LIONIC
Security Solution Provider

使用者手冊

Dual Ark-UTM 16

版本 1.4.1

更新日期 2025/02

Lionic Corp. www.lionic.com

Dual Ark-UTM 16 使用手冊

版權聲明

商標

LIONIC 是鴻璟科技的註冊商標。
WireGuard 是 Jason A. Donenfeld 的註冊商標。
NO-IP 是 Vitalwerks Internet Solutions, LLC 的註冊商標。

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。

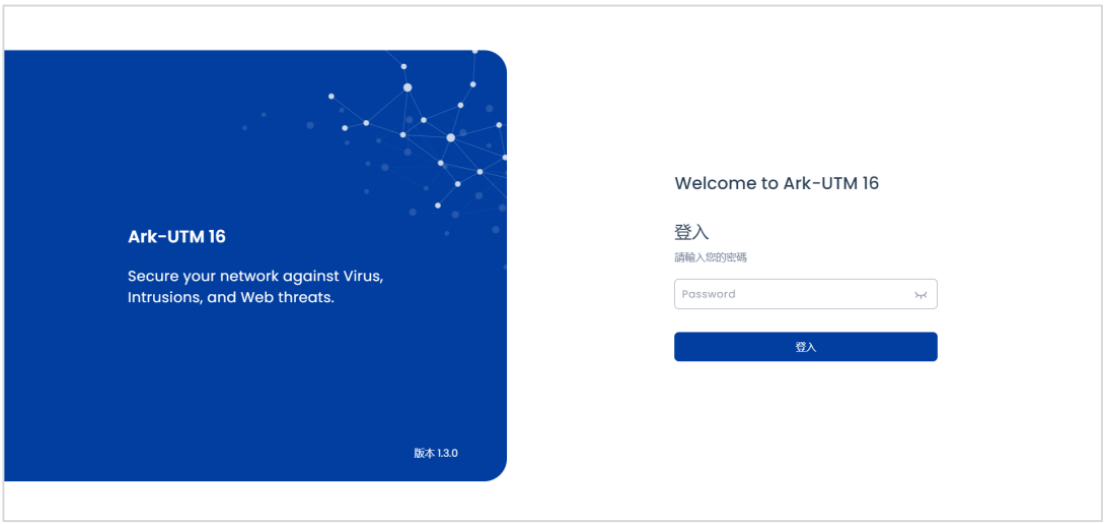
技術支援聯絡資訊 鴻璟科技股份有限公司

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

內容

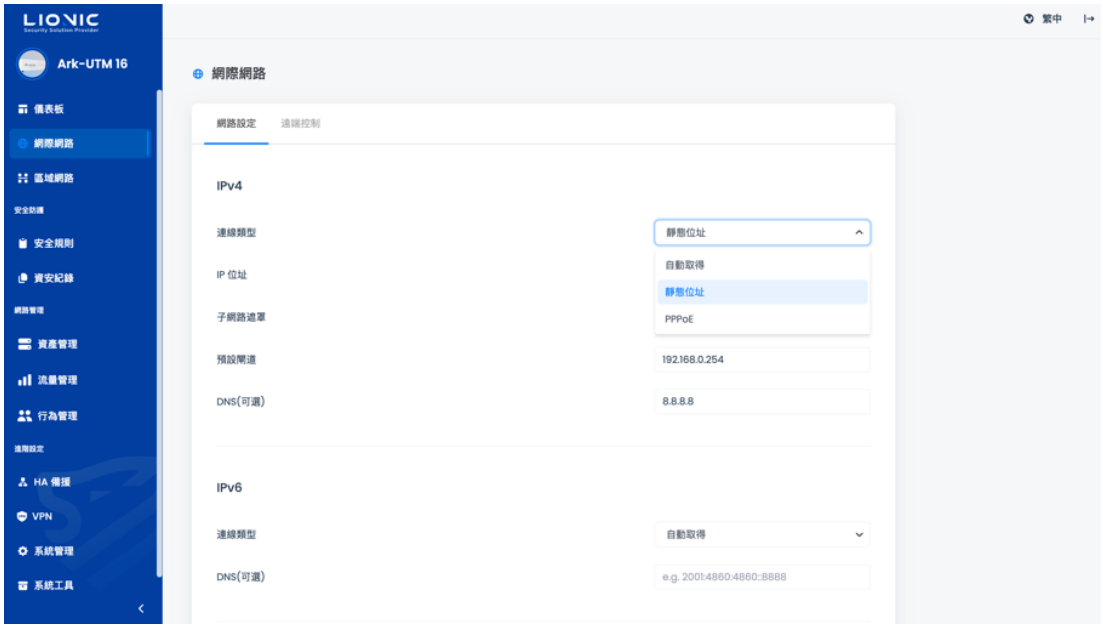
登入網頁控制介面

1. 將電源線插上 Ark-UTM 16。
2. 將網路線的一端插入網路服務供應商提供的數據機網路連接埠或上層路由器/交換機的網路連接埠 (LAN)，另一端插入 Ark-UTM 16 的外網連接埠 (WAN)。
3. 將另一條網路線一端插入 Ark-UTM 16 的內網連接埠 (LAN)，另一端插入筆電/桌機的網路連接埠。
4. 將筆電/桌機的靜態 IP 位址如下設定：
   - IP: 10.254.254.50
   - 子網路遮罩 (Subnet mask): 255.255.255.0
5. 設定完成後，請使用網頁瀏覽器開啟 https://10.254.254.254/



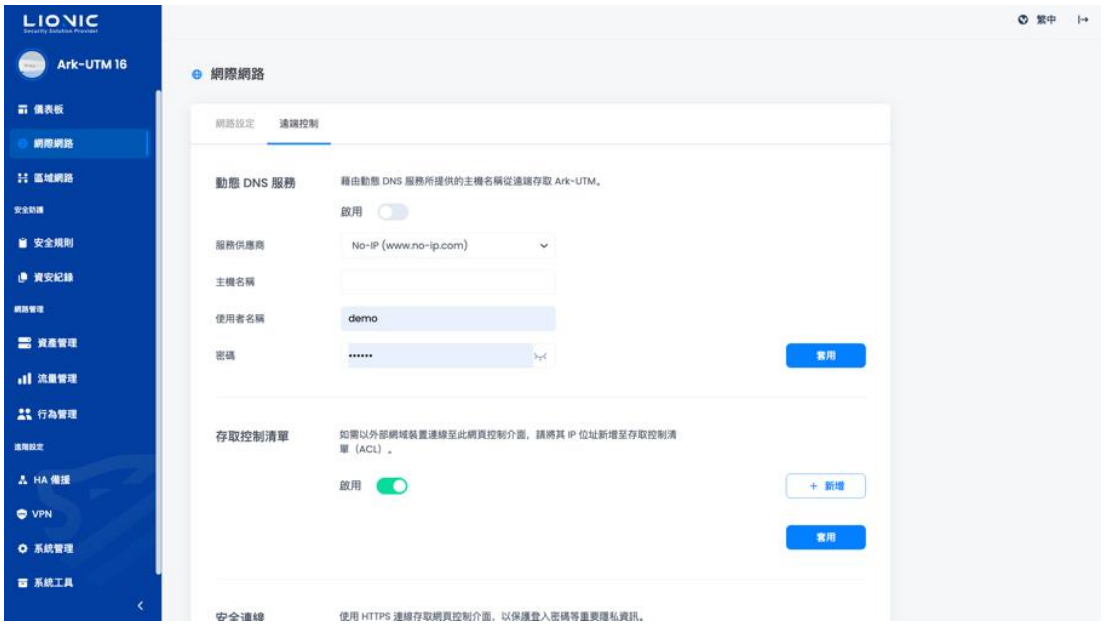
登入畫面

6. 網頁控制介面的預設密碼為貼在機身底部的機身序號。
7. 登入後，請至 [網際網路] 頁面完成 Ark-UTM 16 的 IP 設定。



網際網路-網路設定

8. 在 Ark-UTM 16 取得有效 IP 位址後，請將筆電/桌機的 IP 設定恢復。往後，您可以透過以下方式再次連線網頁控制介面：
   - 當 Ark-UTM 16 與筆電/桌機皆取得同一個內網網域下的私有 IP 位址時，位於 Ark-UTM 16 LAN 端的筆電/桌機可以透過 https://myark.lionic.com/ 連線至網頁控制介面。
   - 當 Ark-UTM 16 取得公有 IP、筆電/桌機透過另外一組公有 IP 連上網際網路時，請先以上述步驟開啟 https://10.254.254.254/ 並登入網頁控制介面，再到 [網際網路] > [遠端控制] 頁面停用 [存取控制清單]，或將筆電/桌機的公有 IP 加入 [存取控制清單]。完成設定後，位於 Ark-UTM 16 LAN 端的筆電/桌機可以透過 https://myark.lionic.com/ 連線至網頁控制介面。


LIONIC
Ark-UTM 16
儀表板
網際網路
區域網路
安全規則
資安紀錄
資產管理
流量管理
行為管理
HA 備援
VPN
系統管理
系統工具
繁中
網際網路
網路設定
遠端控制
動態 DNS 服務
藉由動態 DNS 服務所提供的主機名稱從遠端存取 Ark-UTM。
啟用
服務供應商
No-IP (www.no-ip.com)
主機名稱
使用者名稱
demo
密碼
套用
存取控制清單
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）。
啟用
+ 新增
套用
使用 HTTPS 連線存取網頁控制介面，以保護登入密碼等重要隱私資訊。

網際網路-遠端控制

功能概述

儀表板：

[儀表板] 會顯示 Ark-UTM 16 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 Ark-UTM 16 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 Ark-UTM 16 的控制項。

區域網路：

[區域網路] 可以調整 Ark-UTM 16 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。

網路管理：

- **資產管理：**資產管理功能可以列出辨識到的 LAN 端裝置，並阻擋或允許指定資產連網。
- **流量管理：**流量管理能列出各個 LAN 端裝置當前的連線用量並做頻寬管理。
- **行為管理：**行為管理功能可以對特定內容類別或應用程式做管理。

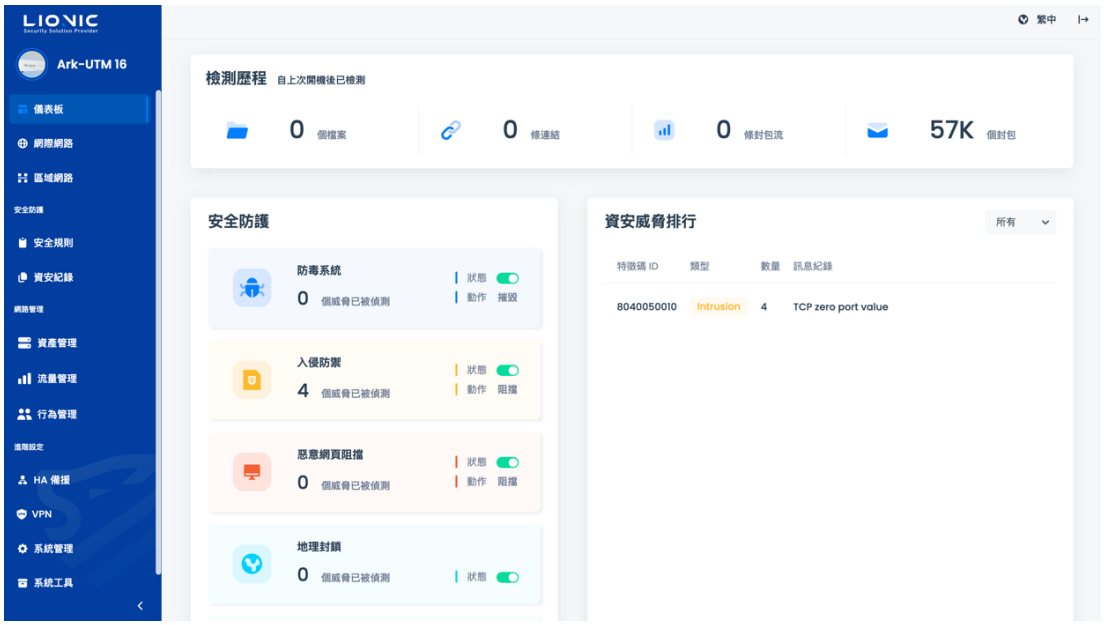
進階設定：

- **HA 備援**:在 2 台或更多 Ark-UTM 16 上設定 HA 備援功能、組成 HA 備援群組，可以在其中一台 Ark-UTM 16 發生異常時自動切換使用其它 Ark-UTM 16、維持網路連線與安全防護不中斷。
- **VPN**:若要延伸 Ark-UTM 16 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

