

使用者手冊 Dual Ark-UTM 16

版本 1.4.1 更新日期 2025/02





Dual Ark-UTM 16 使用手冊

版權聲明

© 2025 鴻璟科技股份有限公司·版權所有

商標

LIONIC 是鴻環科技的註冊商標。 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

鴻環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 鴻環科技股份有限公司

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	4
功能概述	7
儀表板	9
網際網路	
網路設定	
遠端控制	
區域網路	
連線模式	
LAN	
DHCP	
通訊埠轉發	
靜態路由	
安全規則	
防毒系統、入侵防禦、惡意網頁阻擋	
地理封鎖	
防火牆	22
例外網站	23
SSL/TLS 檢測	24
資安紀錄	
資產管理	
流量管理	29
流量監控	
頻寬管理	
行為管理	
管理規則	32
事件	
HA 備援	
VPN 何服器	



系統管理	
裝置資訊	
伺服器	40
通知	42
更新韌體	44
備份&復原設定	45
更改密碼	46
管理日誌	46
摘要報告	47
系统工具	48
	40



登入網頁控制介面

- 1. 將電源線插上 Ark-UTM 16。
- 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 <u>https://10.254.254.254/</u>

	Welcome to Ark-UTM 16
Ark-UTM 16 Secure your network against Virus, Intrusions, and Web threats.	登入 講論入認好的碼 Password 六
版本13.0	

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。



LIONIC			
Ark-UTM 16	⊕ 網際網路		
司 俱表板	網路如空 這是拉到		
• 網際網路	Manager Annual Content		
計 医埃姆路	IPv4		
安全防御		-	
■ 安全規則	連線類型	L	靜態位址 个
· 資安紀錄	IP 位址		自動取得
網路管理			靜態位址
11 资本管理	T male w		PPPOE
	預設開進	1	192.168.0.254
11 流量管理	DNS(可强)	8	8.8.8.8
▲ 行為管理			
推用設定			
A HA 開握	IPv6		
O VPN			
◆ 系統管理	連線類型		自動取得 >
雷 系统工具	DNS(可選)	•	e.g. 2001:4860:4860::8888
<			

網際網路-網路設定

- 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 <u>https://myark.lionic.com/</u> 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 <u>https://10.254.254.254/</u> 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 <u>https://myark.lionic.com/</u> 連線至網頁控制介面。



🥏 Ark-UTM 16	⊕ 網際網路			
a 4886	10100 10 PP 10100 1796			
o mania	WHERE AN ADDRESS OF			
H 重地網路	動態 DNS 服務	藉由動態 DNS 服務所提供的主機名和	育從遠端存取 Ark-UTM。	
9:20M		啟用 🕕		
■ 安全規則	服務供應商	No-IP (www.no-ip.com)	~	
. 漢安紀錄	主機名稱			
	使用者名稱	demo		
= x4¥4	市場		м	8月
山流動管理				
				
11.711.22	存取控制清單	如需以外部網域裝置連線至此網貨控 單(ACL)。	制介面,請將其 IP 位址新增至存取控制清	
A HA WE		啟用 💽		+ 新雄
O VPN				
◎ 系統管理				客用
晋 系统工具				
	内会道线	使用 HTTPS 連結在取線置控制介面	以保護登入家總諾重要國私遵訊	

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。

LIONIC Security Solution Provider				♥ 繁中
	檢測歷程 自上次開機後已檢測			
■ 儀表板		0		574
⊕ 網際網路		⑦ U 修連結	·•• U 條时包流	ち/К 個时包
計 医域網路				
安全防護	安全防護		資安威脅排行	所有 🗸
■ 安全規則				
資安紀錄	防毒系統	状態 ●	特徵碼 ID 類型 數量 訊息紀錄	
網路管理	0 個威脅已被偵測	BUTF MESOR	8040050010 Intrusion 4 TCP zero port value	
2013 資産管理	入侵防禦			
山 流量管理	■ 4 個威脅已被偵測	状態 ● 動作 阻擋		
上 、行為管理				
進期設定	恶意網頁阻擋	↓ 狀態 ●		
▲ HA 備援	- 0 個威脅已被偵測	動作阻擋		
VPN				
◆ 系統管理	地理封鎖			
吉 系統工具	●	狀態 🛑		

