

WPA3 無線加密說明與 WPS 連線失敗排除

什麼是 WPA3？



WPA3 是 Wi-Fi 聯盟推出的最新無線加密標準，旨在全面提升無線網路的安全防禦能力與連線體驗

相較於傳統的 WPA2，WPA3 提供了更強大的演算法加密、更高的破解難度，並大幅改善了在公開 Wi-Fi 網路環境下的隱私保護

Cudy 全系列新世代路由器皆已全面支援 WPA3 加密技術

WPA3 的四大優勢：

- 防暴力破解：**
WPA3 採用更先進的對等安全認證（SAE）技術。即使使用者設定的 Wi-Fi 密碼較為簡單，也能有效阻斷駭客的離線字典與暴力破解攻擊
- 前向保密機制：**
每次設備與路由器連線時，都會建立獨一無二的動態加密金鑰。未來即使網路主密碼不幸外洩，駭客也無法回溯解密過去已經傳輸過的歷史資料流量
- 公用網路隱私強化：**
引入了「機會性無線加密」技術。當您在咖啡廳或機場連線到不需輸入密碼的開放式 Wi-Fi 時，系統仍會自動加密您的連線，保障上網隱私
- 簡化智能設備配對：**
支援「Wi-Fi Easy Connect」技術。未來物聯網設備（如智慧燈泡、攝影機）只需透過手機掃描 QR 碼即可安全配對，用以替代逐漸淘汰且存在安全漏洞的傳統 WPS 按鈕

在 Cudy 路由器中要如何設定 WPA3 加密方式？👉請參考 [SFN-248【在Cudy路由器上如何更改加密模式？】](#)

WPA3 模式下 WPS 連線失敗排除

【常見問題】為什麼在 WPA3-Personal 加密模式下使用 WPS 會連接失敗？

答：這是由於 **WPA3** 的嚴格安全協議與傳統 **WPS** 技術存在相容性限制

WPS 屬於較早期研發的快速連線技術，其設計機制與 WPA3 的高安全標準不完全相容，因此在純 WPA3 環境下極易導致連線中斷或失敗
Wi-Fi 聯盟官方目前更推薦使用高安全性的 **Wi-Fi Easy Connect (QR碼掃描)** 來替代 WPS

【排除步驟】如何解決 WPS 無法連線的問題？

- 確認 WPS 功能是否正常啟用：** 登入 Cudy 路由器 Web 管理介面，前往「無線設定」或「WPS 設定」，確認系統內的 WPS 功能開關是否已被誤關閉
- 將加密模式切換至「混合模式」：** 若您連線的舊設備（如舊款印表機、智能家電）不支援純 WPA3，請將路由器的安全類型更改為「**WPA2/WPA3-Personal 混合模式**」，即可大幅提升設備相容性，並順利完成 WPS 連線
- 改用 Wi-Fi Easy Connect 功能：** 若連線設備與路由器皆有支援，建議直接使用手機掃描產品 QR 碼完成快速安全配對，省去操作 WPS 按鈕的繁瑣步驟
- 檢查並更新路由器韌體：** 確保您的 Cudy 路由器已升級至最新版官方韌體，以修復已知舊版晶片群組與特定裝置間的 WPS 相容性異常
- 改用手動輸入金鑰連線：** 若特定家電設備的 WPS 晶片相容性過低導致連線持續失敗，建議直接手動搜尋 Wi-Fi 名稱並輸入密碼進行連線
- 恢復出廠預設值重試：** 若上述調整皆無效，可能是快取暫存異常。請將路由器重置（Reset）回出廠狀態，在未調整其他進階參數前直接測試 WPS 配對

【注意事項】

- 設備升級建議：** 如果您的老舊設備完全無法識別或連線至 WPA3 網路，建議未來挑選新週邊時優先選擇支援 WPA3 的機型，以確保享有最高層級的居家資安防護
- 資安防護觀念：** 若您的環境中極少用到快速配對，**強烈建議在後台直接關閉 WPS 功能**。由於傳統 WPS 協議存在易被破解的安全漏洞，全面改用手動輸入密碼或 QR 碼配對是更安全、更安心的作法