Ark-UTM 16 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 Ark-UTM 16 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 Ark-UTM 16 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

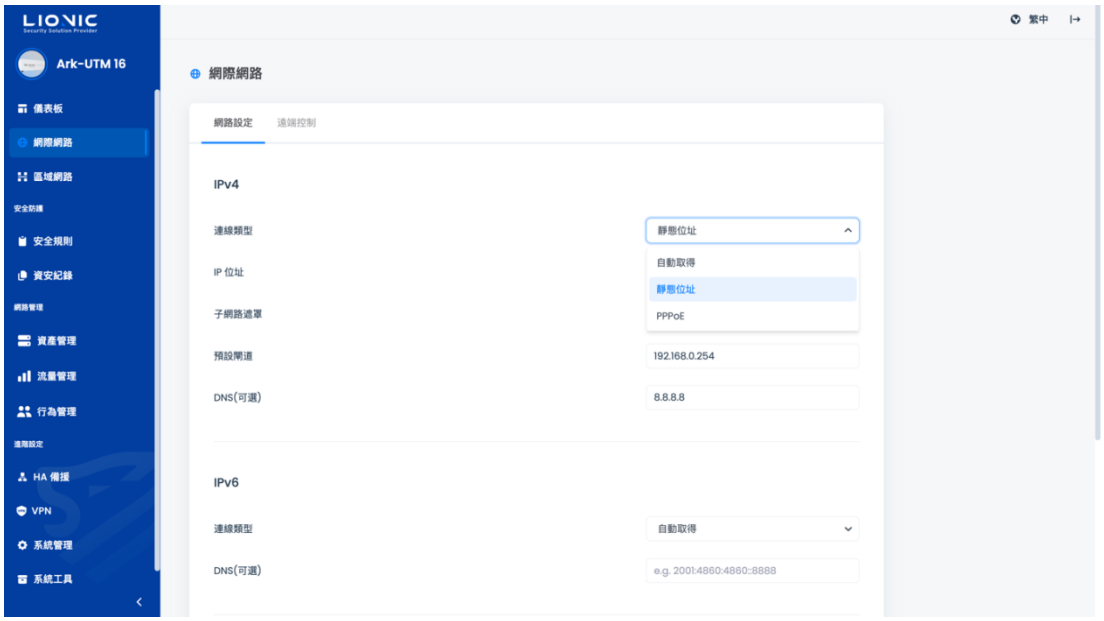
流量監控：顯示經過 Ark-UTM 16 的上傳/下載速度與傳輸量。

裝置資訊：顯示 Ark-UTM 16 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、韌體最後更新日期、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 Ark-UTM 16 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。



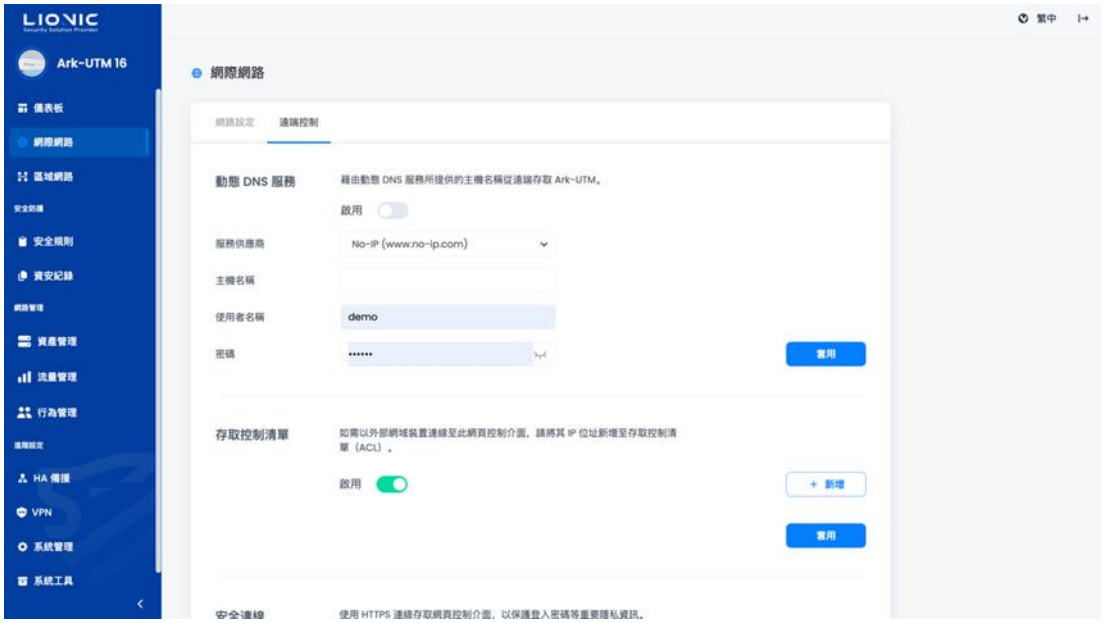
網際網路-網路設定

- **自動取得**：透過 DHCP 自動取得 IP 位址，適合 Ark-UTM 16 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。
- **VLAN**：當 Ark-UTM 16 部署在 VLAN 環境時，可在此輸入 Ark-UTM 16 所屬網域的 VLAN ID。

* 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 Ark-UTM 16 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 Ark-UTM 16 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 Ark-UTM 16 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 Ark-UTM 16 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 Ark-UTM 16 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 Ark-UTM 16 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 Ark-UTM 16，請稍候片刻再嘗試連線。
3. 若 Ark-UTM 16 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，Ark-UTM 16 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 Ark-UTM 16。

* 備註：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

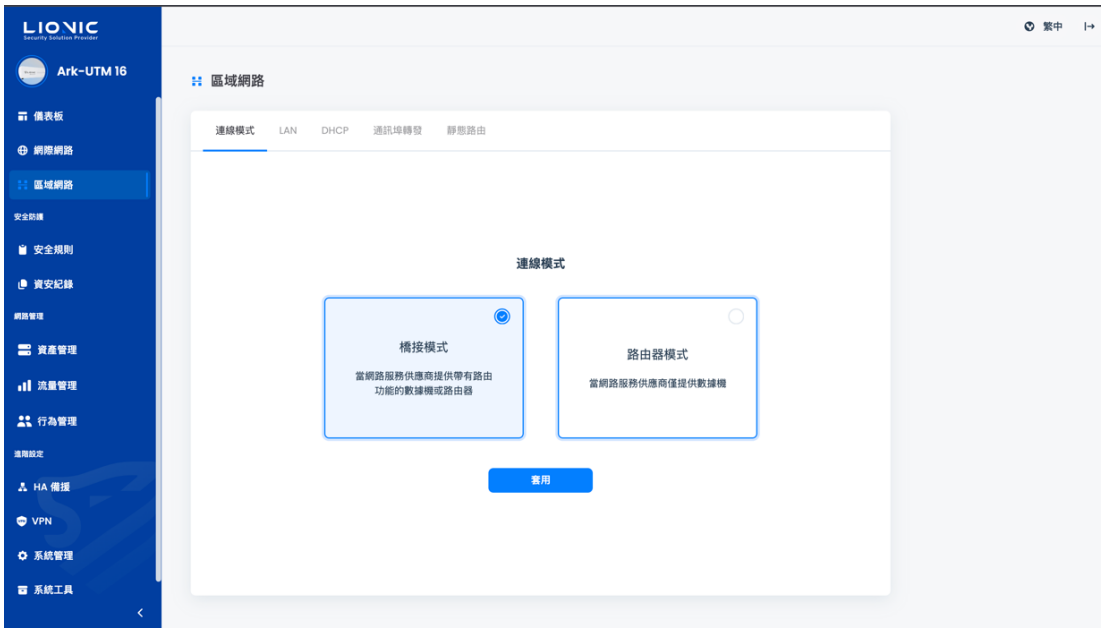
安全連線

啟用 [安全連線] 後，將全面使用 HTTPS 連線至 Ark-UTM 16 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

Ark-UTM 16 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，Ark-UTM 16 僅提供橋接功能，不會對 LAN 端裝置配發 DHCP IP 位址。此模式為 Ark-UTM 16 預設值，適合在部署 Ark-UTM 16 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，Ark-UTM 16 能夠提供 DHCP IP 位址配發及路由功能，適合在部署 Ark-UTM 16 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]，Ark-UTM 16 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。

LAN

在 [路由器模式] 下，使用者能自行設定區域網路 IP 網段。將部署的網段填入輸入框後點擊 [套用]，DHCP Server 會依照設定範圍自動配發 IP 位址。

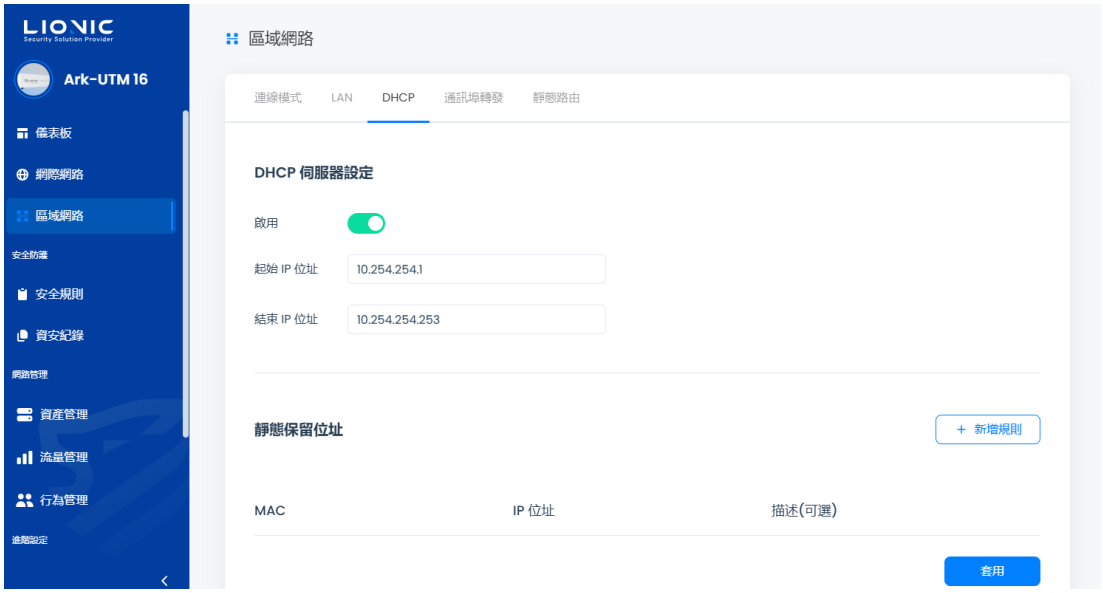
區域網路-LAN IP

- **無 NAT 路由 LAN 位址設定**

  在 [路由器模式] 下，使用者能自行設定無 NAT 路由 IP 網段。當外網與內網連線 IP 不須透過 NAT 轉換時，將部署的網段填入輸入框後點擊 [套用]，即可使用。

DHCP

在 [路由器模式] 下，Ark-UTM 16 能提供 DHCP IP 位址配發功能。當 Ark-UTM 16 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 伺服器設定:

- **啟用**：啟用 / 停用 DHCP 伺服器功能。
- **起始 IP 位址與結束 IP 位址**：依照 [區域網路] > [LAN] > [區域網路 IP 設定] 所自訂的 IP 位址設定 DHCP 伺服器將配發的 IP 範圍