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。



LIONIC	0 (E.R.)	身已被侦测 狀態 💶		
Ark-UTM 16				
4 86	流量監控	展在 按日 按道	裝置資訊	
網際網路		網路傳輸速度	7	
医试明路	3415 Kbps	2	MAC (00)C75955505	
2.	273.2 Htps	2024年12月22日 18:39:04 ● 下載: 16.5 Kbps	授權到期日/狀態確認失敗	
安全規則	204.9 Kbps	• 上傳: 129.8 Kbps	立 看细節 >	
費安紀錄	68.3 Köps			
a	38.16 38.23	38.31 38.38 38.46 38.53 39.01 39.08 39.16	系統時間	2024年12月22日 18:39:16
242		 下載 上得 	. A STRUCTURE OF STRUCTURE OF ST	
流量管理		網路傳輸量	2個間	儲存空間 26%
行為管理	85.4 KB 68.3 KB		0 "*	20%
z	51.2 KB		CPU 使用事	
A 備護	341 KB	- monologia	100% 80%	
PN	17.3 KB		60% 40% 20%	
S.R.WIE	3816 3823	3831 3838 3846 3853 3901 3908 3936 • 下戦 • 上傳	0% 38.22 38.31 38.38	38.46 38.53 39.01 39.08 39.16
系统工具				

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。

			⑦ 繁中 →
Ark-UTM 16	朝際網路		
雷 備表板	網路設定 遠端控制		
+ HINTARIA			
計 医域網路	IPv4		
安全防御			
当 安全規則	連線類型	靜態位址	
資安紀錄	IP 位址	自動取得	
網路管理	子網路遠罩	PPPoE	
資產管理			
1 流量管理	預設開道	192.168.0.254	
11 行為管理	DNS(可選)	8.8.8.8	
建築的方			
	IPv6		
VPN	連線類型	自動取得 🗸	
✿ 系統管理	DME(고38)	a a 2001-4980-4980-9989	
■ 系統工具	אניי)ראט	e.g. 2001/4850/4850/2888	
K			

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。

					¢
Ark-UTM 16	◎ 網際網路				
= (48.6	(0.35.30.27) 读读中型				
	動態 DNS 服務	藉由動態 DNS 服務所提供的主機名和	再從遠端存取 Ark-UTM。		
925 8		啟用 🔵			
會 安全規則	服務供應商	No-IP (www.no-ip.com)	~		
資支記錄	主棚名稱				
ACI6 1978	使用者名稱	demo			
-	密碼		×	2.0	
al ARYS					
11 0asa					
8882	存取控制清單	如需以外部網域裝置連線至此網頁控 單(ACL)。	制介面,請將其 IP 位址新增至存取控制清		
		啟用 🌔		+ 1518	
O VPN					
о жини				意用	
曹 系统工具					
¢	安全連線	使用 HTTPS 連續存取網貨控制介面。	以保護登入密碼等重要随私資訊。		

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。
- 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。

ARKE	安全連線	使用 HTTPS 連線存取網頁控制介張,以保護登入密碼等重要題私資訊。
▲ HA 個援		僅使用安全連線
• VPN		說用後,所有的 HTTP 連續皆會被重新導向至 HTTPS 連續。在存取控制清單停 用後,此道項將強制說用。
○ 系統管理		
च 系统工具		
<		

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。

		© 繁:
Ark-UTM 16	∺ 區域網路	
冨 儀表板		
⊕ 網際網路	連線模式 LAN DHCP 通訊埠轉發 靜態路由	
- 區域網路		
全防護		
安全規則	通線模式	
資安紀錄	AED INFO TOKE YOU	
格管理		
8 資產管理	橋接模式路由器模式	
流量管理	當網路服務供應商提供帶有路由 功能的數據機或路由器 當網路服務供應商僅提供數據機	
行為管理		
設定		
HA 備援	老用	
VPN		
系統管理		
1 系統工具		
<		

