LIONIC
Security Solution Provider

使用者手冊

Pico-UTM 100

版本 2.0
更新日期 2022/06

Pico-UTM 100
https://www.pico-utm.com/

Lionic Corp.
https://www.lionic.com/

Pico-UTM 100 使用手冊

版權聲明

© 2022 鴻璟科技股份有限公司，版權所有

商標

鴻璟科技之商標已註冊使用

免責聲明

鴻璟科技保留對本手冊中所描述的產品/程序進行新增/更改的權利並旨在提供準確的訊息。本手冊可能包含意外的印刷錯誤，因此將定期針對此類訊息進行更改已修正此類錯誤。

技術支援聯絡資訊 鴻璟科技股份有限公司

信箱: sales@lionic.com 電話: +886-3-5789399 傳真: +886-3-5789595

目錄

功能概述

儀表板：

[儀表板] 會顯示 Pico-UTM 100 的運行狀態與裝置資訊，包含檢測歷程、資安威脅統計、流量監控與系統資源監控等。

網際網路：

[網際網路] 可以調整 Pico-UTM 100 對外的網路連線設定，例如取得 WAN IP 位址的方式或開放遠端存取 Pico-UTM 100 的控制項。

區域網路：

[區域網路] 可以調整 Pico-UTM 100 對內的網路連線設定。由預設的 [橋接模式] 改為 [路由器模式] 後，可以設定靜態保留位址或通訊埠轉發。

安全防護：

- **安全規則：**設定各項安全防護功能的執行規則，包含防毒系統、入侵防禦、惡意網頁阻擋、防火牆等。
- **資安紀錄：**顯示各項安全防護功能的執行紀錄。

進階設定：

- **VPN：**若要延伸 Pico-UTM 100 的防護範圍到使用行動網路的裝置，可以啟用 VPN 伺服器功能，讓行動裝置能使用經防護的網路連線。
- **系統管理：**在此頁面可以調整各項系統設定，包含授權管理、伺服器連線設定、更新韌體、備份/還原設定、管理日誌等。
- **系統工具：**此頁面提供各種疑難排解所需功能，例如網路工具、命令列工具、系統日誌匯出等。

儀表板

Pico-UTM 100 的運行狀態與裝置資訊皆會於此顯示，包含檢測歷程、資安威脅統計、流量監控與系統資源監控等。

儀表板-主頁 1

檢測歷程：顯示 Pico-UTM 100 從上次開機後完成檢測的檔案數量、連結數量、封包流數量及封包數量。

安全防護：顯示 Pico-UTM 100 近期偵測到的威脅事件數量、各項安全防護功能啟用/停用狀態以及對威脅的處置動作，點擊後可以快速進入對應功能的資安紀錄頁面或安全規則頁面。

資安威脅排行：統計各項安全防護功能偵測到的資安紀錄，依照偵測次數多寡列出全部或各類威脅排行。

儀表板-主頁 2

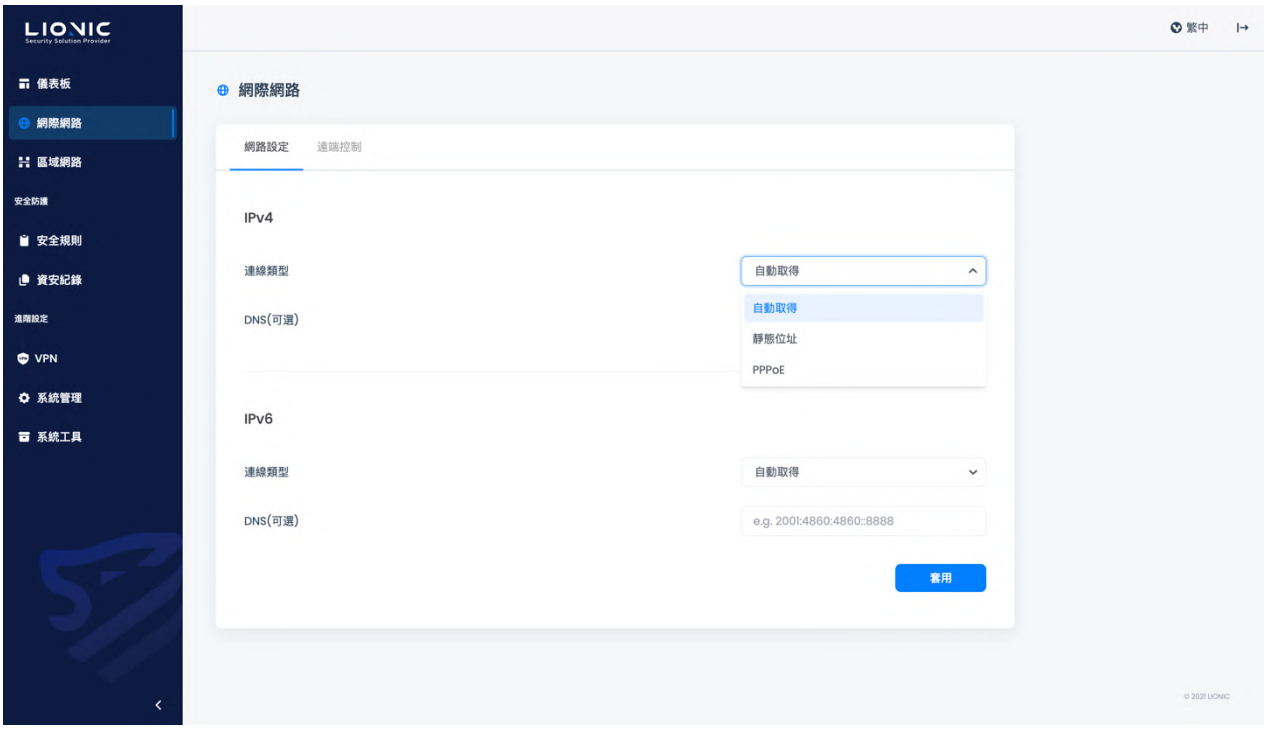
流量監控：顯示經過 Pico-UTM 100 的上傳/下載速度與傳輸量。

裝置資訊：顯示 Pico-UTM 100 的裝置名稱（可自訂）、MAC 位址、授權狀態、韌體版本、各項安全防護功能特徵碼版本、特徵碼最後更新日期、WAN IP 位址、系統時間、系統已運行時間、記憶體與儲存空間用量及 CPU 使用率。

網際網路

網路設定：

在 [網路設定] 頁面裡，使用者可以依照其網路環境選擇連線類型為 [自動取得]、[靜態位址] 或是 [PPPoE] 以進行 IPv4 或 IPv6 的配置。當使用者首次使用 Pico-UTM 100 時，預設的連線類型是 [自動取得]。如需 [靜態位址] 或 [PPPoE] 設定值，請洽網路服務供應業者或網路管理員。



網際網路-網路設定

- **自動取得**：透過 DHCP 自動取得 IP 位址，適合 Pico-UTM 100 前設有路由器的環境。
- **靜態位址**：自行輸入正確的 IP 位址資訊。
- **PPPoE**：自行輸入正確的網路連線使用者名稱與密碼。

* 備註：選擇 PPPoE 連線後可能會因為存取控制清單（ACL）導致無法連線至 Pico-UTM 100 網頁控制介面，相關說明及操作方式請見 [遠端控制] 使用說明。

遠端控制：

為降低 Pico-UTM 100 受到外在威脅入侵的風險，預設僅開放「同網域下的裝置以私有 IP 位址」登入網頁控制介面。若需要從遠端（外部網域）存取網頁控制介面，或 Pico-UTM 100 以公有 IP 位址連接網際網路，請務必提前完成 [遠端控制] 設定。

遠端控制-動態 DNS 服務/存取控制清單

動態 DNS 服務（DDNS）

當 Pico-UTM 100 使用公有浮動 IP 位址時，可以透過 [動態 DNS 服務] 解決遠端連線時須查找 Pico-UTM 100 當前 IP 位址的問題。

在自行向 DDNS 服務供應商申請完主機名稱後，請將設定值填入以下欄位：

- 服務供應商：選擇 DDNS 服務供應商（備註 1）。
- 主機名稱：輸入申請的主機名稱。
- 使用者名稱：輸入申請的使用者名稱。
- 密碼：輸入申請的使用者密碼。

填妥後按下 [套用] 並啟用動態 DNS 服務功能，即可透過固定的主機名稱從遠端連線至 Pico-UTM 100 的網頁控制介面（備註 2）。

* 備註：

1. 目前僅支援 No-IP 的 DDNS 服務。
2. 當套用新設定或 IP 位址改變時，DDNS 服務供應商可能會需要時間更新。若當下無法透過主機名稱連線至 Pico-UTM 100，請稍候片刻再嘗試連線。
3. 若 Pico-UTM 100 是使用私有 IP 位址透過路由器連接至網際網路，請在路由器上設定 DDNS 及通訊埠轉發（Port Forwarding）。

存取控制清單（ACL）

為降低外部入侵風險，Pico-UTM 100 預設僅開放「同網域下的裝置以私有 IP 位址」登入網頁控制介面。如需以外部網域裝置連線至此網頁控制介面，請將其 IP 位址新增至存取控制清單（ACL）。