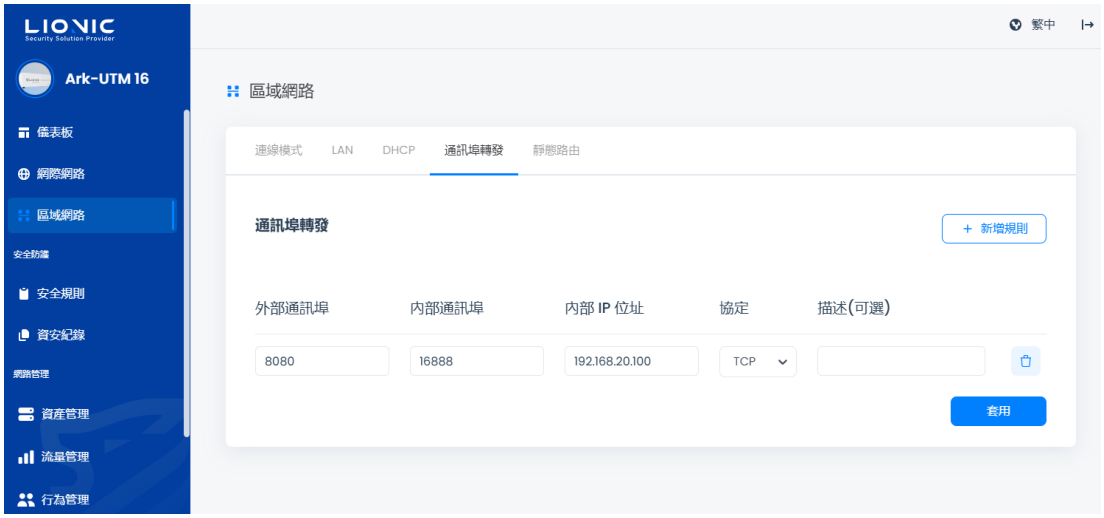
靜態保留位址

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

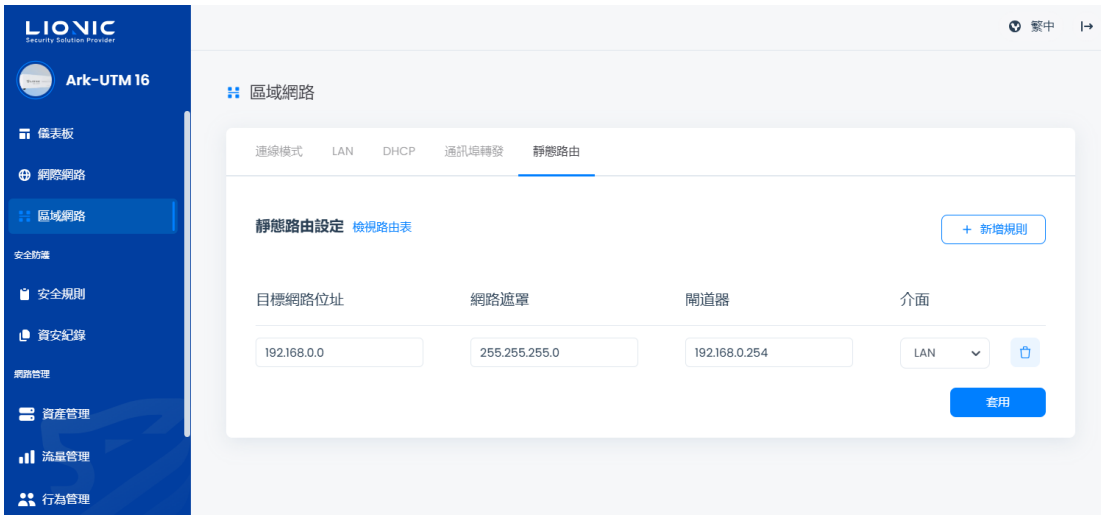
在 [路由器模式] 下，Ark-UTM 16 能提供通訊埠轉發功能。當有需要開放外部裝置存取 LAN 端裝置時，可以使用此項功能設定外部通訊埠轉發至指定內部 IP 位址。



區域網路-通訊埠轉發

靜態路由

在 [路由器模式] 下，Ark-UTM 16 能提供靜態路由功能。當有需要連接不同網段時，可以使用此功能。



區域網路-靜態路由

安全規則

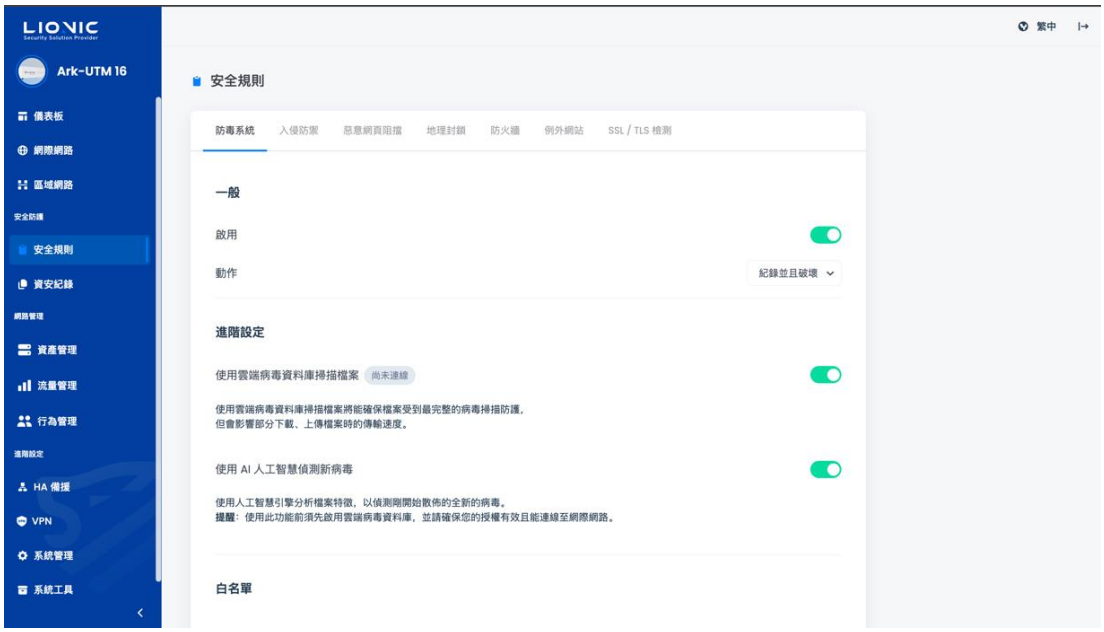
防毒系統、入侵防禦、惡意網頁阻擋

Ark-UTM 16 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 - 使用AI人工智慧偵測新病毒	- 阻擋暴力破解 - 阻擋協定異常 - 阻擋通訊埠掃描與 DoS 攻擊 - 攻擊發現威脅後保存封包 PCAP	- 使用 AI 人工智慧偵測動態的惡意網址 - 外部資料庫
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

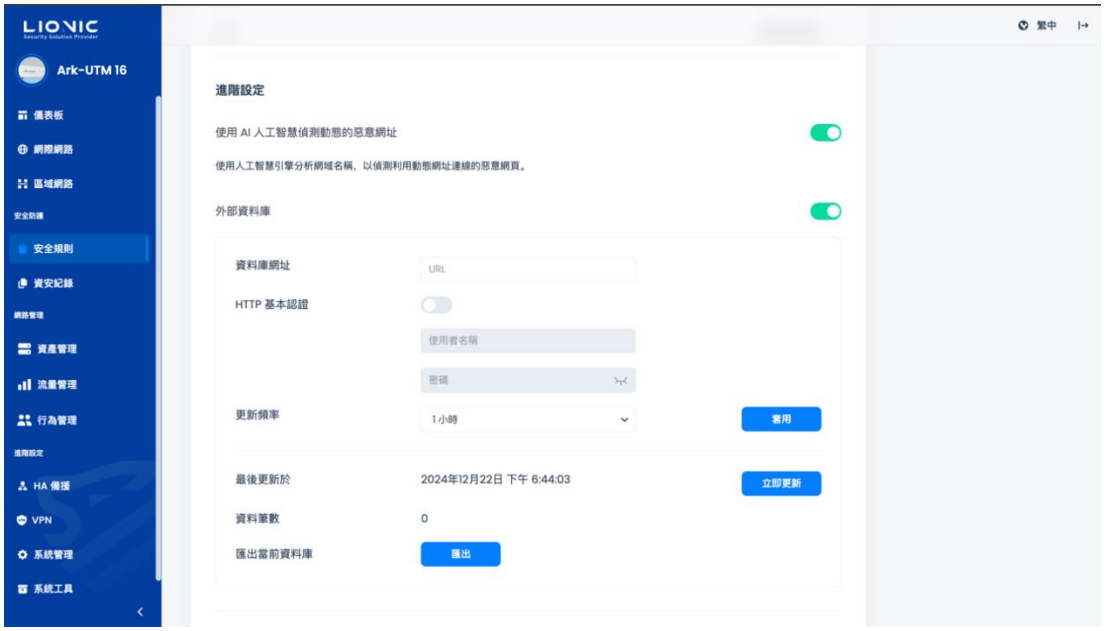


安全規則

- **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 Ark-UTM 16 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，Ark-UTM 16 也能將檔案特徵和雲端病毒資料庫進行比對。在 Ark-UTM 16 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。
- **使用 AI 人工智慧偵測新病毒**： Lionic 的防毒查詢雲端整合了 AI 防毒引擎，此引擎具備了偵測零日病毒的能力。啟用此功能後，將會利用此 AI 技術偵測零日病毒。
- **阻擋暴力破解**：啟用此功能後，Ark-UTM 16 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，Ark-UTM 16 會依據密集程度於 [資安紀錄] 顯示或進而阻擋連線。
- **阻擋協定異常**：啟用此功能後，Ark-UTM 16 的 [入侵防禦] 能偵測不符合通訊協定規範的異常封包並進行阻擋。
- **阻擋通訊埠掃描與 DoS 攻擊**：
    - 防止 TCP、TCP 半開連線、UDP、ICMP、SCTP、IP 協定短時間爆增連線的 DoS 攻擊。

- 阻擋傳送大量異常格式封包的裝置。
- 阻擋 TCP SYN scan、TCP RST scan 以及 UDP scan 等通訊埠掃描嘗試。

- **發現威脅後保存封包 PCAP**：啟用此功能後，Ark-UTM 16 會在 [入侵防禦] 偵測到威脅時保存被視為威脅的封包，以便後續分析使用。
- **使用 AI 人工智慧偵測動態的惡意網址**：啟用此功能後，Ark-UTM 16 會將連線網址與雲端資料庫進行比對。利用人工智慧 DGA 偵測模型判斷此網址其是否為利用DGA生成的惡意網址。
- **外部資料庫**：提供使用者自行設定惡意網頁的外部資料源以滿足進階防護需求。