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。

		● 繁中 →
Ark-UTM 16	∺ 區域網路	
■ 儀表板	連線模式 LAN DHCP 通訊埠轉發 靜態路由	
⊕ 網際網路		
□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	區域網路 IP 設定	
安全防護	IP 位址 10.254.254.254	
■ 安全規則	子網路遊園 255.255.255.0/24	~
資安記錄	進階設定 ~	
和新台理	無 NAT 路由 LAN 位址設定	
📑 資産管理	敞用	
▲■ 流量管理	IP 位址 192.168.1.2	
土 行為管理	子網路這罩 255.255.255.0/24	~
進階設定	□ 在無 NAT 路由網域使用 DHCP	
<		套用

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							
Ark-UTM 16	連線模式 LAN DHCP 通訊時轉發 靜態路由							
■ 儀表板								
⊕ 網際網路	DHCP 伺服器設定							
計 區域網路	啟用 💽							
安全防護	起始 IP 位址 10	坡 IP 位址 10.254.254.1						
	結束 IP 位址 10	IP 位址 10.254.254.253						
■ 貝女記録 網路管理								
↓】 流量管理	靜態保留位址					+ 新增規則		
▲ 【 行為管理	MAC		IP 位址		描述(可理)			
進階設定			11 127-217)田に(つだ)			
<						套用		

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。

						♥ 繁中	∣→
Ark-UTM 16	器 區域網路						
■ 儀表板	連線模式 LAN	DHCP 通訊埠轉發	靜態路由				
⊕ 網際網路							
器 區域網路	通訊埠轉發 +						
安全防護							
≌ 安全規則	外部通訊埠	内部通訊埠	內部 IP 位址	協定	描述(可選)		
資安紀錄							
網路管理	8080	16888	192.168.20.100	TCP 🗸		Ů	
📑 資産管理						套用	
-■■ 流量管理							
♣< </th <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>							

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。

LIONIC Security Solution Provider				♥ 繁中 →
Ark-UTM 16	∺ 區域網路			
■ 儀表板	連線模式 LAN DHCP	通訊埠轉發 靜態路由		
⊕ 網際網路				
品域網路	靜態路由設定檢視路由表			+ 新增規則
安全防護				
當 安全規則	目標網路位址	網路遮罩	閘道器	介面
資安紀錄	192 168 0 0	255 255 255 0	192168.0.254	
網路管理		200120012000		
📑 資産管理				套用
□□□流量管理				
土 行為管理				

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	防毒系統 入侵防禦			
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	
計 儀表板 ⊕ 網際網路	防毒系統 入侵防禦 惡意綱頁阻擋 地理封鎖 防火牆 例外網站 SSL / TLS 检测	
計 医域網路	-#9	
_{安全防護} 安全規則	設用	
資安紀錄	動作	紀録並且破壞 🖌
·····································	進階段定	
•Ⅰ】流量管理	使用雲流病毒資料庫得描檔案 應未通識	
▲ 行為管理 並用設定	3、17日本地が中華メイヤ市市市市市市市市市市市市市市市市大工3日21日本工工工工工工工工工工工工工工工工工工工工工工工工工工工工工工工工工工工	
▲ HA 備援	使用 AI 人工智慧 侦测新病毒 使用人工智慧引擎分析维索特徵、以值测图图绘数纬的全新的病毒。	
● VPN	邏輯 :使用此功能前須先設用雲端病毒資料庫,並請確保您的授權有效且能達總至網際網路。	
■ 系統工具	白名單	
<		

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 協定短時間爆増連線的 DoS 攻撃。



- 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。

LIONIC					◎繁中 →
Ark-UTM 16	進階設定				
罰 儀表板	体田 ai i 丁和韩依阳新新公司帝	AND ALL			
⊕ 網際網路	使用 AI 人工 督愿俱洞 劉悲的 总思				
計 医域網路	使用入上智慧引擎分析剧或名稱,以	資源利用動態劑ជ建線的意意的頁。			
安全訪議	外部資料庫				
安全規則	3de got min 480 à.L				
資安記錄	到此不计算机的以上	URL			
網路管理	HTTP 基本認證				
要 資產管理		使用者名稱			
山 流量管理		密碼	74		
土、 行為管理	更新頻率	1 小時	~	套用	
-					
よ HA 備援	最後更新於	2024年12月22日下午 6:44:0	03	立即更新	
O VPN	資料筆數	0			
◆ 系統管理	匯出當前資料庫	匯出			
■ 系統工具 <					