步驟一：點擊 [新增]。
步驟二：將外網裝置的公有 IP 位址填入輸入框。
步驟三：點擊 [套用]。

若無法提前確定外網裝置公有 IP 位址（例如外網裝置使用公有浮動 IP 位址），可以停用存取控制清單（備註 1）、允許所有外網裝置連線至 Pico-UTM 100。

* 備註：

1. 為維持連線安全性，當 [存取控制清單] 停用時，[安全連線] 會自動啟用且無法停用。

遠端控制-安全連線

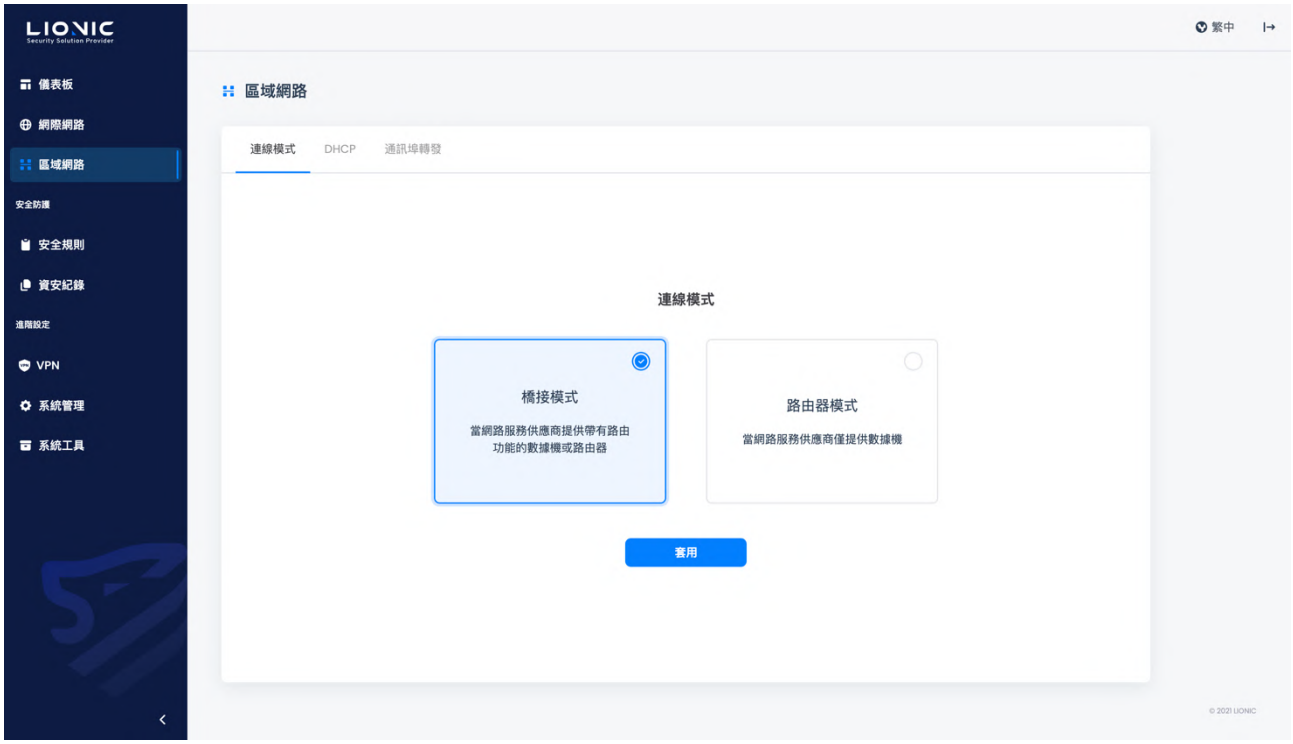
安全連線

啟用 [安全連線] 後，將全面使用 HTTPS 連線至 Pico-UTM 100 的網頁控制介面，以保護登入密碼等重要隱私資訊。當 [存取控制清單] 停用時，[安全連線] 會強制啟用。

區域網路

連線模式：

Pico-UTM 100 支援兩種連線模式，使用者可依照需求選擇適合的連線模式。



區域網路-連線模式

- **橋接模式**

  在 [橋接模式] 下，Pico-UTM 100 僅提供橋接功能，不會對 LAN 端裝置配發 DHCP IP 位址。此模式為 Pico-UTM 100 預設值，適合在部署 Pico-UTM 100 於「能配發多組 IP 位址」的路由器後面時使用。

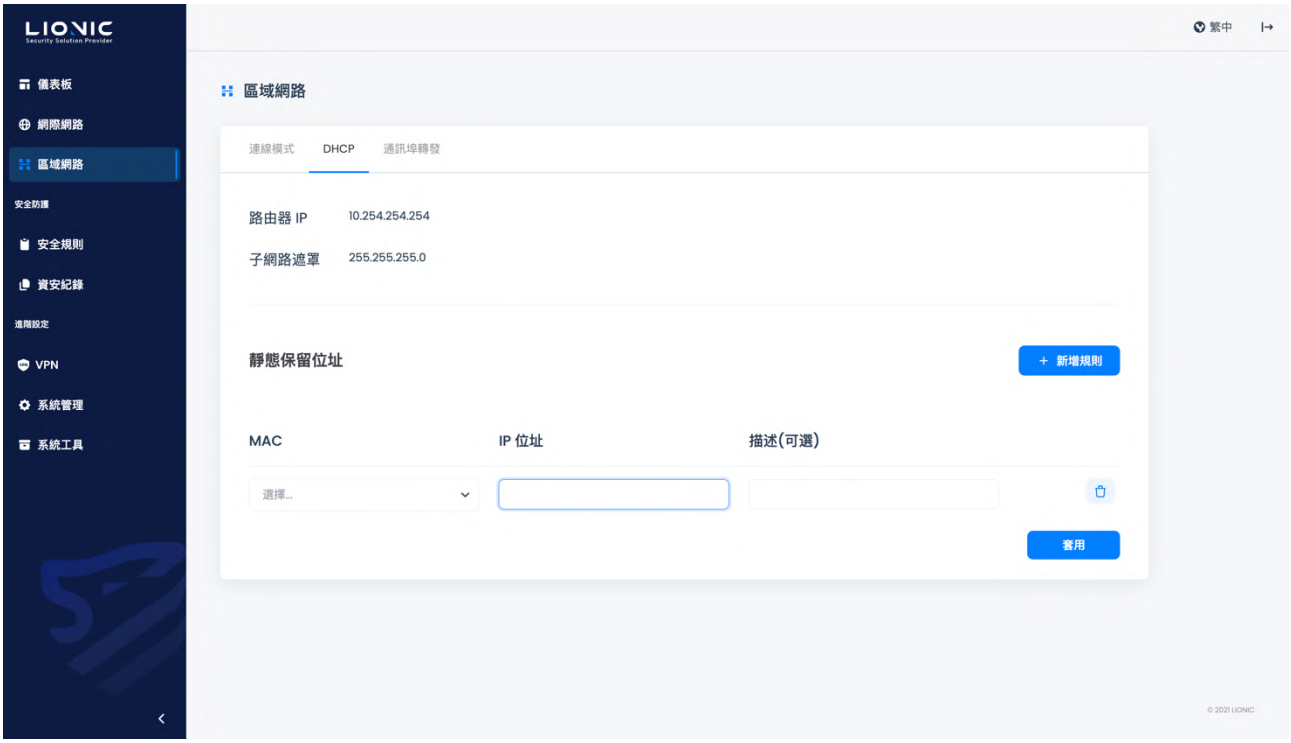
- **路由器模式**

  在 [路由器模式] 下，Pico-UTM 100 能夠提供 DHCP IP 位址配發及路由功能，適合在部署 Pico-UTM 100 於「僅有一組 IP 位址」的環境下使用。

確認適合的連線模式後點擊 [套用]，Pico-UTM 100 將會重新設置網路功能。過程間可能會造成網路連線中斷，也會需要重新連線才能登入網頁控制介面。

DHCP：

在 [路由器模式] 下，Pico-UTM 100 能提供 DHCP IP 位址配發功能。當 Pico-UTM 100 被部署在僅有一組外部 IP 位址的環境時，可以使用此項功能配發私有 IP 位址給多個 LAN 端裝置。



區域網路-DHCP

- **DHCP IP 位址範圍**：10.254.254.100~249
- **路由器 IP 位址**：10.254.254.254
  （LAN 端裝置可透過此 IP 連線至 Pico-UTM 100 網頁控制介面）
- **子網路遮罩**：255.255.255.0