惡意網頁阻擋-進階設定

- **白名單**：當 Ark-UTM 16 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。

地理封鎖

根據使用者設定的國家/地區，針對 IP 位址封鎖來自該地區的攻擊或防止資訊外洩至該地區。

安全規則-地理封鎖

步驟一：啟用地理封鎖。

步驟二：點擊  選擇允許/阻擋地區。

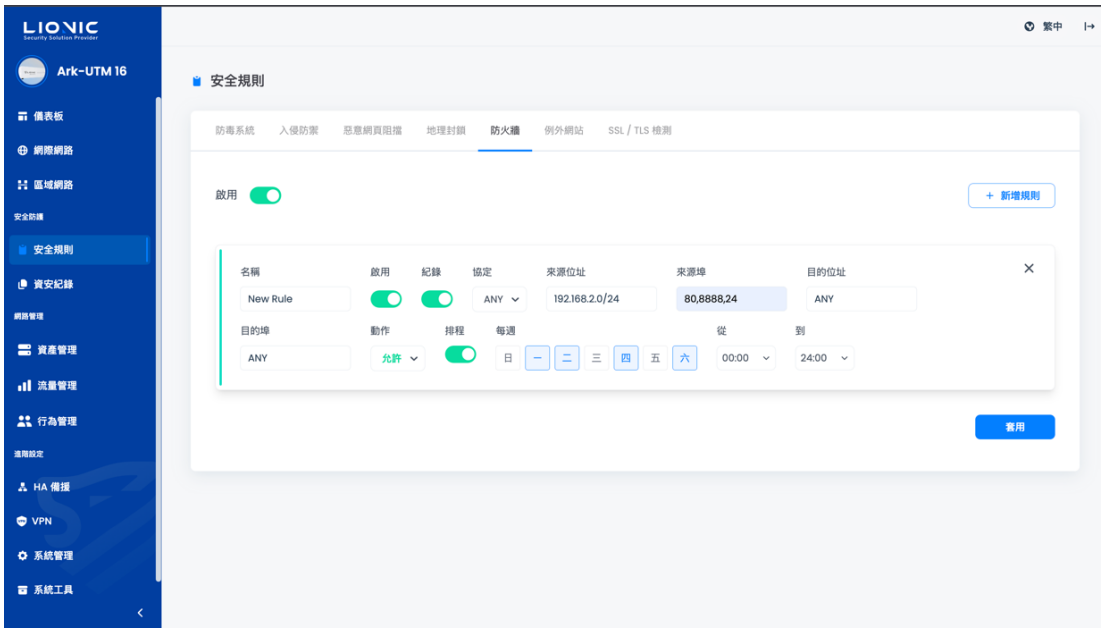
步驟三：填入各項設定值。

步驟四：點擊 [確認] 後開始生效。

- **白名單**：根據已被設定國家/地區可加以設定例外的白名單

防火牆

除三大資安防護功能外，Ark-UTM 16 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。

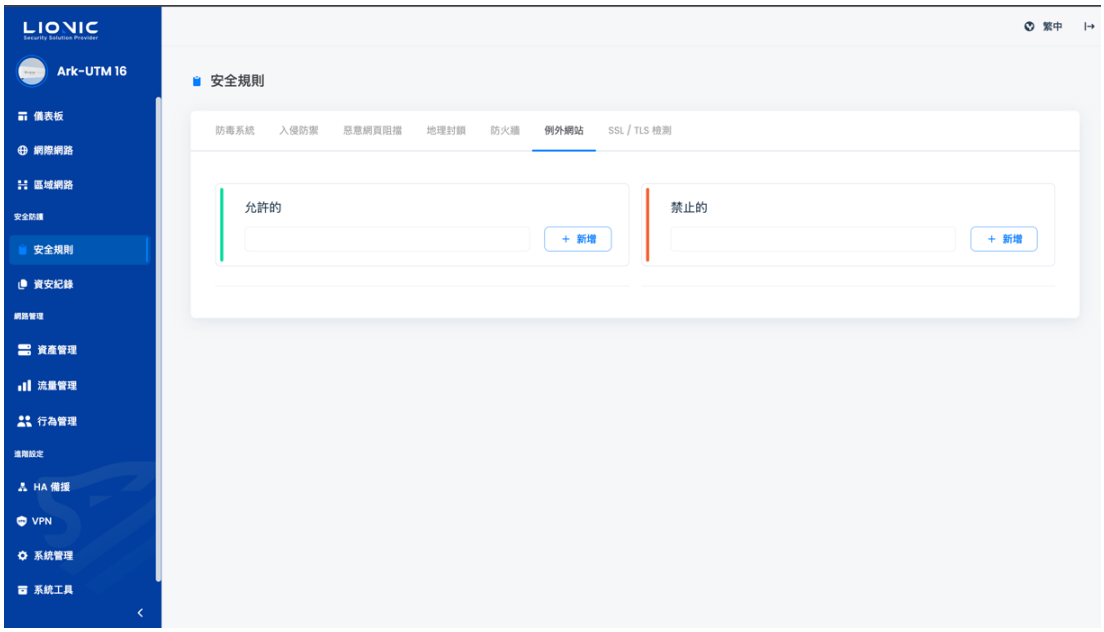
步驟四：點擊 [套用] 後開始生效。

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。
- **排程**：設定防火牆規則生效時間、排程設定。

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。

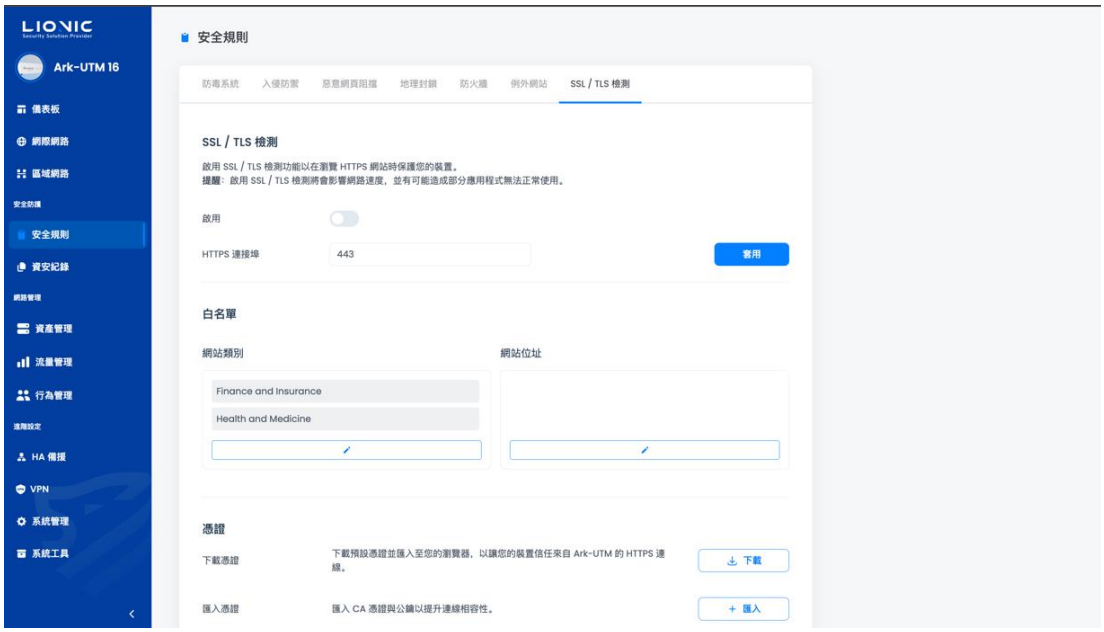
步驟二：點擊 [+新增] 後開始生效。

* 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。

SSL/TLS 檢測

啟用 [SSL/TLS 檢測] 後，Ark-UTM 16 將會檢測經 SSL 或 TLS 加密的封包，以提升瀏覽 HTTPS 網站時的安全性。

* 備註：啟用 [SSL/TLS 檢測] 將會影響網路傳輸速度，並有可能造成部分應用程式無法正常使用。



安全規則-SSL/TLS 檢測

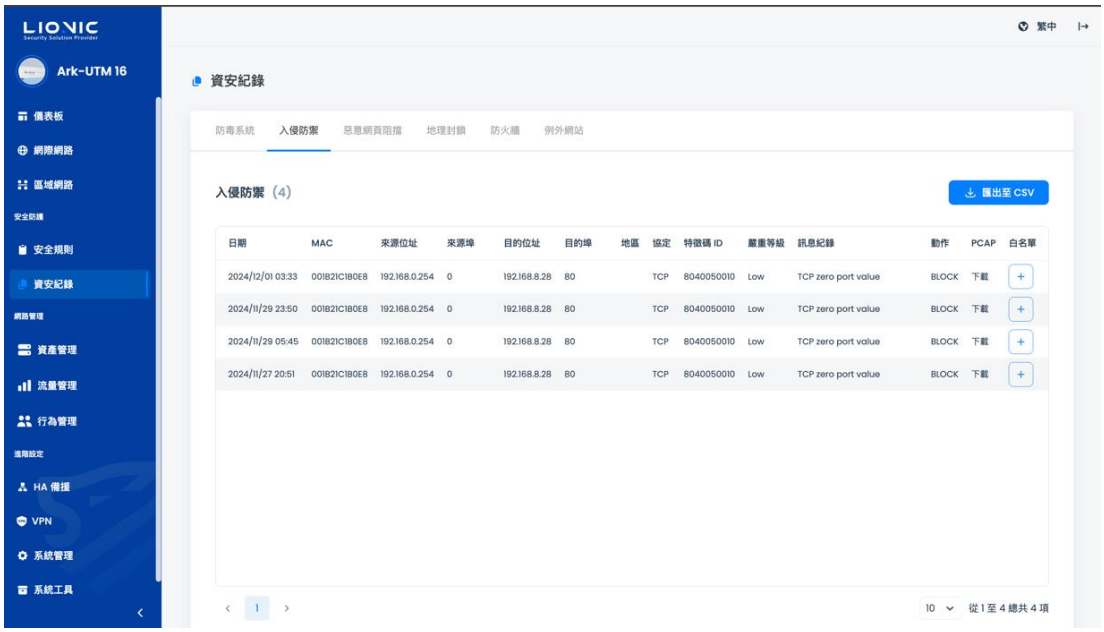
- **啟用**：啟用或停用 [SSL/TLS 檢測]，預設為停用。
- **HTTPS 連接埠**：可自訂 HTTPS 連線使用的連接埠*，預設為 443。若要設定多個連接埠，可以用「,」區隔。
- **白名單**：將網站加入白名單後，Ark-UTM 16 將不會檢測該網站的加密封包。若因相容性或隱私性不希望加密封包被檢測，可將受信任的網站加入白名單。
    - 網站類別：Ark-UTM 16 提供多種網站類別作為白名單的選項，預設白名單包含「Finance and Insurance」和「Health and Medicine」。將指定網站類別加入白名單後，符合該分類標準的網站連線將不會被檢測加密封包。
    - 網站位址：提供使用者自訂欄位，將受信任的網站位址加入白名單。將指定網站位址加入白名單後，該網站連線將不會被檢測加密封包。
- **下載憑證**：可下載 Ark-UTM 16 的預設憑證並匯入至您的瀏覽器，讓您的裝置信任來自 Ark-UTM 16 的 HTTPS 連線。
- **匯入憑證**：若您的組織有 CA 憑證與公鑰，可匯入至 Ark-UTM 16 以提升連線相容性。

* 備註：

1. 自訂 HTTPS 連線使用的連接埠時，建議避開其它網路服務常用的連接埠(例如 FTP 用的 Port 20, 21 或 SMTP 用的 Port 25 等連接埠)，以免發生連接埠衝突問題。
2. 為提升啟用 [SSL/TLS 檢測] 後的相容性，Ark-UTM 16 已將部分受信任的網路服務 （Google, Apple, Microsoft 等）位址加入白名單。

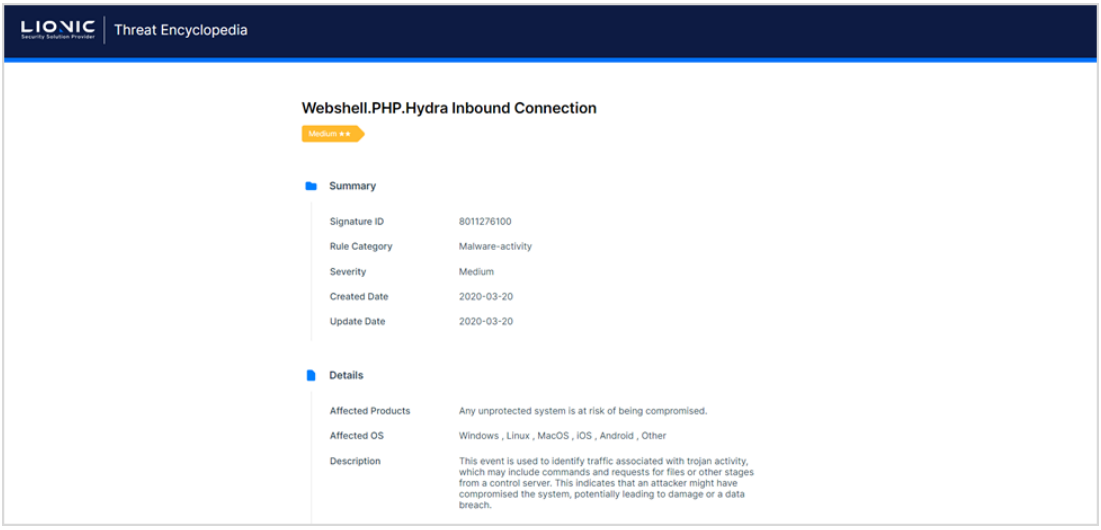
資安紀錄

在 Ark-UTM 16 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。



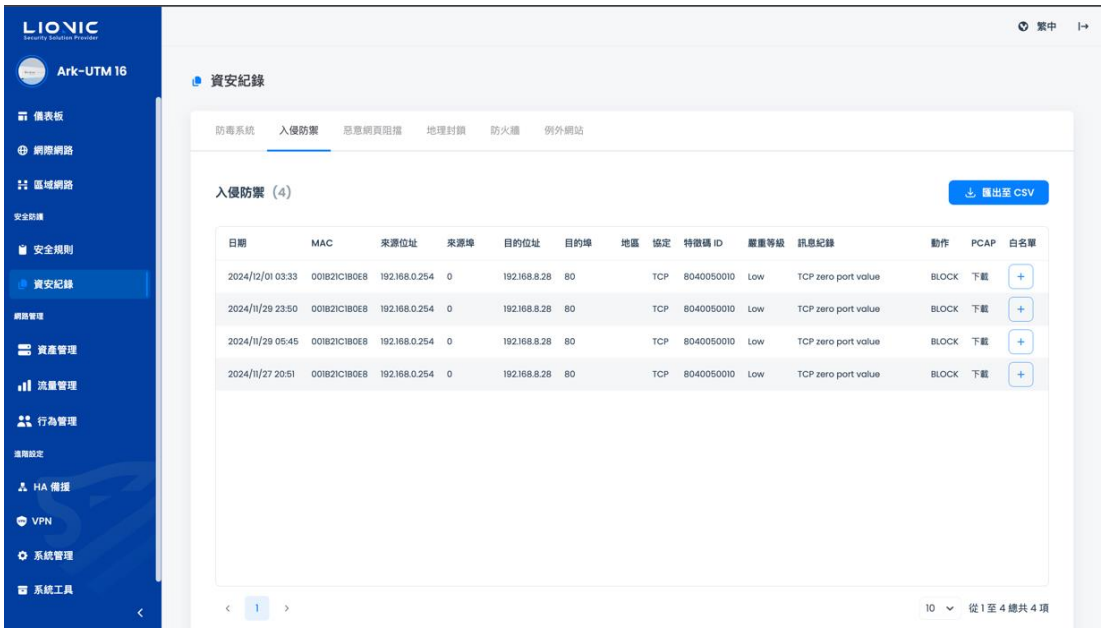
資安紀錄

- **匯出至 CSV**：將紀錄批次匯出成 CSV 檔。
- **白名單**：當 Ark-UTM 16 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。



