度地減少 VPN 連接被偵測的機會。而電腦或行動裝置則可使用 QVPN Device Client 連接到 QNAP NAS 上的 VPN 伺服器，或 QuWAN 服務。

### QVPN Service



## 內建安全基因

除了上述多種可增進安全防護的應用程式之外，QTS/QuTS hero 作業系統內建多元化的安全性設定功能。完整化安全性設定，為您的 NAS 再加一層保障。

- **IP 黑白名單：**IP 白名單可用來限制連線，只有特定 IP 位址才可連線到 NAS；而 IP 黑名單則可用來自動封鎖特定 IP 位址，使其無法連線到 NAS。
- **自動封鎖：**將您的 NAS 設為阻擋登入錯誤太多次的使用者 /IP 位址，以避免暴力攻擊並確保裝置安全性。
- **HTTPS 連線：**啟用對 NAS 的 HTTPS 連線，您可選用自我簽署 / myQNAPcloud/Let's Encrypt 的 TLS 憑證來加密連線，確保更高的安全性。
- **多元備份方案：**您可透過多種方式完整備份 NAS，包括使用快照，以及備份 / 同步到遠端伺服器或雲端儲存服務。
- **權限控管：**設定資料夾權限除了資安控管外，也讓使用者擁有更多隱私，這樣不僅確保機密資訊的安全，也能符合法規要求。
- **日誌與通知：**系統內建完整的事件日誌和通知功能，確保詳盡追溯各項操作，節省 IT 維運所需的時間。



## 移除未知風險

如果您的 NAS 為多人一起共用，您應視需要定時檢視系統狀況。您應定期以管理員身分登入 NAS，前往 [ 控制台 ] > [ 權限 ] > [ 使用者 ]，刪除未知或可疑使用者。此外，您的 NAS 也可能被其他使用者安裝多款應用程式，請定時進入 App Center，驗證所有已安裝應用程式，找出極少使用、未知或可疑應用程式，並予以移除。

## 加裝防毒軟體

QTS 除了內建免費的 ClamAV 防毒功能外，您也可選購知名防毒軟體 McAfee Antivirus，享受進階的保護功能。QNAP 用戶可手動或排程掃描，防止資料遭受病毒威脅，修復已中毒的檔案，避免病毒因檔案分享而再度擴散，更可隨時收到最新的病毒碼為 NAS 提供更有效的防護。您可透過 QNAP Software Store 輕鬆購買 McAfee Antivirus 授權，並有 1 到 3 年的授權期間供您選擇。

Essential	Pro	Premium
Antivirus Annual Subscription For NAS	Antivirus Bi-Yearly Subscription For NAS	Antivirus Tri-Yearly Subscription For NAS
USD \$25.00 /Year	USD \$50.00 /2 Years	USD \$70.00 /3 Years
<a href="#">SUBSCRIBE NOW</a>	<a href="#">SUBSCRIBE NOW</a>	<a href="#">SUBSCRIBE NOW</a>



## QNAP 資安團隊全時守候

QNAP 已於 2018 年獲得國際非營利組織 MITRE 認證，取得 CVE Numbering Authority 資格，能為 QNAP 產品的安全性問題指派 CVE ID (CVE 識別碼)。QNAP 的產品資安事件應變團隊 (Product Security Incident Response Team, PSIRT) 可即時接收來自世界各地的資安通報，主動調查漏洞及公開揭露資安威脅，並於收到弱點通報的 24 小時內提出回應。

我們建議使用者應定期查看 QNAP 資安通報公告，並訂閱 QNAP 資安電子報，以獲得最即時的 QNAP 資安訊息。於資安事件發生之際，依據 QNAP PSIRT 團隊針對事件的建議作法，於第一時間內防堵資安事件侵害您的 NAS。