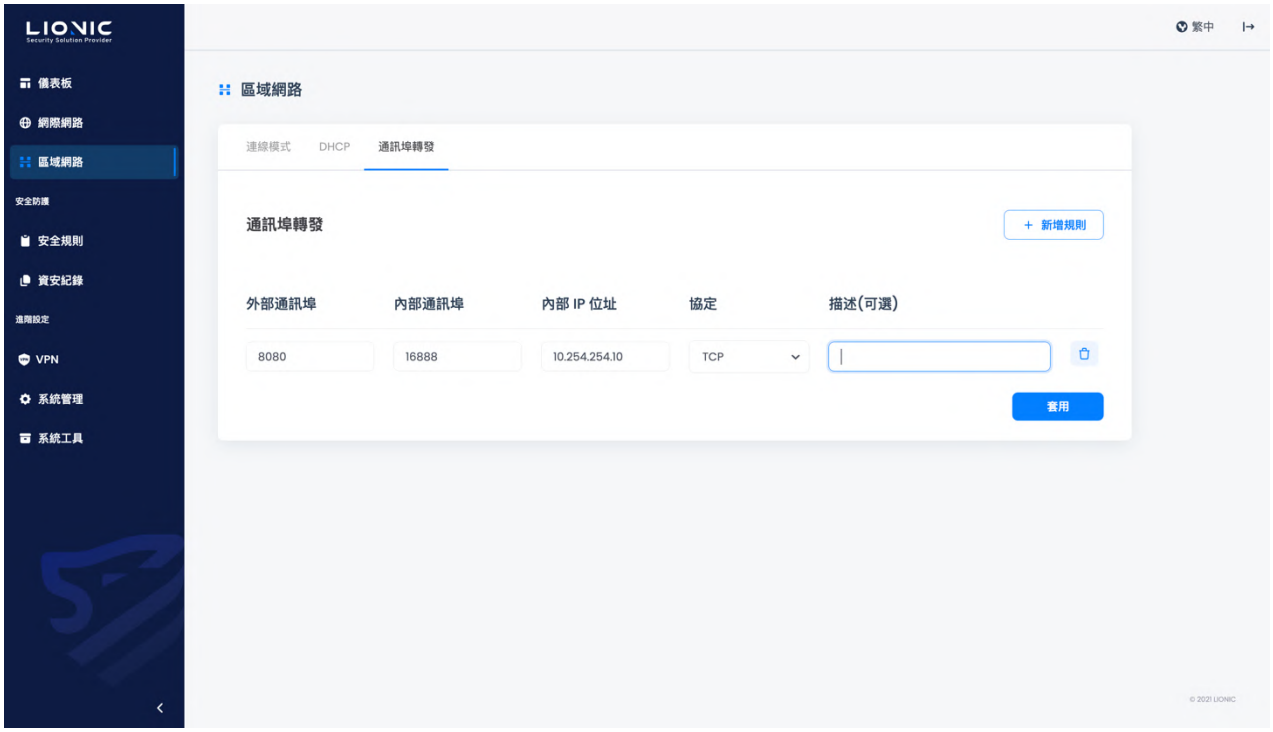
靜態保留位址

當有需要保留固定 IP 位址給指定裝置使用時，可以將該裝置的 MAC 位址以及欲保留的 IP 位址填入輸入框後點擊 [套用]。

* 備註：該裝置可能會需要更新 IP 位址設定才能取得到保留的 IP 位址。

通訊埠轉發

在 [路由器模式] 下，Pico-UTM 100 能提供通訊埠轉發功能。當有需要開放外部裝置存取 LAN 端裝置時，可以使用此項功能設定外部通訊埠轉發至指定內部 IP 位址。



區域網路-通訊埠轉發

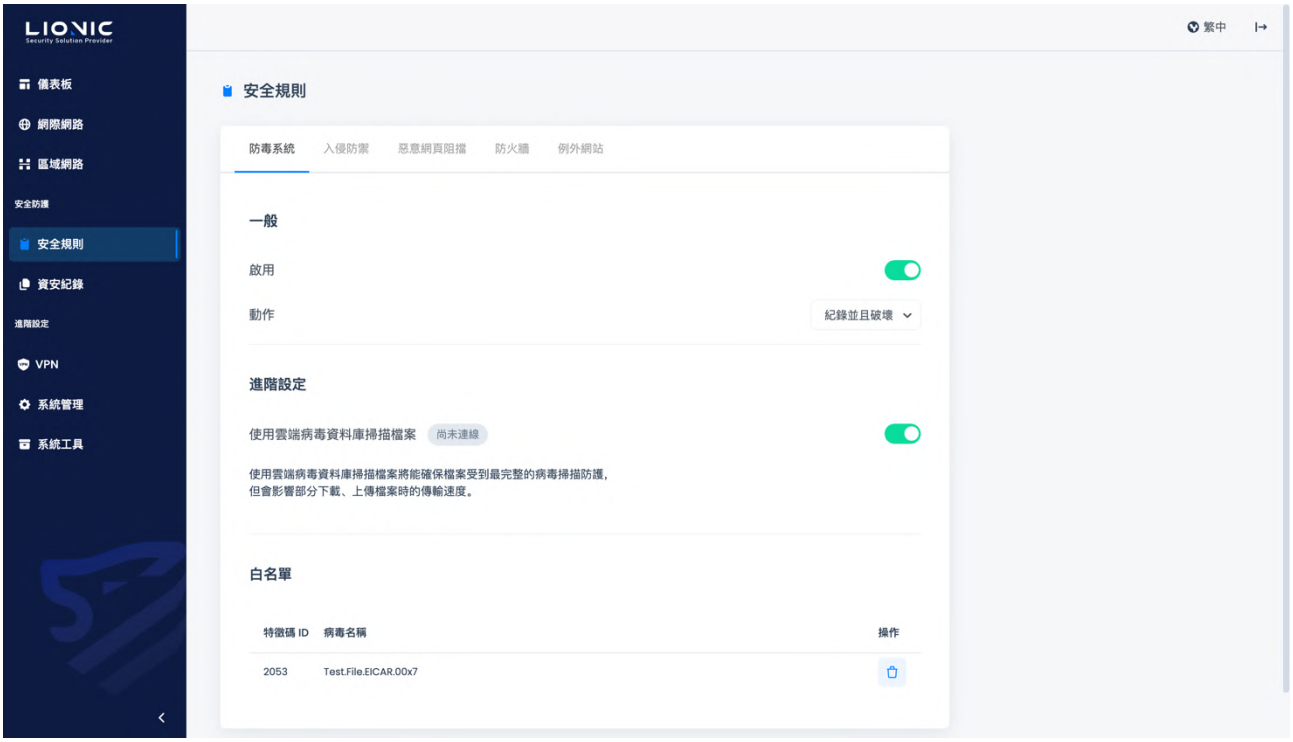
安全規則

Pico-UTM 100 以深度封包檢測提供三大資安防護功能：

- **防毒系統**：從封包中檢測出病毒特徵並破壞病毒檔案。
- **入侵防禦**：從封包中檢測出網路攻擊行為並阻擋攻擊。
- **惡意網頁阻擋**：從封包中檢測出惡意網站存取需求並阻擋連線。

在 [安全規則] 頁面可以分別為三大資安防護功能調整防護設定：

防護功能	防毒系統	入侵防禦	惡意網頁阻擋
啟用	啟用 / 停用	啟用 / 停用	啟用 / 停用
動作	紀錄 / 紀錄並且破壞	紀錄 / 紀錄並且阻擋	紀錄 / 紀錄並且阻擋
進階設定	使用雲端病毒資料庫 掃描檔案	阻擋暴力破解	---
白名單	檢視、刪除白名單設定	檢視、刪除白名單設定	檢視、刪除白名單設定