資安紀錄-威脅百科

- **威脅百科**：在 [入侵防禦] 的資安紀錄中，點擊特徵碼 ID 可以查詢該項攻擊的分析與解決方案。



資安紀錄-PCAP 下載

- **PCAP 封包下載**：當 Ark-UTM 16 被破壞或被阻擋的事件紀錄，點擊 [PCAP] > [下載] 可以將封包下載做進一步分析。

* 備註：需將 [安全規則] > [入侵防禦] > [威脅後保存封包 PCAP] 功能開啟。

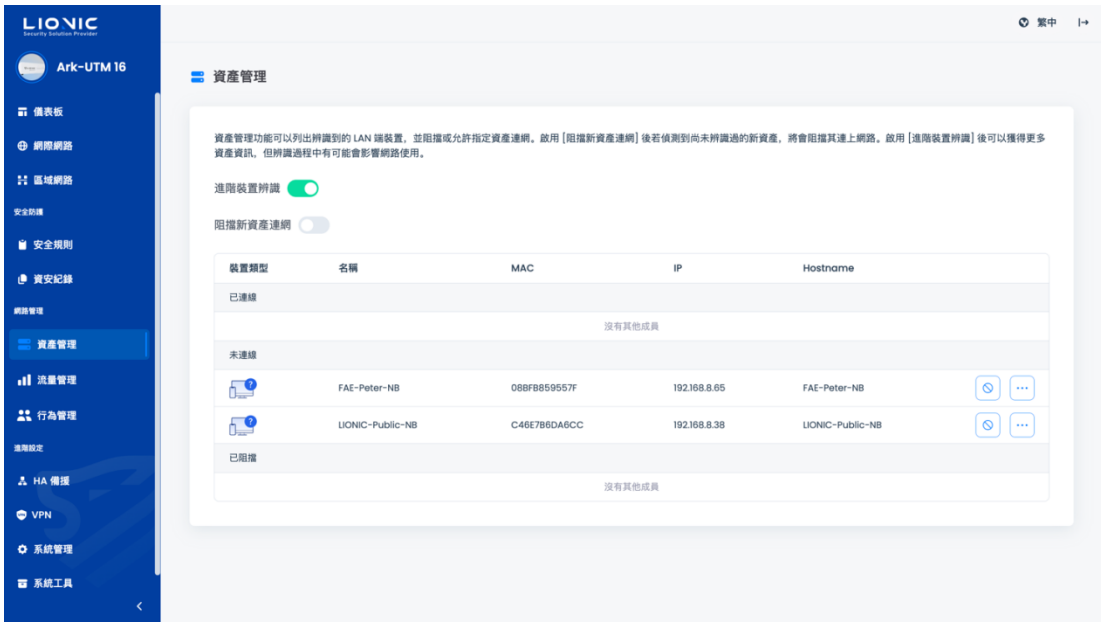
資產管理

資產管理功能可以列出辨識到的 LAN 端裝置，並阻擋或允許指定資產連網。

- **進階裝置辨識**：獲得更多設備資訊。

* 備註：辨識過程中可能會影響網路使用。

- **阻擋新資產連網**：阻擋尚未辨識過的新連線設備。



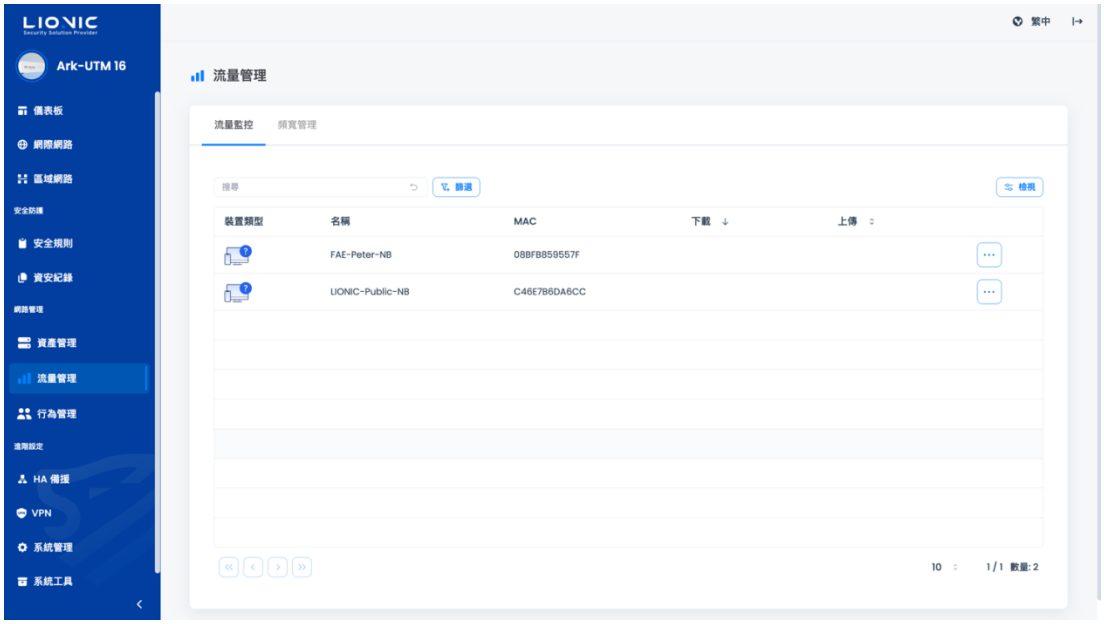
資產管理

流量管理

流量管理能列出各個 LAN 端裝置當前的連線用量並做頻寬管理。

流量監控

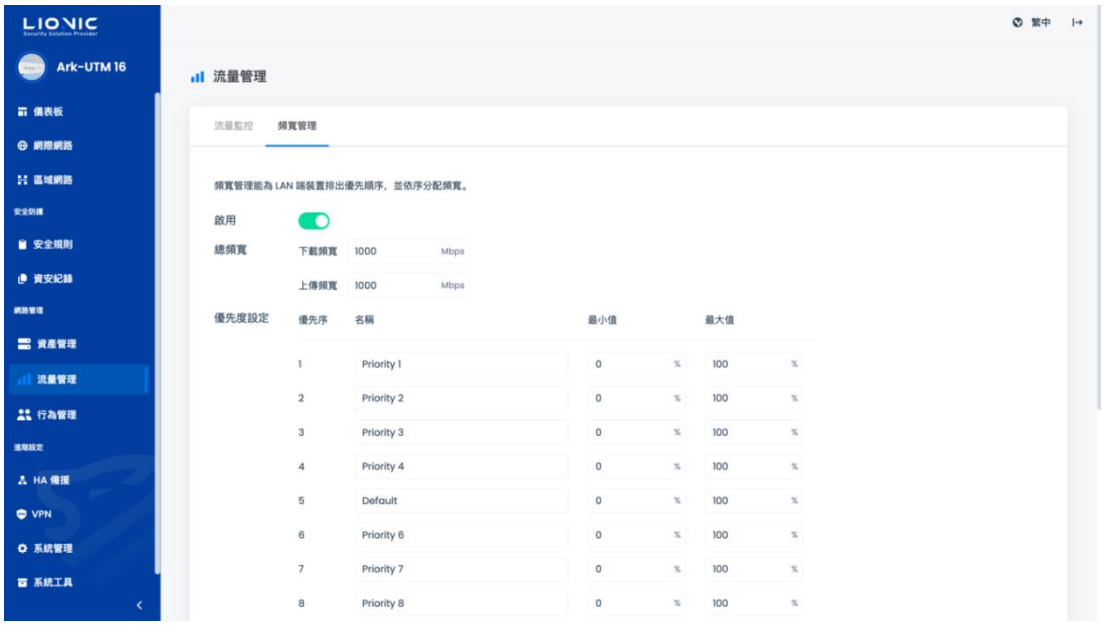
顯示 LAN 端裝置即時的下載與上傳流量，可以依多寡排序顯示。



流量管理-流量監控

頻寬管理

Arc-UTM 能對特定來源 IP、目的 IP 或目的埠進行頻寬管理，讓其流量獲得更高的優先服務。



流量管理-頻寬管理

步驟一：啟用頻寬管理。

步驟二：設定下載/上傳的頻寬。

步驟三：設定優先序、頻寬比例，頻寬管理規則使用。

* 備註：提供八個優先序(priority)，優先程度 1 最高，8 最低，第 5 優先序為預設

步驟四：點擊 [套用] 後開始生效。

頻寬管理-優先度設定

步驟五：點擊 [+新增規則]。

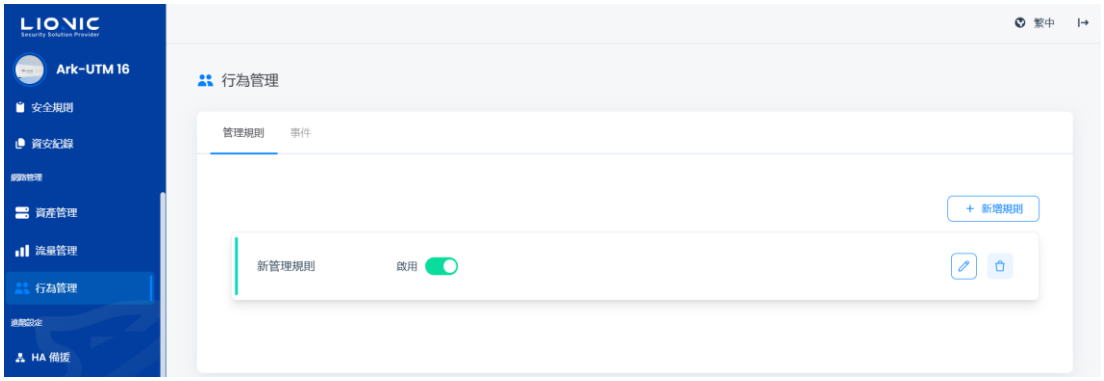
步驟六：填入各項設定值。

步驟七：點擊 [套用] 後開始生效。

頻寬規則-頻寬規則管理

行為管理

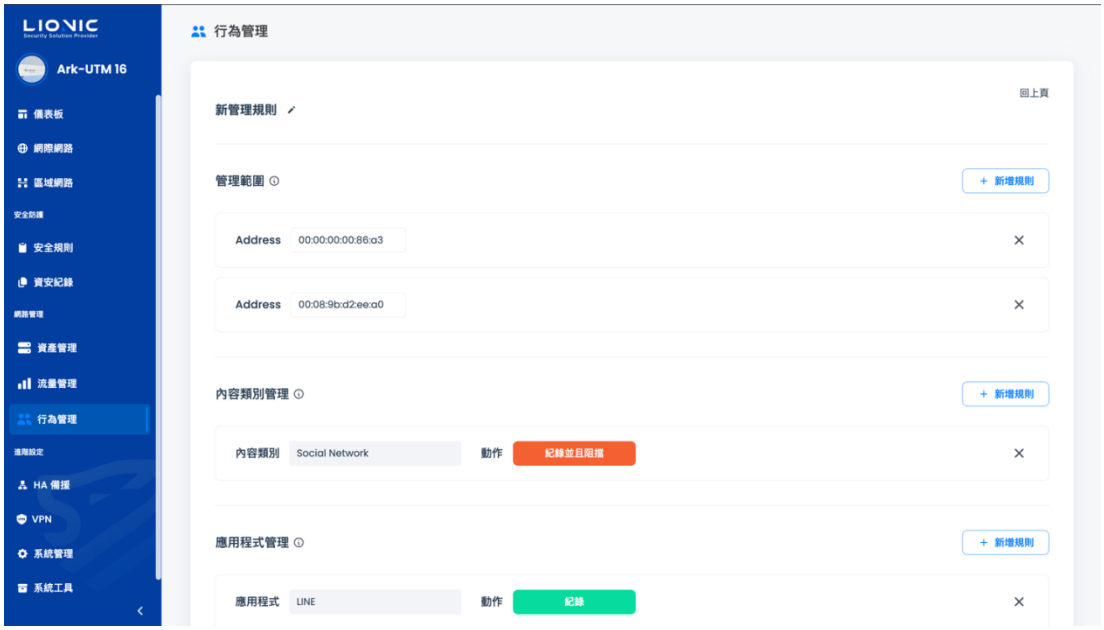
行為管理功能可以對特定內容類別或應用程式做管理，使用者可以根據需求進行設定，以保護家庭成員或員工免受不當內容影響。