- 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。

惡意網頁阻擋-進階設定



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。

		◎繁中 →
Ark-UTM 16	■ 安全規則	
■ 儀表板	訪毒系統 入侵訪課 惡意峭頁阻擋 地理封鎖 防火牆 例外網站 SSL / TLS 檢測	
⊕ 網際網路		
∺ 區域網路	一般	
安全防護	地理封鎖功能能阻握來自或前往指定地區的連線,可以攔阻來自該地區的攻擊或防止資訊外強至該地區,此站點或產品所使用的 iP2Location	
■ 安全規則	utre 数据来自於 https://ite.jp2location.com。	
資安記錄	84/11	
網路管理	選擇您要阻擋的地區 🕢	
📑 資產管理	現攏來自以下地區的傳入達線:	
ⅠⅠ 流量管理	尚未設定	
1. 行為管理		
進階設定	照擋前往以下地區的傳出連續:	
▲ HA 備援	尚未設定	
C VPN	白名單	
◆ 系統管理	將受信任的 9° 位址加入白名瞿,即可不受地理封旗功能阻摧。	
■ 系統工具 く	IPv4 惑 IPv6 + 新聞	

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。

LIONIC Security Solution Provider		◎ 繁中 Ⅰ
Ark-UTM 16	■ 安全規則	
■ 備表板	訪毒系統 入侵防禦 思意原頁阻擋 地理封鎖 防火牆 例外網站 SSL/TLS 检测	
⊕ 網際網路		
計 區域網路	00 E	+ 951948.001
安全防護		
■ 安全規則		
資安紀錄	名稱 飲用 紀錄 協定 來源位址 來源埠 目的位址	×
網路管理	New Rule C ANY ~ 192.168.2.0/24 80,8888,24 ANY	
	目的埠 動作 排程 毎週 從 到	
■:資產管理	ANY 允许 V 日 - 二 三 四 五 六 00:00 V 24:00 V	
11 流量管理		
土、 行為管理		套用
進階設定		
よ HA 備援		
S VPN		
ウ 系統管理		
□ 永統工具		

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。

LIONIC	◎ 繁中 +
Ark-UTM 16	■ 安全規則
司 儀表板	訪進系統 入侵防禦 原實網面回機 始證封領 防火牆 研修網紙 SSI/TIS 持測
⊕ 網際網路	minanina zvolanim nanomizanom montorim mizzona zizziena oko ji vo slani
∺ 區域網路	
安全防護	沈許的
■ 安全規則	
資安記錄	
網路管理	
🚍 資產管理	
11 流量管理	
上 行為管理	
進開設定	
▲ HA 備援	
• VPN	
◆ 系統管理	
百 系統工具	
<	

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。

23



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。

LIONIC Security Solution Provider	■ 安全規則		
	防毒系统 入侵防禦	愿意納買阻擋 地理封鎖 防火牆 勞外網站 SSL/TLS 檢測	
罰 儀表板			
⊕ 網際網路	SSL / TLS 檢測		
計 區域網路	啟用 SSL / TLS 檢測功能 提醒: 啟用 SSL / TLS 檢	以在瀏覽 HTTPS 網站時保護您的裝置。 觀將會影響網路這度,並有可能造成部分應用程式無法正常使用。	
安全於國	啟用		
■ 安全規則		440	
資安記錄	HTTPS 建按苹	443	番用
網路管理	白夕田		
〓 資產管理	口石里		
山族量管理	網站類別	網站位址	
北 行為管理	Finance and Insure	ince	
10122	Health and Medicin	ne	
≛ HA 備援		/ /	
O VPN			
◆ 系統管理	憑證		
च 系统工具	下載憑證	下載預設憑證並匯入至您的瀏覽器,以讓您的裝置信任來自 Ark-UTM 的 HTTPS 連 線。	<u>ط</u> ۳
<	匯入憑證	匯入 CA 憑證與公鑰以提升連線相容性。	+ Ξλ