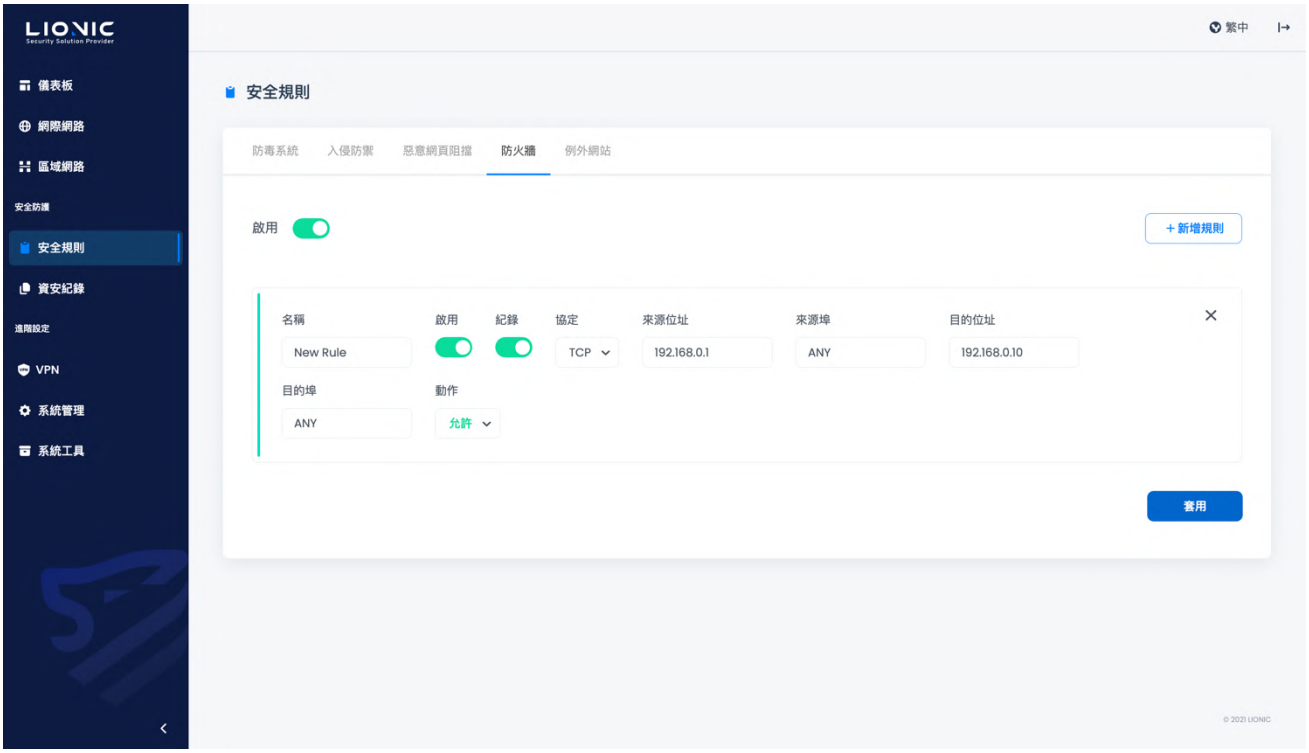


安全規則

- **啟用**：獨立啟用或停用各項安全防護功能，預設為啟用。
- **動作**：偵測到資安威脅時 Pico-UTM 100 採取的動作。
    - 紀錄：僅顯示威脅事件於 [資安紀錄]。
    - 紀錄並且破壞：顯示威脅事件於 [資安紀錄] 並破壞病毒檔案。
    - 紀錄並且阻擋：顯示威脅事件於 [資安紀錄] 並阻擋攻擊或網頁連線。
- **使用雲端病毒資料庫掃描檔案**：除了將檔案特徵和本地端的病毒特徵碼比對外，Pico-UTM 100 也能將檔案特徵和雲端病毒資料庫進行比對。在 Pico-UTM 100 授權有效且能連接至外部網路期間，啟用此功能將能獲得最完整的病毒掃描防護。
- **阻擋暴力破解**：啟用此功能後，Pico-UTM 100 的 [入侵防禦] 能偵測短時間內密集嘗試登入失敗的行為。當發生的頻率超過警戒值時，Pico-UTM 100 會依據密集程度於 [資安紀錄] 顯示或進而阻擋連線。
- **白名單**：當 Pico-UTM 100 的資安防護功能破壞了安全的檔案或阻擋了受信任的連線時，可以透過白名單功能恢復正常使用。
    - 新增白名單規則：請在 [資安紀錄] 頁面中搜尋被破壞或被阻擋的事件紀錄後，點擊 [+] 加入白名單。
    - 檢視、刪除白名單規則：在 [安全規則] 頁面中檢視白名單規則，且可以在此頁面刪除指定白名單規則。

防火牆：

除三大資安防護功能外，Pico-UTM 100 也支援基本的防火牆功能。



安全規則-防火牆

步驟一：啟用防火牆（預設為啟用）。

步驟二：點擊 [+新增規則]。

步驟三：填入各項設定值。

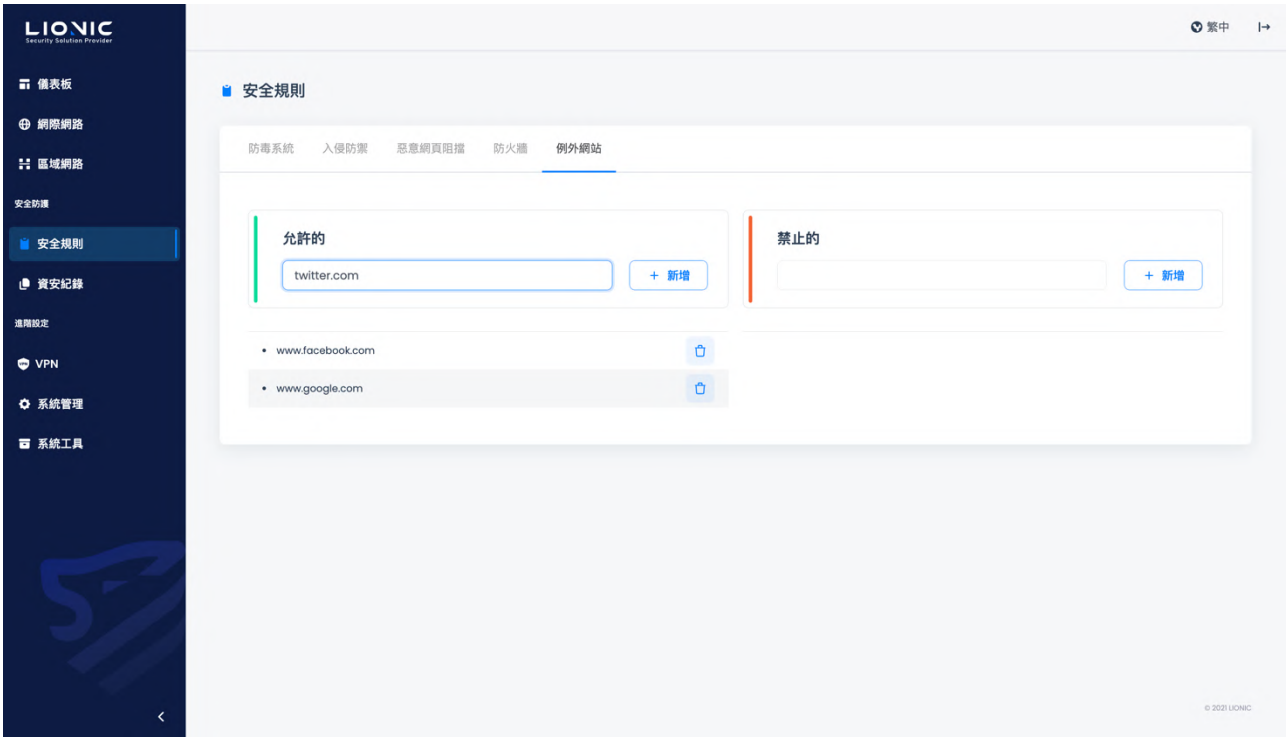
步驟四：點擊 [套用] 後開始生效。

防火牆設定說明：

- 名稱：使用者自定義的防火牆規則名稱。
- 啟用：控制該條防火牆規則啟用 / 停用。
- 紀錄：控制符合該條防火牆規則的事件是否要顯示於 [資安紀錄] 中。
- 協定：TCP / UDP / ANY。
- 來源位址、來源埠、目的位址、目的埠：指定防火牆規則要偵測條件。
- 動作：允許 / 阻擋，設定符合防火牆規則的連線處置方式。

例外網站：

將指定的網站設定至例外網站中，將可以全部允許或全部禁止與該網站之間的連線。



安全規則-例外網站

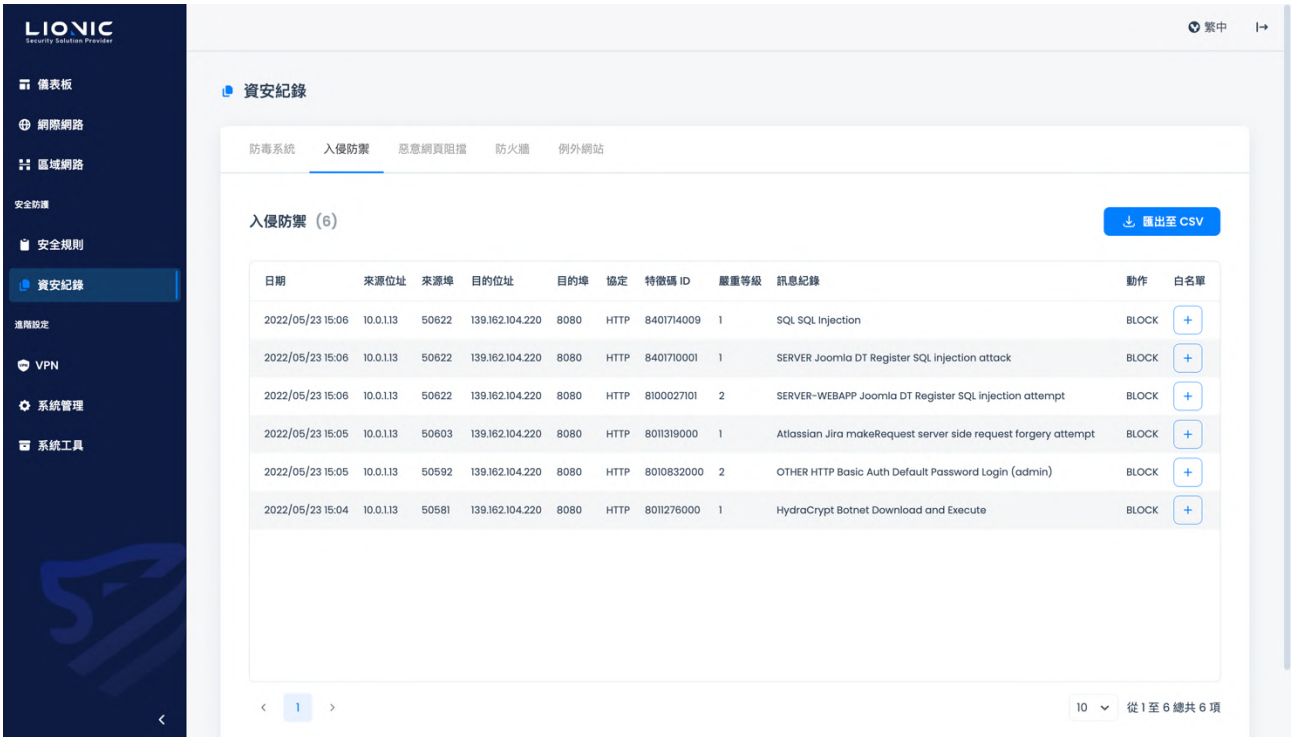
步驟一：將欲允許或欲禁止的網站網址或 IP 位址填入對應的輸入框。

步驟二：點擊 [+新增] 後開始生效。

* 備註：部分大型網站或網路服務會需要透過一個以上的域名或 IP 位址連線到不同頁面。若未將所有域名或 IP 位址設為允許或禁止，將無法完整使用或禁止存取該網站。