行為管理

管理規則

點擊 [+新增規則] 增加新的規則，在管理規則頁面可編輯或刪除規則。



行為管理-管理規則

規則編輯頁面可以增加不同類型的管理：

步驟一：點擊管理範圍 [+新增規則] 設定管理的範圍。

步驟二：填入要管理的 IP 位址或 MAC 位址。

步驟三：選擇要管理的項目點擊 [+新增規則] 設定內容與動作。

步驟四：點擊 [套用] 後開始生效。

步驟五：點擊 [回上頁] 回到管理規則頁面。

規則設定說明：

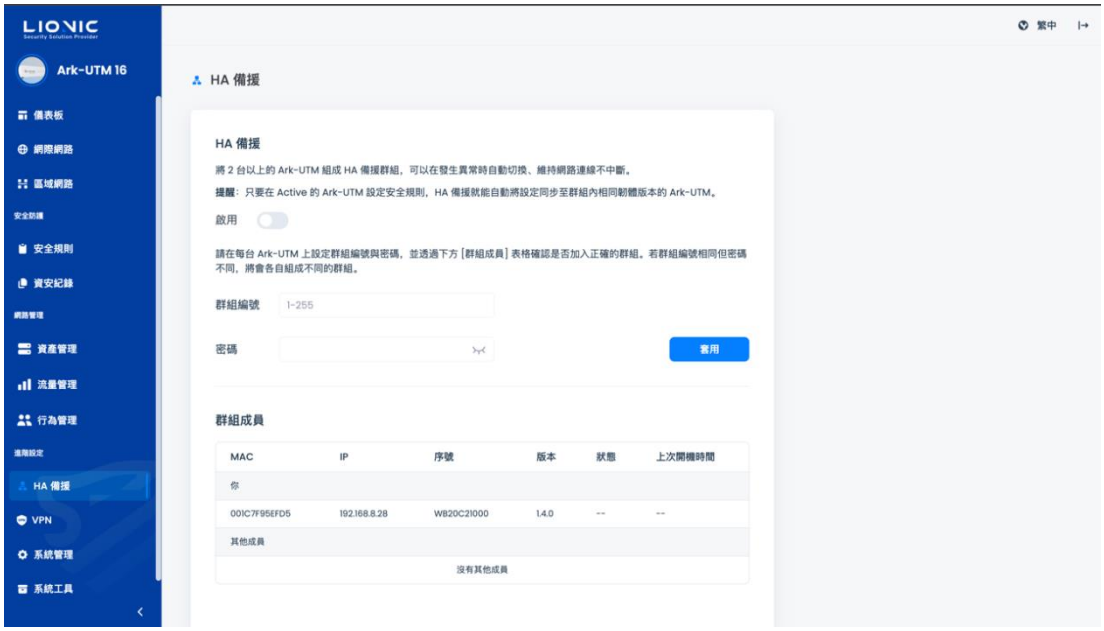
- **管理範圍：**依 IP 位址或 MAC 位址範圍管理。此為必填選項。
- **內容類別管理：**根據網頁內容的類別進行管理。
- **應用程式管理：**根據網路連線所屬的應用程式進行管理。
- **網站黑白名單：**允許或阻擋指定網站的所有連線。

事件

行為管理的偵測結果與動作會顯示在事件頁面中，點擊 [匯出至 CSV] 可以將紀錄匯出成 CSV 檔。

HA 備援

將 2 台或 2 台以上的 Ark-UTM 16 組成 HA 備援群組，可以在發生異常時自動切換、維持網路連線與安全防護不中斷。



HA 備援

- **啟用**：啟用/停用 [HA 備援] 功能，預設為停用。
- **群組編號**：使用者可自定義的 HA 群組編號（1~255）。
- **密碼**：使用者可自定義的群組密碼。

請在每台欲使用 HA 備援功能的 Ark-UTM 16 上設定 [群組編號] 與 [密碼]，並透過設定畫面下方的 [群組成員] 表格確認是否加入正確的群組：若群組編號與密碼皆相同，[群組成員] 表格中可以看到其他 HA 群組成員；若群組編號相同但密碼不同，將會各自組成不同的群組。

設定步驟：

步驟一：完成設定 2 台 Ark-UTM 16 的網際網路 IP 位址，並確保 2 台皆在同一私有網域內。

步驟二：將一條網路線一端插入編號 1 的 Ark-UTM 16 的內網連接埠 (LAN)，另一端插入筆電/桌機的網路連接埠。

步驟三：透過網頁瀏覽器開啟 https://myark.lionic.com/ 連線至網頁控制介面。

步驟四：登入網頁控制介面後到 [HA 備援] 頁面。

步驟五：點擊 [啟用]，並在填入群組編號 (1~255) 及密碼 (自訂) 後點擊 [套用]。

步驟六：完成後，將筆電/桌機透過網路線連接至編號 2 的 Ark-UTM 16 的內網連接埠 (LAN)，並重複步驟三及步驟四。

步驟七：到 [HA 備援] 頁面後點擊 [啟用]，並在填入在編號 1 設定的群組編號及密碼後點擊 [套用]。

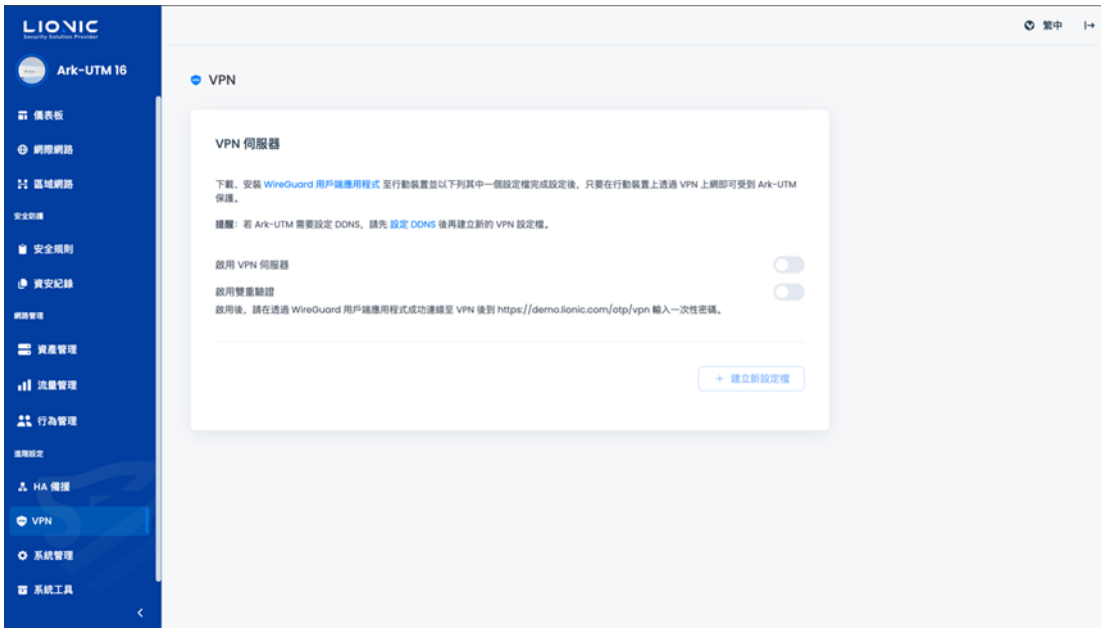
步驟八：完成後，將 2 台 Ark-UTM 16 的內網連接埠 (LAN) 連接至同一台交換器(如圖所示)，即完成 HA 備援功能設定。

HA 拓樸

* 備註：只要在 Active 的 Ark-UTM 16 設定安全規則，[HA 備援] 就能自動將設定同步至群組內相同韌體版本的 Ark-UTM 16、不需逐一設定。

VPN 伺服器

若要延伸 Ark-UTM 16 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 Ark-UTM 16 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：啟用 [VPN 伺服器]。

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 用戶端應用程式以完成設定。

完成設定後，請在需要使用 Ark-UTM 16 的安全防護功能前開啟 WireGuard 用戶端程式並透過 VPN 連線回 Ark-UTM 16。

* 備註：

1. 若您有需要在 Ark-UTM 16 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 Ark-UTM 16 前架設有路由器，請在路由器上設定通訊埠轉發至 Ark-UTM 16 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。

為 VPN 伺服器啟用雙重驗證：

啟用 [雙重驗證] 後，VPN 伺服器使用者在建立 VPN 連線時需要額外輸入一次性密碼才能透過 Ark-UTM 16 存取網路，藉以提升 VPN 伺服器帳號安全性。

前置準備：

1. 下載並安裝 WireGuard 用戶端應用程式至欲使用防護功能的裝置。
2. 下載並安裝 Google Authenticator 等 OTP 應用程式。

設定步驟：

步驟一：啟用 [VPN 伺服器] 及 [雙重驗證]。

步驟二：點擊 [+建立新設定檔]。

步驟三：點擊設定檔中的 [雙重驗證 QR 碼]。

步驟四：以 OTP 應用程式掃描雙重驗證 QR 碼。

步驟五：

- 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 用戶端應用程式以完成設定。

連線步驟：

步驟一：開啟 WireGuard 用戶端程式、透過 VPN 連線至 Ark-UTM 16。

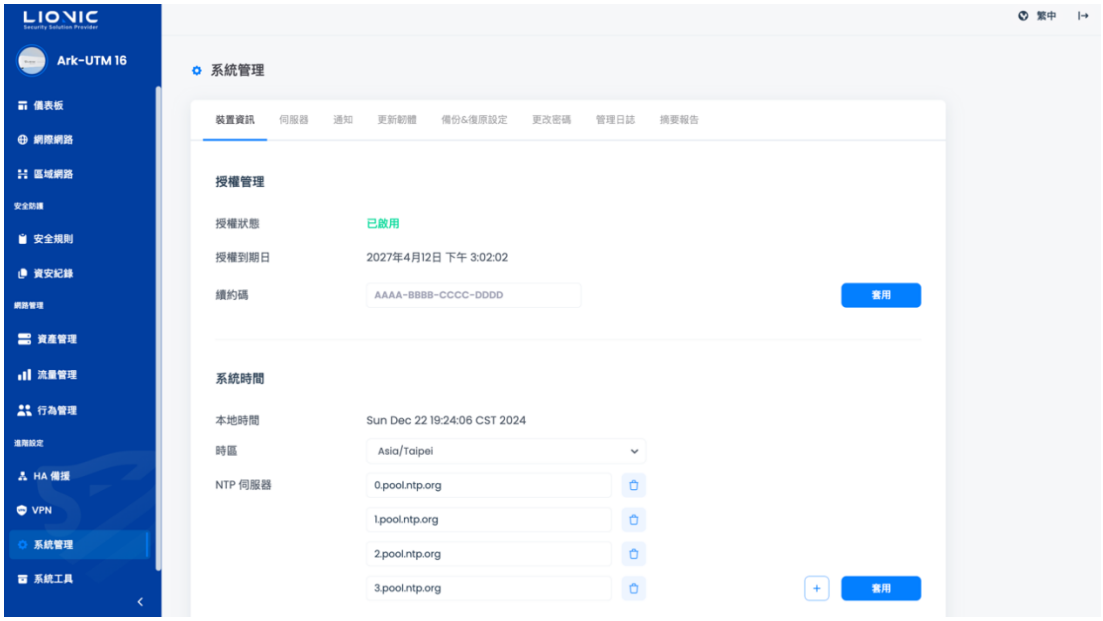
步驟二：開啟 OTP 應用程式以取得一次性密碼。

步驟三：以網頁瀏覽器開啟 https://myark.lionic.com/otp/vpn 並輸入一次性密碼。

完成雙重驗證後，即可以 VPN 連線透過 Ark-UTM 16 存取網路。

系統管理

裝置資訊



系統管理-裝置資訊

授權管理

檢視 Ark-UTM 16 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：**為了能檢測最新的病毒/惡意入侵/釣魚網站/詐騙網站，獲得完整的資安防護功能，請購買授權金鑰，即授權啟用碼（備註 1）。將其輸入到 [啟用碼] 欄位中。在 Ark-UTM 16 連接至網際網路的環境下，點擊 [啟用]以完成啟用。
- **延展授權：**Ark-UTM 16 會在授權到期前 30 天顯示提醒，請儘速完成授權訂閱以取得延展碼（備註 2），將延展碼填入 [續約碼] 並點擊 [套用] 後即可延展授權期限。

