Trend Micro™ Cloud Edge

2023 年 7 月

管理手冊

文件編號：APTM09748/230625

發行日期：2023 年 7 月

受美國專利保護，專利編號： 專利申請中。

本文件介紹了產品的主要功能，並/或提供作業環境的安裝說明。在安裝或使用產品前，請先閱讀此文件。

如需有關如何使用產品特定功能的詳細資訊，請參閱趨勢科技線上說明中心和/或趨勢科技常見問題集。

趨勢科技十分重視文件品質的提升。如果您對於本文件或其他趨勢科技文件有任何問題、意見或建議，請與我們聯絡，電子郵件信箱為 docs@trendmicro.com。

請至下列網站並給予您對此文件的評估意見：

https://www.trendmicro.com/download/documentation/rating.asp

隱私權資料和個人資料蒐集披露

趨勢科技產品中所提供的部分功能會蒐集與產品使用和偵測相關的資訊，並建議傳送回饋給趨勢科技。少數資訊在部分司法管轄權和法規下會視為個人資料。如果您不希望趨勢科技蒐集您的個人資訊，則建議您務必詳細瞭解並確認是否要關閉相關功能。

以下連結列出 Cloud Edge 將蒐集的資料類型，並提供有關如何關閉特定資訊回饋功能的詳細說明。

https://success.trendmicro.com/data-collection-disclosure

趨勢科技所蒐集的資料將遵循趨勢科技隱私權注意事項中的規定：

https://www.trendmicro.com/privacy

目錄

第 3 章：入門

第 4 章：Licensing Management Platform

第 5 章：Trend Micro Remote Manager

第 6 章：Cloud Edge 雲端主控台

第 7 章：Cloud Edge 內部部署

第 8 章：技術支援

索引

序言

序言

歡迎使用 Trend Micro™Cloud Edge 管理手冊。本手冊介紹 Cloud Edge 並說明如何使用 Trend Micro™ Remote Manager 在 Cloud Edge 雲端主控台中註冊設備及同步處理帳號，以及如何在消費者辦公地點部署 Cloud Edge 設備。

文件

Cloud Edge 的文件集包含下列文件：

表 1. 產品文件

文件	說明
線上說明	「線上說明」包含 Cloud Edge 元件和功能的說明，以及設定 Cloud Edge 所需的程序。 Cloud Edge 雲端主控台在每個畫面的右側提供嵌入式的即時說明。
管理手冊	《管理手冊》是一份 PDF 文件，其中介紹 Cloud Edge 並說明如何使用 Trend Micro™ Remote Manager、如何在 Cloud Edge 雲端主控台註冊設備與同步處理帳號以及如何在客戶辦公地點部署 Cloud Edge 設備。
新增功能	「新增功能」檔案提供新功能的說明。
支援入口網站	支援入口網站是提供問題解決方法和疑難排解資訊的線上資料庫。此資料庫提供有關產品已知問題的最新資訊。若要存取支援入口網站，請移至下列網站： https://success.trendmicro.com/tw/contact-support

可於下列位置檢視與下載本文件：

http://docs.trendmicro.com/zh-tw/smb/cloud-edge.aspx

適用對象

Cloud Edge 文件是專為 IT 管理員和安全分析人員所撰寫。本文件假設讀者具備深入的網路和資訊安全知識，包括下列主題：

- 網路拓撲
- 資料庫管理
- 策略管理與實施

本文件未假設讀者具備安全威脅事件關聯的任何知識。

文件慣例

本文件會使用下列慣例：

表 2. 文件慣例

慣例	說明
大寫	頭字語、縮寫、特定的指令名稱和鍵盤上的按鍵
粗體	功能表和功能表指令、指令按鈕、標籤和選項
斜體	參考其他文件
等寬	指令行範例、程式碼、Web URL、檔案名稱和程式輸出
瀏覽 > 路徑	可到達特定畫面的瀏覽路徑 例如，「檔案 > 儲存」代表按一下「檔案」，然後按一下介面上的「儲存」
 注意	組態設定注意事項
 秘訣	推薦或建議
 重要	必要或預設組態設定和產品限制的相關資訊
 警告!	重要的處理行動和組態設定選項

需求

Cloud Edge 採用 Amazon Elastic Compute Cloud™ 並受 Amazon Web Services 制定之要求的約束。若要深入瞭解，請造訪 http://aws.amazon.com/ec2/。

表 3. 支援的 Web 瀏覽器

瀏覽器	版本
Mozilla Firefox™	80 或更新版本
Google Chrome™	83 或更新版本
Microsoft Edge™ (Chromium)	85 或更新版本

第 1 章

Cloud Edge 簡介

Cloud Edge 總覽

Trend Micro Cloud Edge 不僅為 MSP（管理服務提供者）提供新一代內部部署防火牆的優勢，還提供安全即服務的便利性。Cloud Edge 將應用程式控管與使用者和通訊埠識別機制智慧結合，藉以提供多層防護。URL 過濾、頻寬控制、入侵防護、惡意程式防護掃瞄、電子郵件安全以及網頁信譽評等安全機制則提供了額外的保護，免除網路遭入侵、營運被迫中斷之憂。透過內部部署環境或雲端來深入掃瞄及過濾網路封包，Cloud Edge 在設備就擋下安全威脅。此外，虛擬私人網路 (VPN) 支援還能確保來自行動裝置、企業站台與遠端員工的連線安全無虞。

在客戶辦公室部署 Cloud Edge 設備，並使用 Cloud Edge 雲端主控台集中控制使用者存取權與安全策略。您還可以選擇透過 Trend Micro Remote Manager，使用單一登入來存取 Cloud Edge 雲端主控台。Remote Manager 配合 Cloud Edge 使用時，提供了單一進入點來存取所支援設備與趨勢科技產品的圖形報告和資訊中心摘要資料。Remote Manager 還可以協助您管理多個客戶的授權與帳單。

下圖顯示 Cloud Edge 的運作方式。

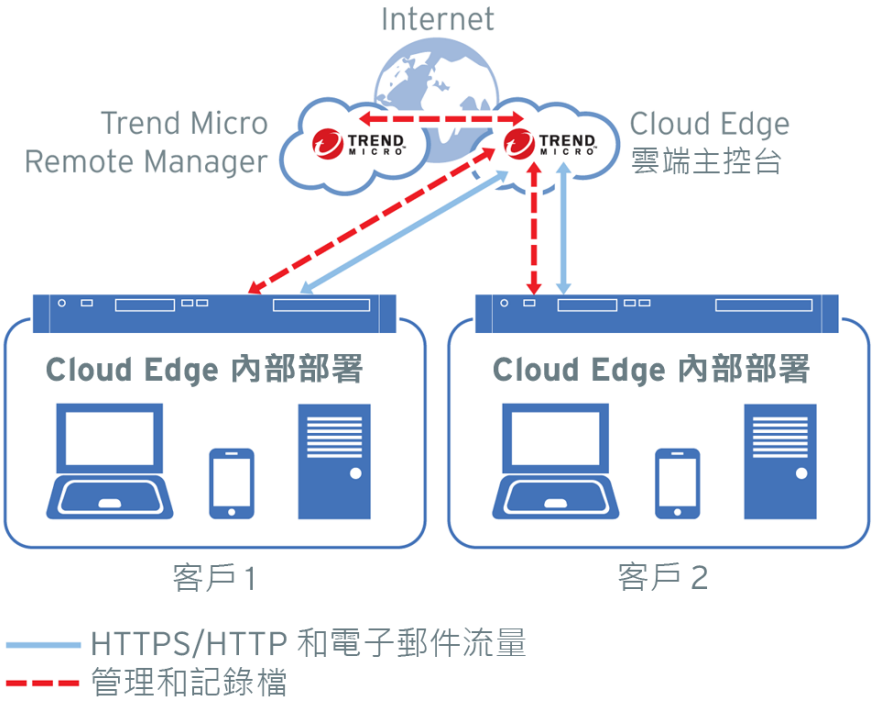


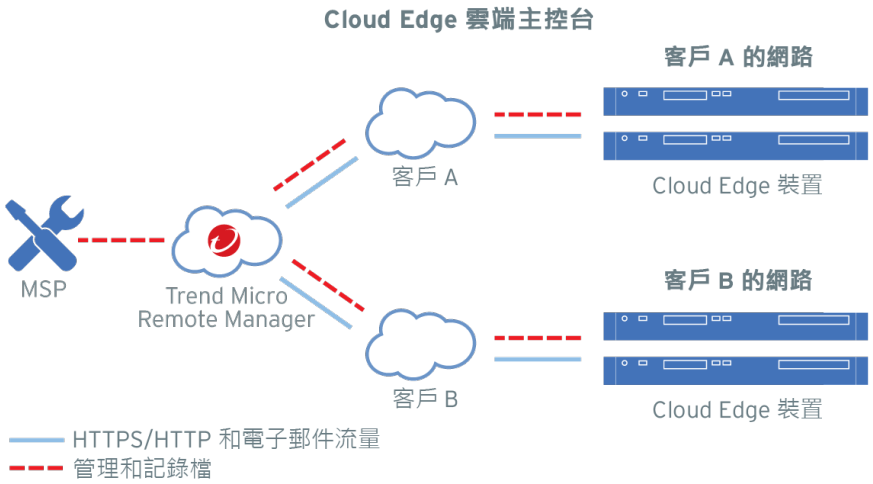
表 1-1. Cloud Edge 元件

元件	說明
Cloud Edge 雲端主控台	Cloud Edge 雲端主控台是一種安全即服務管理主控台，裝載於 AWS (Amazon Web Services) 雲端中。 Cloud Edge 雲端主控台可跨任何數目的網路來控制散佈各地之 Cloud Edge 設備上的使用者存取權與安全策略。您可隨時動態存取雲端中的 Cloud Edge 雲端主控台。

元件	說明
Cloud Edge 設備	Cloud Edge 設備是支援雲端技術、實際提供網路安全防護的 UTM（統一安全威脅管理）裝置。 Cloud Edge 設備的用途為在客戶所在位置實施新一代的安全防護，方法是以內部部署防火牆的形式掃瞄及封鎖惡意內容，或是以網路橋接器的形式暗中監控是否有安全威脅。
Trend Micro Remote Manager	Trend Micro Remote Manager 是針對趨勢科技通路合作夥伴和 MSP 的單一窗口管理主控台，其提供了一個即時的安全面板且可以查看所有客戶的報告以及管理使用授權。 Remote Manager 可用來存取所支援設備與趨勢科技產品的圖形報告和資訊中心摘要資料。Remote Manager 亦可用來管理多個客戶的授權與帳單。您還可以選擇透過 Remote Manager，使用單一登入來存取 Cloud Edge 雲端主控台。

Cloud Edge 的運作方式

下圖說明一般 Cloud Edge 客戶部署的實作方式。



1. 將 Cloud Edge 設備部署到客戶辦公室。
2. 使用 Cloud Edge 雲端主控台來集中管理使用者存取與安全策略。
3. 透過 Trend Micro Remote Manager 以單一登入方式登入 Cloud Edge 雲端主控台。
4. 使用 Remote Manager 作為單一進入點，以存取所支援設備與趨勢科技產品的圖形報告和資訊中心摘要資料。Remote Manager 還可以協助您管理多個客戶的授權與帳單。
5. 記錄檔會從 Cloud Edge 設備傳送到 Cloud Edge 雲端主控台與 Remote Manager。

客戶在部署 Cloud Edge 內部部署後，需將每部設備設定為設備上的防火牆或網路橋接器，以無形的方式掃瞄和封鎖惡意內容。Cloud Edge 設備具有深入的內容檢測功能，能在整個流量通過設備時檢查流量，以搜尋相符的簽章、行為分析、規範與符合性分析，以及與前一個作業階段歷史記錄的作業階段關聯性。

MSP 會使用 Cloud Edge 雲端主控台對所有通過已註冊之 Cloud Edge 設備的流量進行策略管理（無論這些設備分散於多少網路上）。當 MSP 向 Cloud Edge 雲端主控台註冊 Cloud Edge 設備後，就會透過雲端啟動安全的流量轉送。

將電子郵件安全設為雲端掃瞄（預設值）時，所有電子郵件要求會直接透過雲端路由，以進行檢測。透過雲端路由時，Cloud Edge 雲端後端服務會根據管理服務提供者設定的策略來檢測、分析與過濾要求。如果允許要求，流量就會路由到使用者。如果不允許要求（如要求禁止的 URL 類別），就會封鎖要求並通知使用者。

MSP 可使用 Remote Manager 來管理多個使用趨勢科技服務的客戶的授權和計費：LMP (Licensing Management Portal) 或 CLP (Customer Licensing Portal)。使用授權變更或更新會在後端同步處理，並顯示於 Cloud Edge 雲端主控台和 Remote Manager 中。

主要功能

下表說明 Cloud Edge 雲端主控台的主要功能。技術元件的設計目的是要整合透過雲端進行的設備管理作業並最佳化效能。

表 1-2. Cloud Edge 雲端主控台功能

功能	說明
設備管理	透過單一雲端主控台，集中管理多個 Cloud Edge 設備。 管理採用硬體切換晶片組之 Cloud Edge 設備的內部網路安全模式。 管理 Cloud Edge 無線設備的無線網路存取控制並管理無線用戶端連線。 使用 Cloud Edge 雲端主控台建立及管理 HA 群組。您可以使用兩台已註冊設備建立 HA 群組，來提供高可用性存取。當某一台設備故障時，另一台設備就會進行接管，以確保網路流量不會中斷。
多層防護	Cloud Edge 可識別使用者和使用者群組存取網路的時間、使用的通訊埠，以及存取的 Web-based 應用程式，以防範網路滲透攻擊。根據這些多層識別機制實施安全策略，有助於抵禦可能規避傳統安全解決方案的新興複雜安全威脅。
策略管理與部署	在任何數目的受管理設備上部署策略。策略管理選項包括： • 針對特定的設備、介面群組、使用者/使用者群組、IP 位址、FQDN、上網位置、服務、應用程式群組、URL 類別群組、排程和安全資料檔建立策略 • 針對進階策略功能（包括入侵防護系統 (IPS)、惡意程式防護、電子郵件安全、網頁信譽評等服務、HTTPS 檢查、拒絕服務防護和端點識別）建立安全資料檔 • 核可或封鎖 URL 來覆寫策略規則 • 在發生策略事件時傳送通知
隨插即用部署	將 Cloud Edge 設備送到客戶地點，而不必拆開包裝。您的客戶可以拆箱並按照隨附文件中的指示操作。一旦設備經過手動註冊並上線後，設備會接收您的自訂安全策略組態設定。
智慧型資訊中心	檢視網路內以及跨一或多個設備上進行的活動。Widget 代表資訊中心的核心元件，並包含視覺化圖表與圖形，可讓您追蹤安全威脅並與累計的記錄檔資料建立關聯。

功能	說明
記錄檔分析和報告	檢視及分析關於流量頻寬耗用量、安全威脅偵測、Web 2.0 應用程式使用情況、網頁瀏覽活動以及策略實施的彙整記錄檔和事件資料。 將記錄檔查詢過濾條件另存為我的最愛以供日後參考，或產生自訂報告來進一步調查。 檢視策略規則的使用情況資料（僅當客戶運作的設備全是 Cloud Edge 6.0 或更新版本時適用）。
服務品質	透過控制通訊、封鎖非必要流量，以及將適當頻寬配置給重要的流量或服務等動作，控制頻寬耗用量來減少網路壅塞情形。
URL 過濾	設定 URL 過濾策略來拒絕或允許對 Web 網域的存取。 您可以設定策略來掃瞄流量中是否有特定 URL 類別（例如，「成人」和「賭博」），以便過濾流量。當使用者要求 URL 時，設備會先查看類別中是否有該 URL，然後根據策略設定進行存取控制。
應用程式控管	控制超過 3400 種在任何通訊埠執行的應用程式類型，包括使用特定用戶端（Skype、BitTorrent、P2P）或在網站（社群網路、網路郵件、串流媒體）內使用 Web 2.0 技術的應用程式。
安全資料檔	對安全資料檔執行進階策略組態設定。 • 入侵防護 • 惡意程式防護 • 電子郵件安全防護 • 網頁信譽評等 • HTTPS 檢查 • 拒絕服務攻擊防護 • 端點識別
使用者管理	在設備之間同步處理使用者資訊。
使用者 VPN	使用者虛擬私人網路 (VPN) 將 VPN 功能延伸至遠端使用者，讓使用者能夠利用撥號（包括寬頻）、LAN 與行動連線，透過 IPv4 VPN 通道安全地將機密資訊傳達給網路和伺服器。 不適用於不支援 VPN 的 Cloud Edge 設備型號。

功能	說明
Site-to-Site VPN	Site-to-Site VPN（站台對站台虛擬私人網路）可讓分散於多個固定地點的辦公室透過公用網路（例如 Internet）在彼此之間建立安全的 IPv4 連線。 不適用於不支援 VPN 的 Cloud Edge 設備型號。
記錄檔轉送服務	記錄檔轉送服務是授權服務，可讓 Cloud Edge 雲端主控台將授權設備的記錄檔轉送至外部應用程式。管理服務提供者可將「記錄檔轉送服務」服務方案指定給客戶。
設備系統狀態和事件/記錄檔	對於每個設備，您可以檢視設備系統狀態的相關資訊。您也可以檢視網路、系統和 VPN（如果有的話）的事件/記錄檔，以及策略實施記錄檔的事件/記錄檔。 對於不支援 VPN 的 Cloud Edge 設備型號，將不會顯示 VPN 事件。
設備疑難排解工具	您可以使用 Ping、Traceroute 和 ARP 來疑難排解設備網路 IPv4 連線問題。
與 Worry Free Business Security Services 整合	Cloud EdgeWFBSS 端點防護 整合了 WFBSS，可針對具有過期的 WFBSS Security Agent 病毒碼或未安裝 WFBSS Security Agent 的 WFBSS 端點提供符合性檢查。Cloud Edge 可針對不合規端點提供網路存取控制。
可疑端點的網路存取控制	Cloud Edge 透過為端點提供符合性檢查，查看是否已偵測到超過所設閾值的 C&C 回呼數，來提供安全防護服務。Cloud Edge 可以為超過閾值的端點提供網路存取控制。

混合式安全功能

Cloud Edge 可將安全功能分發到內部部署和雲端中，以提升網路頻寬的服務品質，並在必要時有效地實施策略。僅特定流量能轉送到雲端，以根據策略進行分析與控制。您可透過 Cloud Edge 內部部署主控台來管理內部部署的功能，透過 Cloud Edge 雲端主控台則可管理雲端的功能。下表說明內部部署以及雲端安全功能的分發情況。

表 1-3. Cloud Edge 分散式安全功能

功能	內部部署	雲端
高可用性 (HA) 群組		●
進階防火牆防護	●	
應用程式控管	●	
端點管理	●	●
設備管理		●
入侵防護系統 (IPS)	●	
Licensing Management Platform 整合		●
Remote Manager 整合		●
垃圾郵件掃瞄	●	●
切換：軟體切換	●	
切換：硬體切換晶片組	●	●
URL 過濾	●	
虛擬私人網路	●	
病毒和惡意程式掃瞄	●	●
使用沙箱的進階惡意程式防護		●
使用 Machine Learning 的進階惡意程式防護		●
網頁信譽評等服務	●	●
無線網路	●	●

內部部署功能

下表說明 Cloud Edge 提供的內部部署功能。

如需內部部署功能的 IPv6 支援的詳細資訊，請參閱 IPv6 支援 第 1-16 頁。

表 1-4. Cloud Edge 內部部署功能

功能	說明
高可用性 (HA) 群組	您可以將兩台已註冊設備設定為一個 HA 群組，以提供高可用性存取。當某一台設備故障時，另一台設備就會進行接管，以確保網路流量不會中斷。此外，HA 群組能夠提高網路流量效率。
進階防火牆	藉由封鎖攻擊並允許正常的應用程式流量通過，輕鬆部署和管理新一代的防火牆。
防毒	運用多項安全元件以及基於應用程式內容掃瞄的病毒防護，提供更佳的防護、更低的延遲並提升使用者體驗。
垃圾郵件和惡意程式防護掃瞄	當電子郵件安全設定為本機掃瞄時，Cloud Edge 會在本機管理並提供垃圾郵件和惡意程式防護。 注意 電子郵件安全的預設設定是雲端掃瞄。Cloud Edge 可在某些情況下（包括出現網路問題時）自動將設定變更為本機掃瞄。
電子郵件信譽評等服務	使用趨勢科技電子郵件信譽評等服務 (ERS) 偵測電子郵件，並根據郵件寄件者的信譽評等封鎖電子郵件訊息。
IPS	識別和阻擋許多主動式安全威脅、弱點攻擊、後門程式和其他攻擊通過裝置，包括拒絕服務 (DoS) 和分散式拒絕服務 (DDoS) 攻擊。入侵防護系統 (IPS) 可加強防火牆的安全策略，方式是確保防火牆允許的流量經過進一步檢測，確定未包含不想要的安全威脅。
應用程式控管	使用策略自動探索熱門的 Internet 應用程式，並控制對這些應用程式的存取。

功能	說明
網路組態設定	檢視和編輯偵測到的網路介面，或修改實體 L2 和 L3 通訊埠組態設定。L3 通訊埠支援下列 IPv4 組態設定： • 動態主機設定通訊協定 (DHCP) • 依 IP 位址和網路遮罩的靜態路由組態設定 • 乙太網路點對點通訊協定 (PPPoE)
橋接	以透明化的方式橋接兩個介面和過濾網路流量來保護端點和伺服器，將對現有網路環境的影響降至最低。跨距樹狀目錄通訊協定 (STP) 可確保任何橋接的乙太網路區域網路具有無迴圈的拓撲。 「橋接模式」部署支援 IPv6 功能。
軟體切換	將 Cloud Edge 設備設定為以「軟體切換」（從「橋接模式」變化而來）運作，可讓小型企業環境無需另備交換器。Cloud Edge 仍會在設定為「軟體切換」時根據已設定的策略提供安全掃瞄。 「軟體切換」部署支援 IPv6 功能。
硬體切換晶片組	採用硬體切換晶片組的 Cloud Edge 設備兼具安全設備與硬體切換特性。在「橋接模式」下，這款設備提供 7 個直接連線到端點的 LAN 切換通訊埠，可讓許多企業環境無需另備交換器。 如有需要，您也可以採用「路由模式」來部署這款設備。採用「路由模式」部署時，提供 8 個 LAN 通訊埠供內部網路使用。 不論是採用「路由模式」進行部署，還是以「橋接模式」部署為硬體切換，採用硬體切換晶片組的 Cloud Edge 設備皆會根據已設定的策略提供安全掃瞄。 「橋接模式」部署支援 IPv6 功能。
路由	將 Cloud Edge 設備設定為在「路由模式」下時用做路由器。這款設備用做具有安全掃瞄和控制功能的第 3 層路由裝置，在網路中可見。Cloud Edge 設備會在本機管理所有 IPv4 靜態路由。 「路由模式」部署不支援 IPv6 功能。
頻寬控制	透過控制通訊減少網路壅塞，並藉由適當的頻寬配置降低非必要流量並允許重要的流量或服務。
URL 過濾	針對不同的資料檔建立和設定專屬的 URL 過濾程序。URL 過濾以及 WRS 屬於多層、多重安全威脅防護解決方案的一部分。

功能	說明
NAT	設定網路位址轉譯 (NAT) 策略，以指定是否要在公開和私人位址以及通訊埠之間轉換來源或目標 IPv4 位址和通訊埠。
服務	設定下列服務： • 動態主機設定通訊協定 (DHCP) 伺服器
VPN	設定 IPv4 VPN。 • 使用者 VPN 使用第二層通道通訊協定 (L2TP) 或安全通訊端層虛擬私人網路 (SSL VPN) 設定虛擬私人網路 (VPN)。 可讓 iOS 和 Android 行動裝置使用者使用內建的 IPsec VPN 用戶端，輕鬆安全地重新連線到企業環境。行動裝置不需要安裝代理程式。 • Site-to-Site VPN 使用網際網路金鑰交換 (IKE) 和 IP 安全性 (IPsec) 通訊協定建立加密的 L3 通道。 您可以建立單一點對點 VPN 通道、由一個中樞裝置和最多四個分支裝置組成的星狀 VPN 拓撲，或由最多五個裝置組成的完整網狀 VPN 拓撲。 對於不支援 VPN 的 Cloud Edge 設備型號，您無法對其設定 VPN。
記錄檔	檢視及分析稽核記錄、系統事件和 VPN 記錄檔（如果有的話）。
設備系統狀態和事件/記錄檔	對於每個設備，您可以檢視設備系統狀態的相關資訊。您也可以檢視網路事件、系統事件、VPN 事件（如果有的話）和策略實施記錄檔的相關資訊。 對於不支援 VPN 的 Cloud Edge 設備型號，您無法檢視該型號的 VPN 相關資訊。
設備疑難排解工具	您可以使用 Ping、Traceroute 和 ARP 來疑難排解設備 IPv4 網路連線問題。
與 Worry Free Business Security Services 整合	Cloud EdgeWFBSS 端點防護 整合了 WFBSS，可針對具有過期的 WFBSS Security Agent 病毒碼或未安裝 WFBSS Security Agent 的 WFBSS 端點提供符合性檢查。Cloud Edge 可針對不合規端點提供網路存取控制。

功能	說明
可疑端點的網路存取控制	Cloud Edge 透過為端點提供符合性檢查，查看是否已偵測到超過所設閾值的 C&C 回呼數，來提供安全防護服務。Cloud Edge 可以為超過閾值的端點提供網路存取控制。
無線網路	對於具有無線網路功能的 Cloud Edge 設備，您可以設定主要網路和客體網路的無線網路存取，還可使用 MAC 位址過濾來控制存取權。Cloud Edge 對主要網路和客體網路均提供完整的安全防護服務。 您可以對無線網路設定其他網路服務，包括 DHCP 服務、頻寬控制、NAT、VPN 存取，以及可疑端點的網路存取控制。

雲端功能

下表說明雲端可用的 Cloud Edge 功能。

表 1-5. Cloud Edge 雲端功能

功能	說明
設備管理	透過一個雲端主控台集中管理多個 Cloud Edge 內部部署設備。 使用 Cloud Edge 雲端主控台將兩台已註冊設備設定為一個 HA 群組，以提供高可用性存取。管理現有的 HA 群組，包括修改組態設定、啟動或關閉 HA 群組、強制接管，或是移除 HA 群組。
網頁信譽評等	採用趨勢科技網頁信譽評等技術，控制抵禦惡意網站的防護等級。
惡意程式和病毒掃瞄	運用多項安全元件以及基於應用程式內容掃瞄的病毒防護，提供更佳的防護、更低的延遲並提升使用者體驗。 使用雲端沙盒虛擬平台和 Machine Learning，實現電子郵件惡意程式的進階防護。
垃圾郵件掃瞄	使用雲端垃圾郵件掃瞄，根據電子郵件內容來偵測和封鎖或標記垃圾郵件訊息。
報告	針對偵測到的惡意程式和惡意程式碼、封鎖的檔案以及瀏覽的 URL 產生報告，以最佳化程式設定和微調安全策略。

功能	說明
記錄檔分析	檢視及分析關於流量頻寬耗用量、安全威脅偵測、Web 2.0 應用程式使用情況、網頁瀏覽活動以及策略實施的彙整記錄檔和事件資料。 如果客戶運作的設備全是 Cloud Edge 6.0 或更新版本，請檢視策略規則的使用情況資料。 將記錄檔查詢過濾條件另存為我的最愛以供日後參考，或產生自訂報告來進一步調查。

為加強雲端功能，安全資料檔將提供一個機制來控制可能會影響設備的特定安全威脅。為入侵防護系統 (IPS)、惡意程式防護安全、電子郵件安全、網頁信譽評等、拒絕服務攻擊與端點識別設定進階策略控制。下表說明可用的安全資料檔。

如需有關利用安全資料檔支援 IPv6 的詳細資訊，請參閱 IPv6 支援 第 1-16 頁。

表 1-6. Cloud Edge 安全資料檔

功能	說明
IPS 資料檔	每個安全資料檔都可以指定入侵防護資料檔，由這個資料檔決定針對緩衝區溢位、非法程式碼執行與其他入侵系統弱點嘗試的防護等級。預設資料檔可保護用戶端和伺服器不受已知安全威脅的侵犯。
惡意程式防護資料檔	針對 Web-based 惡意程式防護採取預設智慧型處理行動，或為公司自訂處理行動設定，或指定允許或封鎖 URL 中指定的哪個副檔名。 啟動雲端截毒掃瞄來增強惡意程式掃瞄。雲端截毒掃瞄是新一代雲端防護解決方案。此解決方案的核心是一套運用了雲端截毒伺服器的先進掃瞄架構，可利用儲存在雲端的簽章掃瞄安全威脅。

功能	說明
電子郵件安全資料檔	對電子郵件安全採取預設智慧型處理行動，或為組織自訂處理行動設定。電子郵件安全資料檔會對 IPv4 電子郵件流量進行掃瞄並採取處理行動。 惡意程式防護 啟動惡意程式防護掃瞄並定義附件含有惡意程式之電子郵件的主旨行和內文中使用的標籤。 您可以啟動沙盒虛擬平台和 Machine Learning，來設定進階雲端掃瞄和對電子郵件惡意程式的防範。 如果啟動，當檔案展現可疑特徵，但簽章型掃瞄技術找不到未知安全威脅時，Cloud Edge 會將可疑檔案附件傳送給沙盒虛擬平台和 Machine Learning。 標記包含已加密附件的電子郵件並定義在電子郵件內正文中使用的標籤。 垃圾郵件防護 啟動垃圾郵件防護掃瞄並選擇性地啟動 Cloud Edge 來使用趨勢科技 ERS（電子郵件信譽評等服務），根據來源位址的信譽評等來判斷垃圾郵件。設定垃圾郵件的「敏感度」等級或偵測率。 啟動 BEC（商務電子郵件入侵）掃瞄。BEC 詐騙會以公司為目標，透過社交工程的手段，入侵合法的商務電子郵件帳號，以遂未經授權的金錢移轉目的。 定義判斷電子郵件為垃圾郵件和 BEC 時採取的處理行動，如果處理行動為標記，則定義垃圾郵件或 BEC 電子郵件訊息的主旨行和內文中使用的標籤。 內容過濾和例外清單 設定內容過濾器或建立例外清單，以根據寄件者或附件檔案類型（雲端掃瞄根據真實檔案類型，本機掃瞄則根據副檔名）封鎖或核可電子郵件。 進階設定 您可以設定要啟動的電子郵件通訊協定、自訂 SSL 通訊埠與 SMTP 伺服器設定。

功能	說明
網頁信譽評等資料檔	每個安全策略都可選取網頁信譽評等敏感度等級，以封鎖網站。 網頁信譽評等技術會指派信譽評分給 URL。Cloud Edge 會針對所存取的每個 URL 向網頁信譽評等查詢信譽評分，然後根據此評分是低於還是高於使用者指定的敏感度等級來採取必要處理行動。
HTTPS 資料檔	每個安全策略都可選取要從 HTTPS 檢測中排除的 URL 類別與來源 IPv4 位址例外。 Secure Socket Layer (SSL) 和傳輸層安全 (TLS) 是現今網路通訊環境中廣受採用與部署的密碼編譯通訊協定。透過 SSL/TLS 傳輸的流量會經過加密與簽署來確保安全，形成所謂的 HTTPS。由於加密的 HTTPS 連線也可能會與未加密的 HTTP 連線一樣傳送有風險的內容，因此 Cloud Edge 會對所有 IPv4 流量進行掃瞄，以查看是否有潛在風險與安全威脅。 透過指定最多五個要掃瞄的 HTTPS 通訊埠來自訂 HTTPS 資料檔。
DoS 防護資料檔	每個安全策略都可指定「拒絕服務」攻擊的 Flood 防護和位址例外。 拒絕服務攻擊 (DoS) 或分散式拒絕服務攻擊 (DDoS) 的用意是讓機器或網路資源無法提供給使用者使用，旨在讓服務暫時或一直無法提供給與 Internet 連線的主機。 典型的攻擊為利用外部通訊要求讓目標機器滿載，使該機器無法再回應合法流量，或是回應速度慢到形同無法使用的地步。這類攻擊通常會導致伺服器超載。
端點識別資料檔	每個安全策略都可指定網頁驗證入口的 IPv4 位址物件，以用於識別各 IPv4 位址所屬的使用者。端點識別使用「IPv4 位址與使用者」對應快取來提供使用者識別方法，以符合策略。 依預設，端點識別無法自動識別 IP 位址。您必須定義可用於端點識別的 IPv4 位址物件。如果來源 IPv4 位址不在所選 IPv4 位址物件的定義範圍內，則此 IPv4 位址就無法進行端點識別。 您無法使用 IPv6 位址進行端點識別。

IPv6 支援

Cloud Edge 在「橋接模式」和「軟體切換」部署中提供 IPv6 支援。

重要

「路由模式」不支援 IPv6。

下表說明哪些功能與特性可在「橋接模式」和「軟體切換」部署中提供 IPv6 支援。除了表中所列的支援外，Cloud Edge 還可以藉由 Cloud Edge 設備（包括 IPv6 路由器）轉送透過 IPv6 傳輸的流量，來提供對 Internet 的存取。

表 1-7. 橋接模式和軟體切換部署中的 Cloud Edge IPv6 支援

功能	類別	IPv6 支援	不支援 IPv6
資訊中心		●	
	Cloud Edge 支援在資訊中心中顯示 IPv6 位址。		
設備 — 註冊			●
	Cloud Edge 使用 IPv4 連線至 Cloud Edge 雲端主控台。		
設備 — 網路	介面		●
	管理存取權		●
	DHCP		●
	動態 DNS		●
	路由資料表		●
	靜態路由		●
	NAT		●
	Cloud Edge 設備的網路組態設定（任何模式）不支援 IPv6。不過，Cloud Edge 可以將要求（例如適用於 IPv6 的 DNS 和 DHCPv6）轉送到端點。		
設備 — 頻寬控制		●	
設備 — VPN	使用者 VPN		●
	Site-to-Site VPN		●

功能	類別	IPv6 支援	不支援 IPv6
設備 — 終端使用者管理 — 一般設定			●
	依賴於使用者帳號的功能不支援 IPv6。		
設備 — 更新			●
	Cloud Edge 使用 IPv4 連線至主動式更新。		
設備 — 網路存取控制			●
	Cloud Edge 不支援 IPv6 端點的網路存取控制，即使端點屬於雙堆疊且同時具有 IPv4 和 IPv6 位址也是一樣。		
策略 — 策略	來源 IP	●	
	來源 FQDN	●	
	使用者/使用者群組		●
	目標 IP	●	
	目標 FQDN	●	
	流量 — 應用程式和 URL 類別	●	
	以使用者或使用者群組為基礎的策略不支援 IPv6。這類策略不會套用至 IPv6 流量。		
策略 — 物件	IP 位址/FQDN	●	
	MAC 位址	●	
	服務	●	
	應用程式和應用程式群組	●	
	URL 類別	●	
	Cloud Edge 支援 ICMPv6。		

功能	類別	IPv6 支援	不支援 IPv6
策略 – 核可/封鎖清單	IPv6 位址	●	
	FQDN	●	
	URL	●	
策略 – 安全資料檔	IPS	●	
	惡意程式防護	●	
	電子郵件安全 – 本機掃瞄		●
	電子郵件安全 – 雲端掃瞄		●
	DoS 防護	●	
	HTTPS		●
	網頁信譽評等	●	
	端點識別		●
	電子郵件的本機掃瞄和雲端掃瞄皆不支援 IPv6。Cloud Edge 設備會讓 IPv6 電子郵件流量通過，而不加以掃瞄。 Cloud Edge 設備會讓 HTTPS IPv6 流量通過，而不加以掃瞄。 Cloud Edge 不會針對 IPv6 流量觸發端點識別。如果已啟動網頁驗證入口，將不會開啟網頁驗證入口視窗；IPv6 流量會通過 Cloud Edge 設備。		
策略 – 網頁信譽評等服務		●	
策略 – 使用者通知		●	
	Cloud Edge 支援在 IPv6 用戶端顯示使用者通知。		
分析與報告 – 報告		●	
	Cloud Edge 支援在報告中顯示 IPv6 位址。		