資安紀錄

在 Pico-UTM 100 偵測到資安威脅後，相關的威脅資訊會依照不同的資安防護功能顯示在對應的 [資安紀錄] 頁面裡。

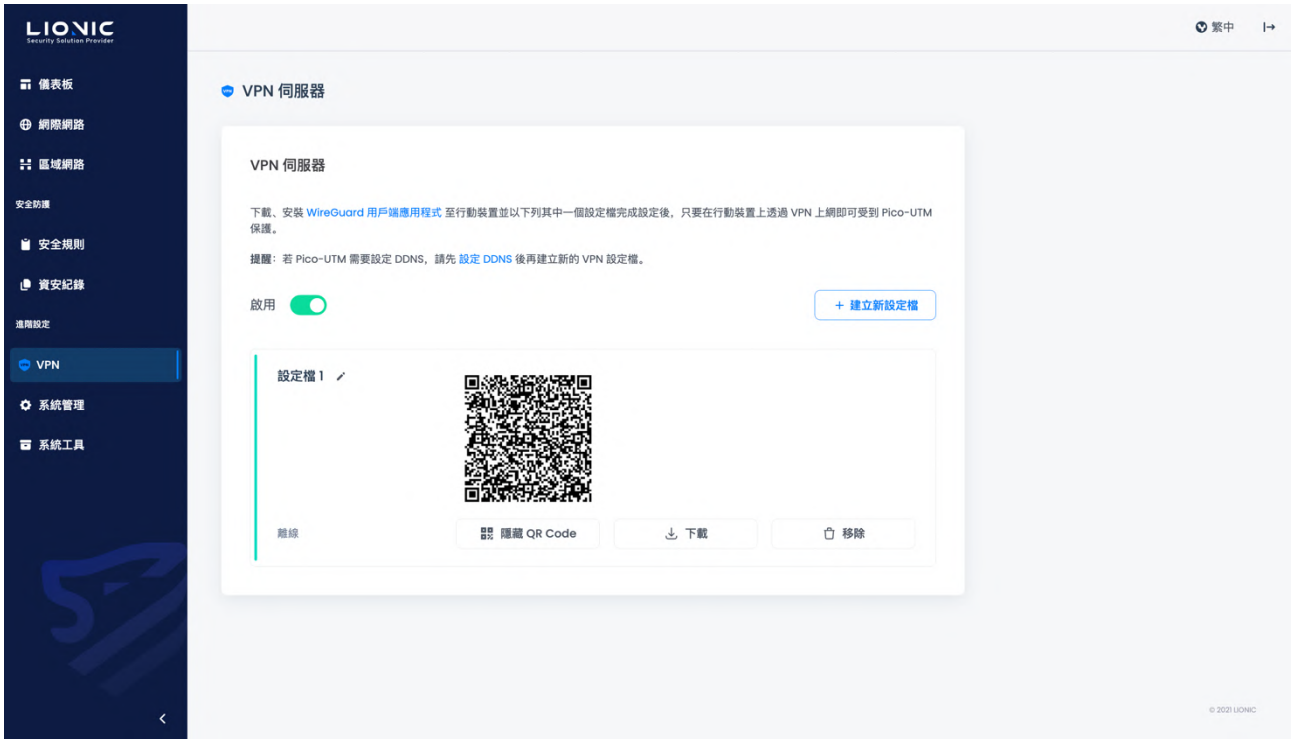


資安紀錄

- **匯出至 CSV**：將紀錄批次匯出成 CSV 檔。
- **白名單**：當 Pico-UTM 100 的資安防護功能破壞了安全的檔案或阻擋了受信任的連線時，可以透過白名單功能恢復正常使用。
    - 新增白名單規則：請在 [資安紀錄] 頁面中搜尋被破壞或被阻擋的事件紀錄後，點擊 [+] 加入白名單。
    - 刪除白名單規則：在 [安全規則] 頁面中可刪除指定白名單規則。

VPN 伺服器

若要延伸 Pico-UTM 100 的防護範圍到使用行動網路或公共無線網路的裝置，可以啟用 VPN 伺服器功能。透過 VPN 連線，不在 Pico-UTM 100 LAN 端網域的裝置也能受到資安防護功能的保護。



VPN 伺服器

前置準備：

下載並安裝 WireGuard 用戶端應用程式至欲使用防護功能的裝置。

設定步驟：

步驟一：點擊 [啟用]。

步驟二：點擊 [+建立新設定檔]。

步驟三：

- 若您使用手機、平板等裝置：點擊 [顯示 QR Code] 並以 WireGuard 用戶端應用程式掃描 QR Code 後完成設定。
- 若您使用筆記型電腦等裝置：點擊 [下載] 並將設定檔匯入 WireGuard 用戶端

Lionic Confidential 2022 Lionic Corp.

應用程式以完成設定。

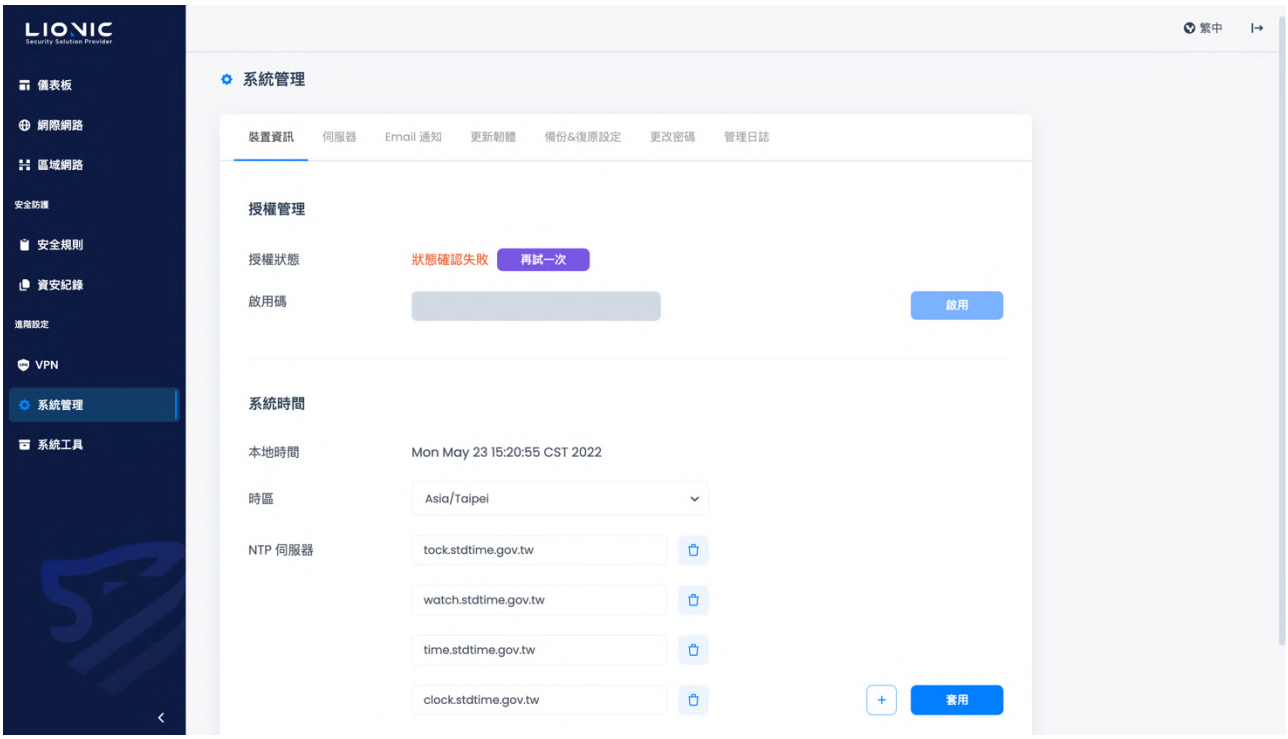
完成設定後，請在需要使用 Pico-UTM 100 的安全防護功能前開啟 WireGuard 用戶端程式並透過 VPN 連線回 Pico-UTM 100。