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。

														♥ 繁中
Ark-UTM 16	資安紀錄													
■ 儀表板	防毒系統 入侵	RAW STR	面田地 他	研究社会部	防火調 砌	05.4回10次								
⊕ 網際網路	10000000 700	CHAINE ADVIDANT	Actual 10	-2.+7 KA	H17508 03	1 102-04								
∺ 區域網路	入侵防禦(4)												と 魔出	≝ csv
安全防護														
■ 安全規則	日期	MAC	來源位址	來源埠	目的位址	目的埠	地區	協定	特徵碼 ID	嚴重等級	訊息紀錄	動作	PCAP	白名單
2 資安紀錄	2024/12/01 03:33	001B21C1B0E8	192.168.0.254	0	192.168.8.28	80		TCP	8040050010	Low	TCP zero port value	BLOCK	下載	+
网络管理	2024/11/29 23:50	001B21C1B0E8	192.168.0.254	0	192.168.8.28	80		TCP	8040050010	Low	TCP zero port value	BLOCK	下載	+
🚍 資產管理	2024/11/29 05:4	5 001B21C1B0E8	192.168.0.254	0	192.168.8.28	80		TCP	8040050010	Low	TCP zero port value	BLOCK	下載	+
11 流量管理	2024/11/27 20:51	001821C180E8	192.168.0.254	0	192.168.8.28	80		TCP	8040050010	Low	TCP zero port value	BLOCK	下載	+
11 行為管理														
1月初史														
▲ HA 備援														
• VPN														
◆ 系統管理														
च 系统工具														
<	< 1 >											10 🗸	從1至4	總共4項

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。



Steventy Statutese Provider Threat Encyclopedia							
Webshell.PHP.Hydra Inbound Connection							
	Summary						
	Signature ID	8011276100					
	Rule Category	Malware-activity					
	Severity	Medium					
	Created Date	2020-03-20					
	Update Date	2020-03-20					
	Details						
	Affected Products	Any unprotected system is at risk of being compromised.					
	Affected OS	Windows , Linux , MacOS , IOS , Android , Other					
	Description	This event is used to identify traffic associated with trojan activity, which may include commands and requests for files or other stages compromised the system, potentially leading to damage or a data breach.					

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。

														0 1
Ark-UTM 16	資安紀錄													
表板	PERSONAL AND	1410 5 1940 55	713 409 iki 13	11-14W P	e.1.40 001	6.600.0.2								
原網路		// # 10.10.10 pt	PETRE ACTI	EEDRA R	0.×181 1912	ragad								
[網路	入侵防禦(4)												1 1 1 1 1 1	至 CSV
													19-04-20	terre superior of
規則	日期	MAC 3	來源位址	來源埠	目的位址	目的埠	地區	協定	特徵碼 ID	嚴重等級	訊息紀錄	動作	PCAP	白名單
紀錄	2024/12/01 03:33	001B21C1B0E8 1	92.168.0.254	0	192.168.8.28	80		TCP	8040050010	Low	TCP zero port value	BLOCK	下載	+
	2024/11/29 23:50	001821C180E8 1	92.168.0.254	0	192.168.8.28	80		TCP	8040050010	Low	TCP zero port value	BLOCK	下載	+
L管理	2024/11/29 05:45	001821C180E8 1	92.168.0.254	0	192.168.8.28	80		TCP	8040050010	Low	TCP zero port value	BLOCK	下載	+
191	2024/11/27 20:51	001B21C1B0E8 11	92.168.0.254	0	192.168.8.28	80		TCP	8040050010	Low	TCP zero port value	BLOCK	下載	+
9管理														
NIN														
管理														
兵工 兵														

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。

						◎ 第5
	■ 資產管理					
計 備表板 の、細胞細致	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。啟用 [阻擋新資產連	綱] 後若偵測到尚未辨識過的新i	資產,將會阻擋其連上網路。啟用[進閃	皆裝置辨識] 後可以獲得更多
計 區域網路	資產資訊, 但辦機過程中有可能會影響網路使用。 進階級置辦機 ()					
^{全防護} ■ 安全規則	阻擋新資產連網					
● 資安紀錄	裝置類型	名稱	MAC	IP	Hostname	
2 資產管理	未連線		没有	其他成員		
流量管理 • 行為管理	.	FAE-Peter-NB	088FB859557F	192.168.8.65	FAE-Peter-NB	…
▲ 1) ##1187年 1892年	已阻擋	LIONIC-Public-NB	C46E7B6DA6CC	192.168.8.38	LIONIC-Public-NB	(o) []
▲ HA 備援 ● VPN			没有:	其他成員		
✿ 系統管理						
■ 系統工具 く						