功能	類別	IPv6 支援	不支援 IPv6
分析與報告 — 記錄檔分析	應用程式頻寬	●	
	策略實施	●	
	Internet 存取	●	
	Internet 安全	●	
	Cloud Edge 支援在記錄檔中顯示 IPv6 位址。		
管理 — 使用者與帳號			●
	依賴於使用者帳號的功能不支援 IPv6。		
管理 — 使用者驗證			●
	依賴於使用者帳號的功能不支援 IPv6。		
管理 — 稽核記錄		●	
管理 — 管理員警訊	設備狀態變更	●	
	郵件安全狀態變更	●	
	C&C 回呼	●	
管理 — 排程更新			●
	Cloud Edge 使用 IPv4 連線至主動式更新。		
管理 — 維護			●
	Cloud Edge 使用 IPv4 連線至外部伺服器。		
管理 — 憑證管理			●

第 2 章

Cloud Edge 部署的最佳做法

本章旨在協助合作夥伴制定一套部署和管理 Cloud Edge 安全解決方案的最佳做法。

Trend Micro Cloud Edge 是支援雲端技術的 UTM（統一安全威脅管理）設備裝置。這項裝置不僅提供新一代內部部署防火牆的優勢，還透過雲端提供安全即服務的便利性。透過結合上述兩大功能，Cloud Edge 可檢查和過濾網路封包，以防堵設備的複雜安全威脅。

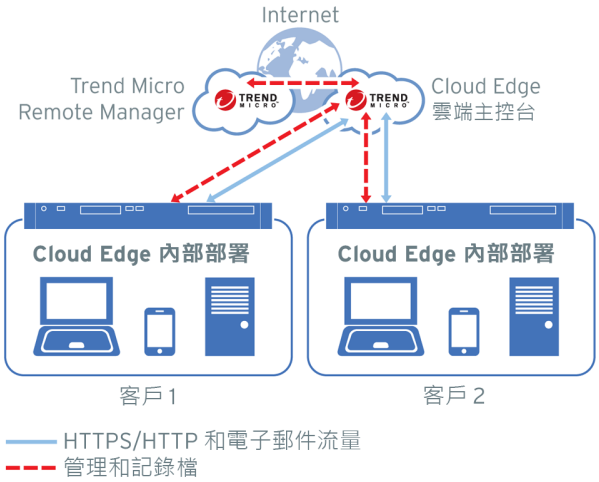
本章介紹輕鬆部署、最佳安全與效能，以及監控與報告的最佳做法。適用對象為部署 Cloud Edge 設備和定期管理運作的管理員。本章並非用來取代本部署指南和其他使用者手冊中的完整資訊集，相關資訊集可以在以下網站找到：http://docs.trendmicro.com/zh-tw/smb/cloud-edge.aspx，包括：

- 授權佈建快速使用卡片（適用於管理服務提供者）
- Cloud Edge 快速使用卡片（適用於內部部署客戶）
- Cloud Edge 雲端主控台線上說明
- Readme

部署最佳做法

由 MSP 進行佈建授權

MSP 合作夥伴可以依照本《部署指南》或《授權佈建快速使用卡片》，將 Cloud Edge 設備適當授權和部署給客戶。快速回顧一下，我們會發現可以從 Trend Micro Remote Manager 啟動所有相關工具。



建立服務方案

請存取 Trend Micro Licensing Management Platform (LMP)，為 Cloud Edge 建立服務方案。

步驟

1. 建立 Cloud Edge 服務方案，其中可能包含下列元件：

a. Cloud Edge — 裝置韌體所需的使用授權

b. 沙箱 — 沙箱模擬的使用授權

c. 記錄檔轉送服務 — 將記錄檔轉送至協力廠商記錄檔維護系統的使用授權

2. 為了遵循最佳做法，請注意以下事項：

- 針對版本類型，由於 Cloud Edge 是裝置，建議使用「完整版」。
- 針對「資料中心」位置，請選取最靠近您的實體位置者。
- 針對「管理產品/服務」，請勾選「Remote Manager」，以允許遠端管理。
- 根據您的行銷策略，「初始使用授權期間」可以是「每月」或「每年」。
- 根據您的行銷設定，啟動授權「自動更新」。

建立客戶

使用 Licensing Management Platform (LMP) 建立「客戶」。

步驟

1. 請填寫必要的資訊來建立「客戶」，包括：

a. 公司

b. 地址

c. 城市

d. 州和郵遞區號

e. 帳號名稱

f. 聯絡人姓名和電子郵件地址

2. 為了遵循最佳做法，請注意以下事項：
   - 您可以將「傳送帳號建立電子郵件」設為「建立客戶時立即傳送」。
   - 最後，由於已建立客戶，可以更容易指派服務方案。
   - 根據您將為建立的客戶部署的 Cloud Edge 設備數目而定，設定「每個使用授權的裝置數目」。

新增設備

建立服務方案和客戶後，您可以新增設備至 Cloud Edge 雲端主控台。

步驟

1. 在 Remote Manager 上，選取新客戶並啟動 Cloud Edge 雲端主控台。

   Cloud Edge 設備可以在這裡使用其產品序號進行註冊。

2. 為了遵循最佳做法，請注意以下事項：
   a. 建議您先在本機測試註冊新的設備，然後再將設備實際部署至客戶站點。

      這樣一來，如果有任何問題，就可以很容易地對註冊程序進行疑難排解。在測試完成後，您可以視需要取消註冊設備。

   b. 在將設備交付給最終客戶之前，請將設備重設為原廠預設值，以便可以在本機進行網路設定。

內部部署設備

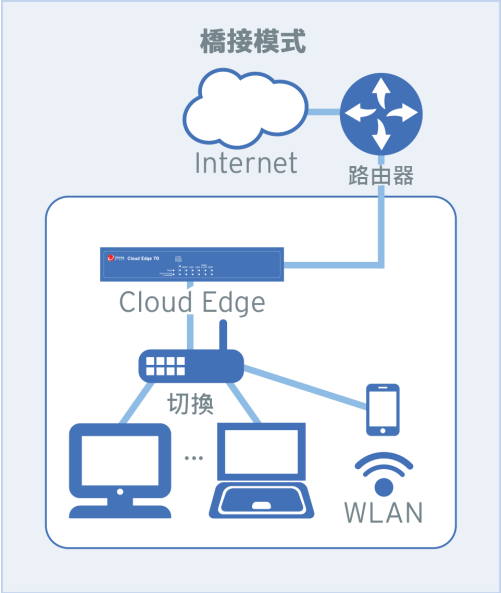
請參閱《快速使用卡片》，瞭解如何在客戶站點部署設備。

選擇部署模式的建議

您應留意下列「橋接模式」與「路由模式」的不同建議。

Cloud Edge 橋接模式

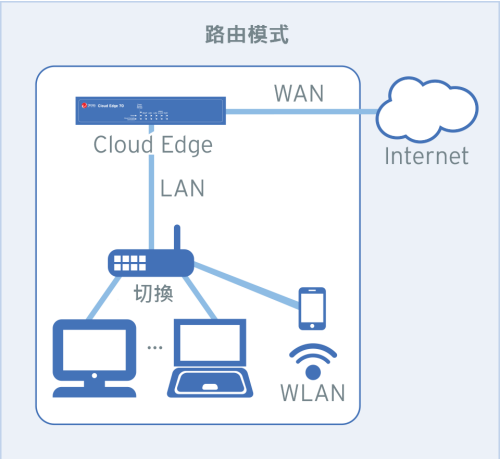
請儘可能選擇「橋接模式」。「橋接模式」部署通常適用於位於路由器後方以及交換器前方的私人網路。這可以透過切換 Cloud Edge 設備背面的實體交換器來設定。設備預設為「橋接」。「橋接模式」允許在不修改現有網路的情況下直接部署 Cloud Edge 設備。Cloud Edge 可帶來進一步的掃瞄和安全威脅防護。



Cloud Edge 路由模式

當您想要將 Cloud Edge 設備當成路由器，同時提供安全與安全威脅防護時，請設定「路由模式」。這款設備在網路中是可見的，用做具有安全掃瞄和控制功能的第 3 層路由裝置。在「路由模式」中，您通常會以 Cloud Edge 設備取

代網路上的現有路由器，或在路由器和交換器之間部署設備。在路由器和 Cloud Edge 設備上需要進行必要的組態設定變更。



使用快速設定

使用「快速設定」可在 Cloud Edge 設備上進行基本設定。

步驟

1. 在內部部署主控台中，移至「快速設定」頁面。
2. 為了遵循最佳做法，請注意以下事項：
   - 上行組態設定 - 請儘可能選擇「DHCP」；若不可用，請指定靜態 IPv4 位址和子網路，並在橋接器介面上設定 DNS。部署「路由模式」時，也可使用 PPPoE。
   - 「開始組態設定測試」應用來檢查設備是否可以存取 DNS 並連線至 Cloud Edge 雲端主控台。
   - 系統設定 - 建議使用「啟動 NTP 伺服器」以自動設定設備時鐘。

- 您可以使用 Cloud Edge 內部部署主控台，在「管理 > 裝置管理」頁面上找到「產品序號」。序號也位於 Cloud Edge 裝置的底部。
- 您可以使用內部部署主控台的「網路 > 服務」頁面，在介面上設定 DHCP 服務。

  建議為 LAN 介面啟動 DHCP 服務。

  注意

  註冊裝置後，就只能使用 Cloud Edge 雲端主控台編輯 LAN2、LAN3 和 MGMT 的 DHCP。
- 若要註冊設備，請存取 Cloud Edge 雲端主控台，然後移至「設備 > 註冊新設備」。

安全組態設定最佳做法

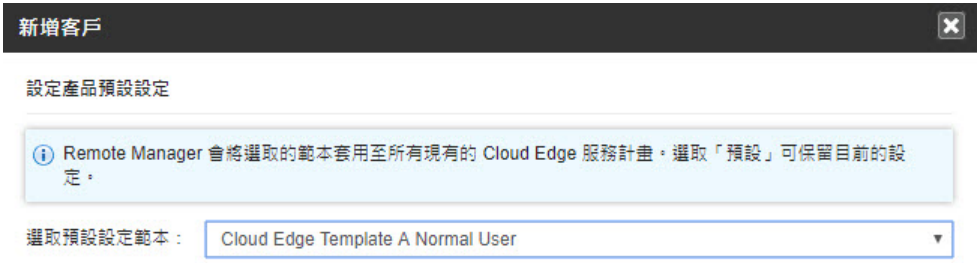
成功註冊後，可以從 Cloud Edge 雲端主控台集中管理和設定 Cloud Edge 設備，也可以使用 Trend Micro Remote Manager 設定與部署策略規則和安全資料檔，以提供多個設備間共用的通用安全設定。然後您可以為每個設備設定專屬的網路設定。

Remote Manager 安全範本

您可以使用 Cloud Edge 雲端主控台進行安全設定。

為了方便起見，Remote Manager 提供「預設設定範本」，其中包含您可以透過 Cloud Edge 雲端主控台進行的相同安全設定。Remote Manager 可讓您將這

些範本指派給設備，以成為與客戶公司關聯的預設設定。此方式可更輕鬆地確保客戶使用相同設定來部署其設備。



建立安全範本

您可以視需要建立其他安全範本。建立其他範本時，請將至少三種情況納入考量：

- Cloud Edge 範本 A - 一般使用者（預設範本）
- Cloud Edge 範本 B - 有安全考量的使用者
- Cloud Edge 範本 C — 效能最佳化使用者

步驟

1. 建立其他安全範本。
2. 移至預設範本頁面上的「設備」或 Cloud Edge 雲端主控台，視需要指派安全資料檔。

為一般使用者建立安全範本

安全資料檔 A — 一般使用者：您可以針對一般使用者使用預設安全範本。所有設定均保留預設值。這樣可以在安全性和效能之間維持最佳平衡。

步驟

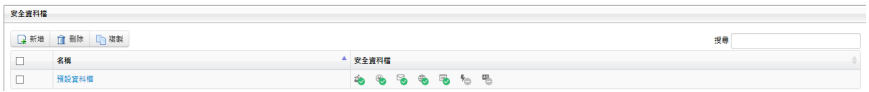
1. 執行適當的處理行動：
   - 在 Remote Manager 中，移至「管理 > 設定預設設定範本」。
   - 在 Cloud Edge 雲端主控台中，移至「策略 > 安全資料檔 > 預設資料檔」。
2. 確認所有值均為預設值。

為有安全考量的使用者建立範本

設備資料檔 B — 有安全考量的使用者：您可以在安全為主要目標時使用此安全範本。系統會更深入檢查並封鎖潛在的惡意流量，以提升安全性。

步驟

1. 執行適當的處理行動：
   - 在 Remote Manager 中，移至「管理 > 設定預設設定範本」。
   - 登入 Cloud Edge 雲端主控台。
2. 在「策略 > 安全資料檔 > 預設資料檔」中啟動下列設定。



a. IPS：

   i. 將 IPS 處理行動從「監控」變更為「封鎖」。

   ii. 「啟動進階設定」，然後使用「規則過濾器」將「嚴重性等級下限」設為「4 – 高」。

   這麼做將會封鎖嚴重性為「4 – 高」和「5 – 嚴重」的 IPS 偵測。

b. 惡意程式防護：除了「啟動 雲端截毒掃瞄」，也要執行「啟動 啟動 Machine Learning」。

   這麼做可運用雲端中的雲端截毒掃瞄即時簽章伺服器。

c. 電子郵件安全：

   i. 「啟動沙盒虛擬平台」以利用雲端沙箱分析可疑的檔案（需要授權）。

   ii. 「啟動 Machine Learning」以利用 AI 偵測先前未知的安全威脅；另外也將「處理行動」從「監控」變更為「封鎖」或「新增標籤」。

   iii. 開啟「標記含有已加密附件的電子郵件」以通知使用者無法掃瞄附件。

   iv. 在「垃圾郵件防護」下方，「啟動電子郵件信譽評等服務」以及「啟動商務電子郵件入侵 (BEC)」。

d. 網頁信譽評等：選擇「中」做為敏感度等級。

e. HTTPS：開啟 HTTPS 掃瞄，並取消勾選「例外」清單下方的「所有 URL 類別」。

3. 請記得儲存並部署設備資料檔。

4. 為提升安全性，您可以定義其他「策略規則」，以在防火牆層級封鎖不想要的應用程式或 URL 類別。

   - 在「Remote Manager 安全範本」畫面上，移至「策略 > 策略規則」。
   - 在 Cloud Edge 雲端主控台中，移至「策略 > 策略規則」。

a. 新增名為“封鎖 Internet 安全 URL” 的「策略規則」。

在「流量類型」下方，選取「選取的應用程式/URL 類別 > URL 類別 > Internet 安全」，然後將「處理行動」設為「封鎖」。

b. 新增名為“封鎖遊戲應用程式”的「策略規則」。

在「流量類型」下方，選取「選取的應用程式/URL 類別 > 應用程式 > 遊戲」，然後將「處理行動」設為「封鎖」。

c. 新增的策略規則應在「“預設策略規則”」之前。

結果可能看起來如下：

5. 在「設備 > <選取的設備>」下方，設定網路存取控制。

- WFBSS 端點防護：在客戶同時使用 Worry Free Business Security Services 時啟動

此功能會在不合規的裝置上封鎖 Internet 存取。

a. 由於此功能預設為關閉，請開啟功能。

b. 針對兩項條件選擇「封鎖」：

- 沒有代理程式的用戶端
- 具有代理程式且使用過時病毒碼的用戶端

c. 在「防護清單」下方，新增網路的 IP 位址集區。

這可確保系統封鎖來自網路上未知裝置的流量。

d. 在「例外清單」下方，新增無法安裝 Worry Free Services Security Agent 之裝置的 IP 位址。

e. 按一下「套用」。

- 可疑端點：設定「可疑端點」，以便為其上偵測到 C&C 回呼超過所設閾值的端點提供網路存取控制
  a. 由於此功能預設為關閉，請開啟功能。
  b. 使用預設閾值，即 1 小時內有 50 個 C&C 回呼事件。
  c. 將處理行動設為「封鎖」。
  d. 按一下「套用」。

為效能最佳化使用者建立安全範本

安全資料檔 C — 效能最佳化使用者：您可以在效能為主要目標時使用此安全範本。此資料檔會使用各種方法來加快指定使用者和群組的傳輸流量。

步驟

1. 執行適當的處理行動：
   - 在 Remote Manager 中，移至「管理 > 設定預設設定範本」。
   - 在 Cloud Edge 雲端主控台中，移至「策略 > 策略規則」。
2. 設定下列設定：
   - 新增名為「略過受信任來源」的「策略規則」— 為受信任的 IP 位址或使用者/群組定義特定策略「來源」，並將「處理行動」設為「略過」，系統即會略過對這些來源的流量進行安全威脅掃瞄。
   - 或者，請為區域對區域網路流量設定略過策略規則。
   - HTTPS — 在「安全資料檔」下方，將 HTTPS 掃瞄保留為預設「關閉」設定。
3. 您也可以設定設備特定的頻寬控制規則，此規則可用來排定重要和非重要應用程序之間流量的優先順序。

   此功能必須從 Cloud Edge 雲端主控台設定。

   為選取的應用程式群組和/或網路服務建立特定頻寬控制規則。當您想為某些要求速度的應用程式配置最小頻寬時，請以「保證頻寬」指定規則；反

之，以「最大化頻寬」指定規則可限制需要大量頻寬的應用程式佔用所有頻寬，而導致其他應用程式無法使用頻寬。

其他最佳做法

部署 Cloud Edge 設備時，您應留意下列建議事項。

監控 Cloud Edge 設備

您可以使用「資訊中心」和「分析與報告」監控 Cloud Edge 活動並檢視安全威脅分析。

使用資訊中心

使用資訊中心監控 Cloud Edge 活動時，請注意下列事項：

在 Cloud Edge 雲端主控台的「資訊中心」頁面上，您可以一覽「安全狀態」和「流量狀態」。

使用分析與報告

在 Cloud Edge 雲端主控台的「分析與報告」頁面中，您可以檢視預先定義的記錄檔統計資料，或設定您自己的查詢並儲存為我的最愛。

排程報告也可以定義為依照每日、每週或每月的間隔執行。透過電子郵件傳送報告通知是相當省時的功能，當您開始新的一天、新的一週或需要產生月結報告進行管理時，摘要報告就已經在收件匣中可供使用。

對管理工作進行管理

對管理工作進行管理時，您應留意下列建議事項。

建立使用者帳號

使用 Cloud Edge 雲端主控台建立使用者帳號時，請注意下列事項。

步驟

1. 移至「管理 > 使用者與帳號」。
2. 為需要存取 Cloud Edge 雲端主控台來檢視記錄檔和報告，但不需要修改組態設定權限的使用者建立「唯讀」帳號。

對管理員警訊進行管理

在對管理警訊進行管理時，請注意下列事項：

步驟

- 透過 Cloud Edge 雲端主控台設定管理員警訊。
- 移至「管理 > 管理員警訊」，並將「啟動」設為「開啟」。
- 設定下列警訊類型：
  - 選取：「C&C 回呼」在 [1 小時] 內發生 [50] 次事件
  - 選取：「設備狀態變更」與「郵件安全狀態變更」
- 登入 Remote Manager 並移至「管理 > 設定通知」，以使用可調整的「警訊閾值」微調「事件通知」設定。

設定排程更新

設定排程更新時，請注意下列事項：

步驟

- 一般來說，「每日一次」元件（病毒碼/引擎）更新設定即已足夠。不過，在惡意程式爆發期間，您可以將更新期變更為「每小時一次」。
- 建議每週進行一次韌體更新；請選擇預設值，或將更新設在下班時間執行。

設定管理存取權

設定管理存取權時，請注意下列事項：

步驟

- 請透過 Cloud Edge 雲端主控台設定不同類型的管理服務。

- 移至「設備 > <選取設備> > 管理存取權」，然後使用內部部署主控台、Ping 或 SSH 指定需要存取 Cloud Edge 設備的 IP 範圍或 IP 位址。

憑證管理

管理憑證時，請注意下列事項：

步驟

- 請移至「管理 > 憑證管理」來管理 Cloud Edge 憑證。
- 匯入您自己的憑證，或匯出 Cloud Edge 用來解密 SSL 流量的憑證，然後將匯出的憑證安裝到終端使用者的受信任憑證存放區。

  這有助於終端使用者避免在存取 HTTPS 網站時收到瀏覽器上顯示的憑證警告。

第 3 章

入門

入門工作

以下程序說明開始使用 Remote Manager 和 Cloud Edge 雲端主控台的必要步驟。完成這些步驟後，將 Cloud Edge 內部部署設備提供給客戶。客戶必須根據其網路環境來進行網路設定。

秘訣

您可以使用 Licensing Management Platform (LMP) 管理服務方案和公司。您可以直接存取 LMP，或透過 Trend Micro Remote Manager 以單一登入 (SSO) 的方式登入 LMP。趨勢科技建議您透過 Remote Manager 存取 LMP，以便更好地存取每日監控和其他資源。

步驟

1. 直接或透過 Remote Manager 存取 LMP。

   請參閱存取 LMP 第 4-3 頁。

2. 建立服務方案。

   請參閱建立服務方案 第 4-4 頁。

3. 建立公司並指派服務方案。

   請參閱建立公司並指派服務方案 第 4-5 頁。

4. 透過 Remote Manager 檢視 Cloud Edge 雲端主控台 Widget。

   請參閱每日監控 第 5-8 頁。

   登入後會顯示「入門」畫面。此畫面可協助您瀏覽 Cloud Edge 雲端主控台和註冊設備。

   請參閱入門畫面 第 6-3 頁。

5. 註冊 Cloud Edge 雲端主控台將管理的所有設備。

   請參閱註冊設備 第 7-38 頁。

6. 選擇性地建立使用者帳號，以存取 Cloud Edge 雲端主控台。

請參閱新增雲端主控台管理員帳號 第 6-176 頁。

7. 開始管理已註冊的設備。

   將 Cloud Edge 內部部署設備提供給客戶後，客戶必須根據您為其網路選取的部署模式進行一些部署設定。

部署工作

下列程序說明設定 Cloud Edge 設備的所有強制和選用步驟。

步驟

1. 決定部署 Cloud Edge 設備要採用哪種模式。

   請參閱部署模式 第 7-2 頁。

2. 根據選取的部署模式切換部署開關。部署開關位於 Cloud Edge 設備背面。

   注意

   將部署開關切換至「橋接」：

   - 針對「軟體切換」部署
   - 針對採用硬體切換晶片組之 Cloud Edge 設備的「橋接模式」部署

3. 收集預先部署檢查清單中列出的資料。

   請參閱預先部署檢查清單 第 7-16 頁。

4. 執行安裝與初始組態設定。

   請參閱執行初始組態設定 第 7-21 頁。

   本步驟包括以下子步驟：

   a. 設定硬體 第 7-19 頁（包含架設網路線）。

b. 透過 MGMT 通訊埠登入內部部署主控台 第 7-21 頁。

c. 執行初始組態設定 第 7-21 頁（包含適用於「橋接模式」、「橋接模式」（採用切換晶片組）、「軟體切換」和「路由模式」的程序）。

   對於具有無線功能的 Cloud Edge 設備，包含適用於「路由模式」的程序。

d. 註冊設備 第 7-38 頁（若尚未註冊）。

e. 執行其他組態設定 第 7-40 頁（選用）。

第 4 章

Licensing Management Platform

Trend Micro™ Licensing Management Platform™

Trend Micro™ Licensing Management Platform™ 可讓服務提供者和其他合作夥伴輕鬆管理及核發趨勢科技產品的使用授權。其中包含可供您用於自訂平台的品牌設定。

Trend Micro Licensing Management Platform 提供利用不同授權詳細資料來使用服務方案的彈性，讓您可以滿足客戶的需求。您可以為客戶建立公司帳號，然後指派服務方案給這些公司帳號。

功能和優點

您可以使用 Licensing Management Platform 自訂產品供應項目與服務。以下是部分主要功能：

表 4-1. 主要功能

功能	詳細資料
服務方案	設定服務方案，為客戶建立產品授權條款。
客戶帳號	為客戶設定公司帳號，並將服務方案加入公司帳號。
使用授權資訊	檢視和管理客戶購買的使用授權。
自訂的通知電子郵件	為客戶設定不同的通知電子郵件。
建立授權碼	產生使用授權，並將使用授權指派給服務方案。
品牌設定	依照您的企業宗旨，自訂品牌設定。包括聯絡資訊、登入頁面以及平台上可見的橫幅。

若要進一步瞭解如何透過 LMP 管理您的客戶、服務方案和使用授權，請參閱支援文件，網址如下：

http://docs.trendmicro.com/zh-tw/smb/trend-micro-licensing-management-platform.aspx

存取 Licensing Management Platform

您可以使用 Licensing Management Platform (LMP) 管理服務方案和公司。您可以直接存取 LMP，或透過 Trend Micro Remote Manager 以單一登入 (SSO) 的方式登入 LMP。趨勢科技建議您透過 Remote Manager 存取 LMP，以便更好地存取每日監控和其他資源。

步驟

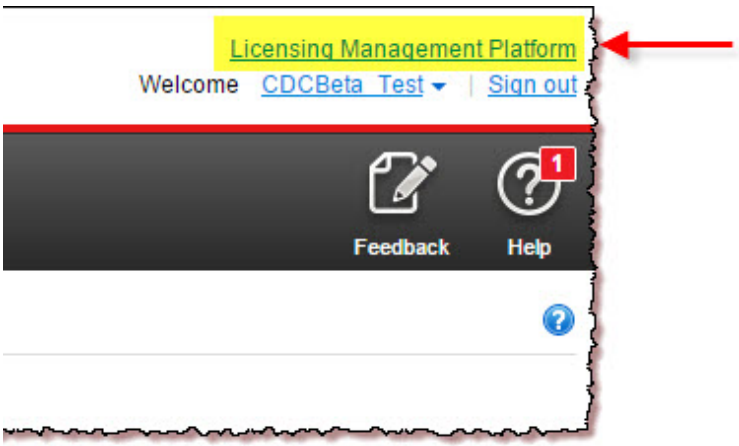
- 直接存取 LMP。

  每個管理服務提供者都有專屬的 LMP URL。趨勢科技會在您建立 LMP 帳號後以電子郵件訊息提供 URL。

- 透過 Remote Manager 以單一登入方式登入 LMP。

  a. 登入 Remote Manager。

  b. 按一下右上角的 Licensing Management Platform。



LMP 資訊中心隨即出現。按一下右上角的 Trend Micro Remote Manager 即可返回 Remote Manager。

注意

若要進一步瞭解如何透過 LMP 管理您的客戶、服務方案和使用授權，請參閱支援文件，網址如下：

http://docs.trendmicro.com/zh-tw/smb/trend-micro-licensing-management-platform.aspx

建立服務方案

使用服務方案可將使用授權核發給客戶，並針對您的產品/服務和客戶設定不同的授權方案。您必須使用 Licensing Management Platform (LMP) 建立服務方案。

步驟

1. 透過 Remote Manager 以單一登入方式登入 LMP。
2. 移至「使用者與使用授權 > 服務方案」。
3. 按一下「建立服務方案」。
4. 指定服務方案設定。

選項	說明
服務方案名稱	指定顯示在 LMP 和 Remote Manager 中的服務方案名稱。
產品/服務	選取相關的 Cloud Edge 產品或服務。 使用授權類型包括 Cloud Edge 設備型號、Cloud Edge 沙盒虛擬平台和 Cloud Edge 記錄檔轉送服務的使用授權。
版本類型	選取「試用版」或「完整版」。
試用表單	選擇性地啟動此服務方案的試用表單。
單位	選取「授權數目」。
資料中心	選取客戶所在的國家/地區。

選項	說明
啟動策略	設定服務方案啟動的時間。
管理產品/服務	選取此選項以允許 Remote Manager 控制 Cloud Edge。 重要 Remote Manager 需要此設定才能管理 Cloud Edge。

5. 指定產品授權策略設定。

選項	說明
初始使用授權期間	設定產品授權有效的初始期間。過了這段期間，必須續約產品授權，否則將會到期。
自動續約	選取此項來自動續約產品授權。
到期通知	選取在產品授權到期前多少天會向客戶傳送到期通知。 當您按一下「使用者與使用授權 > 客戶」並按一下客戶時，就可在表格中看到使用授權狀態。

6. 按一下「確定」。
7. 在確認訊息中，按一下「是」。

建立公司並指派服務方案

步驟

1. 透過 Remote Manager 以單一登入方式登入 LMP。
2. 移至「使用者與使用授權 > 客戶」。
3. 按一下「建立客戶」。
4. 指定「公司資料檔」資訊。

選項	說明
公司和地址	指定客戶的公司名稱以及選擇性地指定客戶地址。
城市、州和郵遞區號	指定客戶的城市、州和郵遞區號。
國家/地區	選取客戶的國家。
注意	選擇性地輸入附註。

5. 指定使用者帳號資訊。

選項	說明
帳號名稱	指定您客戶的帳號名稱。
使用者角色	設為「管理員」（無法設定）。
聯絡人	指定聯絡人的姓名。
電子郵件信箱	指定帳號的電子郵件信箱。
時區	選取客戶的時區。
語言	選取要 Cloud Edge 雲端主控台顯示以及客戶接收報告和通知的偏好語言。
傳送帳號建立電子郵件	選取傳送帳號建立電子郵件訊息給客戶的時間。

6. 按一下「指派服務方案」。
7. 選取在建立服務方案 第 4-4 頁中建立的一或多個服務方案。
8. 針對每個選取的服務方案，選取「使用授權開始日期」。
9. 針對每個選取的服務方案，將「每個使用授權的裝置數目」設為您產品使用授權允許的授權數目上限。
10. 按一下「儲存」。
11. 確認下列各項：
    - 公司已新增至「使用者與使用授權 > 客戶」的「客戶」清單中。

- 公司顯示正確的服務方案。

12. 按一下右上角的 Trend Micro Remote Manager 返回 Remote Manager。

第 5 章

Trend Micro Remote Manager

Trend Micro™ Remote Manager™

Trend Micro™ Remote Manager™ 是一個穩健的主控台，可以與 Trend Micro Licensing Management Platform™ 並行運作，為中小型企業提供受管理的安全服務。

Remote Manager 可讓您透過多種受管理的產品與服務監控多個受管理網路的健全狀況。Remote Manager 可讓經銷商管理員發出命令來管理重要的網路安全事宜。

Remote Manager 由經銷商取得帳號所在的區域性趨勢科技資料中心伺服器代管。經銷商可以使用 Remote Manager 來建立客戶帳號、監控客戶的網路，以及使用 Remote Manager Web 主控台來管理安全性。

Remote Manager 會監控下列產品：

- 趨勢科技 Cloud Edge
- Trend Micro Cloud App Security
- Trend Micro Hosted Email Security™
- Trend Micro InterScan Web Security as a Service (IWSaaS)
- Trend Micro Worry-Free Business Security™ Standard
- Trend Micro Worry-Free Business Security Advanced
- Trend Micro Worry-Free Business Security Services

Remote Manager 的監控資訊中心可讓經銷商透過下列 Widget 全盤掌握 Cloud Edge 網路安全的以下層面：

- 安全威脅最多的 Cloud Edge 裝置
- 安全威脅最多的 Cloud Edge 客戶

Remote Manager 提供多個 Widget，可彙整來自所有支援產品的資訊，包括勒索軟體偵測、安全威脅管理、最需要注意的客戶、使用授權管理與用量、受管理的客戶與產品，以及系統管理等相關資訊。

注意

如需有關 Cloud App Security、IWSaaS、Hosted Email Security、Worry-Free Business Security（所有版本）和 Cloud Edge 的詳細資訊，請參閱這些產品與服務的文件，網址為：http://docs.trendmicro.com/zh-tw/home.aspx。

Remote Manager 提供結構化方式來檢視客戶的網路，並可讓經銷商發出命令來管理網路安全的以下層面：

- 元件更新及受管理伺服器的更新
- 弱點評估
- 損害清除及復原
- 自動病毒爆發回應
- 防火牆和即時掃瞄設定
- 手動掃瞄
- 單一登入

Remote Manager 還支援廣泛的報告功能，並允許經銷商訂閱自動產生報告的單項功能。

設定預設設定範本

注意

只有當您已與 Licensing Management Platform 整合時，才有預設設定範本可用。

預設設定範本是指已針對客戶進行預先設定的範本。此方式可更輕鬆地確保客戶使用相同設定。

如需有關您可在此範本上進行哪些設定的詳細資訊，請參閱 Trend Micro Remote Manager 文件，網址為：

http://docs.trendmicro.com/zh-tw/smb/trend-micro-remote-manager.aspx

步驟

1. 登入 Remote Manager。
2. 移至「管理 > 設定預設設定範本」。

   「設定預設設定範本」畫面隨即開啟。「Cloud Edge」區段提供一份內含五個範本的清單。所有範本是一開始都是空的。在這份清單中，您可以建立五個範本，也可以編輯現有的範本。
3. 在「Cloud Edge」區段中，按一下其中一個尚未設定之範本旁的「建立」，即可建立新範本。

   或者，可以按一下「編輯」來修改已設定的範本。

   「建立範本」畫面隨即出現。

4. 指定範本名稱，並可選擇性地新增說明。說明有助於識別範本的用途。
5. 按一下「設定範本」。

   類似 Cloud Edge 雲端主控台的主控台隨即開啟，並在導覽列中顯示三個功能表：「策略」、「分析與報告」和「管理」

注意

對這個站台進行的任何變更均會以範本的形式儲存，不會影響任何已註冊的產品。

6. 設定相關策略與排程設定。

   您可以進行下列設定：

   - 策略

     規則、物件、核可/封鎖清單、設備資料檔、使用者通知

     注意

     在設定策略安全範本時，您無法設定及使用新的介面物件。您必須在範本部署完成後使用 Cloud Edge 雲端主控台來設定及使用策略規則的介面物件。

     您可以為策略規則範本設定新的安全資料檔區段。僅在 Cloud Edge 6.0 和更新版本的設備上，安全資料檔設定才會起作用。

   - 分析與報告

     報告、摘要報告

   - 管理

     網頁驗證入口網站、稽核記錄、排程更新和管理員警訊

   如需瞭解策略設定，請參閱線上說明，網址為：

   http://docs.trendmicro.com/zh-tw/smb/cloud-edge.aspx

建立公司並指派服務方案

本程序說明如何透過 Remote Manager 建立公司並指派服務方案。您必須使用 Licensing Management Platform (LMP) 建立服務方案。如需使用 LMP 的指示，請參閱建立公司並指派服務方案 第 4-5 頁。

步驟

1. 登入 Remote Manager。
2. 移至「客戶」。
3. 按一下「新增客戶」。
4. 指定公司資料檔資訊。

選項	說明
公司名稱和地址	指定客戶的公司名稱以及選擇性地指定客戶地址。
城市、州/省和郵遞區號	指定客戶的城市、州/省和郵遞區號。
國家	選取客戶的國家。

5. 指定使用者帳號資訊。

選項	說明
帳號 ID	指定您客戶的帳號 ID。
聯絡人	指定聯絡人的姓名。
聯絡號碼	指定區碼、電話號碼和選用的分機號碼。
電子郵件	指定帳號的電子郵件信箱。
時區	選取客戶的時區。
語言	選取要 Cloud Edge 雲端主控台顯示以及客戶接收報告和通知的偏好語言。

6. 按「下一步」。
7. 選取「服務方案」。

注意

您無法透過 Remote Manager 建立服務方案。若要建立服務方案，請直接存取 LMP，或透過 Remote Manager 以單一登入方式登入 LMP。如需詳細資料，請參閱建立服務方案 第 4-4 頁。

8. 按一下行事曆來選取開始日期。
9. 將「使用授權」設為您產品使用授權允許的裝置上限。
10. 按一下「新增裝置」以指定裝置名稱和產品序號。
11. 按「下一步」。