* 備註：

1. 若您有需要在 Pico-UTM 100 上設定動態 DNS 服務 (DDNS)，請先完成 DDNS 設定後再設定 VPN 伺服器。
2. 若 Pico-UTM 100 前架設有路由器，請在路由器上設定通訊埠轉發至 Pico-UTM 100 的私有 IP 位址 / Port 51820，並手動修改 WireGuard 用戶端程式的設定檔，將伺服器位址改成路由器 IP 位址或主機名稱。
3. 若在使用 VPN 的過程中發現連線異常，請先嘗試在 WireGuard 用戶端程式上重啟 VPN 連線。

系統管理

裝置資訊：



系統管理-裝置資訊

授權管理

檢視 Pico-UTM 100 的授權有效狀態、啟用授權或延展授權。

顯示訊息	授權狀態
授權到期日	授權有效
尚未啟用	尚未啟用授權
已過期	授權已過期
狀態確認失敗	與授權伺服器連線異常，無法確認授權狀態

- **啟用授權：**當第一次使用 Pico-UTM 100 時，請在可連接至網際網路的環境下將授權啟用碼（備註 1）填入輸入框並點擊 [啟用]，以確保 Pico-UTM 100 能提供完整的資安防護功能。
- **延展授權：**Pico-UTM 100 會在授權到期前 30 天顯示提醒，請儘速完成授權訂閱（備註 2）以取得延展碼，將延展碼填入輸入框並點擊 [延展] 後即可延展授權期限。

* 備註：

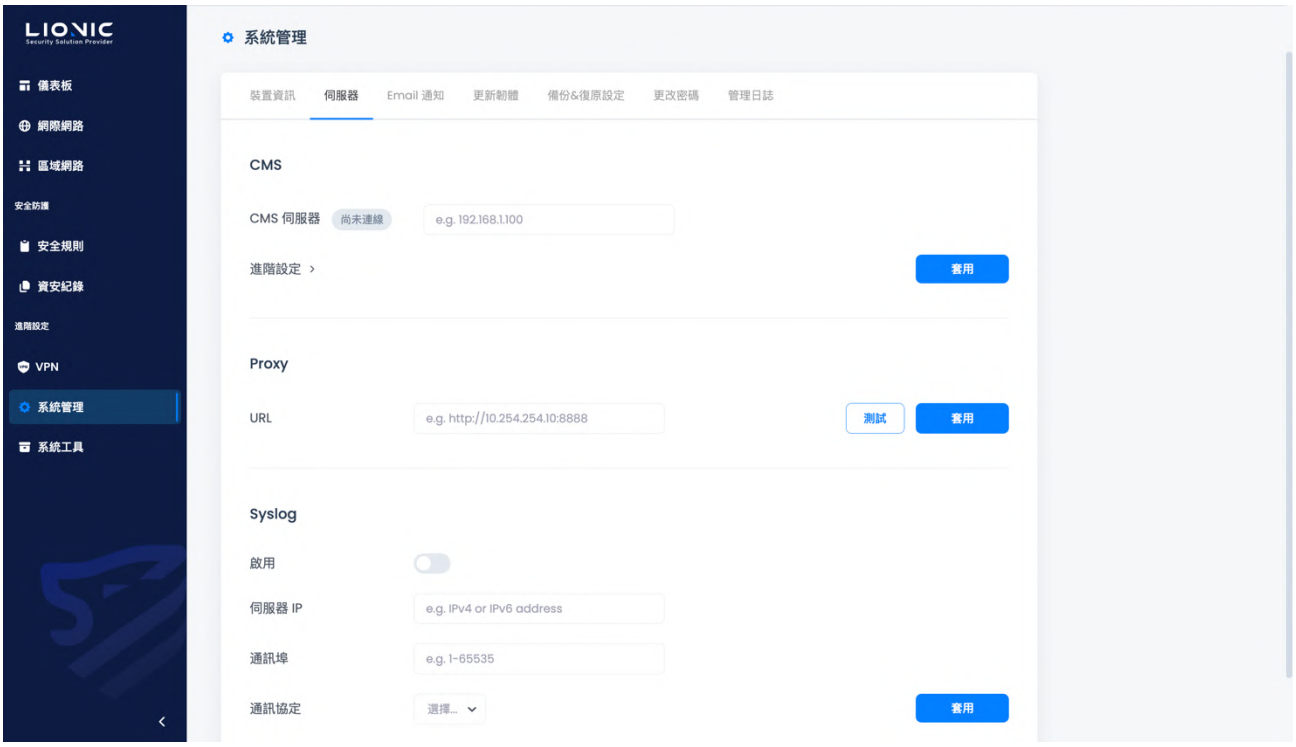
1. 若您沒收到授權啟用碼或啟用碼異常，請聯繫當地經銷商或銷售代表。
2. 若您需要訂閱新的授權以繼續使用 Pico-UTM 100，請聯繫當地經銷商或銷售代表。

系統時間

顯示並設定 Pico-UTM 100 的系統時間。

- **時區：**調整時區設定以符合當地時間。
- **NTP 伺服器：**若有優先選用的 NTP 伺服器，可以新增至 NTP 伺服器設定中。

伺服器：



系統管理-伺服器

CMS

中央管理伺服器（CMS）可以批次控管多台 Pico-UTM 100。在 CMS 建置完成後將 CMS 位址填入輸入框並點擊 [套用]，Pico-UTM 100 即可與 CMS 連線。如有需求，請聯繫當地經銷商或銷售代表。

Proxy

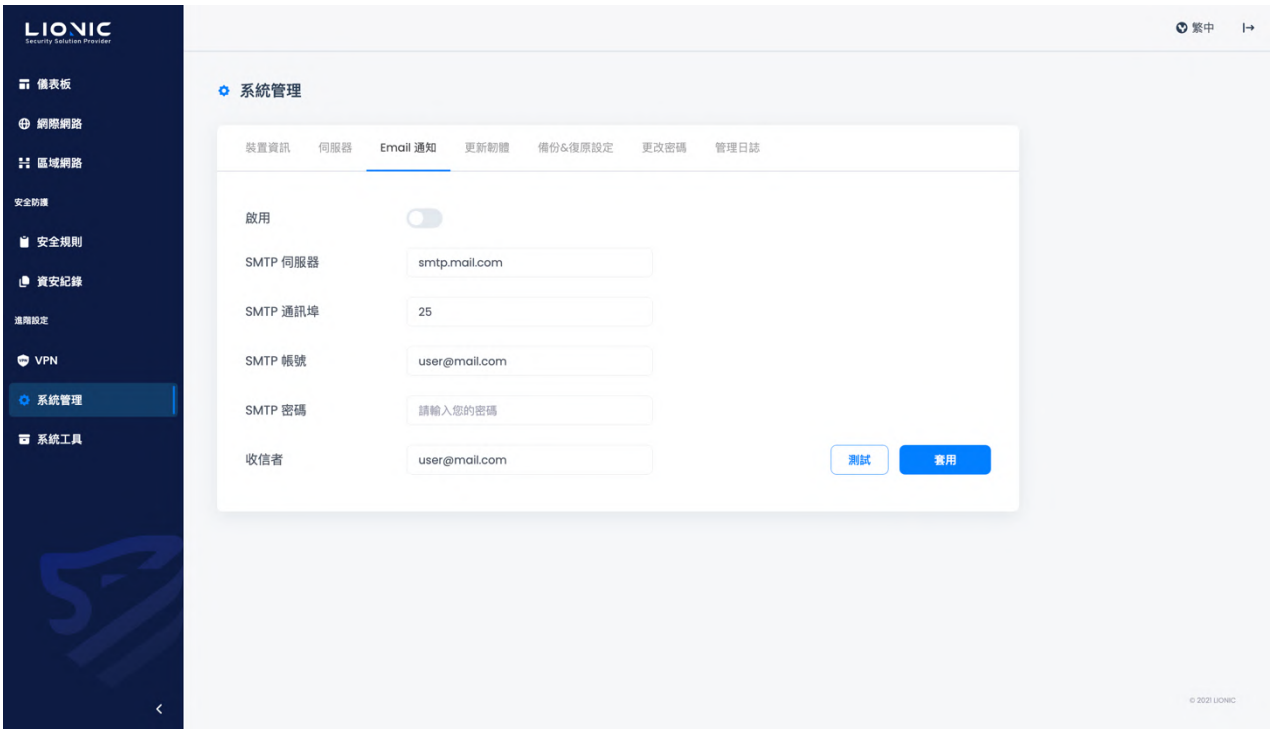
代理伺服器（Proxy）可以協助無法直接連線至網際網路的 Pico-UTM 100 連回 Lionic 的各項雲端服務，以確保 Pico-UTM 100 發揮完整的資安防護功能。當部署 Pico-UTM 100 於內部網路時，可以將 Proxy 位址填入輸入框並點擊 [套用]，Pico-UTM 100 即可透過 Proxy 使用 Lionic 雲端服務。如有需求，請聯繫網路管理員。

