## 群暉 NAS 安全性設定

1. 先用"安全諮詢中心"掃描漏洞,再依提示重新設定。



2. 最高管理者設定複雜的密碼,並啟用兩步驟認證。

8	控制台				
<b>合</b> 2 搜尋	使用者帳號 進階設定				
🔁 共用資料夾	22計使用資本電腦通動後提更電腦 寄送到期通知電子部件				
🖼 檔案服務	寄送時間	00 🕶 : 00 💌			
👤 使用者帳號	到期前的天數:	0			
🕐 使田老群組	▲ 兩步驟驗證				
	✔ 強制下列使用者啟動兩步驟驗證				
Ⅰ 網域 / LDAP	● 管理者群組使用者				
▲ 連總許力	所有使用者				

3. 安全性中防火牆中設定 3-1.DSM 管理介面允許的 IP 範圍, 3-2.DSM 管理介面全部拒絕二個設定

	編輯設定檔 "default"						
新增	編輯 刪除	<u>\$</u>		所有介面	•		
	✔ 已啟動	連接埠	通訊協定	來源IP	操作		
	<b>~</b>	管理介面, File Station, Audio Station, Surveill	ТСР	192.168.0.100 到 192.168.0.120	允許		
	<b>~</b>	管理介面, File Station, Audio Station, Surveill	ТСР	所有	拒絕		



4. DSM HTTP, HTTPS 改埠, DSM 改成 HTTPS(DSM 7.0 以後是載入入口網站中設定)

8	1	空制台
<b>合</b> 2 沒尋	一般 網路介面 流量控制	靜態路由 DSM 設定
▲ 檔案分享	∧ 一般	
< 共用資料夾	DSM 連接埤	
446 STP FIC. 2/7	HTTP:	9990
🛀 1曲 乘出区初日	HTTPS:	9991
🡤 使用者帳號	📝 將 DSM 桌面的 HTTP 連線自動導	1 HTTPS
	您可以在 憑證 頁面匯入憑證。	
👷 使用者群組	啟動 HTTP/2	
	使用加密連線時,HTTP/2 可加快編	I頁的載入速度。

5. 使用者密碼設定加強,停用 admin,guest 帳號



## 6. 啟動自動封鎖

		控制台	? - 8		
● 授尋	安全性 防火牆 保護	<b>帳號</b> 憑證 進階設定			
	▲ 自動封鎖				
← 檔案服務	啟動此選項來封鎖登入失敗次數過多的 IP 位址。欲瞭解支援的服務及套件,請參閱 DSM 說明。				
👤 使用者帳號	✔ 啟動自動封鎖				
	如果在下列設定時間內,登入失敗次數達到下列設定的次數,系統將會自動封鎖登入者的 IP。				
👷 使用者群組	嘗試登入次數:	5			
<b>回</b> 網域 / I DAP	幾分鐘內:	5			
	✔ 啟動封鎖過期				
▲ 連線能力	當啟動封鎖過期功能時,在下列天數後,被封鎖的 IP 將會被解除封鎖。				
💋 QuickConnect	封鎖天數:	7			

## 7. 終端機都設定不啟動

2 控制台		?	_	×
▲ Q 搜尋	終端機 SNMP			
<mark></mark> 使用者 & 群組	使用終端機來登入並管理您的系統。SSH/Telnet 僅支援以 administrators 群組的帳號登入。請參閱 <u>終端機</u> 以取得更多資訊。			
🛓 網域 / LDAP	啟動 Telnet 功能			
	啟動 SSH 功能			
∧ 連線能力	連接埠: 22			
💊 外部存取	進階設定			
🏫 網路	注意: 建議為登入帳號設定高強度的密碼並啟動 自動封鎖,以提升系統安全。			
✓ 安全性				
▶ 終端機 & SNMP				