    「設定產品預設設定」視窗隨即出現。
12. 選取先前建立的策略範本。

    如需詳細資訊，請參閱設定預設設定範本 第 5-3 頁。
13. 在「備註」中選擇性地輸入所選範本的相關資訊。
14. 按一下「儲存」。
15. 確認下列各項：
    - 公司已新增至「客戶」的「客戶」清單中。
    - 公司顯示正確的服務方案。

對 Cloud Edge 雲端主控台使用 SSO

此程序說明如何透過 Remote Manager 單一登入 (SSO) Cloud Edge 雲端主控台。

步驟

1. 登入 Remote Manager。
2. 移至「客戶」。
3. 按一下客戶的名稱。

   預設會出現「產品」標籤。
4. 選取「所有產品」。

5. 按一下出現的產品名稱。
6. 按一下 Cloud Edge 服務方案名稱。

Cloud Edge 雲端主控台隨即出現。

每日監控

步驟

1. 登入 Remote Manager。

   Remote Manager 資訊中心會顯示在「首頁」畫面。
2. 將 Cloud Edge Widget 新增到資訊中心。
   a. 選取適當的標籤。
   b. 按一下「新增 Widget」。
   c. 選取 Cloud Edge Widget。
      - 安全威脅最多的 Cloud Edge 裝置

- 安全威脅最多的 Cloud Edge 客戶

d. 按一下「新增」。

3. 檢視 Cloud Edge Widget。
   - 「具有最多安全威脅的 Cloud Edge 裝置」Widget 第 5-11 頁
   - 「具有最多安全威脅的 Cloud Edge 客戶」Widget 第 5-13 頁
4. 選擇性地以單一登入方式登入 Cloud Edge 雲端主控台。

   請參閱使用 SSO 登入雲端主控台 第 5-7 頁。

報告總覽

Cloud Edge 可讓您產生、下載及自動傳送報告。報告提供您客戶網路中的使用授權狀態、評估結果、安全威脅事件、主要安全威脅及受影響最大的電腦、檔案和電子郵件信箱的總覽。

報告包含許多由 Remote Manager 管理之受支援趨勢科技產品提供的統計資料。設定報告資料檔，以及特定日期範圍內的一次性與週期性報告，然後將報告傳送給多個電子郵件收件者。Remote Manager 會儲存 30 份最近的每日報

告、10 份最近的每週報告，以及 5 份最近的每月報告。一般報告適用於經銷商與客戶。

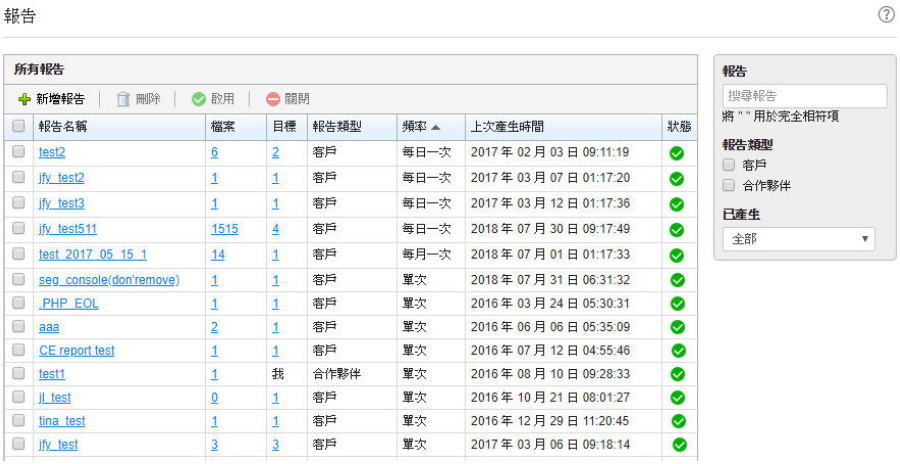


圖 5-1. 報告頁面

報告資料檔可讓您從單一資料檔建立多份報告。例如，今天建立並產生一次性報告，明天變更部分選項並重新產生報告，而不用重新建立整份報告。

如需有關 Remote Manager 報告的詳細資訊，請檢閱 Remote Manager 線上說明：

http://docs.trendmicro.com/zh-tw/smb/trend-micro-remote-manager.aspx

「具有最多安全威脅的 Cloud Edge 裝置」Widget

顯示遭遇最多安全威脅事件的 Cloud Edge 裝置。

- 您可以選取以下選項來變更要顯示哪個時間範圍的資料：
  - 最近 1 小時
  - 最近 24 小時
  - 最近 7 天
  - 最近 30 天（預設值）
- 您可以選取以下選項來變更要顯示何種安全威脅類型的資料：
  - 全部
  - 殭屍網路
  - 入侵防護系統 (IPS)
  - 垃圾郵件
  - 網頁信譽評等

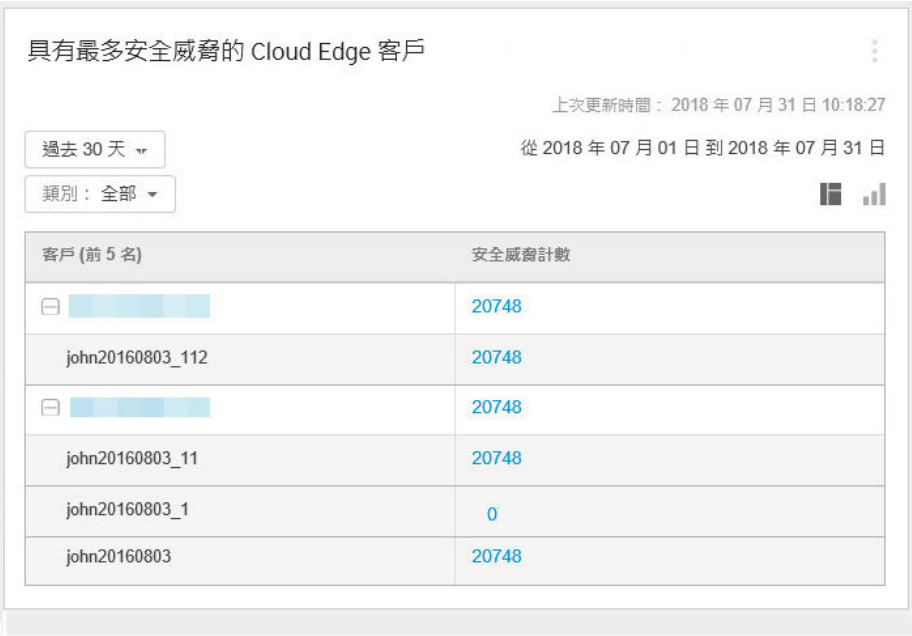
  - 病毒
  - 勒索軟體
  - C&C
- 按一下客戶名稱即可檢視客戶資訊。
- 按一下安全威脅計數，即可從 Cloud Edge 雲端主控台開啟安全威脅資訊。

注意

Cloud Edge Widget 預設不會出現在 Remote Manager 資訊中心。

「具有最多安全威脅的 Cloud Edge 客戶」Widget

顯示遭遇最多安全威脅事件的 Cloud Edge 客戶。資料以資料表和圓餅圖顯示。您可以透過按一下顯示圖示（ ）在資料表和圓餅圖之間切換。



- 您可以選取以下選項來變更要顯示哪個時間範圍的資料：
  - 最近 1 小時
  - 最近 24 小時
  - 最近 7 天
  - 最近 30 天（預設值）
- 您可以選取以下選項來變更要顯示何種安全威脅類型的資料：

  - 全部
  - 殭屍網路
  - 入侵防護系統 (IPS)
  - 垃圾郵件
  - 網頁信譽評等
  - 病毒
  - 勒索軟體
  - C&C
- 按一下客戶名稱即可檢視客戶資訊。
- 按一下安全威脅計數，即可從 Cloud Edge 雲端主控台開啟安全威脅資訊。

注意

Cloud Edge Widget 預設不會出現在 Remote Manager 資訊中心。

管理設備裝置

透過 Remote Manager 的「客戶」畫面管理您的設備裝置。選擇服務方案後，管理您的設備裝置，以便執行以下動作：

- 檢視最近的設備事件
- 立即更新設備裝置的韌體
- 註冊其他設備裝置給客戶

步驟

1. 登入 Remote Manager。

   Remote Manager 資訊中心會顯示在「首頁」畫面。

2. 按一下「客戶」。
3. 在「公司」欄，選取客戶的名稱。
4. 從左瀏覽窗格展開「所有產品」，然後選取服務方案。
5. 執行下列動作：

選項	說明
檢視違規和系統事件	按一下「事件」標籤。
更新韌體	按一下「韌體更新」標籤，選取已過期或無法更新的裝置，然後按一下「更新」。 按一下「更新」後，適用於所選設備裝置的更新會立即執行。
註冊其他設備	按一下「裝置」標籤，然後按一下「註冊」。

6. 執行其他設備工作。
   a. 從左瀏覽窗格選取任何已註冊的設備裝置。
   b. 按一下「事件」標籤，即可檢視過去一小時內的違規與系統事件。
   c. 按一下「元件」標籤，即可檢視每項產品元件的目前版本與最新版本。
   d. 按一下「網路」標籤，即可檢視過去 24 小時內最新的使用者活動。
   e. 按一下「VPN」標籤，即可檢視最近的 VPN 活動。

   注意

   對於不支援 VPN 的 Cloud Edge 設備型號，您無法檢視該型號的 VPN 相關資訊。

瞭解更多有關 Remote Manager 的資訊

如需有關 Remote Manager 的詳細資訊，請參閱線上說明，網址為：

http://docs.trendmicro.com/zh-tw/smb/trend-micro-remote-manager.aspx

第 6 章

Cloud Edge 雲端主控台

本章說明如何使用 Cloud Edge 雲端主控台來註冊及管理設備。

登入雲端主控台

直接登入 Cloud Edge 雲端主控台，或透過 Remote Manager 進行單一登入。

步驟

- 直接登入 Cloud Edge 雲端主控台。
  a. 移至趨勢科技提供的 Cloud Edge 雲端主控台 URL。
  b. 指定您的使用者名稱和密碼。

  注意

  直接登入 Cloud Edge 雲端主控台之前，您必須先從 Remote Manager 使用單一登入功能登入 Cloud Edge 雲端主控台，然後建立管理員帳號。

  請參閱新增雲端主控台管理員帳號 第 6-176 頁。

  如果無法存取 Cloud Edge 雲端主控台，請聯絡趨勢科技。

- 透過 Remote Manager 登入 Cloud Edge 雲端主控台。

  請參閱使用 SSO 登入雲端主控台 第 5-7 頁。

入門畫面

當您首次登入 Cloud Edge 雲端主控台時，會載入「資訊中心」並顯示「入門」畫面。

「入門」畫面整合了快速開始使用 Cloud Edge 雲端主控台所需的資訊。「入門」畫面還提供了 Cloud Edge 使用者協助的連結。

選取「不要再顯示此訊息」，這樣下次登入 Cloud Edge 雲端主控台時，即會隱藏「入門」畫面。

按一下「說明」旁的箭頭並選取「入門」，即可隨時顯示「入門」畫面。

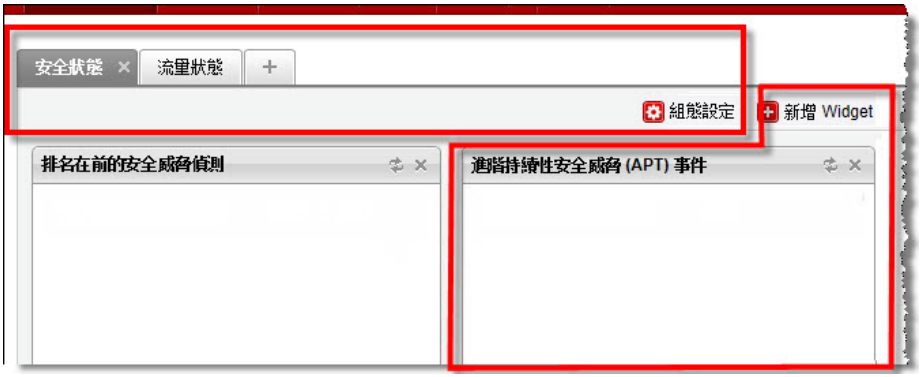
Cloud Edge 雲端主控台總覽

本節提供 Cloud Edge 雲端主控台功能的基本總覽。如需更詳細的資訊，請檢視 Cloud Edge 線上說明。

關於資訊中心

可從資訊中心透過多個 Widget 監控網路的完整性。每個使用者帳號都有獨立的資訊中心。對其中一個使用者帳號資訊中心進行的變更，不會影響其他使用者帳號資訊中心。

資訊中心由下列使用者介面項目組成：



關於設備

您可以在客戶所在位置部署 Cloud Edge 設備，然後向 Cloud Edge 雲端主控台註冊設備做為設備，以便透過雲端進行遠端管理。

在「設備」標籤上，您可以根據設備型號和部署模式執行下列作業：

- 檢視硬體與策略狀態資訊

- 檢視有關 CPU 溫度、CPU 使用率、磁碟分割區使用率及記憶體使用率的設備狀態
- 檢視設備網路事件、系統事件、VPN 事件和策略實施記錄檔
- 使用 Ping、Traceroute 和 ARP 等網路工具，疑難排解設備 IPv4 網路連線問題
- 設定當流量負載過高時，Cloud Edge 設備的處理方式
- 更新韌體或產品元件
- 設定及檢視網路資訊
- 為採用硬體切換晶片組的設備進行內部網路安全模式設定
- 為支援無線網路的設備進行無線網路存取控制設定並管理無線用戶端連線
- 進行使用者虛擬私人網路 (VPN) 設定以使用安全通訊端層 VPN (SSL VPN) 或第二層通道通訊協定 (L2TP) VPN
- 設定頻寬控制規則，以便將頻寬保留給支援商業目標的網路流量，藉以改善服務品質
- 設定 Site-to-Site VPN
- 設定靜態路由和 NAT
- 設定終端使用者管理
- 設定用於驗證的 LDAP 設定（日本地區不支援）
- 設定「WFBSS 端點防護」，這是個與 Worry Free Business Security Services (WFBSS) 整合的解決方案，可控制具有過期 WFBSS Security Agent 病毒碼的 WFBSS 端點或未安裝 WFBSS Security Agent 的端點是否可以存取 Internet
- 設定「可疑端點」，以便為 Cloud Edge 在其上偵測到 C&C 回呼超過所設閾值的端點提供網路存取控制
- 檢視 可疑端點 在您的網路中探索到的端點裝置和弱點的清單。
- 將 可疑端點 設定為掃瞄端點裝置是否存在弱點、弱式密碼和開放的通訊埠。

注意

對於不支援 VPN 的 Cloud Edge 設備型號，您無法設定或檢視該型號的 VPN 相關資訊。

關於記錄檔分析

在「分析與報告」標籤，您可以檢視 Cloud Edge 雲端主控台在收到已註冊的設備所上傳的記錄檔統計資料後，加以彙整而得的互動式圖表與圖形。您可以追蹤資訊中心可能不會顯示的詳細資訊，或向下切入來調查原始記錄檔。

- 應用程式頻寬

  跨網路上的 IP 位址、使用者和應用程式檢視及分析頻寬耗用量。檢閱記錄檔後，可調整策略來控制通訊、封鎖非必要流量，並將頻寬配置給重要的流量或服務。

  如果客戶僅使用執行 Cloud Edge 6.0 或更新版本的 Cloud Edge 50G2 設備，請檢視策略規則的使用情況資料。

- 策略實施

  檢視及分析策略如何控制網路流量。檢閱記錄檔後，可調整策略規則以允許或封鎖特定流量，以及疑難排解未正確設定的策略。

  「策略實施」內附下列事件：

  - 策略規則（應用程式控管、URL 過濾、防火牆）
  - 封鎖清單

- Internet 存取

  檢視及分析特定使用者瀏覽的網站和網域。檢閱記錄檔後，可新增 URL 類別群組來過濾特定類型的流量，並視需要在這些類別之外核可或封鎖特定 URL。

  如果客戶僅使用執行 Cloud Edge 6.0 或更新版本的 Cloud Edge 50G2 設備，請檢視策略規則的使用情況資料。

- Internet 安全

  檢視及分析掃瞄引擎如何保護使用者免遭惡意程式、網路安全威脅及其他潛在危害的侵擾。檢閱記錄檔後，可啟動或關閉安全功能並調整處理行動、排程時程或使用者策略，以更好地保護網路。

  「Internet 安全」內附下列事件：

  - 入侵防護
  - 惡意程式防護
  - 電子郵件安全防護
  - 網頁信譽評等
  - 殭屍網路偵測

設定對特定記錄檔的查詢後，按一下「儲存」並選取「⭐儲存為我的最愛」，可記錄這些設定以供稍後檢視。移至「分析與報告 > 我的最愛」以存取「我的最愛」畫面。

關於策略

在「策略」畫面中，您可以管理 Cloud Edge 雲端主控台策略規則、策略物件、核可清單和封鎖清單、安全資料檔、使用者通知，以及可疑物件清單和封鎖處理行動。Cloud Edge 雲端主控台可以對部分或所有已註冊的設備實施策略。

您可以建立策略物件來自訂策略規則適用的選項。這些策略物件包括要套用策略的介面群組、使用者/使用者群組、IP 位址/FQDN、MAC 位址或上網位置、策略所影響的服務類型、應用程式群組或 URL 群組類別，以及實施策略規則的時程。

您可以針對 IPS、惡意程式防護安全、網頁信譽評等、電子郵件安全、HTTPS 檢查、拒絕服務攻擊以及端點識別設定安全資料檔，藉以微調策略控制。您還可以選擇新增核可與封鎖的 URL 來覆寫已定義的策略規則。

關於報告

在「分析與報告」標籤中，您可以檢視和下載排程或隨選報告。Cloud Edge 雲端主控台會彙整來自所有已註冊設備的記錄檔資訊。從這些記錄檔中，您可以產生關於偵測到的病毒和惡意程式碼、封鎖的檔案以及瀏覽的 URL 的報告。您可以使用這些網路事件相關資訊最佳化設定，以及微調安全策略。

設備管理

MSP 會使用 Cloud Edge 雲端主控台來註冊新的 Cloud Edge 設備。客戶啟動 Cloud Edge 設備並連線到網路後，即會部署策略且 MSP 可檢視相關的資訊中心、記錄檔和報告統計資料。

管理設備

用途：從 Cloud Edge 雲端主控台管理設備。

位置：設備

步驟

1. 如果要從 Cloud Edge 雲端主控台管理設備，請執行下列作業：
   - 檢視已註冊設備的相關資訊。
   - 註冊新設備。
   - 匯入多個設備。
   - 建立新的設備群組。
   - 在搜尋方塊中搜尋 Cloud Edge 裝置。
   - 為所列出的設備選擇預設安全資料檔。

     如果設備屬於 HA 群組的成員，主要設備的安全資料檔將同時用於主要設備和次要設備。

- 對設備執行選取處理行動。

  > **注意**
  > 無法對屬於 HA 群組的設備執行特定處理行動。

  請參閱設備處理行動 第 6-11 頁。

- 按一下設備名稱以管理該設備。

  設備可以是標準/G3 設備或 Cloud Edge 50G2 設備。

  -  ：標準/G3 設備
  -  ：Cloud Edge 50G2 設備

    Cloud Edge 50G2 設備是執行於 Cloud Edge 6.0 和更新版本的第二代型號，硬體更加卓越，效能也更加優異。

  您可以從 Cloud Edge 雲端主控台中修改的設備和可用的管理工作，將視設備型號和部署模式而有所不同。

2. 管理 Cloud Edge 設備的「高可用性」組態設定。

   - 檢視現有 HA 群組的相關資訊。
   - 建立一或多個新 HA 群組。

     若要建立 HA 群組，必須具有至少兩台支援 HA 群組的設備。

   - 啟動 HA 群組。
   - 關閉 HA 群組。
     - 關閉後，兩台 Cloud Edge 設備彼此仍保持配對關係，因此無法使用其中任何一台設備建立新的 HA 群組。
     - 關閉 HA 群組後，終端使用者流量將中斷一段時間，實際時間視使用者的網路拓撲而定。
   - 編輯現有的 HA 群組。

- 對現有 HA 群組執行手動容錯移轉（強制接管）。
- 移除現有的 HA 群組。

注意

所有管理處理行動都會產生稽核記錄。

註冊

可以向 Cloud Edge 雲端主控台註冊的設備數目，視您與趨勢科技簽訂的維護合約而定。

在註冊設備後，按一下名稱以執行下列作業：

- 檢視有關設備的一般資訊
- 檢視有關設備系統狀態的資訊
- 使用 Ping、Traceroute 和 ARP 等網路工具，疑難排解設備 IPv4 網路連線問題
- 檢視設備網路事件、系統事件、VPN 事件和策略實施記錄檔
- 設定當流量負載過高時，Cloud Edge 設備的處理方式
- 設定網路設定
- 為採用硬體切換晶片組的設備進行內部網路安全模式設定
- 檢視支援無線網路之設備的無線網路設定
- 為支援無線網路的設備進行無線網路存取控制設定並管理無線用戶端連線
- 設定頻寬控制
- 設定使用者 VPN
- 設定 Site-to-Site VPN
- 設定終端使用者驗證和 TTL 快取設定

- 設定用於驗證的 LDAP 設定（日本地區不支援）
- 更新 Cloud Edge 設備
- 設定「WFBSS 端點防護」，這是個與 Worry Free Business Security Services (WFBSS) 整合的解決方案
- 設定「可疑端點」，以便為其上偵測到 C&C 回呼超過所設閾值的端點提供網路存取控制

注意

對於不支援 VPN 的 Cloud Edge 設備型號，您無法設定或檢視該型號的 VPN 相關資訊。

設備處理行動

處理行動	說明
	新增設備群組。
	變更設備所顯示的顯示名稱。
	將設備移到不同的設備群組。 無法移動 HA 群組中的設備。
	提供新的設備產品序號來取代設備硬體。 取代屬於 HA 群組的設備時，必須取代為與原始設備相同的型號。必須將原始設備已套用的修補程式套用至替換的設備。此外，還必須對替換的設備重新套用引擎/病毒碼更新。
	變更設備的內部部署主控台密碼。 對於屬於 HA 群組的設備，請分別變更每台設備的密碼。
	更新設備元件來持續防範最新安全威脅。
	遠端重新啟動設備。

處理行動	說明
	從 Cloud Edge 雲端主控台刪除設備。此設備仍會掃瞄內部部署是否有安全威脅，但無法接收遠端指令或更新。 無法刪除 HA 群組中的設備。

註冊設備

用途：註冊設備以透過 Cloud Edge 雲端主控台控制策略並檢視記錄檔統計資料。

位置：「設備」

步驟

1. 按一下「註冊新設備」。
2. 指定設備設定。
   - 顯示名稱

     指定新設備顯示在雲端主控台中的名稱。
   - 型號

     指定 Cloud Edge 設備硬體的型號。
   - 產品序號

     指定 Cloud Edge 設備的產品序號。產品序號位於設備本身或設備包裝上。產品序號由 12 位英數字元組成，並由連字號分隔（範例：4C80-9315-3A0B）。
3. 按一下「儲存」。

   註冊作業可能需要數分鐘才能完成。

在註冊之後，Cloud Edge 雲端主控台會將策略部署到設備。透過資訊中心 Widget、記錄檔分析，以及根據 Cloud Edge 設備傳送之即時流量產生的報告，檢視記錄檔統計資料。

匯入多個設備

用途：允許客戶上傳 CSV 檔案（採用指定格式）來註冊大量設備。

位置：「設備 > 設備管理」

步驟

1. 按一下「匯入設備」按鈕。
2. 在「匯入設備」快顯視窗中，從「型號」下拉式清單中選取設備型號。
3. 按一下「瀏覽」以瀏覽至您本機磁碟機上的 CSV 檔案（按一下「下載範本」可下載 .CSV 檔案）。

   注意

   在 .CSV 檔案中，客戶必須為每個設備填入以下 2 個值。每個設備一行。「設備名稱」欄位可以保留空白，系統會自動為這類設備產生名稱。自動產生的設備名稱範例為「Cloudedge_01」、「CloudEdge_02」。請勿刪除 CSV 檔案的標頭列。

4. 按一下「匯入」。

   在「設備管理」頁面上，匯入的設備會顯示在 Root 群組清單中。「匯入摘要」橫幅會顯示成功匯入的設備數目與匯入失敗的設備數目。按一下「修正錯誤」可在快顯視窗中檢視匯入失敗之設備的詳細資訊，在該視窗中顯示了失敗詳細資料。

5. 按一下「確定」或按一下「匯出錯誤」，即可將 .CSV 檔案匯出到本機磁碟機。

確認註冊

趨勢科技建議在註冊每個設備後都加以確認。下列程序說明如何使用 Cloud Edge 雲端主控台，確認您的設備已正確註冊。

步驟

1. 登入 Cloud Edge 雲端主控台。
2. 移至「設備」。
3. 確認設備出現在「設備管理」清單中。
4. 確認「策略部署狀態」欄中的狀態為「成功」。
5. 按一下設備名稱。
6. 檢查所出現「設備資訊」視窗中的設備資訊。

檢視全部設備的資訊

用途：檢視全部設備的設備資訊和 HA 群組資訊。

位置：「設備」

步驟

1. 檢視全部設備的資訊。
   - 群組/設備名稱：群組名稱或設備名稱。
   - 狀態：設備目前在 Cloud Edge 雲端主控台中的狀態。
   - 上次策略部署時間：最近一次從 Cloud Edge 雲端主控台部署策略到設備時的時間戳記。
   - 策略部署狀態：上次部署策略的結果。
   - 上次記錄檔上傳時間：最近一次從設備上傳記錄檔到 Cloud Edge 雲端主控台時的時間戳記。

- 安全資料檔：已套用至此設備的 Cloud Edge 安全資料檔。
- 處理行動：可用於此設備的處理行動。

  您無法移動或刪除 HA 群組中的設備。這些處理行動圖示不適用於屬於 HA 組的設備。

2. 檢視 HA 群組的相關資訊：
   - HA 名稱：每個 HA 群組的名稱。每個 HA 群組名稱下方會顯示兩台成員 Cloud Edge 設備的名稱。
   - 啟動：HA 群組的狀態是「開啟」或「關閉」。
   - HA 角色：角色可以是「主要」或「次要」。
   - 優先順序：列出主要設備和次要設備的優先順序。
   - 活動訊號介面：列出主要設備和次要設備的活動訊號介面。

     主要設備和次要設備的介面必須相同。
   - IPv4 位址/網路遮罩：列出主要和次要設備的 IPv4 位址和網路遮罩。
   - 版本：列出主要設備和次要設備的版本。

     在一般情況下，兩台設備的版本是一致的，但在升級期間可能短暫不同。
   - HA 狀態：主要設備和次要設備的狀態。

     可能的狀態包括：
   - 動作：列出您可以對 HA 群組執行的動作：編輯、移除、強制接管、啟動、關閉。

     若要執行動作，請按一下所需的動作。

建立 HA 群組

用途：從 Cloud Edge 雲端主控台建立 HA 群組。HA 群組由 2 台 Cloud Edge 設備組成。一台設備只能屬於一個 HA 群組。

位置：「設備」

步驟

1. 檢閱 HA 群組的相關資訊（如有需要）。

   HA 群組 第 6-20 頁

2. 在將成為 HA 群組成員之每台設備的活動訊號介面之間使用乙太網路纜線直接連接。

   對於 Cloud Edge 50G2 設備，只能使用 LAN2 或 LAN3 做為活動訊號 L3 介面。此外，每一台設備都必須使用相同的介面（LAN2 連接 LAN2，或 LAN3 連接 LAN3）。

3. 在「高可用性管理」區段中，按一下「建立 HA 群組」。

   「建立 HA 群組」精靈隨即開啟。

4. 在「建立 HA 群組並選擇作業模式」頁面中，指定下列詳細資料：

選項	說明
HA 群組名稱	名稱長度必須為 1 到 32 個字元，其中可以包含字母、數字或底線符號。
作業模式	預設為「主動-被動式」，這是唯一可用的模式。
驗證方法	選取下列其中一項： • 無 • 簡單，然後輸入用於簡單驗證的密碼。 • HMAC，然後輸入用於 HMAC 驗證的密碼。
啟動	選取下列其中一項： • 開啟 • 關閉

5. 按「下一步」。

6. 在「設定主要設備」頁面中，對將做為 HA 群組中主要設備的 Cloud Edge 設備進行設定。

選項	說明
主要 HA 設備	從下拉式清單中選取您要指定做為 HA 主要設備的設備。 此清單只會列出支援 HA 群組組態設定的設備。
角色	此唯讀欄位設定為「主要」，代表此角色會指派給這台設備。
優先順序	輸入這台設備的優先順序號碼 (1-253)。預設值為 253。 優先順序較高的設備將做為作用中設備。
活動訊號介面	從下拉式清單中選取 Cloud Edge 用於和對等 HA 設備進行通訊的 L3 介面。 對於 Cloud Edge 50G2 設備，只能選取 LAN2 或 LAN3 做為活動訊號介面。
活動訊號介面 IP/網路遮罩	如果尚未設定，則必須輸入活動訊號介面的 IPv4 位址和網路遮罩。 主要和次要設備的活動訊號介面的 IPv4 位址必須位於同一個子網路。 將介面新增到 HA 組後，即無法變更該介面的主要或次要設備。

7. 按「下一步」。
8. 在「設定次要設備」頁面中，對將做為 HA 群組中次要設備的 Cloud Edge 設備進行設定。

選項	說明
次要 HA 設備	從下拉式清單中選取您要指定做為 HA 次要設備的設備。 此清單只會列出支援 HA 群組組態設定的設備。
角色	此唯讀欄位設定為「次要」，代表此角色會指派給這台設備。

選項	說明
優先順序	輸入這台設備的優先順序號碼 (1-253)。預設值為 100。 優先順序較高的設備將做為作用中設備。
活動訊號介面	下拉式清單中會預先選取 L3 介面，這也是選取用於主要 HA 設備的相同介面。 Cloud Edge 會使用此介面來與對等 HA 設備進行通訊。
活動訊號介面 IP/網路遮罩	如果尚未設定，則必須輸入活動訊號介面的 IPv4 位址和網路遮罩。必須與為主要設備設定的活動訊號 IP 位址位於同一個子網路。

9. 按「下一步」。
10. 在「設定發生失敗時的接管」頁面中，設定 Cloud Edge HA 群組在發生失敗時進行接管的設定。

選項	說明
先佔	選取下列其中一項： • 開啟（預設值）：主要設備從上次失敗中恢復後，會回復為作用中角色。 • 關閉：主要設備從失敗中恢復後，不會自動重返作用中角色。使用者必須手動執行容錯移轉。
監控介面	選取一或多個要監控的介面。Cloud Edge 僅會監控實體介面。建議監控所有實體介面的流量。
監控 IP/FQDN	對於每個監控介面，請輸入最多兩個用做監控主機的 IP 位址或 FQDN。

選項	說明
接管觸發條件	輸入下列各項的值： • 活動訊號失敗次數：表示被動式設備接管故障設備前的活動訊號失敗次數（預設值為 3，有效值為 3 到 9） • Ping 失敗次數：表示被動式設備接管故障設備前的 ping 失敗次數（預設值為 3，有效值為 1 到 5）

11. 在「設定 Virtual Router Redundancy Protocol (VRRP) 群組」頁面中，新增一或多個 VRRP 群組。

    a. 按一下「新增」。

    b. 為 VRRP 群組選取一個介面並輸入虛擬 IPv4 位址和網路遮罩。

    可以選取 L3 實體介面或靜態 L3 VLAN 介面，視組態設定而定。

    如需組態設定需求，請參閱 HA 群組 — VRRP 群組 第 6-25 頁。

    c. 按一下「IP 位址/遮罩」欄位右側的核取記號，可儲存 VRRP 群組。

    必須新增並儲存至少一個 VRRP 群組，然後按「下一步」。

    注意

    按一下想要刪除的 VRRP 群組右側的 "X"，即可刪除該 VRRP 群組。

    按「下一步」後，「摘要」頁面隨即開啟。

12. 檢閱 HA 群組設定的摘要。

    注意

    首次建立 HA 群組時，主要 HA 設備會做為作用中設備，次要 HA 設備則做為被動式設備。

13. 按一下「儲存」。

HA 群組

您可以將兩台設備設定為一個 HA 群組，以提供高可用性存取。其中一台設備設定為主要設備，另一台則設定為次要設備。首次建立 HA 群組時，主要設備將做為作用中設備，次要設備則做為被動式設備。當某一台設備故障時，另一台設備就會進行接管（成為作用中），以確保網路流量不會中斷。

HA 群組除了能夠提高網路流量效率外，還可在發生嚴重錯誤時提供備援。

基本資訊

- 您可以使用已註冊或未註冊的設備來建立 HA 群組。
  - 未註冊：

    Cloud Edge 雲端主控台只會檢查選擇用於 HA 群組之每台設備的硬體型號。如果硬體型號不符要求，系統會顯示錯誤，並且不會儲存 HA 群組。
  - 已註冊：

    Cloud Edge 雲端主控台會執行下列檢查：
    - 檢查每台設備的硬體型號、軟體版本和部署模式 — 若有任何一項不符要求，系統會顯示錯誤，並且不會儲存 HA 群組。
    - 檢查活動訊號介面 — 如果不是位於同一個子網路，則會顯示錯誤，並且不會儲存 HA 群組。
    - 檢查 VRRP 介面 — 如果不是位於同一個子網路，則會顯示錯誤，並且不會儲存 HA 群組。
    - 檢查設備是否皆已上線 — 全部兩台 Cloud Edge 設備都必須上線，才能成功儲存 HA 群組。
- 一台設備只能屬於一個 HA 群組。
- 僅支援「主動-被動式」模式。
- 系統會將作用中節點指派為主要設備。
- HA 群組可在先佔模式或非先佔模式下運作

  - 先佔（核取方塊，預設值）：主要設備從上次失敗中恢復後，會回復為作用中角色。
  - 非先佔：主要設備從失敗中恢復後，不會自動重返作用中角色。使用者必須手動執行容錯移轉。
- 建立 HA 群組之前，請確認已為下列項目設定位址
  - HA 群組中的設備必須以路由模式部署。
  - HA 群組中的設備必須屬於同一型號。
  - HA 群組中的設備必須具有相同的韌體版本。

    注意

    當 HA 群組中的一個設備更新或還原韌體版本，HA 群組中的其他設備也必須更新或還原至相同的版本。
  - HA 群組中的設備必須具有相同的時區組態設定，而且時差必須在 5 分鐘內。
  - 建立 HA 群組之前，必須先設定設備的原廠預設介面設定。
- Cloud Edge 雲端主控台會將 HA 群組中設備的組態設定推送至設備；但是當無法進行組態設定更新時，HA 群組中的節點會使用活動訊號連線來進行同步處理。
- 在資訊中心中，支援顯示主要設備、次要設備和 HA 群組的記錄檔、報告和查詢。
- 由於策略範本是在設定 HA 群組之前在 Trend Micro Remote Manager 上設定的，因此不會對 HA 群組造成影響。在 Remote Manager 中，一個 HA 群組會顯示為兩台獨立的設備。