Syslog

Syslog 伺服器可以蒐集 Pico-UTM 100 的運行歷程。若您有自行設置 Syslog 伺服器，請將各項設定值填入輸入框並點擊 [套用]。

Email 通知：

[Email 通知] 功能可以在 Pico-UTM 100 偵測到資安威脅時，將威脅資訊以電子郵件寄到指定信箱。請在輸入框內填入正確設定值後點擊 [套用] 以完成設定，並點擊 [測試] 讓 Pico-UTM 100 發出測試信以確認設定是否正確。

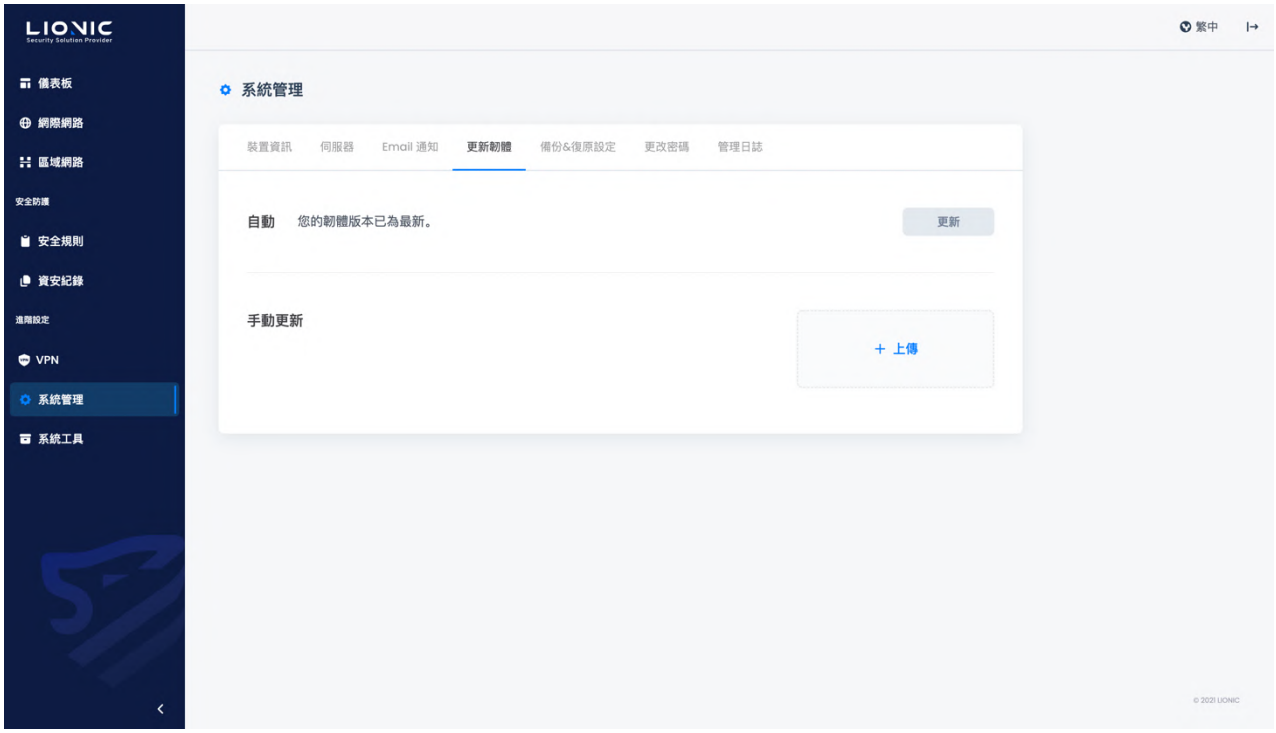


系統管理-Email 通知

* 備註：若您需要使用 Gmail 作為 Email 通知的發信者，請先啟用 Gmail 的 2-Step Verification，並建立 App Password 填入 [SMTP 密碼] 欄位。

韌體更新：

[韌體更新] 頁面會在有新的韌體可以更新時顯示提示，點擊 [更新] 即可開始更新。



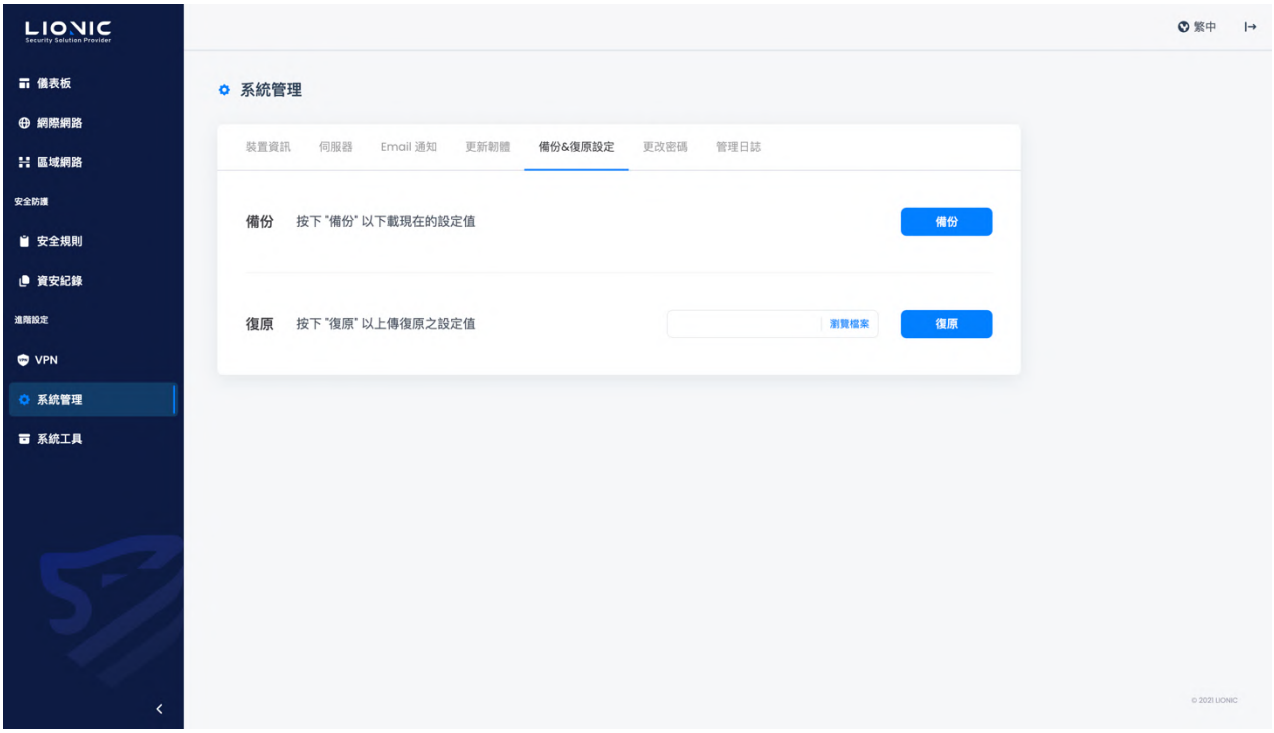
系統管理-更新韌體

若您在疑難排解的過程中需要手動更新韌體，請點擊 [+上傳] 並選擇欲更新的韌體映像檔。

* 備註：韌體更新過程中 Pico-UTM 100 會重新啟動，將會使網路連線暫時中斷。

備份&復原設定：

[備份&復原設定] 功能可以備份 Pico-UTM 100 的各項設定，例如各資安防護功能的安全規則與白名單設定等，並在同一台或其它台 Pico-UTM 100 上復原，適合在疑難排解或部署少量 Pico-UTM 100 時使用。