* 備註：

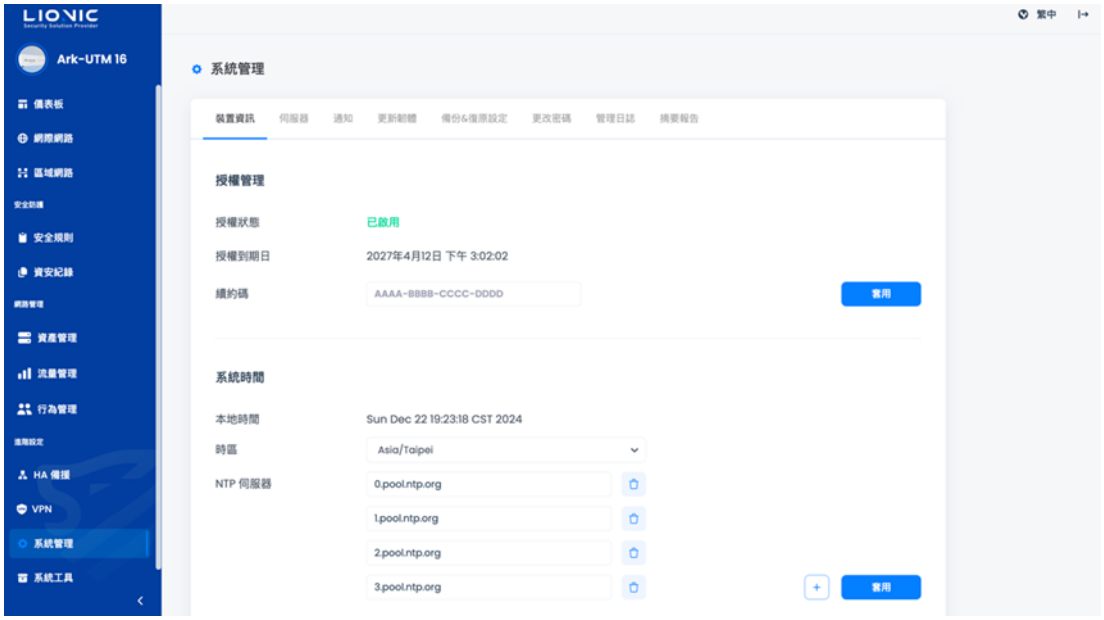
1. 授權啟用碼由 20 位英文與數字組成，成功套用後可以啟用授權。若您沒收到授權啟用碼或啟用碼異常，請聯繫當地經銷商或銷售代表。
2. 授權延展碼由 16 位英文與數字組成，成功套用後可以延展授權期限。若您需要訂閱新的授權以繼續使用 Ark-UTM 16，請聯繫當地經銷商或銷售代表。

系統時間

顯示並設定 Ark-UTM 16 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 Ark-UTM 16。在 CMS 建置完成後將 CMS 位址填入輸入框並點擊 [套用]，Ark-UTM 16 即可與 CMS 連線。如有需求，請聯繫當地經銷商或銷售代表。

- **改由 CMS 伺服器取得韌體或特徵碼更新：**此進階功能是在區域網路無法連線至網際網路時使用。如有相關需求，請聯繫當地經銷商或銷售代表。
- **將由防火牆與例外網站紀錄上傳 CMS：**為提升 CMS 儲存空間使用效率，Ark-UTM 16 設定 CMS 後預設僅上傳防毒系統、入侵防禦、惡意網頁阻擋等三大主要功能的資安紀錄。開啟此功能後，防火牆及例外網站的事件紀錄也會上傳 CMS。

Proxy

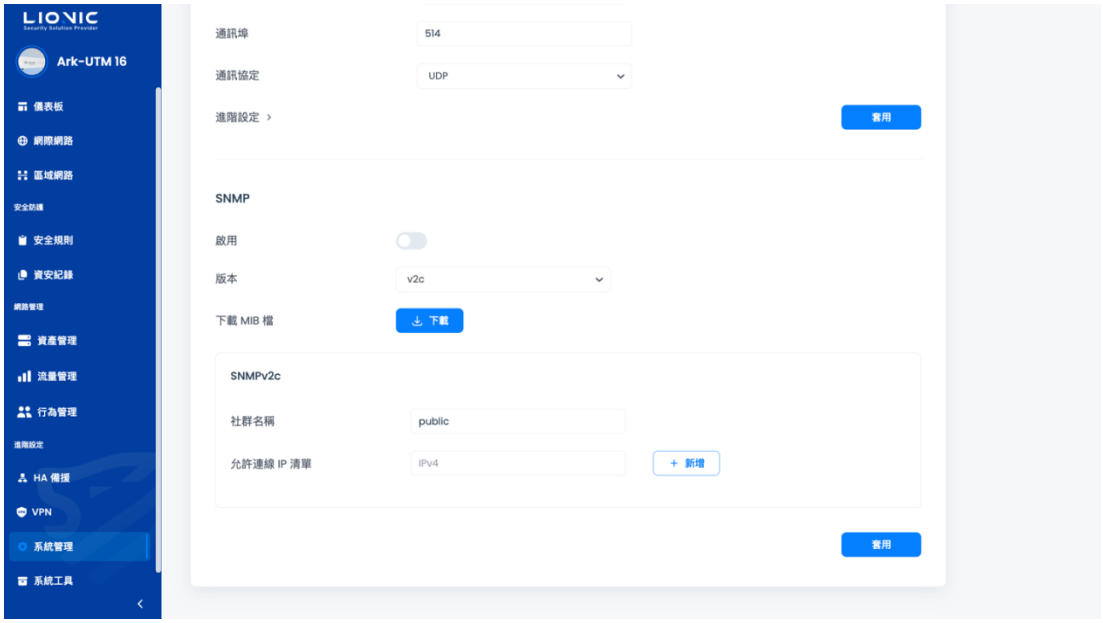
代理伺服器（Proxy）可以協助無法直接連線至網際網路的 Ark-UTM 16 連回 Lionic 的各項雲端服務，以確保 Ark-UTM 16 發揮完整的資安防護功能。當部署 Ark-UTM 16 於內部網路時，可以將 Proxy 位址填入輸入框並點擊 [套用]，Ark-UTM 16 即可透過 Proxy 使用 Lionic 雲端服務。如有需求，請聯繫網路管理員。

Syslog

Syslog 伺服器可以蒐集 Ark-UTM 16 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]。

SNMP

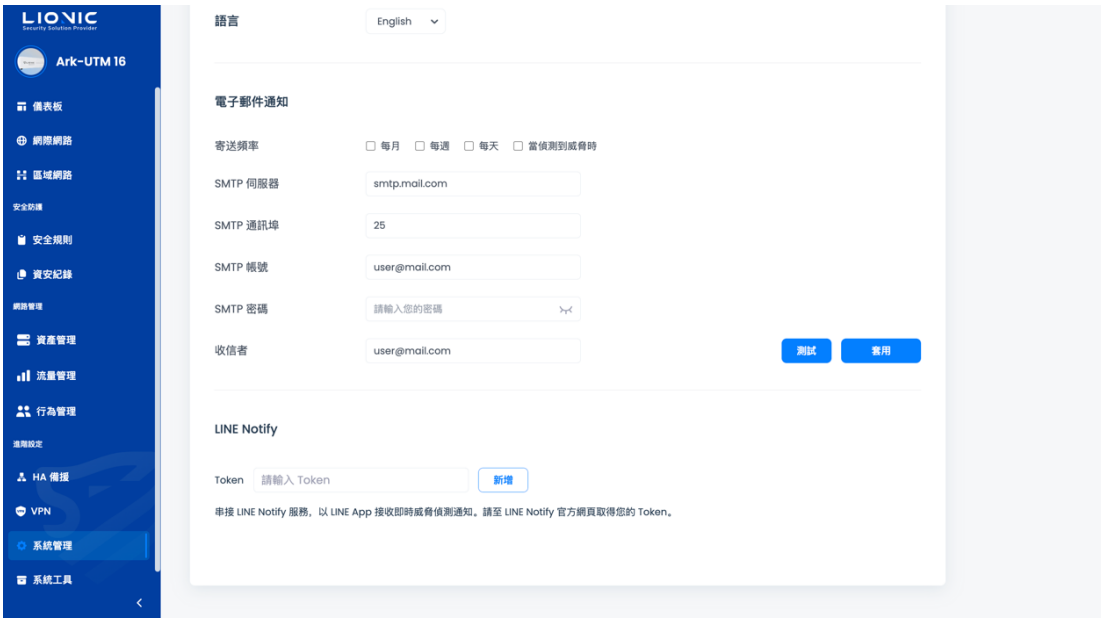
SNMP 可以提供管理者遠端監控 Ark-UTM 16 系統狀態資訊。若您有自行設置 SNMP 伺服器（v2c、v3 版本），請將各項設定值填入輸入框並點擊 [套用]。



伺服器-SNMP

通知

[通知] 功能可以在 Ark-UTM 16 偵測到資安威脅時，將威脅資訊以電子郵件寄到指定信箱，或以 LINE 訊息傳送到指定 LINE 帳號。除此之外，也能定時將檢測歷程、威脅統計、系統異常紀錄等資訊彙整成週報或日報，並寄送到指定信箱。



系統管理-通知

語言

選擇通知信、統計報告及 LINE 訊息內容的語言（中文 / 英文 / 日文）。

電子郵件通知

- **寄送頻率：**
  - 每月：每月 1 日 0:00 寄出月報。
  - 每週：每週日 0:00 寄出週報。
  - 每日：每天 0:00 寄出日報。
  - 當偵測到威脅時：即時寄出威脅資訊。
- **SMTP 伺服器、通訊埠、帳號與密碼：**通知信及統計報告的寄件設定。
- **收信者：**收信者信箱位址。

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 Ark-UTM 16 發出測試信以確認設定是否正確。

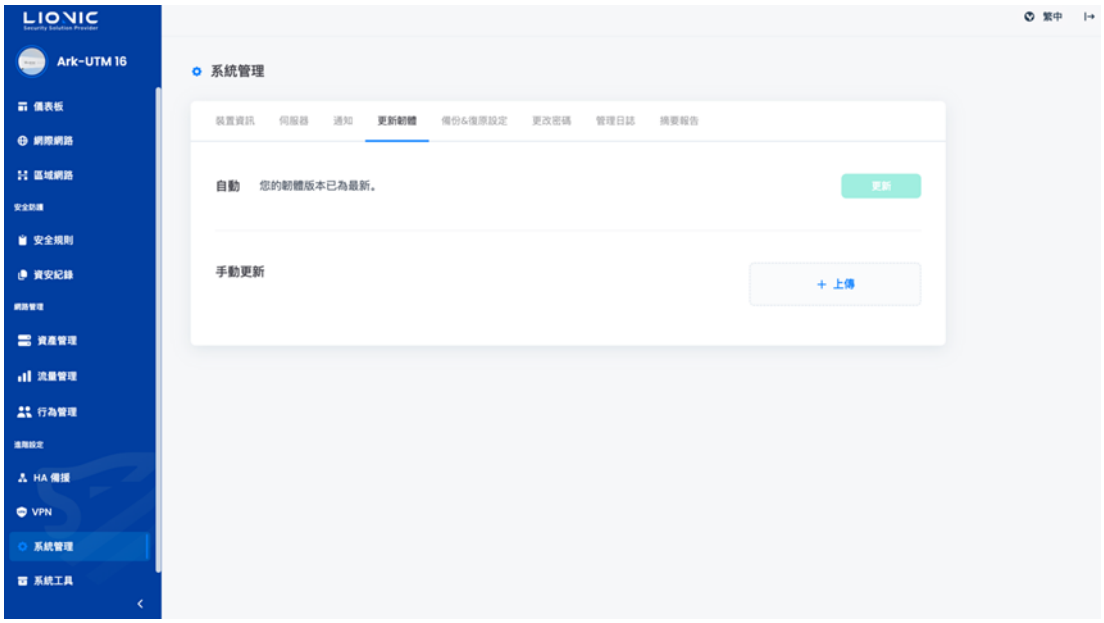
* 備註：若您需要使用 Gmail 作為 Email 通知的發信者，請先啟用 Gmail 的 2-Step Verification，並建立 App Password 填入 [SMTP 密碼] 欄位。

LINE Notify

若要使用 LINE 訊息通知功能，請先依照 LINE Notify 官方網站說明取得 LINE Token，再將 Token 填至輸入框中並點擊 [新增]，就可以用 LINE App 接收即時威脅偵測通知。