其他 HA 群組資訊

- HA 群組 — WAN 拓撲 第 6-23 頁
- HA 群組 — 容錯移轉條件 第 6-24 頁
- HA 群組 — 活動訊號介面 第 6-25 頁

支援 HA 群組的型號

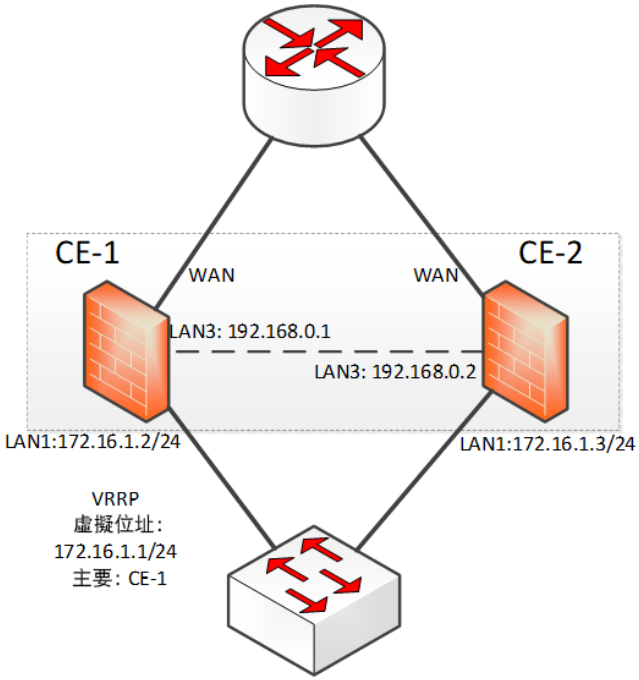
下列型號支援 HA 群組：

- Cloud Edge 50G2 設備

HA 群組 – WAN 拓撲

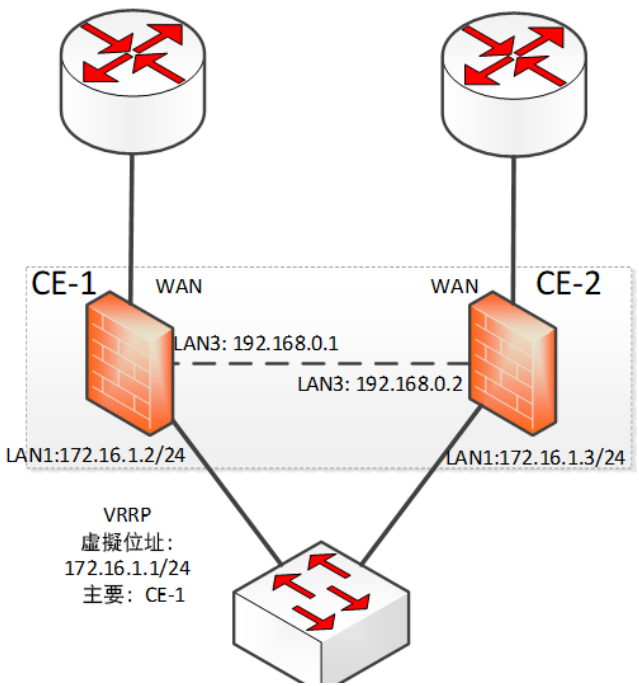
一個路由下一個躍點

在此情境下，由於 CE-1 和 CE-2 連接到一台路由器，因此來自 CE1 之 WAN 介面的封包不能與來自 CE-2 的封包位於同一個子網路。在這種情況下，必須啟動 NAT。



路由器有兩個躍點

此情境沒有任何問題。



HA 群組 — 容錯移轉條件

使用 Cloud Edge HA 群組時，您應瞭解 HA 群組進行容錯移轉的條件，包括：

- 一或多個監控介面離線
- 達到活動訊號或 ping 接管閾值
- 作用中設備進行韌體更新
- 更換作用中設備

- 強制接管

  如果 HA 群組處於異常狀態，將不會進行強制接管。

  觸發強制接管後，主要設備會進入待命狀態，而次要設備會變成作用中設備。

HA 群組 — 活動訊號介面

建立 Cloud Edge HA 群組時，每台 HA 對等設備上都會有一個介面指定做為活動訊號介面。此介面是在建立 HA 群組時選擇的。

- 活動訊號介面必須是 L3 介面。
- 每一台設備的活動訊號介面必須是相同的介面（例如，LAN2 連接 LAN2，或 LAN3 連接 LAN3）。
- 兩個活動訊號介面必須直接互相連接（不可透過交換器連接）。
- 活動訊號介面不可用於其他用途，例如 LAN 流量介面。
- 必須設定活動訊號介面的 IPv4 位址和網路遮罩，且 IPv4 位址必須位於同一個子網路。
- 選取一個介面做為活動訊號介面後，即無法變更該介面的組態設定（包括設備 IP 位址）。

管理核心分裂情況

- 由於 Cloud Edge 僅使用一個介面做為 HA 群組的活動訊號介面，因此活動訊號連線問題可能導致發生稱為「核心分裂」問題的情況。Cloud Edge 必須能夠處理此情況。
- 核心分裂：核心分裂情況是叢集分割區引起的，叢集的每一方都認為另一方已失效，進而接管資源，好像另一方不再擁有任何資源。

HA 群組 — VRRP 群組

建立 Cloud Edge HA 群組時，亦會建立 Virtual Router Redundancy Protocol (VRRP) 群組做為 HA 群組組態設定的一部分。

- 由於 WAN 端可能直接與路由器連接，因此 Cloud Edge 僅支援 LAN 端虛擬 IP 定址。每台主要和次要設備都具有各自的 WAN 組態設定。
- 可以選取 L3 實體介面或靜態 L3 VLAN 介面，視組態設定而定：
  - 兩台設備皆未註冊：只能選取實體介面
  - 兩台設備皆已註冊：可選取實體介面或 VLAN 介面

    兩台設備皆必須存在 VLAN 介面。
  - 主要設備已註冊，次要設備未註冊：只能選取實體介面
  - 只能在一個 VRRP 群組中使用實體介面/VLAN 介面。
  - 無法在 VRRP 群組中使用 WAN 介面。
- VRRP 群組僅支援 IPv4 虛擬 IP 位址。

HA 群組 — 端點網路存取

若要透過 HA 群組提供端點的網路存取，請使用下列其中一種方法：

- 動態定址
  1. 在雲端主控台或內部部署主控台中，在 VRRP 群組介面上為 HA 群組中的主要和次要設備設定 DHCP 服務。

     
     注意

     DHCP 服務的設備位址必須是 VRRP 群組的虛擬 IP 位址。

     在 HA 群組中，主要和次要設備上介面的 DHCP 設定必須完全相同。

     如需詳細資訊，請參閱 DHCP 第 6-66 頁。
  2. 在端點上，將端點設定為透過 DHCP 取得位址。
- 靜態定址
  1. 在端點上，將 IP 位址和子網路遮罩設定為與 VRRP 群組介面位於同一個子網路。

2. 在端點上，將設備位址設定為與 VRRP 群組相同的虛擬 IP 位址。

HA 群組 – 監控介面和接管觸發條件

建立 Cloud Edge HA 群組時，您可以設定用於執行基本介面和通訊協定監控，以判斷是否達到容錯移轉條件的監控介面。還可以設定活動訊號和 ping 接管觸發條件的接管閾值。

- 監控介面：Cloud Edge 對選取的實體介面（WAN 和某些 LAN 通訊埠）執行基本目標追蹤。建議您選取所有可用的實體介面來進行監控。
- 監控 IP/FQDN：可以為選取的每個監控介面輸入最多 2 個要監控的 IP 位址或 FQDN。
- 接管觸發條件：Cloud Edge 追蹤活動訊號和 ping 閾值。

  達到任何一個接管觸發條件都會啟動接管。

  如果設定了兩台監控主機，ping 兩台主機都失敗才會進行接管。若兩台主機中的一台 ping 作業失敗，則不會接管。如果只有一台監控主機，該主機一達到 ping 閾值就會觸發容錯移轉。

HA 群組 – 組態設定列表

下面的列表提供 Cloud Edge 如何管理 HA 群組組態設定的相關資訊。

必須分別對每台設備設定下列功能。「是」代表可在 Cloud Edge 雲端主控台中進行設定。

功能	主要	待命	詳細資料
設備資訊 – 一般、狀態、記錄檔/事件、工具	是	是	
設備資訊 – 進階（「傳統模式」設定）	是	是	

功能	主要	待命	詳細資料
介面	是	是	僅可透過 HA 群組設定活動訊號介面，無法透過「介面」頁面進行設定。
管理存取權	是	是	
DHCP	是	是	
動態 DNS	是	是	
路由資料表	是	是	
靜態路由	是	是	
NAT	是	是	
頻寬控制	是	是	
L2TP VPN	是	是	
SSL VPN	是	是	
Site-to-Site VPN	是	是	
終端使用者管理 — 一般設定	是	是	
LDAP 設定	是	是	
更新	是	是	「已安裝的更新」在短時間內可能不同。
WFBSS 端點防護（一般）	是	是	
WFBSS 端點防護（疑難排解）	是	是	
可疑端點（一般）	是	是	
可疑端點（疑難排解）	是	是	

功能	主要	待命	詳細資料
診斷檔案	是	是	
封包擷取	是	是	
隱藏的頁面	是	是	

HA 群組 – 策略設定列表

您應瞭解策略如何與 HA 群組中的設備搭配使用。

策略設定	詳細資料
在設定「策略規則」、「介面群組」或「核可/封鎖清單」時，設備不是 HA 群組的一部分。	主要設備的組態設定會套用至 HA 組。將不會使用次要設備的舊策略。
在設定「策略規則」、「介面群組」或「核可/封鎖清單」前，設備已經是 HA 群組的一部分。	「策略規則」和「核可/封鎖清單」都是針對 HA 組進行設定，而非針對主要設備或次要設備。 若要在策略規則中選取「介面群組」，請為該規則僅選取一台獨立設備或一個 HA 組。
您可以為 HA 群組中的設備設定「介面群組」。	設定將由 HA 組使用之主要設備的「介面群組」。 如果要這麼做，主要和次要設備必須具有類似的 VLAN 和 VPN 組態設定。 請記住下列考量事項： 如果主要設備已註冊而次要設備未註冊，則當主要設備的策略規則使用的「介面群組」包含 VLAN 或 VPN 時，這些主要設備規則將無法成功套用至次要設備。 在此情況下，請在註冊次要設備後為其設定 VLAN 和 VPN，然後執行策略部署。
策略會部署至 HA 群組中的全部兩台設備。	請記住下列考量事項： 即使策略成功部署至某一台設備，但可能無法部署至另一台設備。

策略設定	詳細資料
您可以為 HA 群組所用的策略設定上網位置。	請記住下列考量事項： 在 HA 群組進行容錯移轉後，某些具有策略規則中所設定之上網位置的策略規則可能無法運作。這是因為設備可能採用不同版本的位置資料庫。
將 HA 群組拆解後，主要設備和次要設備將會使用為 HA 群組所設定的策略。	請記住下列考量事項： 已設定介面群組的策略規則將僅套用至主要設備。

HA 群組限制

您應瞭解 HA 群組存在的一些限制。

限制	說明
NAT 連線	NAT 連線追蹤不會同步。
核心分裂問題	Cloud Edge 設備的通訊埠有限，這表示可能只有一個通訊埠可用於活動訊號。

HA 群組 — 處理行動

處理行動	說明
	編輯 HA 群組組態設定。
	在 HA 群組中強制接管。 觸發強制接管時，主要設備將變成待命狀態，而次要設備會變成作用中狀態。
	啟動 HA 群組。 按一下「全部部署」後，HA 群組即可運作。
	關閉 HA 群組。 按一下「全部部署」後，HA 群組將無法運作。

處理行動	說明
	從 Cloud Edge 雲端主控台移除 HA 群組。

取代設備

將設備取代為另一個 Cloud Edge 設備，可維持 Cloud Edge 雲端主控台中的所有策略、組態設定資料和記錄檔不變。取代設備的原因如下：

- Cloud Edge 設備無法運作或損壞。
- 客戶想要升級為效能更高的 Cloud Edge 設備。

當新的 Cloud Edge 設備與 Cloud Edge 雲端主控台同步處理記錄檔統計資料時，Cloud Edge 雲端主控台會將新的記錄檔統計資料與已取代之 Cloud Edge 設備上的快取資料合併。

注意

如果要取代 HA 群組中的設備，必須使用與將被取代之設備相同型號和韌體版本的設備。

取代 HA 群組中的設備之前，請先從要取代的設備的活動訊號介面移除乙太網路纜線，然後將乙太網路纜線連接到新設備的活動訊號介面。

重要

每個設備都有一個與 Cloud Edge 雲端主控台中已註冊之特定 Cloud Edge 設備相關聯的唯一金鑰（產品序號）。在取代設備後，除非將 Cloud Edge 設備註冊為新設備，否則無法再使用舊的 Cloud Edge 設備。

注意

在取代設備後，只有策略設定會還原。

步驟

1. 移至「設備」。
2. 以滑鼠右鍵按一下要取代的設備，然後選取「 取代」。
3. 指定新 Cloud Edge 設備的產品序號。
4. 按一下「取代」。
5. 從網路移除舊的 Cloud Edge 設備。
6. 將新的 Cloud Edge 設備新增到網路。

   新的 Cloud Edge 設備會註冊到 Cloud Edge 雲端主控台，而舊的 Cloud Edge 設備則會從 Cloud Edge 雲端主控台中移除。

設備資訊

用途：按一下設備名稱以從 Cloud Edge 雲端主控台管理該設備。

位置：「設備 > （選取的設備）」

步驟

1. 如果要從 Cloud Edge 雲端主控台管理選取的設備，請執行下列作業：
   - 在設備資訊區段下方檢視資訊並執行工作。
     - 檢視關於所選設備的一般資訊、系統狀態資訊，以及設備記錄檔和事件。
     - 使用工具對網路連線問題進行疑難排解，或啟動/關閉傳統模式來應對高流量狀況。
   - 設定網路設定。
     - 介面（包括 VLAN）
     - 管理存取權

    - DHCP
    - 動態 DNS
    - 路由資料表（僅檢視）
    - 靜態路由
    - NAT
- 設定頻寬控制。
- 設定使用者 VPN。
    - L2TP VPN
    - SSL VPN
- 設定 Site-to-Site VPN。
- 設定終端使用者管理。
    - 一般設定
    - LDAP 設定
- 設定 LDAP
- 管理設備更新。
- 設定網路存取控制。
    - WFBSS 端點防護
    - 可疑端點

檢視一般設備資訊

用途：檢視所選設備的硬體、網路與註冊資訊。

位置：「設備 >（選取的設備）> 設備資訊 > 一般」

步驟

1. 檢視設備資訊。

   設備資訊

   - 顯示名稱：設備的名稱。您可以使用設備動作來重新命名設備。
   - 狀態：設備目前在 Cloud Edge 雲端主控台中的狀態。
   - 上次策略部署時間：最近一次從設備上傳記錄檔到 Cloud Edge 雲端主控台時所用的時間戳記。
   - 策略部署狀態：上次部署策略的結果。
   - 使用者總數：過去 15 分鐘內作用中作業階段的使用者總數。

   網路設定

   - 部署模式：部署 Cloud Edge 設備時採用的是「橋接模式」還是「路由模式」。

     部署為「軟體切換」組態設定的 Cloud Edge 設備會列示為「橋接模式」裝置。
   - 主機名稱：Cloud Edge 設備主機名稱。
   - DNS：Cloud Edge 設備 DNS 設定。
   - WAN：Cloud Edge 設備與子網路遮罩設定。
   - 介面狀態（「橋接模式」標籤：虛擬介面狀態）：介面連結狀態。

     暫留在介面上以查看下列連結資訊：連結速度、雙工、MTU、傳送和接收封包、傳送和接收位元組

     將滑鼠游標暫留在某個無線介面上，可查看指派給該無線介面的暱稱以及 MTU。

   硬體與註冊

   - 型號：Cloud Edge 設備硬體型號。
   - 產品序號：目前註冊的產品序號。

- 硬碟參數
- 註冊日期：Cloud Edge 設備向 Cloud Edge 雲端主控台註冊的日期和時間。
- 版本：Cloud Edge 設備 Build 號碼。
- 恢復出廠預設值版本：Cloud Edge 設備的恢復出廠預設值套件版本。
- 運作時間：Cloud Edge 設備硬體自開機以來的運作時間。
- 郵件安全狀態：目前的 Cloud Edge 郵件安全掃瞄狀態。
  - 雲端掃瞄已啟動。
  - 本機掃瞄已啟動。
  - 雲端掃瞄失敗，從 YYYY-MM-DD hh:mm:ss TZ 開始回到本機掃瞄。

    TZ 代表公司的時區。
  - 電子郵件安全已關閉。

注意

Cloud Edge 設備離線時，會顯示 "--"。

檢視設備系統狀態

用途：檢視所選設備的 CPU 溫度、CPU 使用率、資料磁碟分割區使用率及記憶體使用率資訊。您可以手動重新整理頁面以查看更新的資料。

位置：「設備 > （選取的設備） > 設備資訊 > 狀態」

步驟

1. 檢視設備系統狀態資訊。

   溫度

- 檢視所選時間範圍內的 CPU 溫度：今天、過去 1 小時、過去 12 小時、過去 24 小時、過去 7 天

CPU 使用率

- 檢視所選時間範圍內的 CPU 使用率：今天、過去 1 小時、過去 12 小時、過去 24 小時、過去 7 天
- 檢視目前的 CPU 使用率。

磁碟分割區使用率

注意

對於 Cloud Edge 5.2 之前的版本，僅顯示系統磁碟資訊。

- 檢視所選時間範圍內的系統磁碟使用率：今天、過去 1 小時、過去 12 小時、過去 24 小時、過去 7 天
- 檢視所選時間範圍內的資料磁碟使用率：今天、過去 1 小時、過去 12 小時、過去 24 小時、過去 7 天
- 檢視目前的系統磁碟使用率。
- 檢視目前的資料磁碟使用率。

記憶體使用率

- 檢視所選時間範圍內的系統記憶體使用率：今天、過去 1 小時、過去 12 小時、過去 24 小時、過去 7 天
- 檢視目前的記憶體使用率。

檢視設備記錄檔和事件

用途：檢視設備網路事件、系統事件、VPN 事件和策略實施記錄檔。您可以手動重新整理頁面以查看更新的資料。

位置：「設備 >（選取的設備）> 設備資訊 > 記錄檔/事件」

步驟

1. 檢視設備事件記錄檔資訊。

   記錄項目會記錄下列資訊：日期/時間、用戶端 IP、子類別、事件、訊息

2. （選用）選取下列其中一個類別可過濾結果：

   - 系統事件
   - 網路事件
   - VPN 事件
   - 策略實施記錄檔
   - 信任憑證事件

   系統、網路和 VPN 事件會顯示在頁面底部。

   選取「策略實施記錄檔」後，會開啟「分析與報告 — 策略實施」畫面來顯示結果。

   注意

   只有支援 VPN 的 Cloud Edge 設備型號才會顯示 VPN 事件。

3. 您可以使用下列項目來進一步過濾事件結果：

   - 期間

     可用時間範圍包括：今天、過去 15 分鐘（預設值）、過去 1 小時、過去 12 小時、過去 24 小時、過去 7 天

   - 用戶端 IP
   - 子類別
   - 事件

     請參閱事件類別和子類別 第 6-38 頁。

事件類別和子類別

表 6-1. 事件類別和子類別

類別	子類別
系統事件	韌體更新
	引擎/病毒碼更新
	系統狀態
	服務
	裝置存取
網路事件	DHCP
	介面
	PPPOE
VPN 事件	L2TP
	SSL VPN
	Site-to-Site VPN
策略實施記錄檔	
信任憑證事件	信任憑證
	不信任憑證
智慧略過事件	

使用工具疑難排解網路連線問題

用途：使用 IPv4 網路工具，來驗證設備組態設定或疑難排解設備連線問題。

位置：「設備 >（選取的設備）> 設備資訊 > 工具」

步驟

1. 執行適當的處理行動：
   - 執行 Ping 測試 第 6-39 頁
   - 執行 Traceroute 測試 第 6-40 頁
   - 擷取 ARP 結果 第 6-40 頁

執行 Ping 測試

用途：使用 Ping 測試，來驗證設備組態設定或疑難排解設備連線問題。

位置：「設備 >（選取的設備）> 設備資訊 > 工具」

步驟

1. 按一下「Ping」工具圖示。
2. 輸入要 Ping 的 IPv4 位址或網域名稱。
3. 選用：輸入執行 Ping 的其他參數。
   - 選取網路介面以傳送 ping：預設值為任何介面。
   - 位元組：預設值為 56。
   - 計數：預設值為 4。最大值為 10。
4. 按一下「Ping」。
5. 檢視頁面底部的 Ping 結果。
   - Ping 歷史結果會儲存兩個星期，並會顯示在目前的 Ping 結果下方。
   - Ping 歷史結果最多顯示十個結果。
   - 如果離開「工具」畫面，頁面上的結果就會清除。

執行 Traceroute 測試

用途：使用 Traceroute 測試，來驗證設備組態設定或疑難排解設備連線問題。

位置：「設備 >（選取的設備）> 設備資訊 > 工具」

步驟

1. 按一下「Traceroute」工具圖示。
2. 輸入您要追蹤路由的 IPv4 位址或網域名稱。
3. 按一下「開始」。
4. 等候追蹤完成，或按一下「停止」以停止追蹤路由。

   一次只能執行一個追蹤路由。如果某個追蹤仍在執行中，而您想要啟動新的追蹤，則您必須先停止執行中的追蹤。
5. 檢視頁面底部的追蹤結果。
   - 追蹤路由歷史結果會儲存兩個星期，並會顯示在目前的追蹤路由結果下方。
   - 追蹤路由歷史結果最多顯示十個結果。
   - 如果離開「工具」畫面，頁面上的結果就會清除。

擷取 ARP 結果

用途：擷取 ARP 結果，來驗證設備組態設定或疑難排解設備連線問題。

位置：「設備 >（選取的設備）> 設備資訊 > 工具」

步驟

1. 按一下「ARP」工具圖示。
2. 執行適當的處理行動：

- 按一下「取得 ARP」以擷取 ARP 資訊。
- 按一下「清除 ARP 快取」以清除設備的 ARP 快取。

注意

這不會清除目前的頁面歷史記錄。

3. 檢視頁面底部的 ARP 快取結果。
   - 將顯示下列資訊：IPv4 位址、主機名稱（如果有的話）、MAC 位址、介面
   - 最多顯示 100 列。
   - 按一下「取得 ARP」可再次擷取 ARP 快取。
   - 如果離開「工具」畫面，頁面上的結果歷史記錄就會清除。

啟動/關閉傳統模式

用途：「傳統模式」允許您設定當流量負載過高時，Cloud Edge 設備的處理方式。

位置：「設備 > （選取的設備） > 設備資訊 > 進階」

步驟

1. 執行所需的處理行動：
   - 按一下「開啟」以啟動傳統模式。

     流量負載過高時封鎖其他流量。當流量負載降低時會自動恢復正常流量檢測。
   - 按一下「關閉」以關閉傳統模式。

     流量負載過高時不檢測流量。流量會周遊裝置而不受檢測。這是預設選項，也是建議的設定。

2. 如果您已按了「開啟」，請在「啟動傳統模式」確認畫面中按一下「啟動」。

網路

在雲端中檢視及設定網路設定，以處理及識別已註冊設備上的網路流量。設備向 Cloud Edge 雲端主控台註冊後，特定網路設定就會移至雲端，且無法透過 Cloud Edge 內部部署主控台進行編輯。會導致網路中斷的某些重要網路設定是透過內部部署主控台進行設定。

注意

- 在設定 Cloud Edge 介面、VLAN 或與設備之實體或虛擬介面相關的功能時，Cloud Edge 僅支援 IPv4。

  僅支援 IPv4 的其他功能包括：管理存取權、DHCP、動態 DNS、DNS、路由、NAT 和 VPN。

  請參閱 IPv6 支援 第 1-16 頁。
- 在「路由模式」下部署時，Cloud Edge 雲端主控台不支援新增或編輯橋接器。
- 「軟體切換」組態設定僅在「橋接模式」下受支援，且必須使用內部部署主控台進行設定。
- 在設定無線介面及相關的網路功能時，具有無線功能的 Cloud Edge 設備僅支援 IPv4。

  只有在「路由模式」下才支援無線功能。
- 若有某些網路設定未成功部署，Cloud Edge 雲端主控台上會顯示原因。
- 設備會收集網路資訊，並透過網路活動訊號傳送到 Cloud Edge 雲端主控台。

移至雲端的網路設定

1. 介面
   路由模式

- 設定各個介面以及 LAN2-LAN3 介面和 MGMT 介面的 L3 VLAN

  對於採用硬體切換晶片組的設備，設定 LAN2-LAN8 介面和 MGMT 介面。

- 設定無線網路存取設定（設備須支援無線功能）

  無線網路介面不支援 L3 VLAN。

橋接模式

- 僅能設定 MGMT 介面的介面設定和 L3 VLAN

2. 管理存取權（設備註冊後）
   - 設定用於使用內部部署主控台、Ping、SSH 和 SNMP（所有介面）的管理存取權
3. DHCP（僅限在路由模式下）
   - 設定 LAN2-LAN3 和 MGMT 介面以充當 DHCP 伺服器

     對於具有無線功能的設備，在已啟動無線網路的情況下，您可以進一步設定主要無線網路和客體無線網路的 DHCP。
   - 對於採用硬體切換晶片組的設備，設定 LAN2-LAN8 和 MGMT 介面的 DHCP
   - 您可以設定屬於上述實體介面之子介面的 L3 VLAN 的 DHCP。
4. 服務 - 動態 DNS
5. 路由（僅限在路由模式下）
   - 檢視路由資料表（也可從內部部署主控台取得）
   - 設定靜態路由
6. NAT
7. 頻寬控制
8. 使用者 VPN
   - SSL VPN

- L2TP VPN

9. Site-to-Site VPN
10. 終端使用者管理
    - 一般驗證設定（驗證快取的 TTL 選項）
11. 無線網路
    - 設定主要無線網路和客體無線網路的網路存取控制
    - 管理無線網路用戶端連線。
    - 檢視無線網路組態設定資訊及疑難排解記錄檔

> **注意**
> 請務必使用內部部署主控台來變更無線組態設定。

保留於設備的網路設定

1. 介面
    - 編輯介面：WAN 或 LAN1
    - 新增/編輯 L3 VLAN：WAN 或 LAN1
    - 啟動或關閉介面：LAN2-LAN3（採用硬體切換晶片組的設備則是 LAN2-LAN7）
    - 無線網路介面：您無法從介面頁面關閉這些介面。

      若要關閉無線介面，必須使用內部部署主控台來關閉各自的無線網路。
2. DNS — 設定 IPv4 DNS 伺服器
3. 位址 - 檢視並編輯策略路由規則中使用的位址物件
4. 「橋接模式」設定
    - 設定 橋接器介面 (br0) 或 切換介面 (sw0)

- 設定其他橋接或切換設定

5. 軟體切換
   - 設定 橋接器介面 (br0)
   - 設定其他軟體切換設定
6. 路由
   - 建立策略路由規則
   - 檢視路由資料表（也可從 Cloud Edge 雲端主控台取得）
7. 服務 - DHCP
   將介面設定為用做 DHCP 伺服器：WAN 或 LAN1
8. 無線網路
   - 啟動及設定主要無線網路和客體無線網路
   - 檢視無線網路疑難排解記錄檔

注意

Cloud Edge 300 沒有 LAN3 介面。

介面

Cloud Edge 會自動偵測 Cloud Edge 設備的 L2 和 L3 介面。

路由模式

在 Cloud Edge 上註冊設備後，必須從 Cloud Edge 雲端主控台管理除了 WAN 和 LAN1 介面以外的所有介面。

- 所有介面均已設定為具有 IPv4 位址的 L3 介面。
- 您必須為 LAN2-LAN3 和 MGMT 介面設定靜態 IPv4 位址。

  對於採用硬體切換晶片組的 Cloud Edge 設備，您必須為 LAN2-LAN8 和 MGMT 介面設定靜態 IP 位址。

對於具有無線功能的 Cloud Edge 設備，必須為無線網路介面設定靜態 IP 位址。

注意

您必須從 Cloud Edge 內部部署主控台設定 WAN 和 LAN1。

橋接模式

在 Cloud Edge 雲端主控台中，「橋接模式」介面是唯讀的。您必須從 Cloud Edge 內部部署主控台設定及管理 橋接器介面 (br0) 和實體介面設定。

- 虛擬 橋接器介面 (br0) 是 Cloud Edge 用於連線到 Internet 的 L3 介面，並已指派了 IPv4 位址。
- 所有實體介面（MGMT 介面除外）均設定為 L2 介面。

  您可以設定實體 L2 介面的 MTU 設定。
- 您可以從 Cloud Edge 雲端主控台將 MGMT 通訊埠設定為 L3 介面。

軟體切換

在 Cloud Edge 雲端主控台中，「軟體切換」介面是唯讀的。您必須從 Cloud Edge 內部部署主控台設定和管理軟體切換組態設定中使用的 橋接器介面 (br0) 以及實體介面。

- 虛擬 橋接器介面 (br0) 是 Cloud Edge 用於連線到 Internet 的 L3 介面，並已指派了 IPv4 位址。
- 您必須向軟體切換組態設定中新增至少三個實體 L2 介面（即 WAN 和 LAN1，以及至少其中一個 LAN2 或 LAN3）。

  您可以設定實體 L2 介面的 MTU 設定。
- 您可以從 Cloud Edge 雲端主控台將 MGMT 通訊埠設定為 L3 介面。

橋接模式（採用切換晶片組）

在 Cloud Edge 雲端主控台中，採用硬體切換晶片組之設備的「橋接模式」介面是唯讀的。您必須從 Cloud Edge 內部部署主控台設定和管理硬體切換組態設定中使用的 切換介面 (sw0) 以及實體介面。不過，您必須從 Cloud Edge 雲

端主控台管理與內部網路安全（在內部 LAN 通訊埠之間周遊的流量）層級相關的 切換介面 (sw0) 設定。

- 虛擬 切換介面 (sw0) 是 Cloud Edge 用於連線到 Internet 的 L3 介面，並已指派了 IPv4 位址。
- 所有實體介面（MGMT 介面除外）均設定為 L2 介面。

  視您為設備選擇的「內部網路安全」模式而定，您可以設定實體介面的特定設定。
- 您可以從 Cloud Edge 雲端主控台將 MGMT 通訊埠設定為 L3 介面。

注意

Cloud Edge 300 沒有 LAN3 介面。

對於每一種部署模式和所有 Cloud Edge 設備型號，您都可以啟動或關閉特定介面。

啟動或關閉介面 第 6-51 頁

管理網路介面

用途：管理所選設備的網路介面設定。

位置：「設備 > （選取的設備） > 網路 > 介面」

步驟

1. 執行下列動作：
   - 檢視資料表以瞭解設備的網路設定與連結狀態。
   - 按一下介面名稱可編輯介面 第 6-48 頁。
   - 按一下 ⊞ 以新增 VLAN 子介面 第 6-63 頁。

   您可以從 Cloud Edge 雲端主控台中修改的介面和建立的 VLAN，將視設備型號和部署模式而有所不同。
2. 對於處於「橋接模式」的 Cloud Edge 設備或其採用硬體切換晶片組處於「橋接模式」的設備，請執行下列作業：

- 檢視橋接器介面 (br0) 或切換介面 (sw0) 設定。
- 按一下「切換介面 (sw0)」以設定內部網路安全模式設定。

3. 對於現有的 VLAN，請執行下列作業：
   - 檢視 VLAN 資料表以瞭解 VLAN 設定與連結狀態。
   - 按一下 VLAN 介面名稱以編輯或關閉/啟動 VLAN 子介面 第 6-63 頁。
   - 按一下「刪除」以刪除所需的 VLAN 介面。

編輯網路介面

用途：管理所選設備的網路介面設定。

位置：「設備 > （選取的設備） > 網路 > 介面」

步驟

- 請根據設備的部署模式設定使用適當的程序。
  - 路由模式：編輯網路介面 第 6-48 頁
  - 路由模式：編輯無線網路介面 第 6-49 頁
  - 橋接模式：編輯網路介面 第 6-50 頁

    請針對「橋接模式」、「橋接模式」（採用切換晶片組）和「軟體切換」等部署使用此程序。

路由模式：編輯網路介面

用途：管理所選設備的網路介面設定。在註冊處於「路由模式」的設備後，必須從 Cloud Edge 雲端主控台編輯除了 WAN 和 LAN1 介面以外的所有介面。

位置：「設備 > （選取的設備） > 網路 > 介面」

步驟

1. 按一下介面的名稱。
2. 設定介面設定。

   若要設定無線網路介面，請參閱路由模式：編輯無線網路介面 第 6-49 頁。

選項	說明
類型	選取 L3。 如果 Cloud Edge 雲端主控台上有任何設定變更待完成，您必須按一下「全部部署」讓現有變更生效，然後才能變更介面類型。
模式	這是唯讀欄位，其中模式已預設為「靜態」。
IPv4 位址	指定 IPv4 位址（範例：`10.10.10.23`）。
IPv4 網路遮罩	指定 IPv4 子網路遮罩（範例：`255.255.254.0`）。
IPv4 預設設備	指定 IPv4 預設設備（範例：`10.10.10.1`）。只有 WAN 組態設定才需要此設定。
MTU	指定 576 到 1500 之間的值。
MSS	選取「覆寫」並指定 536 到 1460 之間的值。 注意 MSS 值不能大於 (MTU - 40)。

3. 按一下「儲存」。

路由模式：編輯無線網路介面

用途：管理所選設備的無線網路介面設定。在註冊處於「路由模式」的設備後，必須從 Cloud Edge 雲端主控台編輯所有無線網路介面。

位置：「設備 > （選取的設備） > 網路 > 介面」

步驟

1. 按一下無線網路介面的名稱。

   無線網路介面名稱是唯讀的，而預設名稱就是指派給該無線網路的 SSID。

2. 設定介面設定。

選項	說明
類型	這是唯讀欄位，其中「類型」已預設為「L3」。
模式	這是唯讀欄位，其中模式已預設為「靜態」。
IPv4 位址	指定 IPv4 位址（範例：`10.10.10.23`）。
IPv4 網路遮罩	指定 IPv4 子網路遮罩（範例：`255.255.254.0`）。
IPv4 預設設備	指定 IPv4 預設設備（範例：`10.10.10.1`）。只有 WAN 組態設定才需要此設定。
MTU	指定 576 到 1500 之間的值。
MSS	選取「覆寫」並指定 536 到 1460 之間的值。 注意 MSS 值不能大於 (MTU - 40)。 如果修改了 WLAN 介面的 MTU，也必須相應地設定 MSS（MSS 值小於 MTU - 40）。

3. 按一下「儲存」。

橋接模式：編輯網路介面

用途：管理所選設備的網路介面設定。以「橋接模式」註冊設備後（包括從「橋接模式」變化而來的「軟體切換」），您僅可從 Cloud Edge 雲端主控台編輯 MGMT 介面。

位置：「設備 > （選取的設備） > 網路 > 介面」

步驟

1. 按一下介面的名稱。
2. 使用靜態模式設定來設定介面。

選項	說明
類型	選取 L3。 如果 Cloud Edge 雲端主控台上有任何設定變更待完成，您必須按一下「全部部署」讓現有變更生效，然後才能變更介面類型。
模式	這是唯讀欄位，其中模式已預設為「靜態」。
IPv4 位址	指定 IPv4 位址（範例：`10.10.10.23`）。
IPv4 網路遮罩	指定 IPv4 子網路遮罩（範例：`255.255.254.0`）。
MTU	指定 576 到 1500 之間的值。
MSS	選取「覆寫」並指定 536 到 1460 之間的值。 注意 MSS 值不能大於 (MTU - 40)。

