Pico-UTM 100 FAQ

Next Generation Network Security

Pico-UTM 100 常見問題

01 登入與管理 Pico-UTM

Q1. 要如何連線至 Pico-UTM 的管理介面？

Step 1: 將 Pico-UTM 的 WAN 埠連接至能自動取得 IP 位址(DCHP)的網域。

Step 2: 以網路線將 Pico-UTM 的 LAN 埠與電腦連接。

Step 3: 使用網路瀏覽器進入 http://mypico.lionic.com，即可連線至 Pico-UTM 的管理介面。

Q2. 如果 Pico-UTM 無法取得 IP 位址，要如何連線至管理介面？

若 Pico-UTM 因以下情況而無法自動取得 IP 位址，可透過替代方案連線至管理介面。

1. 需手動設定靜態 IP 位址時。
2. 需手動設定 PPPoE 以取得 IP 位址時。
3. 因 DHCP 故障或其它因素而無法自動取得 IP 位址時。

替代方案：

Step 1: 以網路線將 Pico-UTM 的 LAN 埠與電腦連接。

Step 2: 手動將電腦的網路設定改為：

- IP 位址：10.254.254.1 (~253)
- 子網路遮罩：255.255.255.0

Step 3: 使用網路瀏覽器進入 http://10.254.254.254，即可連線至 Pico-UTM 的管理介面。

Q3. 要如何管理多台 Pico-UTM？

企業或組織的網路管理員能透過中央管理系統（CMS）集中管理多台 Pico-UTM，在集中控制介面上遠端設定 Pico-UTM 的防護規則，並監控 Pico-UTM 所偵測到的資安威脅。如有 CMS 的使用需求，請洽各區域的銷售夥伴或業務代表。

02 Pico-UTM 的網路設定

Q1. 使用 Pico-UTM 時需要連接至網際網路嗎？

使用 Pico-UTM 時必須連接至網際網路，以取得授權認證、韌體更新、特徵碼更新及使用 Lionic 的資安防護雲端服務，進而獲得最完整的資安防護功能。

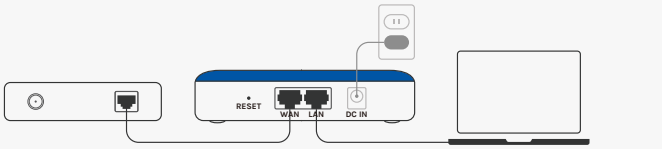
Q2. 該如何將 Pico-UTM 架設在無法連至外部網路（網際網路）的網路環境？

若要將 Pico-UTM 架設在與網際網路隔絕的環境（例如智慧工廠）中，則必須透過 CMS 以及 Proxy Server 的輔助連接至網際網路，以獲得最完整的資安防護功能。如有此類需求，請洽各區域的銷售夥伴或業務代表。

Q3. 如果 ISP 或網路管理員僅提供一組 IP 位址給我，我該如何設定 Pico-UTM 呢？

若 ISP 或網路管理員僅提供一組 IP 位址，可以依照以下步驟將 Pico-UTM 調整為 [路由器模式]：

Step 1: 將 Pico-UTM 依下圖方式連接。



純數據機　　Pico-UTM　　筆電/桌機的網路孔

Step 2: 手動將電腦的網路設定改為：

- IP 位址：10.254.254.50 (~253)
- 子網路遮罩：255.255.255.0

Step 3: 使用網路瀏覽器進入 http://10.254.254.254，連線至管理介面。

Step 4: 至 [網際網路] 頁調整 [連線類型] 並進行設定以取得 IP 位址。

Step 5: 至 [系統管理] > [裝置資訊] 頁，將 [設定] > [連線模式] 改成 [路由器模式]。

完成設定並將電腦置換成路由器或 Wi-Fi 基地台後，Pico-UTM 將會使用 ISP 所提供的 Public IP 作為 WAN 端 IP 位址，並以 DHCP 配發 Private IP 給 LAN 端裝置使用。

附註：建議關閉路由器或 Wi-Fi 基地台的 DHCP 功能以避免造成雙重 NAT。

Q4. 該如何讓 Pico-UTM 取得可以連上網路的 IP 位址呢？

Pico-UTM 有下列三種不同 IP 位址取得方式，可依據不同網路環境調整：
1. 自動取得（DHCP，預設值）　2. 靜態位址　3. PPPoE
請在進入管理介面後至 [網際網路] 頁調整 [連線類型] 並進行設定。