更新韌體

[更新韌體] 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。



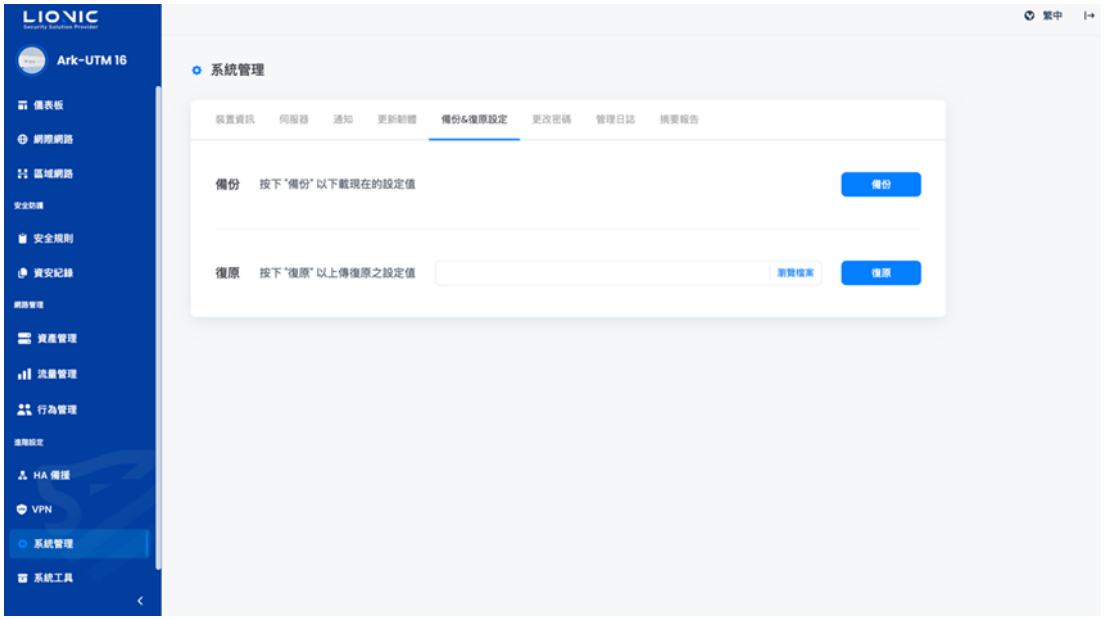
系統管理-更新韌體

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 Ark-UTM 16 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 Ark-UTM 16 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 Ark-UTM 16 上復原，適合在疑難排解或部署少量 Ark-UTM 16 時使用。

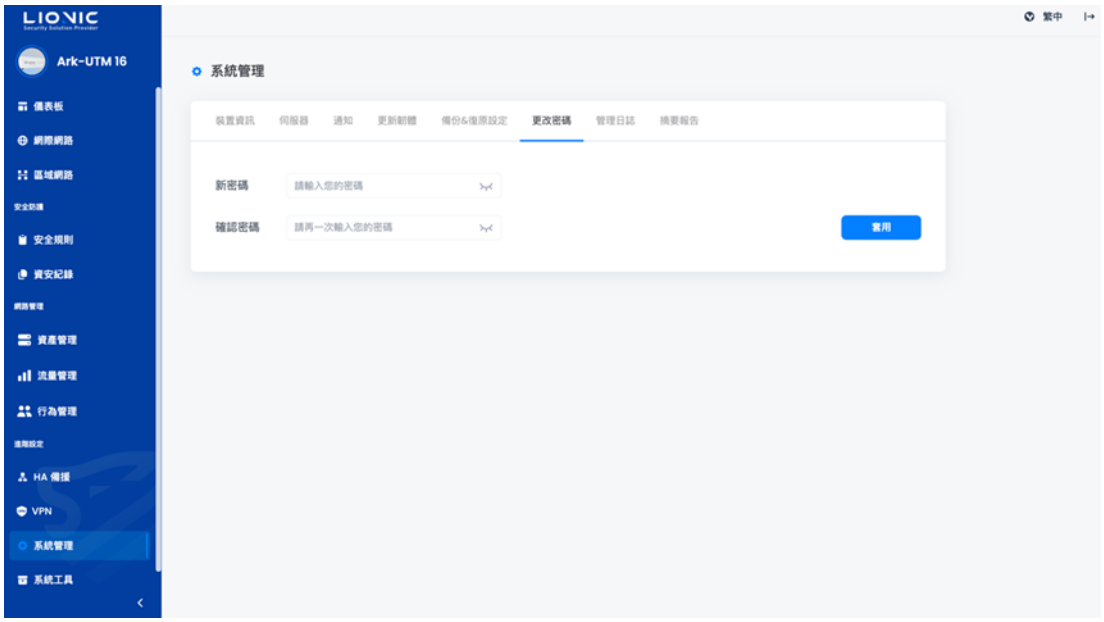


系統管理-備份&復原設定

* 備註：如有部署大量 Ark-UTM 16 的需求，建議使用 CMS。

更改密碼

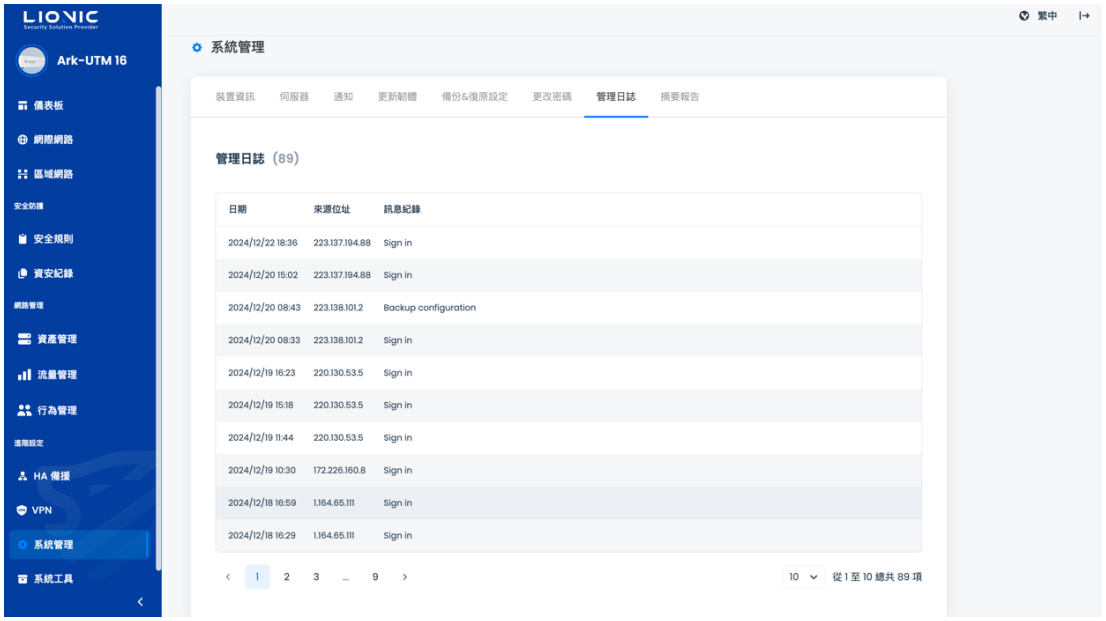
如需變更 Ark-UTM 16 網頁控制介面的登入密碼，請將新密碼填入輸入框後點擊 [套用]。



系統管理-更改密碼

管理日誌

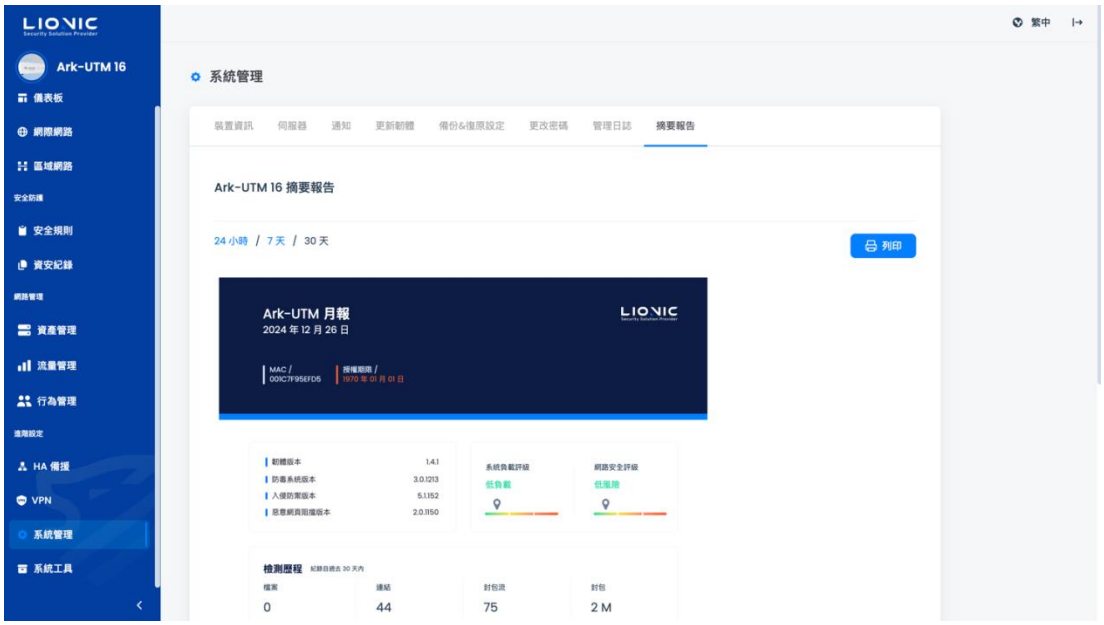
[管理日誌] 頁面會列出 Ark-UTM 管理員在網頁控制介面上所做的各項設定變更。



系統管理-管理日誌

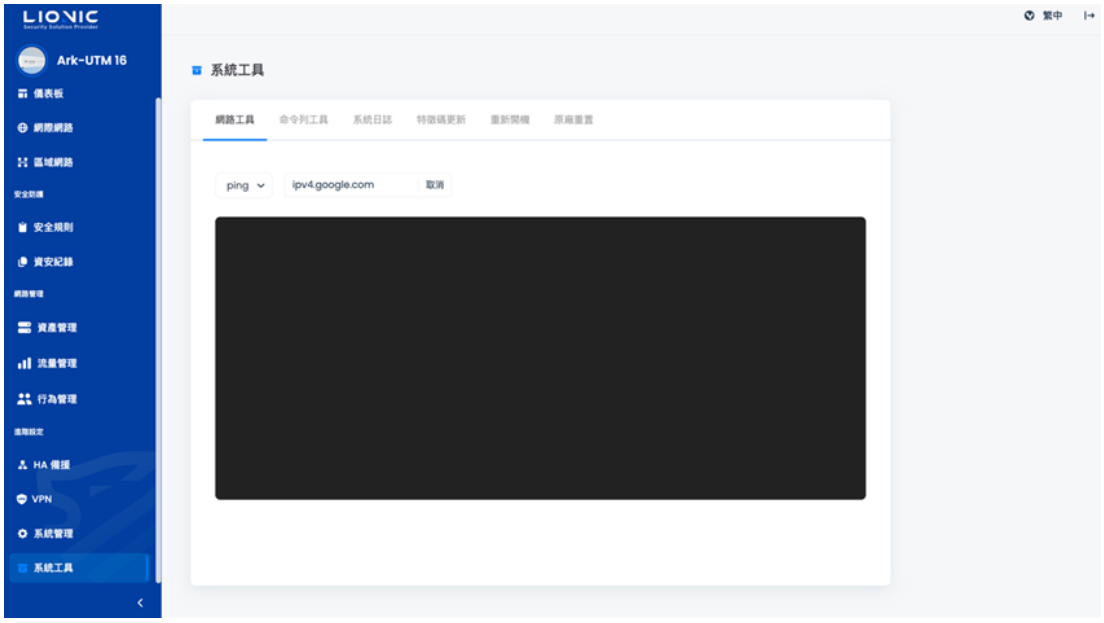
摘要報告

[摘要報告] 頁面會即時生成日報/週報/月報。



系統管理-摘要報告

系統工具



系統工具

Ark-UTM 16 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**：立即重新啟動 Ark-UTM 16 或設定排程重新啟動。
- **原廠重置**：將 Ark-UTM 16 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。

Dual Ark-UTM 16
Makes Security Simple

LIONIC
Security Solution Provider

Sales Contact
Tel : +886-3-5789399
Fax : +886-3-5789595
Email : sales@lionic.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.