3. 按一下「儲存」。

啟動或關閉介面

Cloud Edge 設備的特定介面可能會隨部署模式的不同而預設為啟動或關閉。在特定組態設定中，您可能無法關閉某些介面。

注意

不論在任何一種部署模式下，您皆無法關閉 MGMT 通訊埠。

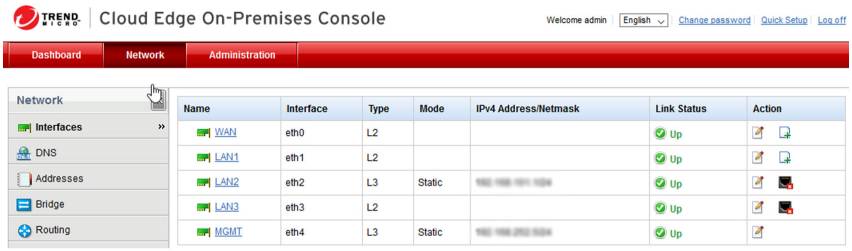


圖 6-1. 範例：處於路由模式的 Cloud Edge 70

請從 Cloud Edge 內部部署主控台啟動或關閉介面。

- 路由模式：LAN2 和 LAN3 介面預設會啟動。

  您可以隨時關閉或重新啟動這些介面。
- 橋接模式：LAN2 和 LAN3 介面預設會關閉。

  您可以隨時啟動或關閉這些介面。
- 軟體切換：將 LAN2 和 LAN3 新增為軟體切換介面時，會自動啟動它們。

  如果介面屬於「軟體切換」組態設定的一部分，則您無法關閉該介面。

注意

Cloud Edge 300 設備沒有 LAN3 介面。

採用硬體切換晶片組的 Cloud Edge 設備

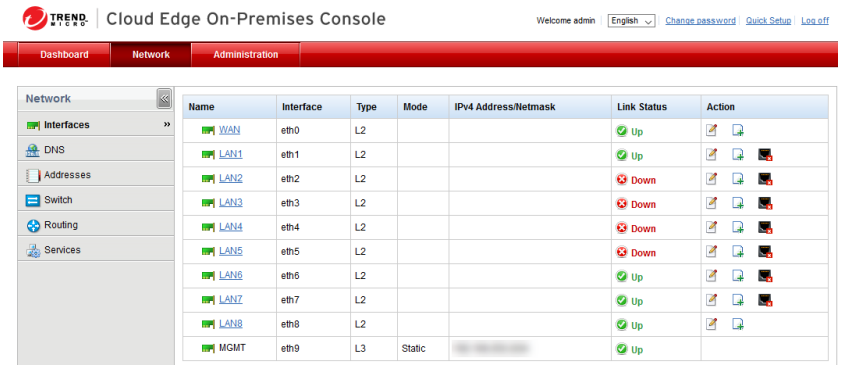


圖 6-2. 範例：處於橋接模式的 Cloud Edge 100 G2

依預設，所有通訊埠均為啟動狀態。您無法關閉 WAN、LAN8 或 MGMT 介面。

- 路由模式

  您可以關閉 LAN1-LAN7 介面。

- 橋接模式

  WAN 和 LAN1-LAN8 介面會自動選取做為硬體切換的通訊埠。您無法從硬體切換組態設定移除這些通訊埠；不過，您可以關閉 LAN1-LAN7 介面。

具有無線網路功能的 Cloud Edge 設備

您無法從「介面」頁面啟動或關閉無線網路介面。

當您啟動無線存取時，系統會自動啟動主要無線網路，而當您啟動客體無線網路時，系統會自動啟動客體無線網路。如果您關閉相應的無線網路，系統會自動關閉無線網路介面。

步驟

1. 從 Cloud Edge 內部部署主控台，移至「網路 > 介面」。

2. 執行下列其中一項作業：

   a. 針對您想要啟動的介面，按一下「啟動」圖示 ( )。

   b. 針對您想要關閉的介面，按一下「關閉」圖示 ( )。

設定切換介面 (sw0) 設定

用途：為採用硬體切換晶片組之 Cloud Edge 設備的切換介面 (sw0) 進行內部網路安全設定。

位置：「設備 > （選取的設備） > 網路 > 介面 > sw0」

步驟

1. 檢閱 切換介面 (sw0) 設定的清單。

   切換介面 (sw0) 設定的清單 第 6-56 頁

2. 選取「內部網路安全模式」。

選項	說明
高安全性	包含下列特性： • Internet：所有安全掃瞄（策略規則、資料檔、湧入和通訊埠掃瞄等） • 內部網路：所有安全掃瞄 (同上)，不含郵件掃瞄 • 安全防護：為內部網路傳輸提供最高層級的安全防護，但效能最低
標準	包含下列特性： • Internet：所有安全掃瞄（策略規則、資料檔、湧入和通訊埠掃瞄等） • 內部網路：部分安全掃瞄（策略規則、湧入和通訊埠掃瞄） • 安全防護：為內部網路傳輸提供中等層級的安全防護，效能也為中等層級
高速	包含下列特性： • Internet：所有安全掃瞄（策略規則、資料檔、湧入和通訊埠掃瞄等） • 內部網路：無安全掃瞄

選項	說明
	• 安全防護：為內部網路流量提供最高層級的效能，但不提供任何安全防護。

3. （僅限「高安全性」和「標準」模式）確保將「異常偵測」設定為所需設定。

重要

此為唯讀欄位，提供 IPS 防護是否已啟動的相關資訊。異常偵測是 IPS 的一項功能。如果要使用異常偵測，您必須在已套用到此設備之設備資料檔的 IPS 頁面上啟動 IPS。必須啟動異常偵測，Cloud Edge 才能提供 Flood 和通訊埠掃瞄防護。

4. （僅限「高安全性」和「標準」模式）選取您想要啟動的「Flood 規則」，然後修改每個 Flood 規則的閾值（若您不想要保留預設閾值）。

依預設，系統會啟動所有 Flood 規則，以防範 Flood 攻擊。

選項	說明
TCP SYN Flood	預設閾值：8000
ICMP Flood	預設閾值：8000
UDP Flood	預設閾值：8000
IGMP Flood	預設閾值：8000

5. （僅限「高安全性」和「標準」模式）選取您想要啟動的「通訊埠掃瞄規則」，然後修改每個規則的閾值（若您不想要保留預設閾值）。

依預設，系統會啟動所有通訊埠掃瞄規則，以防範通訊埠掃瞄攻擊。

選項	說明
UDP 通訊埠掃瞄	預設閾值：1000
TCP 通訊埠 SYN 掃瞄	預設閾值：1000
TCP 通訊埠 FIN 掃瞄	預設閾值：1000

選項	說明
TCP 通訊埠 NULL 掃瞄	預設閾值：1000
TCP 通訊埠 Xmas 掃瞄	預設閾值：1000

6. 按一下「儲存」。

切換介面 (sw0) 設定的清單

在設定 切換介面 (sw0) 之前，務必先檢閱有哪些組態設定可用。有些設定是使用 Cloud Edge 內部部署主控台設定的，有些設定則是使用 Cloud Edge 雲端主控台來設定。

Cloud Edge 雲端主控台用於設定內部網路安全模式設定，這些設定可控制對 LAN 到 LAN 內部網路流量實施的安全層級。

如需有關每一種內部網路安全模式提供之安全防護的詳細資訊，請參閱每一種內部網路安全模式提供的安全防護 第 6-58 頁。

高安全性模式和標準模式

表 6-2. 使用 Cloud Edge 雲端主控台設定

設定	說明
內部網路安全模式	設定內部網路的網路安全層級。 • 高安全性模式 • 標準模式 • 高速模式
異常偵測	唯讀欄位，其顯示套用至此設備的設備資料檔是否啟動了 IPS。 必須啟動 IPS 才能使用 Flood 規則和通訊埠掃瞄規則。
Flood 規則	提供網路 IPS 防護以防範湧入。
通訊埠掃瞄規則	提供網路 IPS 防護以防範通訊埠掃瞄。

表 6-3. 使用 Cloud Edge 內部部署主控台設定

設定	說明
模式	DHCP 或靜態
MTU	範圍：576 到 1500 預設值：1438
管理存取權	僅當設備未註冊時才可用。
進階設定： 啟動跨距樹狀目錄通訊協定	防止具有重複路徑的網路發生迴圈情況。
進階設定： IGMP 窺探 (IGMP Snooping)	監控 IGMP 流量，然後將 IGMP 流量只轉送給彼此間存在關聯的端點。

高速模式

表 6-4. 使用 Cloud Edge 雲端主控台設定

設定	說明
內部網路安全模式	設定內部網路的網路安全層級。 • 高安全性模式 • 標準模式 • 高速模式

表 6-5. 使用 Cloud Edge 內部部署主控台設定

設定	說明
模式	DHCP 或靜態
MTU	範圍：576 到 1500 預設值：1438
管理存取權	僅當設備未註冊時才可用。

設定	說明
進階設定： 啟動跨距樹狀目錄通訊協定	防止具有重複路徑的網路發生迴圈情況。

每一種內部網路安全模式提供的安全防護

在設定 切換介面 (sw0) 之前，您可以檢閱每一種內部網路安全模式所提供的安全防護，以確保為您的設備設定了符合業務需求的安全防護。

每一種內部網路安全模式提供的安全防護列表

	高安全性		標準		高速	
	Internet	內部網路	Internet	內部網路	Internet	內部網路
惡意程式防護	是	是	是	否	是	否
IPS	是	是	是	限於「Flood 控制」和「通訊埠掃瞄切換」設定中所列的 IPS	是	否
其他安全功能	是	是	是	否	是	否

注意

- 其他安全功能包括安全資料檔擁有的所有功能，以及核可清單和封鎖清單。
- 任何一種內部網路安全模式皆不支援對內部網路進行郵件掃瞄。

VLAN 的運作方式

虛擬區域網路 (VLAN) 是由一組端點、伺服器和其他網路裝置組成，不論所在位置如何，彼此的通訊就如在同一個 LAN 區段內。即使分散各地並連線到許多網路區段，端點和伺服器仍可以屬於相同的 VLAN。

VLAN 以邏輯而非實體方式隔開裝置。每個 VLAN 均視為一個廣播網域。VLAN 1 中的裝置可以與 VLAN 1 中的其他裝置連線，但無法與其他 VLAN 中的裝置連線。VLAN 中各裝置之間的通訊獨立於實體網路之外。

VLAN 隔開裝置的方式是對 VLAN 中裝置傳送和接收的所有封包增加 `802.1Q` VLAN 標籤。VLAN 標籤是 4 位元組框架延伸，其中包含 VLAN 識別碼以及其他資訊。

如何在 VLAN 中部署 Cloud Edge

請檢閱下列資訊，以瞭解 Cloud Edge 如何支援 L3 VLAN。

- 僅支援 L3 VLAN。

  
  注意
  任何部署模式或型號皆不支援 L2 VLAN。

- Cloud Edge 支援 50 個 VLAN 子介面及 4096 個 VLAN 標籤。
- 設定 VLAN 的位置：
  - Cloud Edge 雲端主控台：除 eth0 和 eth1 以外的所有介面（若該部署模式和型號支援）
  - 內部部署主控台：eth0 和 eth1（若該部署模式支援）
- 編輯或修改 VLAN 的考量事項：
  - VLAN 模式可以是靜態或 DHCP。
  - 如果 VLAN 已啟動 DHCP，則您無法編輯該 VLAN。
  - 如果 VLAN 已啟動 DHCP 或使用了 NAT，則您無法刪除該 VLAN。
- 在建立策略規則及建立介面群組策略物件時，您無法新增 VLAN 介面。

- 如需有關部署模式的特定資訊，請參閱：
  - 橋接模式 VLAN 第 6-60 頁
  - 路由模式 VLAN 第 6-62 頁

橋接模式 VLAN

請檢閱下列資訊，以瞭解 Cloud Edge 如何在「橋接模式」下支援 VLAN。

橋接模式支援的介面

- Cloud Edge 5.3 或更新版本的裝置：VLAN 組態設定僅支援 MGMT 介面
- 早於 5.3 的 Cloud Edge：VLAN 組態設定支援除 eth0 和 eth1 以外的所有介面
- 橋接器介面（br0 或 sw0）：不支援 VLAN 組態設定

橋接模式考量事項

在「橋接模式」下設定 VLAN 時，有一些特殊考量。

- Cloud Edge 本身並不像標準交換器一樣支援 VLAN，因此存在下列限制：
  1. 您無法對 Cloud Edge 通訊埠設定存取/主幹模式，因此 Cloud Edge 無法標記或取消標記任何通過的流量。
  2. Cloud Edge 無法隔離來自不同 VLAN 的廣播或多點傳送流量。
- Cloud Edge 僅能透過保留現有的 VLAN 標籤來支援通過的 VLAN 流量。Cloud Edge 可以對通過的 VLAN 流量提供所有安全防護功能。

「橋接模式」案例

將 Cloud Edge 部署於主幹連結時，趨勢科技建議您只使用兩個 Cloud Edge 通訊埠：

- 將 WAN 連接到上游主幹通訊埠。
- 將 LAN1 連接到下游主幹通訊埠。

重要

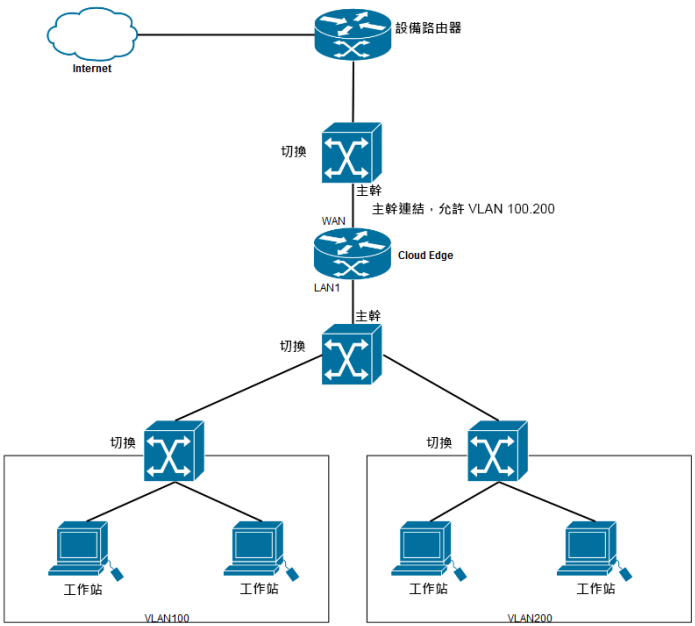
連接到主幹連結的通訊埠請勿超過兩個。

注意

部署採用硬體切換晶片組的設備或處於「軟體切換」模式的其他型號時，請將 WAN 通訊埠連接到上游主幹通訊埠，並將任何 LAN 通訊埠連接到下游主幹通訊埠。

下列案例說明建議的「橋接模式」部署。

主幹案例



在本案例中，您必須在原生 VLAN 中設定設備，才能向 Cloud Edge 雲端主控台註冊 Cloud Edge 設備。

- 在主幹連結上，所有流量都會帶有 VLAN 標籤，但屬於原生 VLAN 的流量除外。Cloud Edge 設備本身只能傳送不含 VLAN 標籤的流量。
- 因此，如果 br0 設定了 DHCP，則您必須在原生 VLAN 上設定 DHCP 伺服器和設備。如果 br0 設定了靜態 IP 位址，則您必須在原生 VLAN 上設定設備。

路由模式 VLAN

請檢閱下列資訊，以瞭解 Cloud Edge 如何在「路由模式」下支援 VLAN。

路由模式支援的介面

VLAN 組態設定支援除 eth0 和 eth1 以外的所有介面。

路由模式考量事項

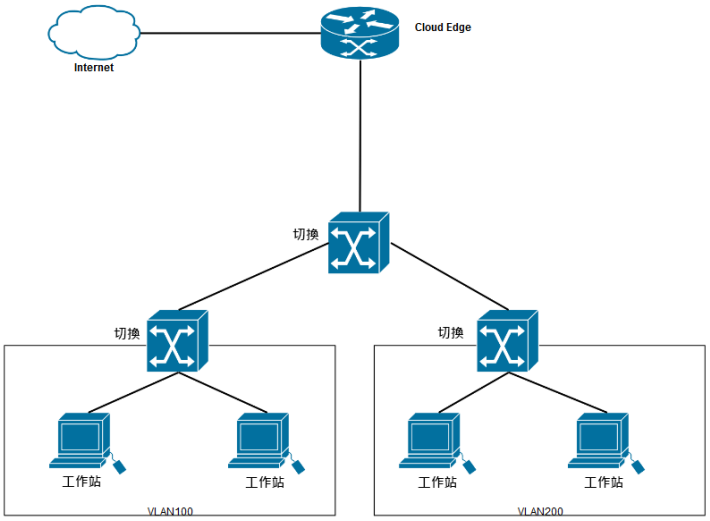
在「路由模式」下設定 VLAN 時，沒有任何特殊考量。

「路由模式」案例

當 Cloud Edge 設備處於「路由模式」時，您可以在 LAN 介面上設定 VLAN 介面，以滿足您的需求。

下列案例說明典型的「路由模式」部署。

主幹案例



新增/編輯 VLAN 介面

用途：將 L3 VLAN 介面新增到接收標記為 VLAN 之封包的 Cloud Edge 實體介面。您必須為每個 L3 VLAN 介面設定唯一的 IPv4 位址和網路遮罩。如有需要，您可以編輯 VLAN 介面。

位置：「設備 > （選取的設備） > 網路 > 介面」

步驟

1. 在新增 VLAN 介面之前，請先檢閱有關如何藉由 Cloud Edge 設備運作 VLAN 的重要資訊。

   如何在 VLAN 中部署 Cloud Edge 第 6-59 頁

2. 執行適當的處理行動：

   - 若要新增 VLAN，請按一下「處理行動」欄中的 VLAN 新增組態設定圖示 (⊞)(⊞)。
   - 若要編輯 VLAN，請按一下「VLAN」區段中的 VLAN 名稱。

   「新增/編輯 VLAN」頁面隨即開啟。

   注意

   您無法將 VLAN 介面新增到無線介面。

3. 指定 VLAN 設定。

   - 名稱：為 VLAN 介面命名。
   - 類型：會自動顯示 L3 VLAN，並且為唯讀。

     不支援 L2 VLAN。
   - 模式：選取「DHCP」或「靜態」。

     如果選取靜態，請指定「IPv4 位址」和「IPv4 網路遮罩」。
   - VLAN ID：指定 VLAN ID，其必須與此 VLAN 介面所接收封包的 VLAN ID 相符。

     每個 VLAN 介面的 VLAN ID，都必須與連接 VLAN 介面之 IEEE 802.1Q 相容路由器或交換器所新增的 VLAN ID 相符。VLAN ID 可以是 1 和 4094 之間的任何數字（0 和 4095 為保留數字）。

     您無法變更現有 VLAN 介面的 VLAN ID。

4. 按一下「儲存」。

管理存取權

您可以使用 Cloud Edge 雲端主控台來設定 Cloud Edge 設備的管理介面，以允許或封鎖來自此設備後方 IPv4 裝置之特定類型的管理服務（或流量）。Cloud

Edge 設備支援從 IPv4 用戶端使用內部部署主控台、Ping、SSH 和 SNMP 等服務進行管理存取。

如果 Cloud Edge 設備未向 Cloud Edge 雲端主控台註冊，您可以在編輯 L3 介面時使用內部部署主控台啟動管理存取權。在設備註冊後，您必須使用 Cloud Edge 雲端主控台啟動或關閉設備的管理存取權。

一旦啟動 SNMP 後，您必須在 Cloud Edge 設備的內部部署主控台中移至「管理 > 裝置管理 > SNMP 設定」來進行 SNMP 設定。啟動和設定 SNMP 支援後，使用者就可以使用 SNMP 管理程式取得支援的物件資訊。

對於具有無線網路功能的 Cloud Edge 設備，您可以啟動其主要無線網路或客體無線網路的管理存取權。在允許客體無線網路的管理存取權時，請務必注意安全問題。

啟動管理存取權

用途：啟動設備的遠端管理存取權。啟動 SNMP 可讓使用者從 SNMP 管理程式取得支援的物件資訊。

位置：「設備 >（選取的設備）> 網路 > 管理存取權」

步驟

1. 選取要為介面啟動的服務。
   - 內部部署主控台
   - Ping
   - SSH
   - SNMP
2. 在表格下的欄位中，指定允許遠端存取設備的 IPv4 位址。

注意

此設定決定可遠端存取設備的 IPv4 位址範圍。支援單一 IPv4 位址，並可使用 '-' 符號作為範圍標記。將 IPv4 位址與網路遮罩的格式設定為 `192.168.1.1/24`。若未指定任何項目，將允許所有 IPv4 位址。

管理存取權不支援 IPv6 位址。

3. 按一下「儲存」。

DHCP

您可以對 Cloud Edge 設備上的一個或多個 LAN 介面啟動動態主機組態設定通訊協定 (DHCP) 服務。每個啟動了 DHCP 服務的介面均做為 DHCP 伺服器，可指派 IPv4 位址和其他網路設定（例如預設設備與 DNS 設定）給內部用戶端。

如果有 DHCP 要求被導向至設有 DHCP 服務的介面，則 Cloud Edge 會自動回應這些要求。

- 指派 DNS 位址給用戶端時，您可以將 DHCP 設定為使用系統 DNS 設定、介面 IPv4 位址，也可以手動指定 DNS IPv4 位址的清單。
- 您可以設定 IPv4 位址集區，DHCP 伺服器會使用該集區來指派位址給 DHCP 用戶端。
  Cloud Edge 支援多個集區。您可以為每個介面建立單獨的 DHCP 集區。
- 還可以為每個 DHCP 伺服器進行 DCHP 進階伺服器設定（IPv4 位址靜態對應和 DHCP 租用時間）。

檢視 DHCP 服務

用途：檢視及管理 DHCP 設定。

位置：「設備 >（選取的設備）> 網路 > DHCP」

步驟

1. 檢視與任何 DHCP 服務相關聯的參數。

選項	說明
啟動	圖示表示服務的狀態：已啟動（綠色/開啟）或已關閉（紅色/關閉）。
名稱	DHCP 服務的名稱（範例：LAN1、LAN2）。 按一下介面名稱可修改 DHCP 設定。
IPv4 位址/網路遮罩	指派給介面的 IPv4 位址和子網路遮罩。
IP 集區	該 DHCP 服務之 IP 位址集區中的適用 IPv4 位址範圍。
選項	DNS 伺服器 IPv4 位址、設備 IPv4 位址和租用時間。只有當 DHCP 伺服器使用指定的 DNS 時，才會顯示 DNS IPv4 位址。

編輯 DHCP 設定

用途：修改設備 DHCP 設定。

位置：「設備 >（選取的設備）> 網路 > DHCP > 新增/編輯」

步驟

1. 視需要檢閱下列資訊：
   - DHCP 的部署模式資訊 第 6-68 頁

     您可以針對每一種部署模式將哪些介面設定為 DHCP 伺服器的相關資訊。
   - 預設 DHCP IP 位址集區 第 6-69 頁

     哪些 IP 位址已依預設指派給各 IP 位址集區。
2. 設定 DHCP 設定。

選項	說明
啟動 DHCP	選取以啟動服務。

選項	說明
IP 位址/網路遮罩	指派給介面的 IPv4 位址和子網路遮罩。
偏好的 DNS	選取偏好的 DNS 方法。 • 選取「使用系統 DNS 設定」，可使用「網路 > DNS」中所設定的設備系統 DNS。 • 選取「使用介面 IP 位址」，可使用介面 IPv4 位址做為 DNS。 • 選取「使用指定的 DNS 伺服器」，可手動設定 IPv4 位址做為 DNS 設定。
設備	系統會自動根據介面 IPv4 位址和網路遮罩設定填入 DHCP 伺服器設備。您可以選擇性變更 IPv4 設備位址。
IP 位址範圍的起點與終點	指定 IPv4 位址範圍，可建立 DHCP 組態設定適用的 IP 位址集區。

3. 設定「進階設定」。
   - 對於「租用時間」，調整所租用的 IPv4 位址與網路遮罩不再有效的時間與日期。

     指定天數、小時數或分鐘數。例如，如果您僅指定時數，則會限制只能在這個時數內使用租用。
   - 您可以使用靜態對應，手動將靜態 IPv4 位址繫結至特定 MAC 位址。

     對於「靜態對應」，指定 MAC 位址/IPv4 位址對應。您可以逗點分隔清單的形式輸入多個對應。範例：

     `00-FF-8A-B9-5A-49 / 192.168.1.1, 00:0C: 29:A9:69:25 / 192.168.2.1`。
4. 按一下「儲存」。

DHCP 的部署模式資訊

您應瞭解，對於每一種部署模式，您可以在哪些介面上設定 DHCP 服務。

- 橋接模式：MGMT 介面是唯一可設定為 DHCP 伺服器的介面。

  軟體切換：依預設，除了 MGMT 介面之外的所有介面都是屬於軟體切換的 L2 介面。WAN、LAN1 和 LAN2 介面都必須包含在切換組態設定中。

  如有需要，您可以從切換組態設定中移除 LAN3。從軟體切換組態設定中移除 LAN3 介面後，您可以將它變更為 L3 介面、為其指派 IPv4 位址，然後在介面上啟動 DHCP 服務。

- 路由模式：所有已啟動的 L3 介面皆可設定為 DHCP 伺服器。

採用硬體切換晶片組之設備的部署模式資訊

- 橋接模式：MGMT 介面是唯一可設定為 DHCP 伺服器的介面。

  除了 MGMT 介面之外的所有介面都是 L2 介面，並且是切換組態設定的一部分。這些介面無法從切換組態設定中移除，也無法設定為 DHCP 伺服器。

- 路由模式：所有已啟動的 L3 介面皆可設定為 DHCP 伺服器。

具有無線網路功能之設備的部署模式資訊

- 橋接模式：只有 MGMT 介面可設定為 DHCP 伺服器。
- 路由模式：所有 L3 介面皆可設定為 DHCP 伺服器，包括主要無線網路介面和客體無線網路介面在內。

  無線網路介面依預設會啟動 DHCP 服務。依預設，當您啟動無線網路時，會一併啟動該介面的 DHCP 服務。

  不過，如果在啟動無線網路之前關閉了無線介面的 DHCP 服務，然後稍後再啟動無線網路，則在啟動無線網路時不會啟動 DHCP 服務。在此情況下，您必須手動啟動該無線介面的 DHCP 服務。

預設 DHCP IP 位址集區

Cloud Edge 會為特定 L3 介面指派預設 DHCP IP 位址集區。

預設 DHCP IP 位址集區

介面	介面名稱	IP 位址集區
eth0	WAN	無
eth1	LAN1	192.168.100.1/24
eth2	LAN2	192.168.101.1/24
eth3	LAN3	192.168.102.1/24
eth4	MGMT	192.168.103.1/24

採用硬體切換晶片組之設備的預設 DHCP IP 位址集區

介面	介面名稱	IP 位址集區
eth0	WAN	無
eth1	LAN1	192.168.100.1/24
eth2	LAN2	192.168.101.1/24
eth3	LAN3	192.168.102.1/24
eth4	LAN4	192.168.103.1/24
eth5	LAN5	192.168.104.1/24
eth6	LAN6	192.168.105.1/24
eth7	LAN7	192.168.106.1/24
eth8	LAN8	192.168.107.1/24
eth9	MGMT	無

具有無線網路功能之設備的預設 DHCP IP 位址集區

無線介面	介面名稱	IP 位址集區
wlan0	<WIRELESS_SSID>	192.168.201.1/24
wlan1	<GUEST_WIRELESS_SSID>	172.16.20.1/24

動態 DNS

動態網域名稱系統 (DDNS) 會即時自動更新 Internet DNS 名稱伺服器，以將主機名稱的作用中 DNS 組態設定、位址與其他資訊保持最新。當企業經常變更公開「主機名稱與 IP 位址」對應（通常發生在公司使用 PPPoE 或 DHCP 來存取 Internet）時，一般會使用 DDNS。

但如果客戶想提供服務（如 Web 服務）給 Internet 上的其他使用者，動態 IP 位址會造成問題。由於 IP 位址可能會經常變更，因此必須快速重新對應 DNS 中的對應網域名稱，才能繼續存取已知的 URL。許多提供者會針對這種情況提供商用或免費的 DDNS 服務。通常會在使用者的路由器或電腦實作自動重新設定，以執行軟體來更新 DDNS 服務。雖然隨時間推移出現了一些標準的 Web-based 更新方法（RFC 2136 或其他通訊協定），但是使用者設備與提供者之間的通訊仍未標準化。

使用 DDNS 可自動化 Internet 上的新「主機名稱與 IP 位址」對應的散播。DDNS 服務提供者是管理此程序的代理人。Cloud Edge 設備的設計目的是，作為外部用戶端在嘗試連線到企業時，所連到的第一個連線 Internet 的裝置，它必須確保所有 Internet 使用者將其在企業端嘗試連線的每個主機名稱/網域的流量路由到自己。使用 DDNS 用戶端，Cloud Edge 可將「主機名稱與 IP 位址」變更傳遞給 DDNS 服務提供者。

支援的 DDNS 服務提供者

以下是 3 個支援的 DDNS 服務提供者：

提供者	使用者所在地
動態 DNS	全球
免費 DNS	
DNSPod	中國

注意

不支援 IPv6。

設定動態 DNS 設定

用途：根據服務廠商進行基本設定。所需資訊會因服務而異。基本上，每種服務皆需要網域名稱、帳號與密碼資訊。

位置：「設備 >（選取的設備）> 網路 > 動態 DNS」

步驟

1. 選取「開啟」以「啟動動態 DNS」。
2. 選取「廠商」。

   可用廠商包括 DynDNS、FreeDNS 和 DNSPod。

   如果設備上安裝的是 Cloud Edge 5.5 之前的版本，則「廠商」下拉式方塊中將不會提供「DNSPod」選項。
3. 執行適當的處理行動：
   - 對於 DynDNS 或 FreeDNS，請輸入「使用者名稱」和「密碼」。
   - 對於 DNSPod，請輸入「使用者識別碼」和「使用者 Token」。
4. 輸入網域資訊：
   - 對於 DynDNS 或 FreeDNS，請在「網域」中輸入 FQDN。
   - 對於 DNSPod，請在「主機記錄」中輸入主機名稱，並在「網域」中輸入網域名稱。
5. 選取 WAN 介面：

自動：	（預設）Cloud Edge 會根據 RFC 1597 自動探索具有非私人 IP 位址的介面。
（介面名稱）：	從可用介面清單中選取 WAN 介面（例如，WAN 或 LAN1）。

6. 如果已在「廠商」中選取「DynDNS」，則可選擇性啟動 HTTPS。

   DynDNS 會提供 HTTPS 連線的選項。有些廠商（例如 FreeDNS）不會公開 HTTPS 介面，而 DNSPod 則要求必須使用 HTTPS 連線。

7. 按一下「儲存」。

檢視 DDNS 狀態

用途：檢視目前的 DDNS 執行狀態。

位置：「設備 >（選取的設備）> 網路 > 動態 DNS > 狀態」

步驟

1. 檢視 DDNS 狀態訊息。

   請參閱 DDNS 狀態訊息 第 6-73 頁。

DDNS 狀態訊息

「動態 DNS > 狀態」標籤顯示目前的 DDNS 執行狀態，包含目前的介面（自動探索或指定）、WAN IP 位址與狀態訊息。

可能的狀態訊息包括：

- 成功
- 錯誤：驗證失敗
- 錯誤：帳號尚未啟動
- 錯誤：網域資訊無效或未註冊
- 錯誤：Internet 存取無法使用或無法連線到服務廠商
- 錯誤：已使用部分付費使用者專屬功能（例如，HTTPS 連線服務），相關設定已重設
- 錯誤：服務廠商發出服務無法使用的訊息
- 錯誤：未偵測到可用的 WAN IP
- 錯誤：指定的介面沒有適當的 IP
- 錯誤：服務介面可能已變更，請聯絡趨勢科技進行更新

- 錯誤：驗證失敗次數過多，已暫時禁用帳號
- 錯誤：子網域資訊無效或未註冊
- 錯誤：不允許以循環配置資源方式更新主機。
- 錯誤：未知的錯誤，請檢查您的 `Internet` 存取。
- 未啟動

路由資料表

在原廠預設組態設定中，Cloud Edge 路由資料表包含一個靜態 IPv4 預設路由。透過定義其他 IPv4 靜態路由，可新增路由資訊到路由資料表。資料表可能包含數個路由到相同目標的不同路由，這表示這些路由中指定的下一個躍點路由器的 IPv4 位址或與這些路由相關聯的 Cloud Edge 介面可能不同。

Cloud Edge 會評估路由資料表中的資訊，然後選取到目標的最佳路由，通常是 Cloud Edge 設備與最接近之下一個躍點路由器之間的最短距離。在某些情況下，如果最佳路由不可用，則會選擇距離較長的路由。Cloud Edge 會在裝置的轉送資料表（裝置之路由資料表的子集）中安裝可用的最佳路由。系統會根據轉送資料表中的資訊轉送封包。

注意

Cloud Edge 不支援 IPv6 路由。

檢視路由資料表

用途：檢視路由資料表以瞭解不同來源的 IPv4 網路流量如何路由至目標 — 這些路由中指定的下一個躍點路由器的 IPv4 位址或與這些路由相關聯的 Cloud Edge 介面可能不同。

位置：「設備 >（選取的設備）> 網路 > 路由資料表」

步驟

1. 檢視資料表指標。

請參閱路由資料表指標 第 6-75 頁。

路由資料表指標

下表說明路由資料表指標。

代碼	定義
K	核心路由
C	已連線
S	靜態

靜態路由

靜態路由會控制流量在連線至網路的端點之間移動的方式。定義 IPv4 靜態路由可為 Cloud Edge 提供將封包轉送至特定目標的資訊。設定 IPv4 靜態路由的方式是定義要 Cloud Edge 設備攔截的封包的目標 IPv4 位址和網路遮罩，以及指定這些封包的設備 IPv4 位址。設備位址會指定流量將路由到的下一個躍點路由器。

您可以指定封包經由哪個介面傳輸出去，以及將封包路由到哪個裝置。位於「設備 > （設備名稱） > 網路 > 靜態路由」的靜態路由清單會顯示 Cloud Edge 設備用於比對封包標頭以路由封包的資訊。

新增靜態路由

新增 IPv4 靜態路由時，Cloud Edge 會檢查 Cloud Edge 路由資料表中是否已存在相符的路由和目標。如果找不到相符項，Cloud Edge 就會將路由新增到路由資料表中。

注意

由於路由模式不支援 IPv6，您只能設定 IPv4 靜態路由。

步驟

1. 移至「設備 > （設備名稱） > 網路 > 靜態路由」。
2. 按一下「新增」以新增預設路由。

   「新增/編輯靜態路由」視窗隨即出現。
3. 選取「啟動靜態路由」。
4. 在「目標網路」中，指定網路位址。

   下列任何選項均屬有效選項：

   - IP 位址
   - 預設設備（範例： `10.10.10.10/16`）

     注意

     如果設定多個預設設備，則會使用循環配置資源選取方式從這些設備路由輸出流量。
   - 位元遮罩

     注意

     位元遮罩是網路遮罩的十進位等值。
   - 類別網域間路由 (CIDR) 標記法（範例： `255.255.255.0/24`）
5. 在「下一個躍點」中，指定下一個躍點的 IPv4 位址。
6. 按一下「儲存」。

啟動/關閉靜態路由

步驟

1. 移至「設備 > （設備名稱） > 網路 > 靜態路由」。
2. 在靜態路由清單中，執行下列其中一項作業：
   - 選取「啟動」圖示 () 來啟動靜態路由。
   - 取消選取「啟動」圖示 () 來關閉靜態路由。

修改靜態路由

步驟

1. 移至「設備 > （設備名稱） > 網路 > 靜態路由」。
2. 執行下列其中一項作業：
   - 在「路由 ID」欄，按一下路由名稱。
   - 在「處理行動」欄，按一下編輯圖示 ()。

   「新增/編輯靜態路由」畫面隨即出現。
3. 使用核取方塊啟動或關閉靜態路由。
4. 檢視網路 IP 位址/位元遮罩。這是唯讀欄位。
5. 指定下一個躍點參數。
6. 按一下「套用」。

刪除靜態路由

步驟

1. 移至「設備 > （設備名稱） > 網路 > 靜態路由」。
2. 在「處理行動」欄中，按一下刪除圖示 ( )。
3. 按一下「刪除」以確認刪除。

網路位址轉譯 (NAT)

使用網路位址轉譯 (NAT) 策略，以指定是否要在第 3 層介面上的公開和私人位址以及通訊埠之間轉換來源或目標 IP 位址和通訊埠。例如，可以將從內部（受信任）區域傳送至公用（不受信任）區域之流量的私人來源位址轉址為公用位址。

下列 NAT 策略規則會將私人來源位置範圍（`10.0.0.1` 到 `10.0.0.100`）轉址為單一公用 IP 位址 (`200.10.2.100`) 和一個唯一的來源通訊埠號碼（動態來源轉譯）。此規則僅會套用至內部（受信任）區域中第 3 層介面上接收的流量，而該流量的目標是公用（不受信任）區域中的介面。由於私人位址是隱藏的，因此將從公用網路起始網路作業階段。如果公用位址不是 Cloud Edge 介面位址（或位於同一子網路），則本機路由器需要靜態路由來將流量直接傳回至 Cloud Edge。