Advisory	Status	Impact	CVE	Last Updated	Affected Product(s)
<b>Improper Access Control Vulnerability in Legacy HBS 3 (Hybrid Backup Sync)</b>  <b>QNAP SA ID:</b> QSA-21-19  <b>First Published:</b> 2021-07-06	Resolved	Critical	CVE-2021-28809	2021-07-06	Certain QNAP NAS
<b>Summary:</b> An improper access control vulnerability has been reported to affect certain legacy versions of HBS 3 (Hybrid Backup Sync). If exploited, this vulnerability allows attackers to compromise the security of the operating system. We have already fixed this vulnerability in the following versions of HBS 3: QTS 4.3.6...					
<a href="#">Learn More</a>					
Multiple Command Injection Vulnerabilities in QTS and QUTS hero	Resolved	Medium	CVE-2021-28802 CVE-2021-28804	2021-06-25	Certain QNAP NAS
Stored XSS Vulnerability in QLog Center	Resolved	Medium	CVE-2020-36196	2021-06-25	Certain QNAP NAS
Stored XSS Vulnerability in Q-center	Resolved	Medium	CVE-2021-28803	2021-06-25	Certain QNAP NAS
XSS Vulnerability in QTS and QUTS hero	Resolved	Medium	CVE-2020-36194	2021-06-25	Certain QNAP NAS
DNSpoof Vulnerabilities in QTS	Resolved	Medium	CVE-2020-25684 CVE-2020-25685 CVE-2020-25686	2021-06-28	Certain QNAP NAS



## 如果我的 NAS 不幸遭受加密攻擊，該怎麼做？

由於加密勒索軟體攻擊行為變化多端，難以僅僅透過單一模式即可一招通用。我們建議為您儘可能地進行多個備份，並且啟用檔案快照及快照備份功能，並且訂閱 QNAP 的資安電子報，隨時保持軟體更新。

若發現 NAS 出現異常狀況，例如 CPU 用量異常飆高、登入失效、資料夾出現未知檔案，或是發現檔案受到非授權的加密行為等狀況。請立即將您的 NAS 移除網路連接，並立即關機\*。馬上聯繫 QNAP 客服人員，並確認備份端設備資料、快照檔案是否完整存在，再依照 QNAP 客服人員指示再進行下一個動作。

如果您的 NAS 異常症狀與 QNAP 揭露的病徵描述相符，且 QNAP 已釋出 Maleware Remover 更新版本，請即刻執行 Maleware Remover 掃描，並依照 QNAP 所揭露資訊更新應用程式或作業系統。

如果您平時有執行快照功能，且確認您的快照檔案未受影響。您可以使用快照復原功能來恢復您的寶貴資料。

\* 在多數情況下，第一時間發現 NAS 受攻擊狀況時，將 NAS 立即關機是最好的止損做法。唯有極少數加密攻擊型態會使 NAS 關機後遺失解密密鑰。建議用戶關注 QNAP 資安通報。

## 資安是 QNAP 第一要務

QNAP 對資安的承諾不打折，我們積極維護資安，並結合相關合作夥伴及社群的力量，確保 QNAP 產品安全性，讓您使用更安心。



# QNAP SYSTEMS, INC.

TEL : +886-2-2641-2000 FAX: +886-2-2641-0555 Email: [qnapsales@qnap.com](mailto: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 © 2021 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.

## Netherlands (Warehouse Services)

Email: [nlsales@qnap.com](mailto:nlsales@qnap.com)

TEL: +31(0)107600830

## China

Email: [cnsales@qnap.com](mailto:cnsales@qnap.com)

TEL: +86-400-028-0079

## Japan

Email: [jpsales@qnap.com](mailto:jpsales@qnap.com)

FAX: 03-6435-9686

## US

Email: [usasales@qnap.com](mailto:usasales@qnap.com)

TEL: +1-909-595-2782

## India

Email: [indiasales@qnap.com](mailto:indiasales@qnap.com)

## France

Email: [Frsales@qnap.com](mailto:Frsales@qnap.com)

## Thailand

Email: [thsales@qnap.com](mailto:thsales@qnap.com)

TEL: +66-2-5415988

## Germany

Email: [desales@qnap.com](mailto:desales@qnap.com)