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。

							♥ 繁中 Ⅰ
e Ark-UTM 16	11 流	這管理					
副 債表板	流	量監控 须宽管理					
⊕ 網際網路							
計 医球網路	1	搜尋	5 C	. 183 3E			等 檢視
安全防護		裝置類型	名稱	MAC	下載↓	上傳 ○	
曾 安全規則		1	FAE-Peter-NB	08BFB859557F			
資安記錄		1	LIONIC-Public-NB	C46E7B6DA6CC			
■ 資產管理							
11 流量管理							
▲行為管理	-						
進用設定							
○ 系統管理							
實 系統工具	. (1	0 ○ 1/1 數量:2

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。

Sincurity Selution Provider	
Ark-UTM 16 II 流量管理	
置域現然 頻寬管理能為 LAN 編装置指出優先順序,並依序分配頻寬。	
2.1	
安全規制 總頻寬 下截頻寬 1000 Mbps	
資安記錄 上海規範 1000 Mbps	
理 優先度說定 優先序 名稱 最小值 最大值	
R盘管理	
PN Uerout U % (00 %	
7 Priority 7 0 % 100 %	

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。

1Priority 12Priority 23Priority 3	20	%	60	%
2 Priority 2 3 Priority 3	0	%	100	
3 Priority 3				%
	0	%	100	%
4 Priority 4	0	%	100	%
5 Default	80	%	100	%
6 Priority 6	0	%	100	%
7 Priority 7	0	%	100	%
8 Priority 8	0	%	100	%

頻寬管理-優先度設定

流量管理-頻寬管理



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。

名稱	啟用	優先序	來源位址	目的位址	目的埠	3
Qos 01		1 0	192.168.8.34	ANY	ANY	
名稱	啟用	優先序	來源位址	目的位址	目的埠	C

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。

LIONIC Security Solution Provider		② 繁中 →
ark-UTM 16	業 行為管理	
■ 安全規則		
資安紀錄	管理規則 事件	
STATE:		
📑 資產管理		+ 新增規則
↓ 流量管理	新管理規則	
土 行為管理		
進開設定		
🙏 HA 備援		

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	
e Ark-UTM 16		同上百
罰 備表板	新管理規則 /	ELR
⊕ 網際網路		
計 區域網路 安全防護		
当 安全規則	Address 00.00.00.86.a3	×
資安記錄	Address 0008-9hd2eea0	×
明語管理 		<u>^</u>
11 流量管理	山奈縣の総理()	
🙏 行為管理	1380/J#*2 V	1 101/00/03
20182	內容類別 Social Network 動作 紀錄並且開始	×
L HA 備援		
 ♥ FN ♥ 系統管理 	應用程式管理 ①	+ 新増規則
吉 系統工具		
	IB/HJ程24, LINE III/F IC/F	×

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。

💿 Ark-UTM 16	📩 HA 備援						
冨 備表板 ⊕ 網際網路	HA 備援 蔣2台以上的 Ark-UTN	▲ 組成 HA 備援群組。	可以在發生異常時自動地	刀換、維持網路	連線不中斷。		
計 医域網路 安全問題	提醒:只要在 Active 部 啟用	TT - LIYAL-BIOK VIIIA 開放 ID 國旗的程度,可以以至其正相用的目期的以及、國目的國旗通過國「TT III。 建羅: 只要在 Active 的 Ark-UTM 設定安全規則, HA 傳道就能自動將設定同步至詳絕內相同動體版本的 Ark-UTM。 說用					
■ 安全規則● 資安記録	請在每台 Ark-UTM 上書 不同,將會各自組成不	设定群組編號與密碼, 同的群組。	並透過下方 [群組成員]	表格確認是否加	口入正確的群組	8。若群組編號相同但密發	
ARETE 111 英產管理	群組編號 1-255 密碼		244			客用	
」』 法量管理 ▲1 行為管理	群組成員						
進和設定 A HA 備援	MAC 你	IP	序號	版本	狀態	上次開機時間	
	001C7F95EFD5 其他成員	192.168.8.28	WB20C21000	1.4.0		**	
■ 系統工具			沒有其他成員				