圖 6-3. 簡單 NAT 規則

NAT 規則

NAT 位址轉譯規則的依據是來源和目標 IPv4 位址及通訊埠。如同安全策略，系統會針對輸入流量逐一比對 NAT 策略規則，然後套用與流量相符的第一個規則。

您可以將 NAT 規則套用至除 MGMT 介面之外的所有實體介面。

對於具有無線網路功能的 Cloud Edge 設備，在已啟動無線網路（主要或客體）的情況下，您可以設定無線網路介面的 NAT 規則。

如有需要，可在本機路由器中新增靜態路由，以將流向所有公用 IPv4 位址的流量路由至 Cloud Edge。此外，也可以在 Cloud Edge 上的接收介面中新增靜態路由，以將流量路由回私人 IPv4 位址。

用戶端和伺服器皆透過同一個 LAN 介面存取設備時的考量事項

當用戶端和伺服器透過同一個 LAN 介面存取 Cloud Edge 設備時，用戶端將無法根據網域名稱存取此伺服器。您可以同時新增來源 NAT 規則和目標 NAT 規則到這個 LAN 介面，來解決此情況。請參閱新增 NAT 規則以支援 Hairpin NAT 第 6-83 頁。

新增目標 NAT 規則

目標 NAT (DNAT) 會變更封包的 IP 標頭中的目標位址。這項作業的主要目的是，將目標為公開位址/通訊埠的內送封包重新導向至網路內的私人 IP 位址/通訊埠。

步驟

1. 移至「設備 > （選取的設備） > 網路 > NAT > 新增」。
2. 選取「目標」做為「NAT 類型」。
3. 進行 NAT 設定：

選項	說明
入口介面	從下拉式清單中選取「任意」或任何 L3 介面，以作為來自網路路由器外部並朝網路內部目標方向前進的網路流量的介面。

選項	說明
	對於具有無線網路功能的 Cloud Edge 設備，在已啟動無線網路（主要或客體）的情況下，您可以選取無線網路介面做為入口介面。
目標 IP 轉譯	您可以選取下列選項： • 「入口介面 IP 位址」，然後指定「轉譯的 IP 位址/範圍」。 入口介面用於外部 IP 位址，而指定的轉譯 IP 位址/範圍則是用於將入口介面 IP 位址轉譯（對應）至內部 IP 位址。 • 「虛擬 IP」，然後指定「外部 IP 位址/範圍」和「轉譯的 IP 位址/範圍」。 您必須明確指定外部 IP 位址/範圍，方可用於進行 NAT 對應。 系統會根據開頭 IP 位址自動產生轉譯的 IP 位址範圍。系統會以一對一方式，將外部 IP 位址對應到轉譯的 IP 位址。
說明	指定 NAT 規則用途或組態設定的識別特性。
通訊埠轉送	通訊埠轉送：選取「開啟」可使用通訊埠轉送來進行靜態一對一 NAT 對應。 勾選「開啟」後，外部 IP 位址會一律轉譯為相同的對應 IP 位址，而外部通訊埠號碼則會一律轉譯為相同的對應通訊埠號碼。 如果設定為「開啟」，請指定下列項目： • 通訊協定：選取「TCP」或「UDP」。 • 外部服務通訊埠：指定通訊埠範圍。 對應至通訊埠：指定通訊埠。 指定「外部服務通訊埠」範圍時，系統會根據開頭通訊埠自動產生「對應至通訊埠」。對應方式為一對一對應。
設定比對條件	您可以指定更詳細的資訊或比對條件，包括： • 來源 IP 位址範圍 • 來源通訊埠範圍

4. 按一下「儲存」。
5. 確認新規則是否新增到 NAT 規則的清單中。

修改 NAT 規則

步驟

1. 移至「設備 > （選取的設備） > 網路 > NAT」。
2. 在「轉址自」欄中，按一下要變更的 NAT 規則。
3. 視需要編輯參數。
4. 按一下「儲存」。

變更 NAT 規則優先順序

步驟

1. 移至「設備 > （選取的設備） > 網路 > NAT」。
2. 選取要變更優先順序之 NAT 規則的核取方塊。
3. 若要重新安排順序，請選取「移動」，並使用 NAT 規則清單上方的運算子（上移、下移、頂端、底端）。

新增來源 NAT 規則

來源 NAT (SNAT) 會變更封包的 IP 標頭中的來源位址。主要目的是為離開網路的封包，將私人 (RFC 1918) 位址/通訊埠變更為公開位址/通訊埠。Cloud Edge 會自動建立預設來源 NAT 規則。您可以建立其他來源 NAT 規則或修改預設來源 NAT 規則。若要修改預設來源 NAT 規則，請參閱修改 NAT 規則 第 6-81 頁。

步驟

1. 移至「設備 > （選取的設備） > 網路 > NAT > 新增」。
2. 為「NAT 類型」選取「來源」。

3. 進行 NAT 設定：

選項	說明
出口介面	從下拉式方塊清單中選取「任意」或任何 L3 介面（例如 WAN），以做為出口流量（即來自網路內部的流量）的介面。 對於具有無線網路功能的 Cloud Edge 設備，在已啟動無線網路（主要或客體）的情況下，您可以選取無線網路介面做為出口介面。
來源 IP 轉譯/轉址為	針對來源 IP 轉譯，選取下列其中一種方法： • 出口介面 IP 位址 如果選取此方法，則無法使用「轉址為」選項。出口介面的 IP 位址用於轉譯。 • 「單一 IP 位址」，然後為「轉址為」指定 IP 位址 指定的 IP 位址用於轉譯。 • 「IP 位址範圍」，然後為「轉址為」指定 IP 位址範圍 指定的 IP 位址範圍用於轉譯。 • 「子網路」，然後為「轉址為」指定子網路 子網路用於轉譯。 注意 如果選取「單一 IP 位址」、「IP 位址範圍」或「子網路」，則必須為「出口介面」選項明確指定 L3 介面。
說明	指定 NAT 規則用途或組態設定的識別特性。
設定比對條件	您可以展開「設定比對條件」區段，以指定更詳細的資訊或比對條件，包括： • 通訊協定 — 任意、TCP、UDP 或 ICMP。「任意」表示所有通訊協定。 • 來源 IP 位址範圍 — 由網路指定。 • 來源通訊埠範圍 — 由管理員指定。 • 目標 IP 位址範圍 — 由管理員指定。 • 目標通訊埠範圍 — 由管理員指定。

選項	說明
	注意 如果您為「通訊協定」指定 ICMP，則無法使用「來源通訊埠範圍」和「目標通訊埠範圍」選項。

4. 按一下「儲存」。
5. 確認新規則是否新增到 NAT 規則的清單中。

刪除 NAT 規則

步驟

1. 移至「設備 > （選取的設備） > 網路 > NAT」。
2. 選取要刪除的 NAT 規則所在的列。
3. 按一下「刪除」。

   「刪除」確認訊息隨即出現。
4. 若要確認，請按一下「刪除」。
5. 確認 NAT 規則已不在 NAT 規則清單中。

新增 NAT 規則以支援 Hairpin NAT

當用戶端和伺服器透過同一個 LAN 介面存取 Cloud Edge 設備時，用戶端將無法根據網域名稱存取此伺服器。若要解決此情況，請同時新增來源 NAT 規則和目標 NAT 規則到此 LAN 介面。請使用下列程序來執行此組態設定。

步驟

1. 移至「設備 > （選取的設備） > 網路 > NAT > 新增」。
2. 針對「NAT 類型」選取「來源」。

3. 針對「出口介面」設定用戶端和伺服器所連結的 LAN 介面。
4. 針對「來源 IP 轉譯」選取「出口介面 IP 位址」。
5. 按一下「儲存」。
6. 移至「設備 > （選取的設備） > 網路 > NAT > 新增」。
7. 針對「NAT 類型」選取「目標」。
8. 針對「入口介面」設定用戶端和伺服器所連結的 LAN 介面。
9. 針對「目標 IP 轉譯」選取「虛擬 IP」。
10. 將「外部 IP 位址/範圍」設定為已向 DNS 伺服器註冊的伺服器 Internet IP 位址。
11. 將「轉譯的 IP 位址/範圍」設定為伺服器的本機 IP 位址。
12. 按一下「儲存」。
13. 確認新規則已新增至 NAT 規則清單中。

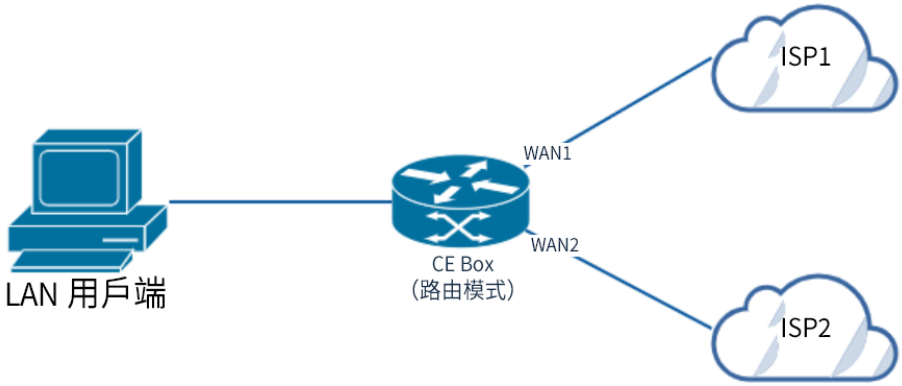
SD-WAN

軟體定義廣域網路 (SD-WAN) 是一種以軟體管理廣域網路的技術，不僅能簡化部署、實現集中管理並降低成本，還可提升與 Internet 及雲端的連線能力。

SD-WAN 的關鍵應用在於可讓企業採用低成本的市售 Internet 存取權建置高效能 WAN，從而使企業能夠局部或全部取代費用較高的私人 WAN 連線技術（例如 MPLS）。

為了完整利用 SD-WAN 功能，使用必須在 CE 內部部署 UI 中對其網路拓樸進行變更並執行組態設定。

Cloud Edge WAN 支援三種模式：PPPoE、DHCP 和靜態。如果想要啟動 SD-WAN，您必須有兩個已就緒的 WAN 連結（WAN1 和 WAN2/LAN1）。請參閱下圖：



注意

- 如果您的 WAN 介面使用靜態 IP，請務必在內部部署主控台中正確設定 WAN1 和 WAN2 的設備。如果您將適用於 CE box 的設備保持為未設定（空白），則在部署 SD-WAN 設定時，該部署將會失敗。

Cloud Edge 提供三種類型的路由策略：

- 靜態路由
- SD-WAN 路由
- 策略路由

在部署 SD-WAN 後，路由策略的優先順序應為：

靜態路由 > SD-WAN 路由 > 策略路由

啟動 SD-WAN 和頻寬設定

用途：啟動 SD-WAN 功能並檢視 SD-WAN 總覽組態設定和介面使用情況。

位置：「設備 >（選取的設備）> SD-WAN > 首頁」

步驟

1. 按一下「啟動 SD-WAN」旁的「開啟」按鈕。
2. 「SD-WAN 上行」下方的「WAN1」和「WAN2」欄位均為唯讀，只能在 Cloud Edge 內部部署主控台中進行編輯。若要瞭解如何管理所選設備的網路介面設定，請參閱編輯網路介面 第 6-48 頁。
3. 在「頻寬設定」下方，請從下拉式清單中選取「WAN1」（預設值）。設定上游頻寬和下游頻寬並指定限制值。此外，也請使用下拉式清單來設定 Mbps 和 Kbps 限制值。

   注意

   步驟為 3 為選擇性執行的步驟。

4. 按一下「儲存」。

總覽 Widget

在啟動 SD-WAN 後，您可以在「SD-WAN 首頁」上查看磁碟區和頻寬資料。其中還會顯示您設定了多少個 SD-WAN 規則和健全狀況檢查 SLA。

在「SD-WAN 首頁」底部，顯示兩種類型的總覽 Widget。它們分別是「組態設定總覽」和「頻寬和磁碟區使用量」。

- 組態設定總覽：顯示已新增的 SD-WAN 規則數目，以及已建立的健全狀況檢查 SLA 數目。
- 頻寬和磁碟區使用量：「頻寬」標籤顯示 WAN 介面（WAN1 和 WAN2）的上游和下游。「磁碟區」標籤顯示 WAN 介面（WAN1 和 WAN2）的已傳送和已接收的流量磁碟區。

注意

若要快速取得 SD-WAN 規則和健全狀況檢查 SLA，請在「組態設定總覽」下方按一下連結至「規則」頁面或「SLA」頁面的編號（在「SD-WAN 規則」或「健全狀況檢查 SLA」的上方）。

SD-WAN 規則

SD-WAN 規則用於路由所需流量，並在 SLA 的協助下，將流量動態轉送至最佳連結。SD-WAN 規則提供三種模式：

- 最佳品質：在所需的網路效能參數中選取最佳連結。
- 最大化頻寬：選取可完全利用 Internet 頻寬的連結。
- 偏好的連結：選取優先順序較高的連結來轉送流量。

Cloud Edge 使用 DPI 引擎來偵測流量並快取身分識別，以實作應用程式感知路由。

使用 SD-WAN 規則為 SD-WAN 成員介面之間的 WAN 流量進行動態路徑選擇。

SD-WAN 規則具有下列功能與特性：

- 預設的 SD-WAN 規則可以按來源 IP、來源-目標 IP、作業階段或磁碟區來執行負載平衡。您無法設定預設規則中的任何 SLA。
- 對於預設的 SD-WAN 規則，「作業階段」和「磁碟區」的權重是以百分比表示。權重的總和必須是 100%。
- 您可以定義最多 200 個 SD-WAN 規則（包含一個預設規則在內）。

請在「設備 > （選取的設備） > SD-WAN > 規則」中執行下列作業：

- 檢視現有規則清單
- 新增、編輯、複製及刪除規則
- 變更規則優先順序
- 啟動和關閉規則
- 搜尋

注意

按一下「全部部署」按鈕以部署 SD-WAN 設定（所有組態設定會同時部署，而不會分多次部署 SD-WAN 設定）。

注意

您無法關閉、刪除、移動或複製預設的 SD-WAN 規則。

有 3 種事件會觸發 SD-WAN 規則來重新路由流量：

- 介面離線：此介面的實際狀態為離線。例如，纜線已拔除、介面發生硬體問題，或定向介面連線已中斷。
- SLA 已關閉：從 Cloud Edge 設備到監控伺服器的流量，無法接收超過使用者所設定之「失敗次數閾值」值的回應。
- 不符合 SLA：SLA 效能偵測資料超過使用者所設定的閾值。

對於所有「最佳品質」策略，當策略本身已指定效能指標時，所選健全狀況檢查 SLA 的 SLA 參數將不會生效。

對於「最大化頻寬」和「偏好的連結」策略，如果兩個 WAN 連結中的某一個不符合 SLA 參數，系統便會將流量重新路由至替代連結。

其他 2 種事件將在透過各種策略重新路由流量時生效。

此外，上述全部 3 種事件的優先順序排序如下所示：

1. 介面離線（最高）
2. SLA 已關閉（中）
3. 不符合 SLA（最低）

管理 SD-WAN 規則

用途：管理 SD-WAN 規則以控制通過已註冊設備的流量。

位置：「設備 >（選取的設備）> SD-WAN > 規則」

步驟

1. 執行下列動作：
   - 檢視現有 SD-WAN 規則的相關資訊。

- 按一下規則名稱左側的展開箭頭，即可檢視關於該規則之 SD-WAN 組態設定的其他詳細資訊。
- 按一下「新增」以建立新規則。

注意

第一次啟動 SD-WAN 時，系統會自動新增預設的 SD-WAN 規則。

- 使用右上方的「搜尋」來尋找規則。
- 按一下規則的名稱以檢視或修改設定。
- 選取規則，然後按一下「編輯」以檢視或修改設定。
- 選取規則，然後按一下「移動」以變更規則優先順序。
- 選取規則，然後按一下「更多」以變更狀態或複製規則。
- 選取規則，然後按一下「刪除」以移除規則。

新增/編輯 SD-WAN 規則

用途：透過指定使用者或使用者群組、IP 位址或 FQDN，來新增或編輯 SD-WAN 規則。

位置：「設備 > （選取的設備） > SD-WAN > 規則 > 新增/編輯」

步驟

1. 在「新增/編輯 SD-WAN 規則 > 規則名稱」頁面上：
   a. 指定「規則名稱」（長度為 1 到 32 個字元，且包含字母、數字或底線）。
   b. 指定「說明」（選用）。
   c. 按「下一個」。

> **注意**
>
> 按一下 SD-WAN 規則名稱即可對其進行編輯。

2. 請在「新增/編輯 SD-WAN 規則 > 來源」頁面上，設定「來源」。

   a. 如果要將此 SD-WAN 規則套用至任何使用者群組或 IP，請選取「任意」。

   b. 如果要將此 SD-WAN 規則套用至特定使用者或使用者群組，請選取「選取的使用者/使用者群組」。然後在「從下列選項中選取」方塊中選取使用者或使用者群組，並將其移至「已選取」方塊。

   c. 如果要將此 SD-WAN 規則套用至特定 IP 位址和 FQDN，請選取「選取的 IP 位址/FQDN」。然後在「從下列選項中選取」方塊中選取 IP 位址或 FQDN，並將其移至「已選取」方塊。按一下「新增 IP 位址/FQDN 物件」以新增 IP 位址或 FQDN 物件（請參閱新增/編輯 IP 位址/FQDN 物件 第 6-161 頁）。請使用「搜尋」方塊來搜尋任何已選取的使用者/使用者群組/IP 位址/FQDN。

   d. 按「下一個」。

3. 請在「新增/編輯 SD-WAN 規則 > 目標」頁面上，設定「目標」。

   a. 如果要將此 SD-WAN 規則套用至任何 IP 位址或 FQDN，請在「位址」下方選取「任意」。如果要將此 SD-WAN 規則套用至特定 IP 位址和 FQDN，請選取「選取的 IP 位址/FQDN」。

   b. 如果要將此 SD-WAN 規則套用至任何服務或應用程式，請在「服務與應用程式」下方選取「任意」。如果要將此 SD-WAN 規則套用至特定服務，請選取「選取的服務」。按一下「新增服務物件」以新增服務物件。如果要將此 SD-WAN 規則套用至特定應用程式，請選取「選取的應用程式」。按一下「新增應用程式群組」以新增應用程式群組。

   c. 按「下一個」。

4. 請在「新增/編輯 SD-WAN 規則 > 策略」頁面上，設定「策略」。

   a. 如果要使用低延遲的連結，請選取「最佳品質 — 延遲」。

   b. 如果要根據下列 3 個選項來排定流量的優先順序，請選取「進階」：

- 最大化頻寬：使用「最大化頻寬」可讓流量分佈在所有可用的連結。
- 最佳品質：使用「最佳品質」可從下拉式清單中選取品質條件（「時基誤差」、「封包遺失」或「頻寬」）。或在下拉式清單中按一下「自訂資料檔」以設定「延遲」、「時基誤差」、「封包遺失」或「頻寬」的百分比配置。
- 偏好的連結：若要將流量傳送到您從「選取連結」下拉式清單中選取的實體連結，請使用「偏好的連結」，但不符合 SLA 的連結則不適用。從「選取連結」下拉式清單中選取「WAN1」或「WAN2」。

c. 按「下一個」。

5. 在「新增/編輯 SD-WAN 規則 > 健全狀況檢查 SLA」頁面上，選取使用者定義的健全狀況檢查 SLA 或建立新的健全狀況檢查 SLA。（請參閱 SLA 第 6-94 頁）您可以選擇性地按一下「新增健全狀況檢查 SLA」來新增健全狀況檢查 SLA。

   a. 在「新增/編輯健全狀況檢查 SLA > 一般」頁面上，請指定「SLA 名稱」、「說明」、「監控伺服器」和通訊協定的「類型」。按一下「新增伺服器」以新增第二台伺服器。（注意：您可以新增第二台伺服器，亦可在不需要時將其移除。）然後按「下一個」。

   b. 在「新增/編輯健全狀況檢查 SLA > SLA 參數」頁面上，從「建議的 SLA」中選擇 SLA 參數，或是針對「延遲」、「時基誤差」和「封包遺失」輸入自訂參數。[注意：Cloud Edge 雲端主控台 (CECC) 提供 4 個預先定義的 SLA（VoIP 視訊、音訊串流、一般網路和 Office 365）]（請參閱「建議的 SLA 類型和說明」資料表）。然後按「下一個」。

   c. 在「新增/編輯健全狀況檢查 SLA > 連結檢查狀態」頁面上，請設定連結檢查狀態的閾值和時間間隔。然後按「下一個」。

   d. 在「新增/編輯健全狀況檢查 SLA > 離線時的處理動作」頁面上，透過選取「更新靜態路由」，即可在出現不符合 SLA 參數的情況時關閉靜態路由。（注意：當連結處於離線狀態時，如果啟動了路由，該連結上的路由將會被移除，而流量會透過其他連結路由。當連結恢復上線時，路由即會重新啟動。）然後按一下「儲存」。（注意：按一下「儲存」後，畫面會回到「新增/編輯 SD-WAN 規則 > 健全狀況檢查 SLA」頁面。）然後按「下一個」。

6. 在「新增/編輯 SD-WAN 規則 > 檢閱」頁面上，請檢閱 SD-WAN 規則的詳細資訊，然後按一下「儲存」。按一下「儲存」後，畫面會回到「規則」頁面。

編輯預設 SD-WAN 規則

用途：用於變更負載平衡模式或調整介面權重。

位置：「設備 >（選取的設備）> SD-WAN > 規則 > 編輯預設 SD-WAN 規則」

啟動並儲存 SD-WAN 後，系統即會建立預設的 SD-WAN 規則。預設的 SD-WAN 規則可以按來源 IP 和目標 IP、作業階段或磁碟區來執行負載平衡。您無法設定預設規則中的任何 SLA。對於預設的 SD-WAN 規則，「作業階段」和「磁碟區」的權重是以百分比表示。權重的總和必須是 100%。

第一次啟動 SD-WAN 時，系統會建立預設的 SD-WAN 規則，其會出現在「設備 >（選取的設備）> SD-WAN > 規則」頁面中。

步驟

1. 在「負載平衡模式」下方，選取用於對 WAN1 連結與 WAN2 連結之間流量進行負載平衡的模式。
   a. 如果要根據來源 IP 進行流量負載平衡，請選取「來源 IP」。
   b. 如果要根據來源 IP 和目標 IP 的組合進行流量負載平衡，請選取「來源 IP 和目標 IP」。
   c. 如果要根據作業階段數目的比例來進行負載平衡，請選取「作業階段」。請使用百分比來設定權重（權重的總和必須是 100%）。
   d. 如果要根據頻寬比例來進行負載平衡，請選取「磁碟區」。請使用百分比來設定磁碟區的權重（權重的總和必須是 100%）。
2. 按一下「儲存」。

複製 SD-WAN 規則

用途：複製 SD-WAN 規則。新規則的優先順序最高。

位置：「設備 >（選取的設備）> SD-WAN > 規則」

注意

您無法複製預設的 SD-WAN 規則。

步驟

1. 選取要複製的 SD-WAN 規則旁的核取方塊，然後按一下「更多」下拉式功能表。
2. 按一下「複製」。
3. 確認新的 SD-WAN 規則（名稱帶有複製的編號）出現在「SD-WAN > 規則」的清單中。

移動 SD-WAN 規則

用途：移動並變更使用者定義的 SD-WAN 規則的優先順序。

位置：「設備 >（選取的設備）> SD-WAN > 規則」

注意

您無法移動預設的 SD-WAN 規則。

步驟

1. 選取要移動並變更優先順序的 SD-WAN 規則旁的核取方塊。
2. 按一下「移動」下拉式功能表，然後選取「上移」、「下移」、「頂端」或「底端」。

啟動/關閉 SD-WAN 規則

用途：啟動使用者定義的 SD-WAN 規則，或是關閉已啟動的 SD-WAN 規則。

位置：「設備 >（選取的設備）> SD-WAN > 規則」

注意

您無法啟動或關閉預設的 SD-WAN 規則。

步驟

1. 選取要啟動或關閉的 SD-WAN 規則旁的核取方塊。
2. 按一下「更多」下拉式功能表，然後選取「啟動」或「關閉」。

刪除 SD-WAN 規則

用途：刪除使用者定義的 SD-WAN 規則。

位置：「設備 >（選取的設備）> SD-WAN > 規則」

步驟

1. 選取要刪除的 SD-WAN 規則旁的核取方塊。
2. 按一下「刪除」。
3. 確認已刪除的 SD-WAN 規則未列在「SD-WAN > 規則」的清單中。

SLA

服務層級合約 (SLA) 是服務提供者與其客戶雙方之間簽訂的合約。

SLA 連結的監控會透過以下方式來測量已連線至 SD-WAN 成員介面之連結的健全狀況：將探查封包透過每個 WAN 介面傳送到伺服器，並根據延遲、時基誤差和封包遺失來測量連結品質。如果某個連結損壞，SLA 會偵測此事件，並通知 Cloud Edge 設備將流量重新路由至替代連結。當損壞的連結恢復運作時，Cloud Edge 設備會復原該連結，並重新在可用的連結上路由流量。這可避免流量被傳送至損壞的連結，進而導致流量中斷。

Cloud Edge 建議使用以下四種 SLA：

- VoIP 視訊
- 音訊串流
- 一般網路
- Office 365

注意

在「管理 SLA」頁面的底端，提供四個建議的 SLA。當您將滑鼠游標移到建議的 SLA 上方時，將會顯示範例說明。

Cloud Edge 支援最多 50 個 SLA。

管理 SLA

用途：管理 SLA 以測量已連線至 SD-WAN 成員介面之連結的健全狀況。

位置：「設備 >（選取的設備）> SD-WAN > SLA」

步驟

1. 執行下列動作：
   - 選取 SLA，然後按一下「延遲」、「時基誤差」或「封包遺失」按鈕，以檢視該 SLA 的相關資訊。
   - 使用下窗格右上方的「搜尋」，以搜尋 SLA。
   - 按一下「新增」以建立新 SLA。
   - 選取 SLA 並按一下「編輯」以修改 SLA 設定，或按一下 SLA 名稱以編輯 SLA。
   - 選取 SLA，然後按一下「刪除」，可移除該 SLA。

   在「SLA 組態設定」頁面上，Cloud Edge 雲端主控台提供逐步操作 UI，讓使用者用於設定 SLA。設定 SLA 時，請注意下列事項：

- 設定 SLA 名稱和監控伺服器。伺服器可以是 FQDN 或 IP 位址。
- 最多可設定兩台監控伺服器。

> **注意**
>
> 如果設定兩台監控伺服器，第一台伺服器的優先順序更高。在 Cloud Edge 雲端主控台中，顯示的 SLA 資料預設為第一台伺服器的資料。當第一台伺服器離線時，系統會檢查是否可連線到第二台伺服器。如果可連線，系統會使用第二台伺服器的 SLA 資料。如果兩台伺服器皆無法連線，表示 SLA 已關閉。

- 要設定的偵測類型包括 PING 和 HTTP。

> **注意**
>
> 有些伺服器會禁止 PING 或 HTTP，因此在設定監控伺服器時，務必確認監控伺服器允許 PING 或 HTTP。

新增/編輯健全狀況檢查 SLA

用途：新增或編輯可測量已連線至 SD-WAN 成員介面之連結健全狀況的健全狀況檢查 SLA。

位置：「設備 >（選取的設備）> SD-WAN > SLA」

步驟

1. 在「新增/編輯健全狀況檢查 SLA > 一般」頁面上，請指定「SLA 名稱」、「說明」、「監控伺服器」和通訊協定的「類型」。按一下「新增伺服器」以新增第二台伺服器。（注意：您可以新增第二台伺服器，亦可在不需要時將其移除。）然後按「下一個」。
2. 在「新增/編輯健全狀況檢查 SLA > SLA 參數」頁面上，從建議的 SLA 中選擇 SLA 參數，或是輸入自訂參數。此外，也請指定「延遲」、「時基誤差」和「封包遺失」的參數。注意：Cloud Edge 雲端主控台 (CECC) 提供 4 個預先定義的 SLA（VoIP 視訊、音訊串流、一般網路和 Office 365）（請參閱「建議的 SLA 類型和說明」資料表）。然後按「下一個」。

3. 在「新增/編輯健全狀況檢查 SLA > 連結檢查狀態」頁面上，請設定連結檢查狀態的閾值和時間間隔。然後按「下一個」。

4. 在「新增/編輯健全狀況檢查 SLA > 離線時的處理動作」頁面上，透過選取「更新靜態路由」，即可在出現不符合 SLA 參數的情況時關閉靜態路由。（注意：當連結處於離線狀態時，如果啟動了靜態路由，該連結上的靜態路由將會被移除，而流量會透過其他連結路由。當連結恢復上線時，靜態路由即會重新啟動。）然後按一下「儲存」。按一下「儲存」後，畫面會回到「管理 SLA」頁面。

刪除 SLA

用途：刪除 SLA。

位置：「設備 >（選取的設備）> SD-WAN > SLA」

步驟

1. 選取要刪除的 SLA 旁的核取方塊。

2. 按一下「刪除」。

3. 確認已刪除的 SLA 未列在「SD-WAN > SLA」的清單中。（注意：如果 SLA 已在 SD-WAN 規則中使用，則無法將其刪除。）

無線

針對已註冊的設備，檢視其無線一般設定的相關資訊，以及設定其無線網路存取控制設定。

檢視無線網路資訊

您可以從 Cloud Edge 雲端主控台檢視無線網路的相關資訊。

檢視無線網路一般設定

用途：檢視無線網路的一般設定。

位置：「設備 > （選取的設備） > 無線 > 無線設定 > 一般設定」

步驟

1. 檢視下列設定的資訊：
   - 無線網路存取點

     顯示無線存取是否已啟動。啟動此設定，亦會啟動主要無線網路。但不會啟動客體無線網路。不過，必須先啟動此設定，然後才能啟動客體無線網路。預設為啟動。
   - 國家/地區
   - 頻率

     Cloud Edge 支援 2.4 Ghz 和 5.0 Ghz 頻率。
   - 啟動 SSID 廣播

     啟動後，Cloud Edge 設備會廣播 SSID，讓附近的用戶端可以在「可用的無線網路」畫面上看到主要無線網路。
   - SSID

     顯示主要無線網路的 SSID。
   - 通道
   - 模式

     此設定同時適用於主要無線網路和客體無線網路。
   - 安全性

     顯示主要無線網路的安全設定。
2. 檢視下列進階設定的資訊：
   - DTIM 間隔（預設）

- 指標間隔
- 簡短前序編碼
- RTS 閾值
- 啟動短 GI
- 傳輸功率

注意

網路頻率設定為 5 GHz 時，只會顯示「DTIM 間隔」、「指標間隔」和「傳輸功率」等欄位。

檢視無線客體網路設定

用途：檢視無線網路的一般設定。

位置：「設備 > （選取的設備） > 無線 > 無線設定 > 客體網路」

步驟

1. 檢視下列設定的資訊：
   - 啟動客體網路

     顯示客體網路處於啟動還是關閉狀態。預設為關閉。
   - 啟動存取區域網路

     顯示客體無線網路上具有適當權限的使用者是否可以存取內部區域網路上的資源。預設為關閉。
   - 啟動 SSID 廣播

     啟動後，Cloud Edge 設備會廣播 SSID，讓附近的用戶端可以在「可用的無線網路」畫面上看到客體無線網路。
   - SSID

     顯示客體網路的 SSID。

- 安全性

  顯示客體網路的安全設定。

檢視無線疑難排解資訊

用途：檢視無線網路的疑難排解資訊。

位置：「設備 > （選取的設備） > 無線 > 無線設定 > 疑難排解」

步驟

1. 檢視無線記錄檔，以便進行疑難排解。
2. 按一下「重新整理」以更新顯示的記錄項目。

無線網路存取控制

您可以從 Cloud Edge 雲端主控台設定無線網路存取控制及管理用戶端連線。

無線網路存取控制規則的運作方式

您可以使用 MAC 位址過濾清單來控制主要無線網路和客體無線網路的網路存取。

系統提供兩個 MAC 位址過濾清單：封鎖清單和核可清單。您可以擇一使用封鎖清單或核可清單，但無法同時使用這兩個清單。

MAC 位址過濾選項的運作方式

選取的 MAC 位址過濾清單將套用至主要無線網路還是客體無線網路，視您對「啟動全域 MAC 位址過濾」和「對客體無線網路實施 MAC 過濾」選項所做的設定而定。以下內容說明這些設定如何影響無線網路存取控制：

啟動全域 MAC 位址過濾設定是...	對客體無線網路實施 MAC 過濾設定是...	選取的 MAC 位址過濾清單會套用至...
開啟	開啟	主要無線網路和客體無線網路。
開啟	關閉	主要無線網路和客體無線網路。
關閉	開啟	客體無線網路，而不會套用至主要網路。
關閉	關閉	不會套用至主要無線網路或客體無線網路。

使用封鎖清單**和**使用核可清單**的運作方式**

- 選擇使用使用封鎖清單時：
  - 除非用戶端 MAC 位址列在封鎖清單中，否則 Cloud Edge 會接受所有無線連線。
  - 如果切換至使用封鎖清單，則目前已連線但其 MAC 位址列在封鎖清單中的用戶端將會中斷連線。
  - 將 MAC 位址新增到封鎖清單後，目前已連線的用戶端將會中斷連線。
  - 如果您要普遍允許存取無線網路，但想要封鎖少數用戶端，請考慮使用封鎖清單。
  - 封鎖清單的項目數上限：256
- 選擇使用使用核可清單時：
  - 除非用戶端 MAC 位址列在核可清單中，否則 Cloud Edge 會拒絕所有無線連線。
  - 如果切換至使用核可清單，則目前已連線但其 MAC 位址不在核可清單中的用戶端將會中斷連線。
  - 將 MAC 位址新增到核可清單後，具有該 MAC 位址的用戶端將可連線到無線網路。

- 如果您不想要讓大量用戶端存取無線網路，而只想允許少數獲准的用戶端存取，請考慮使用核可清單。
- 核可清單的項目數上限：256

設定無線網路的存取控制

用途：設定 Cloud Edge 設備之無線網路的存取控制。存取控制用於允許或限制（拒絕）特定用戶端存取主要無線網路和客體無線網路。

位置：「設備 > （選取的設備） > 無線 > 存取控制」

步驟

1. 在「啟動全域 MAC 位址過濾」下，按一下「開啟」。

   設定為「開啟」後，系統會同時對主要無線網路和客體無線網路實施 MAC 位址過濾。

2. （選用）在「對客體無線網路實施 MAC 過濾」下，按一下「開啟」。

   當全域 MAC 位址過濾處於「關閉」狀態時，如果您想要對客體網路實施 MAC 位址過濾，則請針對此選項選取「開啟」。

3. 在「MAC 位址過濾清單」下，選取適當的選項：
   - 若要使用封鎖清單來進行存取控制，請選取「使用封鎖清單」。
   - 若要使用核可清單來進行存取控制，請選取「使用核可清單」。

   您可選擇使用封鎖清單或核可清單來提供無線網路的存取控制。這兩個清單無法同時使用。

4. 按一下「儲存」。

接下來需執行的動作

您可透過將用戶端新增到封鎖清單或核可清單（視所選清單而定），來允許或限制特定用戶端存取無線網路。

- 新增無線網路存取控制規則 第 6-104 頁

- 將已連線的用戶端新增到存取控制規則 第 6-104 頁

檢視無線連線的用戶端

用途：在「已連線的用戶端」區段中檢視無線連線用戶端的相關資訊。

位置：「設備 > （選取的設備） > 無線 > 存取控制」

步驟

1. 在「已連線的用戶端」區段中，您可以檢視已連線用戶端的下列相關資訊：
   - 用戶端 ID

     指派給每個已連線用戶端的唯一識別碼。
   - MAC 位址

     已連線用戶端的 MAC 位址。
   - IP 位址

     與連線之 MAC 位址相關聯的 IP 位址。
   - 主機名稱

     與連線之 MAC 位址相關聯的主機名稱。
   - SSID

     您可以使用 SSID 來判斷用戶端是連線到主要網路還是客體網路。

接下來需執行的動作

您可以將特定的已連線用戶端新增到「MAC 位址過濾清單」封鎖清單或核可清單，以控制對於無線網路的網路存取。請參閱將已連線的用戶端新增到存取控制規則 第 6-104 頁