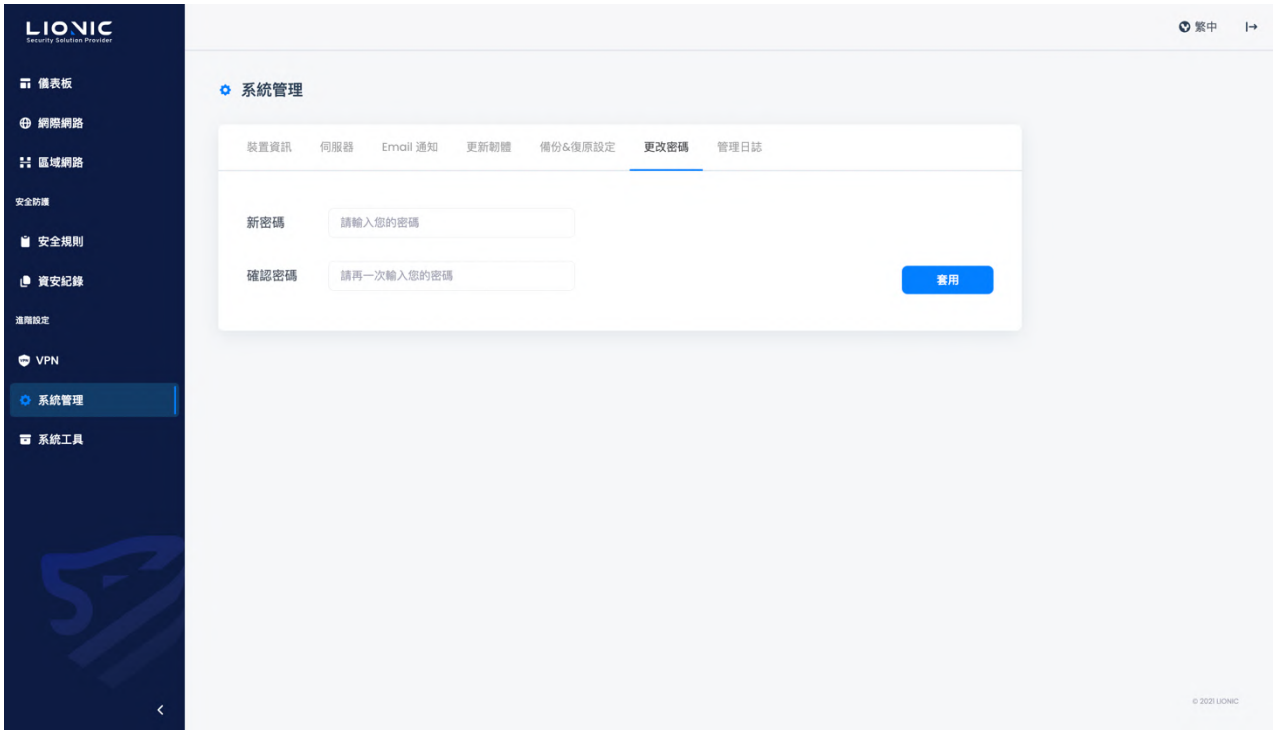


系統管理-備份&復原設定

* 備註：如有部署大量 Pico-UTM 100 的需求，建議使用 CMS。

更改密碼：

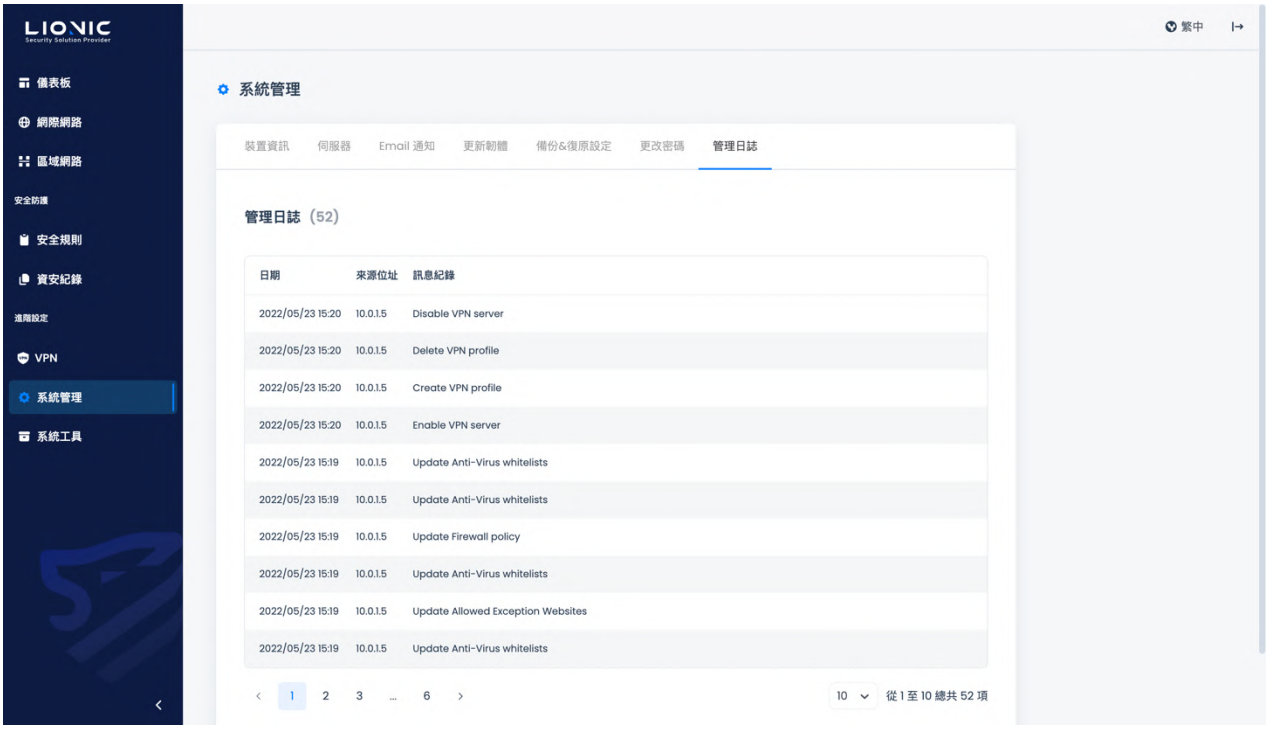
如需變更 Pico–UTM 100 網頁控制介面的登入密碼，請將新密碼填入輸入框後點擊［套用］。



系統管理-更改密碼

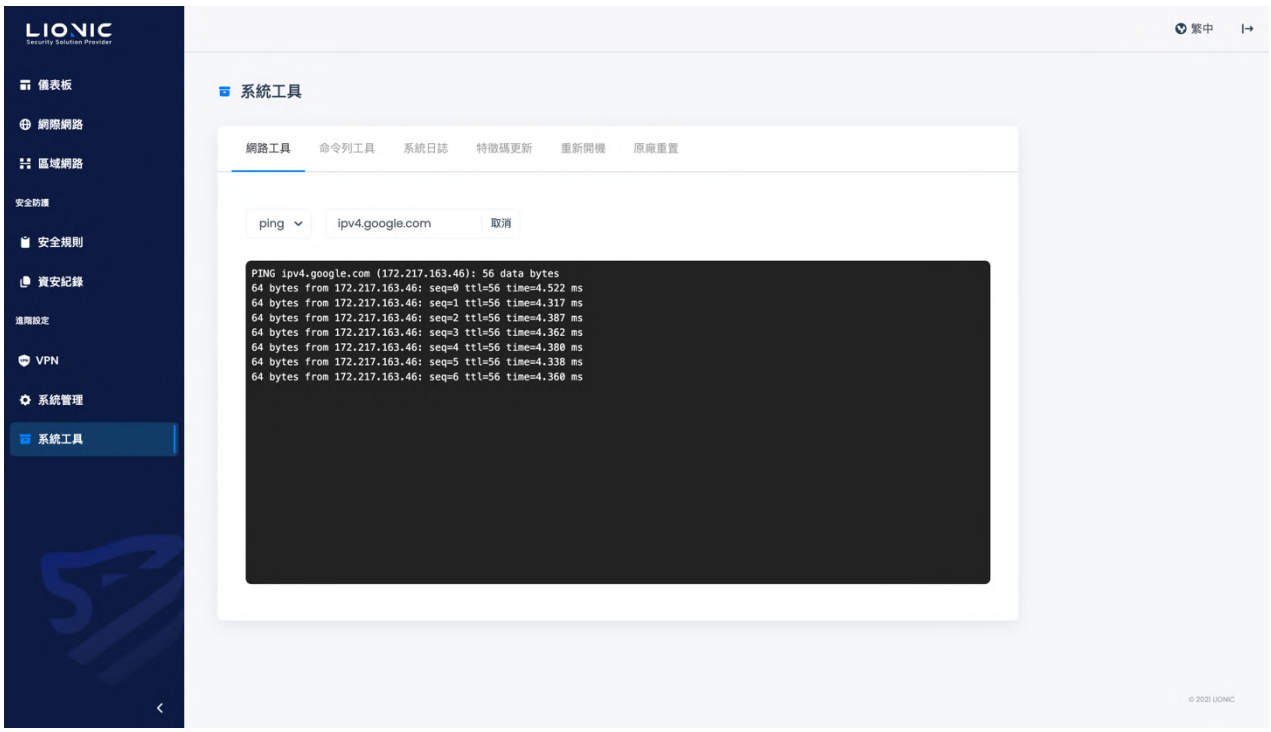
管理日誌：

[管理日誌] 頁面會列出 Pico-UTM 管理員在網頁控制介面上所做的各項設定變更。



系統管理-管理日誌

系統工具



系統工具

Pico-UTM 100 提供以下疑難排解功能：

- **網路工具**：以 ping、traceroute、nslookup 功能查找網路連線問題。
- **命令列工具**：進階的疑難排解功能，使用前須和 Lionic 技術支援聯繫。
- **系統日誌**：匯出系統運行日誌以便技術支援協助排除問題。
- **特徵碼更新**：手動上傳威脅特徵碼*以排除系統問題。
- **重新開機**：重新啟動 Pico-UTM 100。
- **原廠重置**：將 Pico-UTM 100 所有設定重置成出廠預設值。

* 備註：授權有效、網路連線及系統運作正常時，特徵碼會自動下載並更新。

Pico-UTM 100
Makes Security Simple

LIONIC
Security Solution Provider

© Copyright 2022 Lionic Corp. All rights reserved.

Sales Contact
Tel : +886-3-5789399
Fax : +886-3-5789595
Email : sales@lionic.com
https://www.pico-utm.com/

Lionic Corp.
https://www.lionic.com/
1F-C6, No.1, Lising 1st Rd.,
Science-Based Industrial Park,
Hsinchu City 300, Taiwan, R.O.C.