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。
- 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 <u>https://myark.lionic.com/otp/vpn</u> 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

LIONIC Security Solution Previder					⑦ 紫中 →
Ark-UTM 16	✿ 系統管理				
訂 儀表板	裝置資訊 (回照器) 通知	● 更新新聞 偏份心復原設定 更改家碼	管理日誌 拖萊報告		
⊕ 網際網路					
11 医域網路	授權管理				
安全防護	埛欉狀覸	已約用			
当 安全規則	四雄 四 田 日	2007年4月12日 下午 2:02:02			
資安記錄	1又作图主引用力 口	2027449120 1-7 3.02.02		_	
網路管理	續約碼	AAAA-BBBB-CCCC-DDDD		書用	
🚍 資產管理					
山 流量管理	系統時間				
土 、行為管理	本地時間	Sun Dec 22 19:24:06 CST 2024			
追用股定	時區	Asia/Taipei	~		
▲ HA 個援	NTP 伺服器	0.pool.ntp.org	0		
O VPN		1.pool.ntp.org	0		
○ 系統管理		2.pool.ntp.org	0		
■ 系統工具		3.pool.ntp.org	0	+ 客用	

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:
- 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。
- 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

LIONIC				
e Ark-UTM 16	• 系統管理			
罰 俱表板	N	面积40.6 的 的 40.6 的 的 40.6 的	8 00178 D 10 10 20 20 40	
⊕ мала		3C8140788 19177-0180768242 3C13.0219	0 H-E140 203C4E1	
14 III.46.0038	授權管理			
安全印刷	授權狀態	PMM		
■ 安全規則	授權到期日	2027年4月12日 下午 3:02:02		
資安記錄	總約四	AAAA-BRRR-CCCC-DDDD		
網路管理	10,170	1000 000 0000 0000		
28 資產管理				
11 法量管理	系統時間			
<u>11</u> 行為管理	本地時間	Sun Dec 22 19:23:18 CST 2024		
BAR2	89.00	Asia/Taipei	~	
▲ HA 備援	NTP 伺服器	0.pool.ntp.org	0	
• VPN		1.pool.ntp.org	0	
◆ 系統管理		2.pool.ntp.org	0	
■ 系統工具 く		3.pool.ntp.org	0	+ 第用

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]。

LIONIC Breatly, Statement Prevent	通訊埠	514		
■ 備表板 ● 網際網路	進階設定 >	UDP	Ŭ	2月
計 區域網路 安全防備	SNMP			
当 安全規則 ● 資安記録	啟用版本	v2c	×	
#15世祖 書 資產管理	下載 MIB 檔	<u>له</u> م ب		
↓ 流量管理 \$1 行為管理	SNMPv2c			
327810-2	社群名稱 允許連線 IP 清單	IPv4	+ 新知	
VPN				
 ○ 系統管理 □ 系統工具 				兼用

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。

LIONIC Security Solution Provider	語言	English 🗸
Ark-UTM 16		
罰 儀表板	電子郵件通知	
⊕ 網際網路	寄送頻率	□ 每月 □ 每週 □ 每天 □ 當偵測到威脅時
計 医域網路	SMTP 伺服器	smtp.mail.com
安全防御	SMTP 通訊埠	25
● 資安紀錄	SMTP 帳號	user@mail.com
網路管理	SMTP 密碼	調輸入窓的密碼 😽
📑 資產管理	收信者	user@mail.com 割試 書用
↓ 流量管理		
【行為管理 進用設定	LINE Notify	
▲ HA 備援	Token 請輸入 Token	斯博
C VPN	串接 LINE Notify 服務,以	LINE App 接收期時威脅偵測通知。請至 LINE Notify 官方網頁取得您的 Token。
◎ 系統管理		
■ 系統工具 く		

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。

		♥ 第中 →
Ark-UTM 16	 系統管理 	
罰 偏表板	装置資訊 何服器 通知 更新物情 偏份4個原設定 更改密碼 管理日話 摘要暗告	
⊕ 網際網路 11 區域網路		
920 0	自動 您的聪微版本已為最新。	
 ·	手動更新	
AD41	+ 上傳	
■ 資産管理 」」 決定管理		
北 行為管理		
ARIOZ		
© VPN		
 		