將已連線的用戶端新增到存取控制規則

用途：將「已連線的用戶端」區段中的用戶端新增到核可清單或封鎖清單（位在「MAC 位址過濾清單」區段中）中的存取控制規則，以允許或限制（拒絕）特定用戶端存取無線網路。

位置：「設備 > （選取的設備） > 無線 > 存取控制」

步驟

1. 在「已連線的用戶端」區段下，執行適當的動作：
   - 使用封鎖清單：選取要新增的用戶端，然後按一下「新增到封鎖清單」。
   - 使用核可清單：選取要新增的用戶端，然後按一下「新增到核可清單」。
2. 按一下「儲存」。

已連線的用戶端隨即新增到「MAC 位址過濾清單」區段中適當的清單內。

新增無線網路存取控制規則

用途：將存取控制規則新增到「MAC 位址過濾清單」區段中的核可清單或封鎖清單。存取控制規則可允許或限制（拒絕）特定用戶端（按其 MAC 位址加以識別）存取主要無線網路和客體無線網路。

位置：「設備 > （選取的設備） > 無線 > 存取控制」

步驟

1. 在「MAC 位址過濾清單」區段下，根據您用於進行存取控制的清單來執行適當的動作：
   - 使用封鎖清單：按一下「使用封鎖清單」下的「新增」。
   - 使用核可清單：按一下「使用核可清單」下的「新增」。

   「新增/編輯 MAC 位址過濾規則」對話方塊隨即出現。

2. 指定要在「MAC 位址」中用於過濾的 MAC 位址。
3. （選用）指定說明。
4. 按一下「儲存」。

刪除無線網路存取控制規則

用途：從封鎖清單或核可清單中刪除 MAC 位址過濾規則，以移除施加於這些 MAC 位址的無線網路存取控制。

位置：「設備 > （選取的設備） > 無線 > 存取控制」

步驟

1. 在「MAC 位址過濾清單」區段下，執行適當的動作：
   - 在封鎖清單中選取要刪除的 MAC 位址存取控制規則，然後按一下「刪除」。
   - 在核可清單中選取要刪除的 MAC 位址存取控制規則，然後按一下「刪除」。

頻寬控制

點對點下載、影片串流與即時訊息應用程式會耗用網路頻寬且會影響生產力。透過控制通訊、減少非必要流量，以及讓重要的流量或服務有適當頻寬可用等動作進行頻寬控制，可減少網路壅塞情形。頻寬控制可讓所有使用者都能公平存取資源，並可確保更高效地存取對公司更為重要的資源。與策略規則類似，頻寬控制可以根據來源或目標 IP 位址、應用程式或服務以及當日的時間來限制流量。

頻寬控制規則可以是一般規則，也可以是特定規則，視需求而定。由於頻寬控制規則會依序與輸入流量比較，而對流量套用的將是第一個符合的規則，因此較特定的規則必須排在較一般的規則之前。例如，如果所有其他流量相關設定都相同，則單一應用程式適用的規則必須排在所有應用程式適用的規則之前。如果流量不符合任何規則，即會使用剩餘的頻寬。

注意

頻寬控制策略所用的值不能超過介面頻寬設定。

管理頻寬控制

用途：透過控制通訊、減少非必要流量，以及讓重要的流量或服務有適當頻寬可用等動作進行頻寬控制，可減少網路壅塞情形。

位置：「設備 >（設備名稱）> 頻寬控制」

步驟

1. 執行下列動作：
   - 按一下「新增」以建立新規則。
   - 使用右上方的「搜尋」來尋找規則。
   - 按一下規則的名稱以檢視或修改設定。
   - 選取規則，然後按一下「編輯」以檢視或修改設定。
   - 選取規則，然後按一下「移動」以變更規則順序。
   - 選取規則，然後按一下「更多」以變更狀態或複製規則。
   - 選取規則，然後按一下「刪除」以移除規則。
2. 設定可用的設定。
3. 按一下「儲存」。

新增/編輯頻寬控制規則

用途：指定來源使用者、使用者群組或位址、目標、流量類型、排程、出口介面和其他頻寬設定，以新增或編輯頻寬控制規則。

位置：「設備 >（設備名稱）> 頻寬控制 > 新增/編輯」

步驟

1. 指定長度為 1 到 32 個字元，且包含字母、數字或底線的規則名稱。
2. 指定說明。
3. 啟動或關閉規則。
4. 設定來源使用者/使用者群組/IP 位址/MAC 位址。
   - 針對規則選取「任意」可影響所有使用者以及所有 IP 位址。
   - 針對規則選取「選取的使用者/使用者群組」，只會影響特定使用者或群組。
   - 針對規則選取「選取的 IP 位址」，只會影響特定 IP 位址。
   - 針對規則選取「選取的 MAC 位址」，只會影響特定 MAC 位址。
5. 設定目標位址。
   - 針對規則選取「任意」以納入所有 IP 位址（預設）。
   - 針對規則選取「選取的 IP 位址」，只會影響特定 IP 位址。
6. 設定流量類型。
   - 針對規則選取「任意」或「選取的應用程式」，以納入所有應用程式群組（預設），或只納入特定應用程式。
   - 針對規則選取「任意」或「選取的服務」，以納入所有服務（預設），或只納入特定服務。
7. 設定排程。

選項	說明
一律	包括所有排程時程。（預設）
排程時程名稱	顯示可用排程物件的名稱。
新增排程物件	存取「新增/編輯」排程物件建立對話方塊。

8. 從下拉式功能表中選取介面來設定出口介面。

9. 指定上游和下游設定來設定頻寬。
10. 按一下「儲存」。

複製頻寬控制規則

用途：複製現有規則。

位置：「設備 >（設備名稱）> 頻寬控制」

步驟

1. 選取規則，然後按一下「更多」下拉式功能表。
2. 按一下「複製」。
3. 確認新規則出現在清單中。

啟動/關閉頻寬控制規則

用途：可將頻寬控制規則佈建為關閉。此程序適用於已建立但未啟動的頻寬控制規則。按一下「全部部署」後，變更即會生效。

位置：「設備 >（設備名稱）> 頻寬控制」

步驟

1. 選取要啟動或關閉的規則旁的核取方塊。
2. 按一下「更多」下拉式功能表，然後選取「啟動」或「關閉」。
3. 按一下「全部部署」以使變更生效。

刪除頻寬控制規則

用途：刪除頻寬控制規則。

位置：「設備 >（設備名稱）> 頻寬控制」

步驟

1. 選取要刪除的規則旁的核取方塊。
2. 按一下「刪除」。
3. 按一下「確定」進行確認。
4. 確認已刪除的規則不在清單中。

使用者 VPN

每當使用者從遠端位置存取公司資源，不僅需要符合一般的安全連線要求，還必須滿足遠端用戶端的特殊需求。使用者虛擬私人網路 (VPN) 將 VPN 功能延伸至遠端使用者，讓使用者能夠利用撥號（包括寬頻）、LAN 與行動連線，透過 VPN 通道安全地將機密資訊傳達給網路和伺服器。

虛擬私人網路

虛擬私人網路 (VPN) 技術通常用於確保在異地工作的員工能夠在有適當安全措施的情形下，從遠端存取企業網路。一般而言，驗證是指嘗試確認（數位）身分來允許存取網路資源及登入 VPN 網路的過程。VPN 運用了現有基礎架構 (Internet) 來安全建置並加強現有連線。VPN 是以標準的安全 Internet 通訊協定為基礎來實作，能夠讓特殊類型的網路節點（安全的設備）間有安全的連結。Site-to-Site VPN 可確保設備間有安全的連結。使用者 VPN 則可確保設備與遠端存取用戶端間有安全的連結。

典型的 Cloud Edge 部署可讓使用者使用 VPN 從遠端連線至企業網路資源。其他遠端站台受 Cloud Edge 防護，而所有網路資源與遠端端點間的通訊均受嚴格的安全策略所規範。

Cloud Edge 可支援 IPV4 對 IPV4 VPN 的存取。

加密演算法

下表說明加密演算法。數位加密標準 (DES) 是使用 56 位元金鑰的 64 位元區塊演算法。進階加密標準 (AES) 是一種私密金鑰演算法，可支援 128 到 256 位元的金鑰長度以及變動長度資料區塊。

演算法	說明
AES 128 CBC	使用 128 位元金鑰的 128 位元區塊加密區塊鏈結 (CBC) 演算法。
AES 192 CBC	使用 192 位元金鑰的 192 位元區塊加密區塊鏈結 (CBC) 演算法。
AES 256 CBC	使用 256 位元金鑰的 256 位元區塊加密區塊鏈結 (CBC) 演算法。
DES EDE3 CBC	三重 DES，純文字會由三個金鑰加密三次。
BF-CBC	Blowfish 提供的 64 位元區塊機碼式對稱加密區塊鏈結 (CBC) 演算法。

驗證演算法

演算法	說明
MD5	訊息摘要（第 5 版）雜湊演算法（以單向雜湊函數為基礎）是由 RSA Data Security 所制訂，旨在數位簽章應用，在此演算法中，較大的檔案必須先透過安全的方式進行壓縮，然後才能使用私密金鑰/公開金鑰演算法進行加密。
SHA1	安全雜湊演算法 1，此演算法會產生 160 位元的訊息摘要。大型訊息摘要可防範暴力碰撞和反向攻擊。
SHA-256 和 SHA-512	安全雜湊演算法 2，此演算法可讓您選擇 256 位元或 512 位元訊息摘要。SHA-512 訊息摘要可提供最高的安全性來防範暴力碰撞和反向攻擊。

「網際網路金鑰交換」(IKE) 通訊協定

「網際網路金鑰交換」(IKE) 通訊協定可建立通道來傳輸經過 IP 安全性 (IPSec) 編碼的資料。

SSL VPN

安全通訊端層虛擬私人網路 (SSL VPN) 是一種可搭配標準 Web 瀏覽器使用的 VPN 格式。SSL VPN 需要安裝用戶端軟體，適用於各種應用，包括 Web-based 電子郵件、企業與政府名錄、檔案共用、遠端備份、遠端系統管理，以及消費者層級的電子商務。

如果使用者擁有其端點的完整管理權限，並且使用多種應用程式，那麼通道模式可以讓已經直接連線到網路的遠端用戶端存取內部區域網路。

注意

Cloud Edge 支援 IPv4 對 IPv4 SSL VPN 的存取。

某些 Cloud Edge 設備型號不支援 VPN。

管理 SSL VPN

用途：設定 Secure Sockets Layer 虛擬私人網路 (SSL VPN)，以透過標準 Web 瀏覽器使用 VPN。

位置：「設備 >（設備名稱）> 使用者 VPN > SSL VPN > 一般」

步驟

1. （選擇性）啟動 SSL VPN。
2. 設定基本設定。
   - 通訊協定
   - 通訊埠
   - 新增位址物件

- 區域網路
- 用戶端網路集區

3. 設定進階設定。
   - 加密演算法

     請參閱加密演算法 第 6-110 頁。
   - 驗證演算法

     請參閱驗證演算法 第 6-110 頁。
   - 金鑰大小
   - 金鑰存留時間
   - 本機 DNS
   - 本機網域
   - 啟動壓縮流量
   - 啟動偵錯模式
   - 啟動同時登入
   - 啟動網路偽裝

檢視 SSL VPN 用戶端

用途：檢視目前透過 VPN 連線的所有用戶端。此表格顯示使用者名稱、啟動作業階段的時間、用戶端公開 IP 位址以及虛擬 IP 位址。已連線用戶端的總數會顯示在表格上方。

位置：「設備 >（設備名稱）> 使用者 VPN > SSL VPN > 用戶端」

步驟

1. 檢視資料表中所有正在透過 SSL VPN 連線的用戶端。

疑難排解 SSL VPN

用途：設定 SSL VPN 時檢視一般疑難排解指導方針。

位置：「設備 >（設備名稱）> 使用者 VPN > SSL VPN > 疑難排解」

步驟

1. 執行下列操作以疑難排解 SSL VPN：
   - 閱讀瞭解 SSL VPN 錯誤訊息 第 6-113 頁以瞭解錯誤訊息。
   - 確認用戶端可以成功 Ping Cloud Edge 設備。
   - 確認用戶端可以存取設定了 SSL VPN 的 TCP 或 UDP 通訊埠。
   - 確認 Windows 用戶端組態設定檔 `openvpn.ovpn` 的設定與 `https://<設備伺服器 IP 位址>/Config/openvpn.ovpn` 檔案相同。
   - 確認行動用戶端組態設定檔 mobile.ovpn 的設定與 `https://<設備伺服器 IP 位址>/Config/mobile.ovpn` 相同。

瞭解 SSL VPN 錯誤訊息

錯誤訊息	說明	建議的處理行動
`TCP:連線至 X.X.X.X:8445 失敗，5 秒後將再試一次：連線遭拒`	SSL VPN 用戶端無法連接 Cloud Edge 設備。	1. 對 Cloud Edge 設備執行 Ping 動作，假設 SSL VPN 用戶端與 Cloud Edge 設備間能夠進行 Ping（不會遭封鎖）。確認 SSL VPN 用戶端與 Cloud Edge 設備之間有網路連線。 2. 若要允許 SSL VPN 流量，請設定網路防火牆，以向 Cloud Edge 設備開放 SSL VPN 所設定的 TCP 或 UDP 通訊埠。

錯誤訊息	說明	建議的處理行動
`SIGTERM[soft,auth-failure]` 已收到，正在結束程序	使用者名稱和/或密碼無效。	指定正確的使用者名稱和/或密碼，或是要求管理員重設密碼。

L2TP VPN

Cloud Edge L2TP VPN 可讓遠端使用者透過公用網路（例如 Internet）與內部公司網路建立安全連線。

Cloud Edge 使用 L2TP 通道通訊協定在用戶端和 Cloud Edge 設備之間設定點對點連線。確保安全的方式是在透過 L2TP 通道將資料傳送到端點之前，先使用 IPsec 加密 L2TP 封包。VPN 通道由 L2TP 建立，然後會用於傳輸 IPsec 編碼的資料。L2TP 就像是建造通道的過程，而 IPsec 封包就是載送加密資料穿梭通道的貨車。

Cloud Edge 支援在 Windows 7、8.1 和 10 用戶端及 iOS 與 Android 行動用戶端使用 L2TP/IPsec VPN。

終端使用者無須安裝 VPN 用戶端。Cloud Edge L2TP/IPsec VPN 使用 Windows 標準 L2TP/IPsec 組態設定。

依預設，Cloud Edge L2TP/IPsec VPN 會透過 VPN 從用戶端傳送所有資料。若只要透過 VPN 通道傳送目的地為內部網路的流量，則可以在用戶端的 L2TP 組態設定中設定 VPN 使用分割通道模式。

Cloud Edge 會與端點保持持續性的 L2TP/IPsec 連線，直到手動中斷 VPN 連線或除非端點無法使用。

注意

Cloud Edge 可支援 IPv4 對 IPv4 L2TP VPN 的存取。

某些 Cloud Edge 設備型號不支援 VPN。

相關資訊

→ 虛擬私人網路

管理 L2TP VPN

用途：使用 IPsec 設定第二層通道通訊協定虛擬私人網路 (L2TP VPN)，以用作遠端 Windows 用戶端的 VPN。

注意

若要設定 L2TP VPN，Cloud Edge 設備必須處於「路由模式」。

位置：「設備 >（設備名稱）> 使用者 VPN > L2TP VPN > 一般」

步驟

1. 選擇性地啟動 L2TP VPN。
2. 針對「用戶端網路集區」，請以 CIDR 格式輸入 IPv4 位址集區。

   重要

   指派的 IP 位址必須是獨立網路區段的一部分（該網路區段不同於任何其他介面上使用的網路區段）。
3. 在「預先共用金鑰」中輸入兩個端點已知的金鑰。

   此金鑰會在建立連線時用來驗證 L2TP 端點。

   建立連線之前，遠端使用者必須使用 Cloud Edge 代管使用者提供驗證憑證。

   若要設定代管使用者，請參閱代管使用者與群組 第 6-166 頁。
4. 設定進階設定。
   - 「主要 DNS 伺服器」和「次要 DNS 伺服器」

     如果「主要 DNS 伺服器」和「次要 DNS 伺服器」均保留空白，則會使用設備的預設 DNS 伺服器作為 L2TP DNS 伺服器。
   - 「主要 WINS 伺服器」和「次要 WINS 伺服器」
   - MTU

支援的值為 500 到 1400。這是必要欄位。「MTU」欄位不能空白。

- 啟動 L2TP 偵錯模式
- 啟動失效同儕節點偵測

  失效同儕節點偵測會識別離線或無法使用的 VPN 同儕節點，並可協助還原無法使用同儕節點時所遺失的資源。選取「啟動失效同儕節點偵測」會在閒置連線上重新建立 VPN 通道，並視需要清除失效的 VPN 同儕節點。

  使用此選項可在通道內沒有流量產生時保持通道連線開啟。
- 啟動網路偽裝
- IKE 驗證演算法
  - MD5
  - SHA1
  - SHA-256
  - SHA-512

  SHA1 為預設值。

  請參閱驗證演算法 第 6-110 頁。
- IPsec 驗證演算法
  - MD5
  - SHA1
  - SHA-256
  - SHA-512

  SHA1 為預設值。
- IKE 偵錯

  啟動或關閉 IKE 偵錯。

5. 按一下「儲存」。

接下來需執行的動作

如果您不想要所有流量都透過 VPN 通道路由，可以在 Windows 用戶端上設定分割通道。

- 您必須先在用戶端上設定 L2TP，然後再連接 L2TP VPN。
- 中斷 L2TP 連線並以滑鼠右鍵按一下 L2TP 新連線，然後選取「內容」。
- 您接著可以選取「網際網路通訊協定第 4 版 (TCP/IPv4)」，然後依序按一下「內容」和「進階」。
- 您可以取消選取「使用遠端網路的預設設備」來啟動分割通道。只有目的地為設備內部網路的流量會透過 L2TP 設備路由。

檢視 L2TP VPN 用戶端

用途：檢視目前透過 L2TP VPN 連線的所有用戶端。此表格顯示使用者名稱、啟動作業階段的時間、用戶端公開 IP 位址以及虛擬 IP 位址。已連線用戶端的總數會顯示在表格上方。

位置：「設備 >（設備名稱）> 使用者 VPN > L2TP VPN > 用戶端」

步驟

1. 檢視資料表中所有正在透過 L2TP VPN 連線的用戶端。

疑難排解 L2TP VPN

用途：檢視設定 L2TP VPN 時的一般疑難排解指導方針。

位置：「設備 >（設備名稱）> 使用者 VPN > L2TP VPN > 疑難排解」

步驟

1. 檢視即時 L2TP 和 IPsec 記錄檔輸出。

注意

即時 IPsec 記錄檔為 L2TP 與 Site-to-Site VPN 所共用。

Site-to-Site VPN

站台對站台虛擬私人網路 (VPN 第 6-109 頁) 可讓分散於多個固定地點的辦公室透過公用網路（例如 Internet）在彼此之間建立安全連線。Site-to-Site VPN 擴大了公司的網路，讓某個地點的電腦資源可供其他地點的員工使用。例如，在全球各地有多家分公司的客戶，非常適合使用 Site-to-Site VPN。

Cloud Edge 使用網際網路金鑰交換 (IKE) 和 IP 安全性 (IPsec) 通訊協定來建立加密通道。VPN 通道由 IKE 建立，然後會用於傳輸 IPsec 編碼的資料。IKE 就像是建造通道的過程，而 IPsec 封包就是載送加密資料穿梭通道的貨車。

Cloud Edge 設備採用封裝式安全酬載 (ESP) 通訊協定。加密後的封包看起來與原始封包無異，可透過任何 IP 網路進行路由。

IKE 可以採用預先共用金鑰或 X.509 數位憑證來自動執行。您也可以指定手動金鑰。僅在 NAT/路由模式下支援的介面模式會為 VPN 通道的本機端建立虛擬介面。

注意

Cloud Edge 支援 IPv4 對 IPv4 Site-to-Site VPN 的存取。

某些 Cloud Edge 設備型號不支援 VPN。

IPsec 連線

IPsec（或 VPN）通道是與現有 VPN 連線關聯的安全設備上的虛擬介面，且 IP 路由會將其用作直接連線到 VPN 對等設備的點對點介面。

輸出封包會使用下列路由程序：

- 將具有目標位址 X 的 IP 封包與路由資料表進行比對

- 路由資料表指出 IP 位址 X 應該透過點對點連結來路由，該點對點連結是與對等設備 Y 關聯的 VPN 通道介面
- VPN 核心會在其指定虛擬通道介面時攔截封包
- 將使用正確的 IPsec 驗證類型參數與對等設備 Y 來加密封包，且新封包會收到對等設備 Y 的 IP 位址作為目標 IP
- 根據新目標 IP，封包會根據 Y 位址的適當路由資料表項目重新路由到實體介面

輸入封包會使用下列路由程序：

- IPsec 封包指定來自設備 Y 的機器
- VPN 核心攔截實體介面上的封包
- VPN 核心識別來源 VPN 對等設備
- VPN 核心取消封裝封包，然後解壓縮原始 IP 封包
- VPN 核心偵測到對等 VPN 設備的 VPN 通道介面存在，然後將來自實體介面的封包重新路由到關聯的 VPN 通道介面
- 封包透過 VPN 通道介面指定 IP 堆疊

支援的組態設定資訊

- Cloud Edge Site-to-Site VPN（非加強模式）支援使用 Yamaha VPN 路由器。

  注意

  Yamaha FWX 120 和 RTX 1200 型號經過測試並受支援。

- Cloud Edge 設備可以是邊緣裝置（直接連線至 Internet）或內部裝置（在 NAT 裝置後方設定為使用通訊埠轉送或 NAT 規則）。
- Cloud Edge 支援在執行 Cloud Edge 6.0 或更新版本的 Cloud Edge 設備的雙 WAN 環境中進行 Site-to-Site VPN 連線。

> **注意**
>
> 對於執行 Cloud Edge 5.x 或更早版本的設備，您只能設定單一 WAN 來支援 VPN，即使啟動了雙 WAN 存取也是一樣。

- 某些 Cloud Edge 設備型號不支援 VPN。

Site-to-Site VPN 拓撲

規劃和建立 VPN 組態設定之前，您應先瞭解三種 Site-to-Site VPN 拓撲。

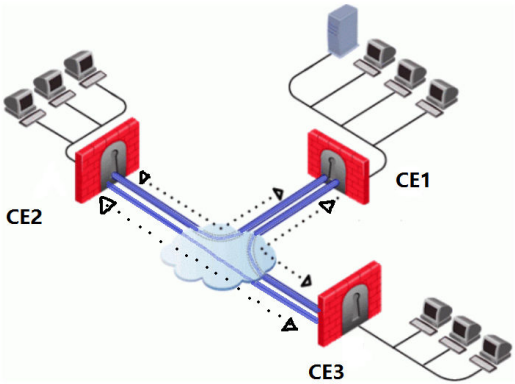
點對點 VPN 拓撲

兩個站台之間的單一加密 VPN 設備。

完整網狀 VPN 拓撲

每個遠端站台均連線至每個其他遠端站台以及中央站台。所有遠端站台都可以直接與中央站台以及每個其他遠端站台通訊，無須透過中央站台路由。

完整網狀 VPN 極為可靠，因為即使主要站台停機，所有遠端站台仍可進行通訊。完整網狀組態設定還可為敏感的應用程式提供縮短的延遲時間，因為每個遠端站台都可以直接與其他遠端站台進行通訊。

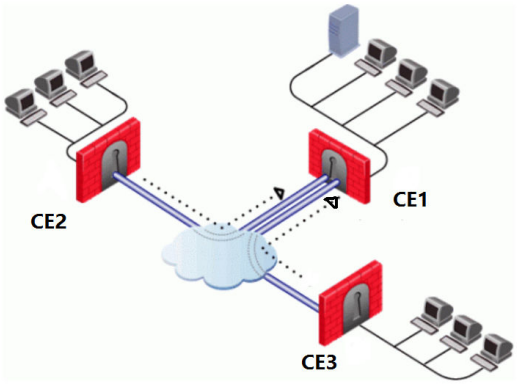


每個裝置都可以與其他四個裝置建立 VPN 連線，包括協力廠商裝置在內。任意兩個直接連線的同儕節點可進行通訊。任何間接連線的同儕節點則無法進行通訊。

請參閱 範例：完整網狀 Site-to-Site VPN 第 6-121 頁

星狀 VPN 拓撲

多個遠端站台均連線至中央站台。這種拓撲類似軸輻式組態設定。所有遠端站台均可直接與中央站台進行通訊，不過，兩個遠端站台之間要進行通訊，必須將 IPsec 流量送至中央站台，再由中樞裝置將流量路由至目標遠端站台。



星狀拓撲支援一個中樞裝置和四個分支裝置，包括協力廠商裝置（共五個裝置）。分支裝置可直接與中樞裝置進行通訊。分支裝置之間則採取間接通訊方式，因為所有 IPsec 流量都會先傳送到中樞裝置。

請參閱 範例：星狀 Site-to-Site VPN 第 6-124 頁

範例：完整網狀 Site-to-Site VPN

以下範例使用三個 Cloud Edge 設備來建立完整網狀 Site-to-Site VPN 組態設定。

組態設定摘要

裝置名稱：CE1、CE2 和 CE3

- 在 CE1 中，設定兩個連線，分別連至其餘每台裝置：CE1 至 CE2、CE1 至 CE3
- 在 CE2 中，設定兩個連線，分別連至其餘每台裝置：CE2 至 CE1、CE2 至 CE3
- 在 CE3 中，設定兩個連線，分別連至其餘每台裝置：CE3 至 CE1、CE3 至 CE2

CE1 上的組態設定


新增/編輯 IPSec 連線
啟動 IPSec 連線：
開啟
關閉
名稱：
CE1_CE2
介面名稱：
eth0
設備：
IP 位址
設備名稱
CE2
本機 ID：
CE1
遠端 ID：
CE2
新增位址物件
新增區域網路：
CE1_local
新增遠端網路：
CE2_local
驗證類型：
預先共用金鑰
金鑰：
確認金鑰：
政策名稱：
預設
儲存
取消


新增/編輯 IPSec 連線
啟動 IPSec 連線：
開啟
關閉
名稱：
CE1_CE3
介面名稱：
eth0
設備：
IP 位址
設備名稱
CE3
本機 ID：
CE1
遠端 ID：
CE3
新增位址物件
新增區域網路：
CE1_local
新增遠端網路：
CE3_local
驗證類型：
預先共用金鑰
金鑰：

CE2 和 CE3 上的組態設定

CE2 和 CE3 設備的連線設定方式與 CE1 類似。

範例：星狀 Site-to-Site VPN

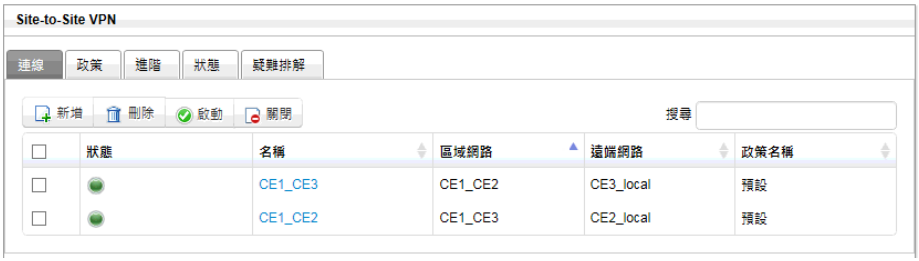
以下範例使用三個 Cloud Edge 設備來建立星狀 Site-to-Site VPN 組態設定。

組態設定摘要

裝置名稱：CE1（中樞）、CE2（分支）和 CE3（分支）

- 在中樞裝置 CE1 中，設定兩個連線來連至分支裝置：CE1 至 CE2、CE1 至 CE3
- 在分支裝置 CE2 中，設定連線來連至中樞裝置 CE1：CE2 至 CE1。
- 在分支裝置 CE3 中，設定連線來連至中樞裝置 CE1：CE3 至 CE1。

CE1（中樞）上的組態設定



CE1 連線至 CE2：

- 本機 ID：CE1
- 遠端 ID：CE2

注意

CE2 是 CE2 設備的組態設定中的本機 ID。

- 區域網路：位址物件包含 CE1 和 CE3 的區域網路的 IPv4 範圍
- 遠端網路：位址物件包含 CE2 的區域網路的 IPv4 範圍

CE1 連線至 CE3：

- 本機 ID：CE1
- 遠端 ID：CE3

注意

CE3 是 CE3 設備的組態設定中的本機 ID。

- 區域網路：位址物件包含 CE1 和 CE2 的區域網路的 IPv4 範圍
- 遠端網路：位址物件包含 CE3 的區域網路的 IPv4 範圍


新增/編輯 IPSec 連線
啟動 IPSec 連線：
開啟
關閉
名稱：
CE1_CE2
介面名稱：
eth0
設備：
IP 位址
設備名稱
CE2
本機 ID：
CE1
遠端 ID：
CE2
新增位址物件
新增區域網路：
CE1_CE3
新增遠端網路：
CE2_local
驗證類型：
預先共用金鑰
金鑰：
確認金鑰：
政策名稱：
預設
儲存
取消


新增/編輯 IPSec 連線
啟動 IPSec 連線：
開啟
關閉
名稱：
CE1_CE3
介面名稱：
eth0
設備：
IP 位址
設備名稱
CE3
本機 ID：
CE1
遠端 ID：
CE3
新增位址物件
新增區域網路：
CE1_CE2
新增遠端網路：
CE3_local
驗證類型：
預先共用金鑰
金鑰：

CE2（分支）上的組態設定

CE2 連線至 CE1：

- 本機 ID：CE2

> **注意**
> CE2 是 CE1 設備的組態設定中的遠端 ID。

- 區域網路：位址物件包含 CE2 的區域網路的 IPv4 範圍
- 遠端網路：位址物件包含 CE1 和 CE3 的區域網路的 IPv4 範圍


新增/編輯 IPSec 連線
啟動 IPSec 連線：
開啟
關閉
名稱：
CE2_CE1
介面名稱：
eth0
設備：
IP 位址
設備名稱
CE1
本機 ID：
CE2
遠端 ID：
CE1
新增位址物件
新增區域網路：
CE2_local
新增遠端網路：
CE1_CE3
驗證類型：
預先共用金鑰
金鑰：
確認金鑰：
政策名稱：
預設
儲存
取消

CE3（分支）上的組態設定

CE3 連線至 CE1：

- 本機 ID：CE3

> **注意**
> CE3 是 CE1 設備的組態設定中的遠端 ID。

- 區域網路：位址物件包含 CE3 的區域網路的 IPv4 範圍
- 遠端網路：位址物件包含 CE1 和 CE2 的區域網路的 IPv4 範圍

設定完整網狀 Site-to-Site VPN

設定完整網狀 Site-to-Site VPN 需要數個步驟。

每個設備都必須設定通往每個其他設備的通道。

步驟

1. 建立 VPN 組態設定期間將需要的本機和遠端位址物件。

新增/編輯 IP 位址/FQDN 物件 第 6-161 頁

如需有關所需位址物件的資訊，您可以參考此範例：範例：完整網狀 Site-to-Site VPN 第 6-121 頁

2. 選擇要在設定 IPsec VPN 連線時使用的 IPsec 策略。

   設定 IPsec VPN 連線時會選取 IPsec 策略。您可以使用預設 IPsec 策略、使用其他現有策略，或新增 IPsec 策略。

   新增 IPsec 策略 第 6-137 頁

3. 在中樞設備上，設定通往每個遠端設備的通道。

   新增 IPsec VPN 連線 第 6-134 頁

4. 在每個遠端設備上，設定通往每個遠端設備以及返回中樞的通道。

   新增 IPsec VPN 連線 第 6-134 頁

5. 選擇性：設定 Site-to-Site VPN 設定的進階選項，包括失效同儕節點偵測以及啟動 IKE 偵錯。

   設定進階的 Site-to-Site VPN 設定 第 6-139 頁

設定星狀 Site-to-Site VPN

設定星狀 Site-to-Site VPN 需要數個步驟。

首先，必須在中樞設備上設定通往每個遠端設備的通道連線。接著，必須在每個遠端設備上設定返回中樞的連線。

步驟

1. 建立 VPN 組態設定期間將需要的本機和遠端位址物件。

   新增/編輯 IP 位址/FQDN 物件 第 6-161 頁

   如需有關所需位址物件的資訊，您可以參考此範例：範例：星狀 Site-to-Site VPN 第 6-124 頁

2. 選擇要在設定 IPsec VPN 連線時使用的 IPsec 策略。

   設定 IPsec VPN 連線時會選取 IPsec 策略。您可以使用預設 IPsec 策略、使用其他現有策略，或新增 IPsec 策略。

   新增 IPsec 策略 第 6-137 頁

3. 在中樞設備上，設定通往每個分支裝置的連線。

   新增 IPsec VPN 連線 第 6-134 頁

4. 在每個分支設備上，設定通往中樞裝置的連線。

   新增 IPsec VPN 連線 第 6-134 頁

5. 選擇性：設定 Site-to-Site VPN 設定的進階選項，包括失效同儕節點偵測以及啟動或關閉 IKE 偵錯。

   設定進階的 Site-to-Site VPN 設定 第 6-139 頁

設定點對點 Site-to-Site VPN

設定點對點 Site-to-Site VPN 需要數個步驟。

在點對點組態設定中，本機設備會連線到一個遠端設備。

步驟

1. 建立 VPN 組態設定期間將需要的本機和遠端位址物件。

   新增/編輯 IP 位址/FQDN 物件 第 6-161 頁

2. 選擇要在設定 IPsec VPN 連線時使用的 IPsec 策略。

   設定 IPsec VPN 連線時會選取 IPsec 策略。

   您可以使用預設 IPsec 策略、使用其他現有策略，或新增 IPsec 策略。

   新增 IPsec 策略 第 6-137 頁

3. 在其中一個同儕裝置上，設定通往彼方同儕裝置的連線。

新增 IPsec VPN 連線 第 6-134 頁

4. 在彼方同儕裝置上，設定返回此方裝置的連線。

   新增 IPsec VPN 連線 第 6-134 頁

5. 選擇性：設定 Site-to-Site VPN 設定的進階選項，包括失效同儕節點偵測以及啟動或關閉 IKE 偵錯。

   設定進階的 Site-to-Site VPN 設定 第 6-139 頁

管理 Site-to-Site VPN

您可以管理 Site-to-Site VPN 組態設定，包括：

- 管理 IPSec 連線 第 6-133 頁
- 管理 IPsec 策略 第 6-136 頁
- 設定進階的 Site-to-Site VPN 設定 第 6-139 頁

管理 IPsec VPN 連線

用途：管理用來在 Cloud Edge 設備或協力廠商裝置之間建立 IPsec 通道的 Site-to-Site IPsec VPN 連線。

位置：「設備 >（設備名稱）> Site-to-Site VPN > 連線」

步驟

1. 檢閱與設定 Site-to-Site VPN 有關的資訊：
   - 支援的組態設定資訊 第 6-119 頁
   - Site-to-Site VPN 拓撲 第 6-120 頁
   - 設定完整網狀 Site-to-Site VPN 第 6-130 頁
   - 設定星狀 Site-to-Site VPN 第 6-131 頁

- 設定點對點 Site-to-Site VPN 第 6-132 頁
- 針對周遊多個設備之 IPsec 流量的最佳做法組態設定 第 6-140 頁

2. 執行下列動作：
   - 按一下「新增」，即可建立新 IPsec 連線。
   - 按一下連線的名稱，即可檢視或修改設定。

     注意

     您無法在擁有現有 Site-to-Site VPN 連線的情況下修改區域網路或遠端網路設定。如果要變更區域網路或遠端網路，您必須刪除現有站台對站台 VPN 連線，然後以所需設定建立新連線。