03 使用授權相關問題

Q1. 為什麼 Pico-UTM 需要訂閱使用授權？

訂閱並啟用授權後，Pico-UTM 才能夠取得有效認證，並在連上網際網路時獲得韌體更新、特徵碼更新、Lionic 的資安防護雲端服務等完整防護功能。

Q2. 要如何更新 Pico-UTM 的韌體？

每當有新版韌體釋出時，會在 [系統管理] > [更新韌體] 頁中顯示更新通知。按下 [更新] 後，Pico-UTM 將會自動完成韌體更新程序。
附註：更新韌體的過程中將會重啟 Pico-UTM，網路連線會因此中斷，並在完成重啟後恢復連線。

Q3. 要如何更新 Pico-UTM 的特徵碼？

在授權有效且 Pico-UTM 能連線至網路網路期間，特徵碼資料庫每週會有兩次自動更新，不需額外操作。

Q4. 授權過期之後還能使用 Pico-UTM 嗎？

授權過期後，Pico-UTM 將會停止韌體更新、特徵碼更新以及 Lionic 的資安防護雲端服務，造成防護能力下降，建議恢復授權訂閱後再繼續使用。

Q5. 為什麼「授權到期日」會顯示「狀態確認失敗」？

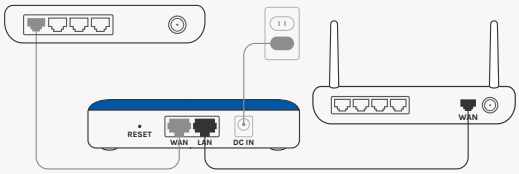
若 [儀表板] > [裝置資訊] > [授權到期日] 顯示「狀態確認失敗」，代表 Pico-UTM 無法順利連線至 Lionic 的授權認證伺服器。請先檢查 Pico-UTM 的對外網路連線狀態，若無異常請洽各區域銷售夥伴或技術支援。

04 安全防護相關問題

Q1. 該如何確認裝置在 Pico-UTM 的防護範圍之內？

只要裝置對外連線的封包有經過 Pico-UTM（LAN 埠傳至 WAN 埠或 WAN 埠傳至 LAN 埠），即在 Pico-UTM 的防護範圍內。

附註：若 ISP 所提供的設備是「數據機、路由器及 Wi-Fi 基地台多合一裝置」，直接透過該裝置連網的設備將不會被 Pico-UTM 保護，必須要在 Pico-UTM 的 LAN 埠再接一台路由器或 Wi-Fi 基地台，如下圖：



Q2. 為什麼網路速度在串接 Pico-UTM 後下降了？

由於 Pico-UTM 需要解析封包內容並和特徵碼進行比對，將會對網路傳輸速度造成些許影響，速度的下降幅度會依據傳輸的內容與所使用的應用程式而有差異。

Q3. 一台 Pico-UTM 可以防護幾台裝置？

一台 Pico-UTM 正常狀況下可承受約 50 台裝置的連線存取，會依實際產生的連線數而有些微差異。

Q4. Pico-UTM 在偵測到資安威脅後會採取什麼動作？

Pico-UTM 的三大防護功能在偵測到威脅時各會採取不同的動作：

1. Anti-Virus：「紀錄並且破壞」（預設）或「僅記錄」
2. Anti-Intrusion：「紀錄並且阻擋」（預設）或「僅記錄」
3. Anti-WebThreat：「紀錄並且阻擋」（預設）或「僅記錄」

若要調整，請連上管理介面後至 [安全規則] > [Anti-Virus] [Anti-Intrusion] [Anti-WebThreat] 頁中調整 [動作]。

Q5. Pico-UTM 擋下了我信任的連線或檔案，我該如何處理？

若 Pico-UTM 誤擋下了受信任的連線或檔案，請依循以下步驟處理：

Step 1: 連線至 Pico-UTM 管理介面。

Step 2: 進入 [資安紀錄]，在 [Anti-Virus] [Anti-Intrusion] [Anti-WebThreat] 的資安紀錄中尋找被誤擋的資安事件。

Step 3: 點擊事件紀錄右手邊的 [+加入]，將該項事件加入白名單。

Step 4: 重新連線或下載檔案。

此外，您還可以通過我們的網站報告此類問題: https://www.lionic.com/reportfp_lc