CUDY 路由器安全設定與進階防護指南

一般建議：

1. 修改 Wi-Fi 名稱與密碼，不使用預設值

請進入【無線設定】頁面，自訂 Wi-Fi 名稱（SSID）及密碼，建議密碼長度超過 8 位，並混合大小寫、數字與符號

2. 設定管理介面與 Wi-Fi 密碼為不同組合

避免使用相同密碼，以降低只知道 Wi-Fi 密碼的使用者存取路由器管理頁面的風險

3. 避免啟用 DMZ 功能

DMZ 會將內部某裝置完全暴露在外部網路中，極易被攻擊，若需開放服務，建議使用「通訊埠轉發」取代

4. 維持韌體為最新版本

定期進入路由器管理頁，確認是否有最新韌體更新，以修補潛在安全漏洞，也可透過 CUDY APP 檢查更新

5. 關閉不必要的遠端管理

此功能預設為關閉，若無特別需求，請勿開啟，遠端管理功能會開放管理介面於公網，需謹慎使用

6. 啟用防火牆功能

請前往【安全性設定】>【防火牆】確認已啟用 (預設為開啟)，防火牆為第一層過濾機制，可攔截來自外部網路的可疑請求

7. 無線網路加密選擇

在設定無線網路密碼時，加密方式可選擇至少 WPA2-PSK/WPA3-SAE 的加密方式 (單獨使用 WPA3 加密方式可能會使一些設備無法正常連上)

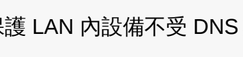
進階安全設定（加強防護）：

1. 僅允許特定 IP 登入管理介面 (白名單 IP)

在支援的機型中，您可設定「白名單 IP」，限制僅某些 IP 可存取管理頁，防止內網設備遭非法控制

2. 關閉 UPnP 功能

UPnP 雖方便設備自動開啟埠口，但也可能被惡意程式利用，建議在【進階設定】中將其關閉，除非確實需要



3. 啟用 HTTPS 存取管理頁面

HTTPS 可在管理頁存取時加密瀏覽資料。啟用後，請手動輸入網址為 `https://IP位址:443`

首次使用自簽憑證會跳出警告訊息，可放心忽略

注意：**請勿點選來路不明的網址，如點選進入後不是連到路由器設定頁面，看到此警告訊息請提高警覺，不要隨意進入**

4. 設定 IP/MAC 位址過濾

您可設置此功能把陌生的 IP/MAC 位址給封鎖，只允許白名單中的設備連入此網路，以加強防護

5. 啟用 DNS 重新綁定防護

此功能可防止網路遭假冒 DNS 導向惡意網站，保護 LAN 內設備不受 DNS 欺騙攻擊影響