■ 系統工具 〈		

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。

		S 繁中 I→
e Ark-UTM 16	o 系統管理	
罰 俱表板	英言世民 但是是 通知 更新新婚 信任人物质较少 更改原语 管理日达 建香菇失	
• милиз		
11 E 4008	備份 按下"偶份"以下載現在的設定值 嘎 份	
安全時間 		
曽 安全規則		
資安記錄	復原 按下"復原"以上傳復原之說定值 加股檔案 使原	
RINK I		
= 8493		
al anga		
北 行為管理		
1962		
▲ HA 佣援		
O VPN		
◆ 系統管理		
晋 系统工具		
<		

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]。

LIONIC	
Ark-UTM 16	○ 系統管理
偏表板	如田田田 山田 通知 新新知識 使心力地回动学 新冷漠波 领用日本 新闻和本
an an an an an	CALVER LINE AND ADDRESS MICHAELES ADDRESS
医埃利洛	新密碼 這种人型的思想 云
200	
安全规则	確認密碼 該再一次輸入您的密碼 📈
戦安記録	
<u><u><u>R</u></u><u>R</u><u>R</u><u>R</u></u>	
沈晨堂理	
(GANE)	
БZ	
HA 佣握	
VPN	
系統管理	
KRIA	
<	

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。

LIONIC Security Solution Provider		♥ 繁中
Ark-UTM 16	◎ 系統管理	
司 儀表板	装置資訊 伺服器 通知 更新朝髓 偏份4億原設定 更改密碼 管理日誌 携要稽告	
⊕ 網際網路		
計 医域網路	星塔口玲 (88)	
安全防護	日期 來源位址 訊息紀錄	
■ 安全規則	2024/12/22 18:36 223.137.194.88 Sign in	
資安記錄	2024/12/20 15:02 223.137.194.88 Sign in	
網路管理	2024/12/20 08:43 223.138.101.2 Backup configuration	
🚍 資產管理	2024/12/20 08:33 223.138.101.2 Sign in	
↓ 流量管理	2024/12/19 16:23 220.130.53.5 Sign in	
上、 行為管理	2024/12/19 1518 220.130.53.5 Sign in	
進用設定	2024/12/19 11:44 220.130.53.5 Sign in	
L HA 備援	2024/12/19 10:30 172:226:160.8 Sign in	
I VPN	2024/12/181659 1364.65.111 Sign in	
◎ 系統管理	2024/12/18 18:29 1.164.65.111 Sign in	
音系統工具 く	< 1 2 3 _ 9 > 10 * 從1至10總共89項	

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。

Ark-UTM 16	◎ 系統管理		
■ 備表板			
⊕ 網際網路	裝置資訊 伺服器 通知 更新紡體 備份6復原設定 更改密碼	管理日誌 摘要報告	
计 医球網路			
完全防護	Ark-UTM 16 摘要報告		
■ 安全規則	24 小時 / 7天 / 30天		
資安紀錄			C Sylph
KRA W ID			
28 資產管理	Ark-UIM 月報 2024 年 12 月 26 日	Generative Enderhander	
▲■ 流量管理	MAC / 按權期限 /		
1 行為管理			
NRE			
▲ HA 備援	初推版本 1.4.1 所成負載評級	網路安全評級	
VPN	■ 27番 用1500-0- 3.0.1273 低負載 入侵防策的本 5.1152	dEnalina ₽	
◎ 系統管理	8.88.89.99.98.98.99.4 20.050		
百 系統工具	检测照程 #280日時点 30 天内		
	檔案 連結 封包 法	时包	
<	0 44 75	2 M	

系統管理-摘要報告



系統工具

Ark-UTM 16 日 系统工具
= 9.86
● 期間構築 前分別工具 系統日誌 特徵碼更新 重新開稿 原油重量
21 814998
setom ping ∽ ipv4.google.com ID/II
¥ प्र±्रम्म
e recu
Anna and an
■ XAN3
, तो अन्नभूत्र
11 行為解理
ANKZ
A HA 88
© VPN
O 系统管理
U KRIA

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



© Copyright 2025 Lionic Corp. All rights reserved.

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

1F-C6, No.1, Lising 1st Rd., Science-Based Industrial Park, Hsinchu City 300, Taiwan, R.O.C.