   - 選取連線，然後按一下「刪除」，即可刪除該連線。
   - 選取連線，然後按一下「啟動」，即可啟動該連線。
   - 選取連線，然後按一下「關閉」，即可關閉該連線。

相關資訊

→ 新增 IPsec VPN 連線

新增 IPsec VPN 連線

用途：新增 Site-to-Site IPsec VPN 連線，以在 Cloud Edge 設備或協力廠商裝置之間建立 IPsec 通道。

位置：「設備 >（設備名稱）> Site-to-Site VPN > 連線」

如需有關支援的 Site-to-Site VPN 拓撲，以及實作這些拓撲的組態設定步驟的詳細資訊，請參閱：

- Site-to-Site VPN 拓撲 第 6-120 頁
- 支援的組態設定資訊 第 6-119 頁
- 設定完整網狀 Site-to-Site VPN 第 6-130 頁

- 設定星狀 Site-to-Site VPN 第 6-131 頁
- 設定點對點 Site-to-Site VPN 第 6-132 頁
- 針對周遊多個設備之 IPsec 流量的最佳做法組態設定 第 6-140 頁

注意

設定完 Site-to-Site VPN 連線後，您即無法修改區域網路或遠端網路設定。如果您在儲存組態設定後想要變更區域網路或遠端網路，您必須刪除現有 Site-to-Site VPN 連線，然後以所需設定建立新連線。

步驟

1. 請點選「新增」。

   「新增/編輯 IPSec 連線」視窗隨即開啟。

2. 指定 IPsec 連線參數。

啟動 IPSec 連線	選取「開啟」以啟動通道。
名稱	輸入識別 IPsec VPN 通道的名稱。
介面名稱	從下拉式清單中選取介面名稱。
設備	選取要用來指定設備的方法： IP 位址：指定設備 IP 位址。 設備名稱：從下拉式清單中選取可用的設備。  注意 如果 VPN 裝置為 Cloud Edge，您可以選取「IP 位址」或「設備名稱」。如果 VPN 裝置為協力廠商裝置，則必須選擇「IP 位址」。
本機 ID	輸入「本機 ID」的文字字串。Cloud Edge 會使用「本機 ID」協助識別哪些設備在拓撲中是本機的。
遠端 ID	輸入「遠端 ID」的文字字串。Cloud Edge 會使用「遠端 ID」協助識別哪些設備在拓撲中是遠端的。

新增區域網路	選取區域網路或新增位址物件。
新增遠端網路	選取遠端網路或新增位址物件。
驗證類型	從下拉式清單中選取「預先共用金鑰」或「RSA 金鑰」。
針對「預先共用金鑰」	指定金鑰並進行確認。 如果選取「預先共用金鑰」，請在「金鑰」中指定預先共用金鑰，然後在「確認金鑰」中進行確認。Cloud Edge 會使用該金鑰來向遠端同儕節點或撥號用戶端驗證自己。務必在遠端同儕節點或用戶端定義相同的值。金鑰必須包含至少六個可列印字元，且只有網路管理員可以知道。為了妥善防範目前已知的攻擊，金鑰應包含至少 16 個隨機選擇的英數字元。
策略名稱	從下拉式清單中選取套用至 IPsec 通道的策略名稱（「預設值」或特定策略）。 **注意** 在「設備 > Site-to-Site VPN > 策略」中設定非預設的 IPsec 策略。請參閱新增 IPsec 策略 第 6-137 頁。

3. 請點選「儲存」。

管理 IPsec 策略

用途：管理在 Cloud Edge 設備或協力廠商裝置之間建立 Site-to-Site VPN 通道時使用的 IPsec 策略。

位置：「設備 >（設備名稱）> Site-to-Site VPN > 策略」

步驟

1. 執行下列動作：
   - 按一下「新增」以建立新的 IPsec 策略。
   - 按一下策略的名稱以檢視或修改設定。

- 選取策略並按一下「刪除」以刪除該策略。

新增 IPsec 策略

用途：新增 IPsec 策略，以設定用於 Site-to-Site VPN 連線的 IKE 加密和驗證演算法。

位置：「設備 >（設備名稱）> Site-to-Site VPN > 策略」

步驟

1. 請點選「新增」。

   「新增/編輯 IPSec 策略」視窗隨即開啟。

2. 指定新 IPsec 策略的名稱。

3. 從下拉式清單方塊中選取「IKE 加密演算法」。

   注意

   數位加密標準 (DES) 是使用 56 位元金鑰的 64 位元區塊演算法。進階加密標準 (AES) 是一種私密金鑰演算法，可支援 128 到 256 位元的金鑰長度以及變動長度資料區塊。

選項	說明
3DES	三重 DES，純文字會由三個金鑰加密三次。
AES 128	使用 128 位元金鑰的 128 位元區塊加密區塊鏈結 (CBC) 演算法。
AES 192	使用 128 位元金鑰的 192 位元區塊加密區塊鏈結 (CBC) 演算法。
AES 256	使用 128 位元金鑰的 256 位元區塊加密區塊鏈結 (CBC) 演算法。

4. 從下拉式清單方塊中選取「IKE 驗證演算法」值。

   - MD5 — 訊息摘要（第 5 版）雜湊演算法（以單向雜湊函數為基礎）是由 RSA Data Security 所制訂，旨在數位簽章應用，在此演算法中，較大的檔案必須先透過安全的方式進行壓縮，然後才能使用私密金鑰/公開金鑰演算法進行加密。

- SHA1 — 安全雜湊演算法 1，此演算法會產生 160 位元的訊息摘要。大型訊息摘要可防範暴力碰撞和反向攻擊。
- SHA-256 — 包含 256 位元摘要的安全雜湊演算法 2。SHA2 摘要可提供較高的安全性來防範暴力碰撞和反向攻擊。
- SHA-512 — 包含 512 位元訊息摘要的安全雜湊演算法 2。最大的訊息摘要可提供最高的安全性來防範暴力碰撞和反向攻擊。

5. 從下拉式清單方塊 (1-24) 中選取「IKE SA 存留時間」值（以小時為單位，最長 24 小時）。這會指定交涉的金鑰保持在有效狀態的時間長度。
6. 從下拉式清單方塊中選取安全設備支援的「IKE DH 群組」值。
   - 群組 2：MODP — 1024 位元（預設）
   - 群組 5：MODP — 1536 位元
   - 群組 14：MODP — 2048 位元

     上述群組是指 Diffie-Hellman 金鑰運算方式（也稱為指數金鑰協定），這是以 IKE 和 IPsec 安全關聯 (SA) 的安全設備支援的 Diffie-Hellman (DH) 數學群組為基礎。
7. 從下拉式清單方塊中選取「IPsec 加密」值。
   - 沒有加密 — 不使用加密演算法。
   - 3DES
   - AES 128
   - AES 192
   - AES 256
8. 從下拉式清單方塊中選取「IPsec 驗證演算法」值。
   - MD5
   - SHA1
   - SHA-256

- SHA-512

9. 從下拉式清單方塊 (1-24) 中選取「IPsec 存留時間」值（以小時為單位，最長 24 小時）。
10. 從下拉式清單中選取「IPsec PFS 群組」值。
    - 無
    - 群組 2：MODP
    - 群組 5：MODP
    - 群組 14：MODP
11. 按一下「儲存」。

設定進階的 Site-to-Site VPN 設定

用途：設定 Site-to-Site VPN 設定的進階選項，包括是否使用失效同儕節點偵測以及啟動/關閉 IKE 偵錯。進階設定會套用到設備上的所有 Site-to-Site VPN 連線。

位置：「設備 >（設備名稱）> Site-to-Site VPN > 進階」

步驟

1. 設定進階的 Site-to-Site VPN 設定。

選項	說明
失效同儕節點偵測	失效同儕節點偵測 (DPD) 會識別離線或無法使用的 IKE 同儕節點。利用 IPsec 流量模式，DPD 可使用最少數目的 IKE 訊息來確認連線是否有效。DPD 可用來還原無法使用同儕節點時所遺失的資源。選取「啟動失效同儕節點偵測」會在閒置連線上重新建立 VPN 通道，並視需要清除失效的 VPN 同儕節點。
IKE 偵錯	啟動或關閉 IKE 偵錯。

2. 按一下「儲存」。

IPsec 狀態

用途：檢視即時 IPsec 連線狀態。

位置：「設備 >（設備名稱）> Site-to-Site VPN > 狀態」

步驟

1. 檢視 IPsec 狀態。

IPsec 疑難排解

使用 IPsec 疑難排解記錄檔來檢視 IPsec VPN 通道上的活動。

您應瞭解特定 IPsec 連線組態設定的效能問題，以及可消除該效能問題的最佳做法建議。如需詳細資訊，請參閱針對周遊多個設備之 IPsec 流量的最佳做法組態設定 第 6-140 頁。

針對周遊多個設備之 IPsec 流量的最佳做法組態設定

您應瞭解特定 IPsec 連線組態設定的效能問題，以及可消除該效能問題的最佳做法建議。

當客戶環境中包含多個 Cloud Edge 設備且具有多個 IPsec VPN 連線時，可能會發生效能問題。當流量通過多個 IPsec 連線時，Cloud Edge 會在流量每周遊一個連線時就掃瞄一次流量。多次掃瞄並不會提供更佳的偵測結果，而多次掃瞄相同的流量反倒會令效能下降。

為了避免執行任何不必要的掃瞄，最佳做法是只讓離輸入流量最近的 Cloud Edge 設備掃瞄一次流量，並設定從來源到目標這條路由中的其他設備略過掃瞄。

為了達到這個目的，您可以使用設備策略規則，讓離 IPsec 流量最近的設備以外的其他所有設備略過掃瞄。

最佳做法組態設定規則

設備在組態設定中的角色	規則指導方針
完整網狀 IPsec 設備	建立一個「處理行動」為「略過」流量的策略規則，然後在指定的欄位新增下列項目： • 目標 新增一個網路物件，其中包含設備本身的私人網路。 • 來源使用者/使用者群組/IP 位址/FQDN/MAC 位址 新增一個網路物件，其中包含網狀 VPN 中的所有其他私人網路。
星狀 IPsec 設備的分支	建立一個「處理行動」為「略過」流量的策略規則，然後在指定的欄位新增下列項目： • 目標 新增一個網路物件，其中包含設備本身的私人網路。 • 來源使用者/使用者群組/IP 位址/FQDN/MAC 位址 新增一個網路物件，其中包含星狀 VPN 中的所有其他私人網路。
星狀 IPsec 設備的中樞	建立一個「處理行動」為「略過」流量的策略規則，然後在指定的欄位新增下列項目： • 目標 新增一個網路物件，其中包含所有私人網路（包括其本身的私人網路）。 • 來源使用者/使用者群組/IP 位址/FQDN/MAC 位址 新增一個網路物件，其中包含星狀 VPN 中的所有分支私人網路（不包含其本身的私人網路）。

範例：包含一個中樞和兩個分支的星狀 Site-to-Site IPsec VPN

設備	角色	私人網路	略過規則
分支 IPsec 設備 (GS1)	星狀分支	NS1	• 處理行動：略過 • 來源：NH1、NS2（所有其他私人網路） • 目標：NS1（其本身的私人網路）
中樞 IPsec 設備 (GH1)	星狀中樞	NH1	• 處理行動：略過 • 來源：NS1、NS2（所有其他私人網路） • 目標：NS1、NS2 和 NH1（所有其他私人網路）
分支 IPsec 設備 (GS2)	星狀分支	NS2	• 處理行動：略過 • 來源：NH1、NS1（所有其他私人網路） • 目標：NS2（其本身的私人網路）

檢視疑難排解記錄檔

用途：使用 IPsec 疑難排解記錄檔來檢視 IPsec VPN 通道上的活動。

位置：「設備 >（設備名稱）> Site-to-Site VPN > 疑難排解」

步驟

1. 檢閱疑難排解記錄檔。

更新

在「更新」畫面，您可以輕鬆執行趨勢科技不時發行的 Cloud Edge 設備更新。「更新」畫面提供下列兩個區段：

- 可用更新：如果您的設備有任何可用的更新，這個區段會顯示該更新。若要更深入地瞭解任何可用的更新，請按一下「讀我檔案」連結以檢視讀我檔案。
- 已安裝的更新：這個區段會顯示已經安裝的更新。

更新 Cloud Edge 設備

用途：安裝 Cloud Edge 設備更新。

位置：「設備 >（設備名稱）> 更新」

步驟

1. 在所要安裝之可用更新的「處理行動」欄下，按一下「立即更新」。

   若要深入瞭解目前的更新，請按一下「讀我檔案」連結。

   注意

   如果更新依賴任何其他檔案，則 Cloud Edge 會自動安裝該檔案。

   重要

   系統會以特定順序對 HA 群組進行更新（手動或預約） — 首先對待命設備進行更新，然後從主要設備容錯移轉到次要設備。在容錯移轉完成後，主要設備隨之完成更新。然後，系統會再次容錯移轉，將主要設備回復為作用中狀態。在更新過程中，網路不會中斷。

   如果設備屬於 HA 群組，並且其中一台設備離線或 HA 群組處於核心分裂狀態時，則不允許對 HA 群組設備進行手動更新。

管理網路存取控制

您可以使用 Cloud Edge 雲端主控台來管理網路存取控制，以提供端點防護。

- Cloud Edge 整合了 Worry Free Business Security Services (WFBSS)，可檢查 WFBSS 端點的符合性。Cloud Edge 可針對具有過期的 WFBSS Security Agent 病毒碼或未安裝 WFBSS Security Agent 的 WFBSS 端點提供網路存取控制。

  請參閱 WFBSS 端點防護 第 6-144 頁。

- Cloud Edge 透過為端點提供符合性檢查，查看是否已偵測到超過所設閾值的 C&C 回呼數，來提供安全防護服務。Cloud Edge 可以為超過閾值的端點提供網路存取控制。

  請參閱可疑端點 第 6-151 頁。

WFBSS 端點防護

Worry Free Business Security Services (WFBSS) 為端點提供安全防護服務。為了提供安全防護服務，WFBSS 客戶必須在端點上安裝 WFBSS Security Agent。這些代理程式可協助管理網路存取控制。如果代理程式的病毒碼已過期，或端點未安裝代理程式，將無法保證符合性。

Cloud Edge WFBSS 端點防護整合了 WFBSS，可提供實施符合性的方式。Cloud Edge 透過判斷端點是否具有過期的 WFBSS Security Agent 病毒碼或是否未安裝 WFBSS Security Agent，來為端點提供符合性檢查。此外，Cloud Edge 可針對不合規端點提供網路存取控制。

注意

「WFBSS 端點防護」不支援 IPv6 端點的端點檢查和符合性。

啟動符合性檢查

您必須啟動此功能。預設為關閉。

啟動此功能後，您可指定要針對下列兩種情況採取何種處理行動（封鎖或偵測）：

- 端點已安裝 WFBSS Security Agent，但病毒碼過期。
- 端點未安裝 WFBSS Security Agent。

Cloud Edge 會每小時與 Worry Free Business Security Services 同步處理資訊，以取得有關端點之最新病毒碼狀態的更新資訊。

防護清單

系統不會自動檢查端點的符合性。您必須設定防護清單，以指定哪些端點要接受符合性防護。

- 系統會檢查防護清單中的端點，以判斷它們是否已安裝代理程式，如果已經安裝，再接著判斷所安裝代理程式的病毒碼是否為最新版本。
- 如果端點不合規，就會採取已設定的處理行動。
- 您可以新增 MAC 位址或 IPv4 位址（單一位址或位址範圍）。
- 最多 256 個項目。

處理行動

如果符合性檢查發現防護清單中的端點不合規，Cloud Edge 可以採取兩種處理行動方案中的一種：

- 封鎖

  封鎖對 Internet 的所有存取。

  例外：如果流量/URL 列在全域核可清單中，則不封鎖端點。不會封鎖 DNS 和 DHCP 的流量。

  如果某個端點遭到「WFBSS 端點防護」功能封鎖，則用戶端瀏覽器會重新導向至「WFBSS 端點防護違規」通知頁面。

  注意

  對於沒有代理程式的端點，如果您將處理行動設定為「封鎖」，則沒有代理程式的端點會無法存取 Internet。

  如果使用者嘗試在這些端點上安裝代理程式，則應將下列 URL 新增至「核可清單」，否則安裝可能會失敗。

  - `*.symcb.com/*`
  - `*.digicert.com/*`

- `*.affirmtrust.com/*`
- `crl.microsoft.com/*`

此外，如果使用者在沒有代理程式的端點上存取趨勢科技 CLP 網站，則應將下列 URL 新增至「核可清單」，否則下列存取要求可能會受到影響：
`www.google-analytics.com/*www.googletagmanager.com/*`

- 偵測

  允許存取 Internet，但存取會記錄在「WFBSS 端點防護」疑難排解頁面中，並附上端點不合規的原因。

例外清單

您可以設定例外清單，指定哪些端點不受符合性防護。對於例外清單中的端點，不會實施符合性處理行動。

- 您可以新增 MAC 位址或 IPv4 位址（單一位址或位址範圍）。
- 最多 256 個項目。

用戶端清單

您可以使用「用戶端清單」區段檢視 Cloud Edge 設備在過去 24 小時內偵測到的所有端點。

- 此清單一開始是空的。
- 在您啟動 WFBSS 端點防護並按一下「套用」將更新部署至 Cloud Edge 設備後，設備才會開始將過去 24 小時內有流量通過 Cloud Edge 設備的端點相關資訊製成表格。Cloud Edge 會在「用戶端清單」區段中顯示結果清單。

  為了方便起見，自 WFBSS 端點防護部署後最初偵測到的端點都會自動新增至防護清單。
- 在執行初始端點偵測後，您可以透過按一下為每個所列端點提供的「防護清單」或「例外清單」選項，輕鬆將列出的端點新增至防護清單或例外清單。

管理 WFBSS 端點防護

用途：管理「WFBSS 端點防護」，這是個與 Worry Free Business Security Services (WFBSS) 整合的解決方案，可檢查端點上的 WFBSS 防護狀態，以及管理不合規端點的網路存取控制。

位置：「設備 >（設備名稱）> 網路存取控制 > WFBSS 端點防護 > 一般」

步驟

1. 執行下列動作：
   - 啟動 WFBSS 端點防護。
   - 選取要對沒有 WFBSS Security Agent 的端點採取的處理行動。預設值為「偵測」。
   - 選取要對具有已過期 WFBSS Security Agent 病毒碼的端點採取的處理行動。預設值為「偵測」。
   - 向防護清單新增端點或從其中刪除端點。
   - 向例外清單新增端點或從其中刪除端點。
   - 檢視 Cloud Edge 設備下端點清單中的資訊。
   - 使用 Cloud Edge 設備下的端點清單，將特定端點新增至防護清單或例外清單。
   - 重新整理端點清單。

設定 WFBSS 端點防護

用途：進行設定以加強設備對新興安全威脅的防禦力。

位置：「設備 >（設備名稱）> 網路存取控制 > WFBSS 端點防護 > 一般」

步驟

1. 選擇性地啟動 WFBSS 端點防護。

2. 選擇處理行動來執行下列作業：

   a. 沒有代理程式的用戶端：偵測 或 封鎖

   b. 有使用過期病毒碼的代理程式的用戶端：偵測 或 封鎖

   - 封鎖：封鎖對 Internet 的所有存取。

     如果任何用戶端遭到 WFBSS 端點防護 功能封鎖，則用戶端瀏覽器會重新導向至 WFBSS 端點防護 違規通知頁面。

   - 偵測：記錄但不封鎖對網路資源的存取。此為預設值。

3. 設定 防護清單。

   請參閱將端點新增至防護清單 第 6-148 頁。

4. 設定 例外清單。

   請參閱將端點新增至例外清單 第 6-149 頁。

5. 按一下「套用」。

將端點新增至防護清單

用途：將端點新增至 WFBSS 端點防護的防護清單。

位置：「設備 >（設備名稱）> 網路存取控制 > WFBSS 端點防護 > 一般」

步驟

1. 將端點新增至「防護清單」。

   a. 在 防護清單 區段中，按一下「新增」。

      新增防護清單 畫面隨即開啟。

   b. 請指定下列項目，將端點新增至防護清單：

選項	說明
名稱	指定可協助您識別此項目相關資訊的名稱。

選項	說明
	範例：JSmith 範例：Office
位址類型	選擇 IPv4 或 MAC。
IP/MAC 位址	根據選擇的類型，輸入適當資訊： • IPv4：以逗點分隔清單的形式輸入資訊。 值可以是單一 IP 位址、IP 位址範圍或 CIDR。 範例：192.168.0.1,10.0.0.1-10.0.0.4,10.0.0.8/24 • MAC：輸入單一 MAC 位址 範例：00:FF:8A:B9:5A:49 範例：00-FF-8A-B9-5A-49

2. 按一下「儲存」。
3. 繼續將端點新增至防護清單（如有需要）。

   您最多可以新增 256 個項目到防護清單。

將端點新增至例外清單

用途：將端點新增至 WFBSS 端點防護的例外清單。

位置：「設備 >（設備名稱）> 網路存取控制 > WFBSS 端點防護 > 一般」

步驟

1. 將端點新增至「例外清單」。
   a. 在 例外清單 區段中，按一下「新增」。

      新增例外清單 畫面隨即開啟。

   b. 請指定下列項目，將端點新增至例外清單：

選項	說明
名稱	指定可協助您識別此項目相關資訊的名稱。 範例：JSmith 範例：Office
位址類型	選擇 IPv4 或 MAC。
IP/MAC 位址	根據選擇的類型，輸入適當資訊： • IPv4：以逗點分隔清單的形式輸入資訊。 值可以是單一 IP 位址、IP 位址範圍或 CIDR。 範例：192.168.0.1,10.0.0.1-10.0.0.4,10.0.0.8/24 • MAC：輸入單一 MAC 位址 範例：00:FF:8A:B9:5A:49 範例：00-FF-8A-B9-5A-49

2. 按一下「儲存」。
3. 繼續將端點新增至例外清單（如有需要）。

   您最多可以新增 256 個項目到例外清單。

檢視 WFBSS 端點防護用戶端清單

用途：檢視 Cloud Edge 設備下目前已檢查 WFBSS Security Agent 符合性的所有端點。

位置：「設備 >（設備名稱）> 網路存取控制 > WFBSS 端點防護 > 一般」

步驟

1. 檢視資料表中所有端點的資訊：
   - 主機名稱
   - IP 位址

- MAC 位址
- 是否已安裝代理程式
- 如果已安裝，代理程式的病毒碼是否已過期
- 作業系統（例如：Windows 10）

2. （選用）按一下「重新整理」可重新整理清單。
3. （選用）針對選取的端點按一下「防護清單」，可將端點新增至防護清單。
4. （選用）針對選取的端點按一下「例外清單」，可將端點新增至例外清單。

疑難排解 WFBSS 端點防護

用途：使用 WFBSS 端點防護 時檢視一般疑難排解資訊。

位置：「設備 >（設備名稱）> 網路存取控制 > WFBSS 端點防護 > 疑難排解」

步驟

1. 若要疑難排解 WFBSS 端點防護，請執行下列作業：
   - 檢視個別記錄項目，以判斷用戶端遭到封鎖的原因。
   - 按一下「重新整理」以更新記錄檔。

可疑端點

「可疑端點」為端點提供安全防護服務。設定「可疑端點」，以便為其上偵測到 C&C 回呼超過所設閾值的端點提供網路存取控制。

注意

- 「可疑端點」不提供 IPv6 端點的端點檢查和符合性。
- 如果 Cloud Edge 設備與端點之間存在 NAT 裝置或 Proxy 伺服器，則 Cloud Edge 無法偵測用戶端的真實 IP 位址，並且 Cloud Edge 會改為計算 NAT/Proxy 伺服器裝置的 C&C 回呼事件數。因此，未來任何觸發違規之來自 NAT/Proxy 伺服器裝置的流量皆會遭到封鎖或監控（視所做的設定而定）。這可能不是預期的行為。

在啟動可疑端點後您可以指定的處理行動

您必須啟動此功能。預設為關閉。

在啟動此功能後，您可以指定當 Cloud Edge 在端點上偵測到 C&C 回呼超過所設閾值時所要採取的處理行動（封鎖或監控）。

當在指定的時間範圍內偵測到指定的事件數目時，即表示達到閾值。您可以設定事件數目和時間範圍：

- 事件數（預設值為 50）

  範圍：1 到 1000

- 時間範圍（預設值為 1 小時）

  有效的時間範圍：30 分鐘、1 小時、6 小時、12 小時、1 天

Cloud Edge 會定期與端點同步處理資訊，以取得更新的資訊。

您可以指定的處理行動

如果符合性檢查發現端點違反閾值設定，Cloud Edge 可以採取兩種處理行動方案中的一種：

- 封鎖

  封鎖對 Internet 的所有存取。

  例外：如果流量/URL 列在全域核可清單中，則不封鎖端點。不會封鎖 DNS 和 DHCP 的流量。

  如果某個端點遭到封鎖，則會向用戶端瀏覽器傳送「可疑端點違規」通知頁面。

注意

如果您將處理行動設定為「封鎖」，則可疑端點將無法存取 Internet。

- 監控

  允許存取 Internet，但可疑端點會新增到違規清單中。

如何使用違規清單

您可以使用「違規清單」區段來檢視其可疑活動偵測數超過閾值之所有端點的相關資訊。

- 在啟動「可疑端點」後，Cloud Edge 會開始將超過閾值的端點填入到違規清單中。
- 如果處理行動設定為「封鎖」，您可以透過按一下適當列中的「解除」，將違規清單中的特定端點排除封鎖。

如何使用疑難排解頁面上的清單

如果處理行動設定為「封鎖」，則您可以檢視疑難排解頁面上的清單，來查看哪些端點因為違規而遭到封鎖。

如果 Cloud Edge 設備已經離線，您可以檢視清單，但無法執行任何操作，例如「解除」。

管理可疑端點

用途：管理「可疑端點」，此安全防護服務可為有風險的端點提供符合性及網路存取控制。

位置：「設備 >（設備名稱）> 網路存取控制 > 可疑端點 > 一般」

步驟

1. 執行下列動作：
   - 啟動 可疑端點。
   - 選取要對不合規端點採取的處理行動。預設為監控。

- 設定指定時間範圍內 C&C 回呼事件達到多少數目就會觸發處理行動的閾值。預設值為 1 小時內 50 個事件。
- 請使用違規清單來檢視違反端點策略之端點的相關資訊。
- 如果您不希望某些端點遭到封鎖，請從違規清單中移除選取的端點。

設定可疑端點

用途：設定「可疑端點」，以加強設備對新興安全威脅的防禦力。

位置：「設備 >（設備名稱）> 網路存取控制 > 可疑端點 > 一般」

步驟

1. 選擇性地啟動 可疑端點。
2. 選擇要對違反策略之端點採取的處理行動：
   - 封鎖：封鎖對 Internet 的所有存取。

     如果任何端點遭到「可疑端點」功能封鎖，則會向用戶端瀏覽器傳送「 可疑端點違規」通知頁面，且事件會記錄在疑難排解畫面中。
   - 監控（預設）：允許存取 Internet，但可疑端點會新增到違規清單中。
3. 設定 C&C 回呼的閾值：
   a. 輸入閾值事件的數目（預設值：50）。

      範圍為 1 到 1000。

   b. 輸入計算閾值事件數目的時間範圍（預設值：1 小時）。

      支援的值包括：「30 分鐘」、「1 小時」、「6 小時」、「12 小時」和「1 天」。
4. 按一下「套用」。

檢視可疑端點違規清單

用途：檢視存在可疑活動的所有端點。

位置：「設備 >（設備名稱）> 網路存取控制 > 可疑端點 > 一般」

步驟

1. 檢視存在違規之所有端點的資訊：
   - 主機名稱
   - IP 位址
   - 觸發時間
2. （選用）按一下「解除」可將選取的端點從違規清單中移除。

疑難排解可疑端點

用途：使用 可疑端點 時檢視一般疑難排解資訊。

位置：「設備 >（設備名稱）> 網路存取控制 > 可疑端點 > 疑難排解」

步驟

1. 若要疑難排解 可疑端點，請執行下列作業：
   - 檢視個別記錄項目，以判斷哪些端點因為可疑活動而遭到封鎖。
   - 按一下「重新整理」以更新記錄檔。

裝置辨識

在 Cloud Edge 雲端主控台中，您可以探索、檢視及管理端點裝置。此外，Cloud Edge 也可以掃瞄端點裝置是否存在弱點。

Cloud Edge 會在您的網路中自動偵測新的端點裝置。Cloud Edge 需要數分鐘時間，才會在您的網路中偵測新的端點裝置。為了探索端點裝置，Cloud Edge 會主動傳送封包來探查新的端點裝置，以及被動偵測透過 Cloud Edge 傳送網路流量的端點裝置。

每個 Cloud Edge 設備最多可支援 2000 台端點裝置。

在「設備 > （設備） > 裝置辨識」下方，使用下列畫面可執行下列功能：

- 端點裝置：此畫面會顯示可過濾的端點裝置清單、各端點裝置的嚴重性，以及各端點裝置的弱點數量。如需詳細資訊，請參閱端點裝置 第 6-156 頁。
- 一般設定：此畫面會提供手動起始或預約弱點掃瞄及設定辨識模式的選項。如需詳細資訊，請參閱一般掃瞄設定 第 6-159 頁。
- 端點裝置詳細資訊：此畫面會顯示詳細的裝置資訊和裝置的弱點。如需詳細資訊，請參閱端點裝置詳細資訊 第 6-158 頁。

雖然大多數的功能都是在「裝置辨識」下方執行的，但下列元素也會與端點裝置管理相關：

- 需要注意的裝置類別：此 Widget 位於「資訊中心」的「裝置對應與安全」標籤，會顯示網路拓樸，以及存在弱點的端點裝置數量、Internet 安全和策略實施。
- 策略規則：此畫面位於「策略」，提供根據端點裝置類別將策略部署到端點裝置的選項。

端點裝置

「端點裝置」畫面包含一個表格，此表格提供有關 Cloud Edge 在您的網路中探索到之端點裝置的下列資訊：

- 名稱：裝置的名稱。
- 裝置類別：由 Cloud Edge 自動指派的裝置類別。
- IP 位址：裝置的 IPv4 和 IPv6 位址。
- MAC 位址：裝置的 MAC 位址。

- 嚴重性：根據裝置上探索到的弱點和弱式密碼的嚴重性等級。

  Cloud Edge 會顯示下列嚴重性等級：

  - 綠色：裝置可能有開放的通訊埠。裝置沒有偵測到的弱式密碼，也沒有偵測到的弱點。
  - 黃色：裝置存在弱式密碼，並且可能有開放的通訊埠。裝置沒有偵測到的弱點。
  - 紅色：裝置存在弱點。裝置可能存在弱式密碼和開放的通訊埠。
- 弱點：裝置上的弱點和弱式密碼數量。

檢視端點裝置

用途：檢視 Cloud Edge 在您的網路上探索到的端點裝置。

位置：「設備 >（設備）> 裝置辨識 > 端點裝置」

步驟

1. （選用）按一下裝置名稱以檢視更多裝置資訊和弱點。
2. （選用）在表格上方，選取時間範圍以檢視這段時間範圍內所探索到裝置的歷史記錄。
3. （選用）在表格上方，按一下「重新整理」按鈕以重新整理 Cloud Edge 雲端主控台畫面。

   注意

   Cloud Edge 設備中的資訊不會重新整理。
4. （選用）在表格的左側，選取特定裝置類別以過濾表格中顯示的裝置。
5. 按一下欄標頭，即可依該欄排序表格。

   注意

   依預設，會先依「嚴重性」，再依「名稱」排序表格。

6. （選用）在表格的底端，使用分頁控制項以瀏覽表格的多個頁面。

端點裝置詳細資訊

「端點裝置詳細資訊」畫面包含有關 Cloud Edge 在您的網路中探索到之端點裝置的下列詳細資訊：

- 裝置資訊
  - 名稱：裝置的名稱。
  - 裝置類別：由 Cloud Edge 自動指派的裝置類別。
  - IP 位址：裝置的 IPv4 和 IPv6 位址。
  - MAC 位址：裝置的 MAC 位址。
  - 主機名稱：裝置的主機名稱。
  - 品牌：裝置的品牌。
  - 型號：裝置的型號。
- 弱點資訊

  注意

  依預設，弱點和弱式密碼掃瞄會關閉。若要啟動此掃瞄，請參閱一般掃瞄設定 第 6-159 頁。

  - CVE ID：裝置上偵測到的弱點的清單。

    注意

    按一下弱點可取得有關該弱點的詳細資訊，例如可能的風險、如何阻止該弱點，以及可從何處取得詳細資訊。

  - 弱式密碼：裝置上偵測到存在弱式密碼的應用程式清單。

    Cloud Edge 僅會掃瞄下列應用程式密碼：SSH、FTP 和 Telnet。

注意

按一下應用程式名稱，可取得有關該弱式密碼的詳細資訊，例如可能的風險，以及如何阻止該弱式密碼。

- 開放的通訊埠：開放的 TCP/UDP 通訊埠以及通成與這些通訊埠關聯之應用程式的清單。

  Cloud Edge 僅會掃瞄下列通訊埠：

  - TCP：21、22、23、53、80、135、139、443、445、515、554、631、2869、5000、5357、5432、7777、8008、8080、8192、9100、9700、12345、49152、49153、49154、49155、62078
  - UDP：53、67、68、69、111、123、137、138、161、427、500、1022、1023、1026、1029、1812、1900、3702、4500、5353

檢視端點裝置

用途： 檢視 Cloud Edge 在您的網路上探索到之端點裝置的詳細資訊和弱點。

位置：「設備 >（設備）> 裝置辨識 > 端點裝置 >（裝置）」

步驟

1. （選用）在「CVE ID」或「開啟的通訊埠」下方，按一下「全部顯示」以檢視其他項目。
2. （選用）按一下 CVE ID 或弱式密碼以檢視更多詳細資訊。
3. （選用）按一下「返回所有裝置」以返回到所有裝置的清單。

一般掃瞄設定

Cloud Edge 可以掃瞄端點裝置是否存在弱點（根據 CVE 清單）以及弱式密碼。此外，Cloud Edge 可以使用進階辨識模式來識別開放的通訊埠，以及識別端點裝置類別。

執行弱點掃瞄後，在下列畫面上會顯示掃瞄結果：

- 端點裝置：此畫面會顯示可過濾的端點裝置清單、各端點裝置的嚴重性，以及各端點裝置的弱點數量。如需詳細資訊，請參閱端點裝置 第 6-156 頁。
- 端點裝置詳細資訊：此畫面會顯示詳細的裝置資訊和端點裝置的弱點。如需詳細資訊，請參閱端點裝置詳細資訊 第 6-158 頁。
- 需要注意的裝置類別：此 Widget 位於「資訊中心」的「裝置對應與安全」標籤，會顯示網路拓樸，以及存在弱點的端點裝置數量、Internet 安全和策略實施。

設定一般掃瞄設定

用途：執行或預約弱點掃瞄，以及設定探索到的端點裝置的辨識模式。

位置：「設備 >（設備）> 裝置辨識> 一般設定」

小心!

依預設，預約弱點和弱式密碼掃瞄會關閉。請注意，安全軟體和裝置可能會將此掃瞄偵測為安全事件。

步驟

1. （選用）針對「辨識模式」，切換下列選項。
   - 進階
   - 標準

   注意

   進階辨識模式會利用主動式掃瞄，協助識別端點裝置的類別與開放的通訊埠。選取標準辨識模式，可能會使識別裝置類別的準確度降低。
2. （選用）按一下「立即掃瞄」以執行隨選弱點掃瞄。
3. （選用）針對「啟動」，選取「開啟」以啟動預約弱點掃瞄，或選取「關閉」以關閉掃瞄。

a. 如果選取了「開啟」，請接著選取掃瞄頻率。

管理 IP 位址/FQDN 物件

用途：透過新增、修改、複製或刪除 IPv4、IPv6 和 FQDN 位址物件來管理位址物件。

位置：「策略 > 身分識別物件 > IP 位址/FQDN」

步驟

1. 執行下列動作：
   - 按一下「新增」以建立新物件。
   - 按一下物件的名稱以檢視或修改設定。
   - 選取物件，然後按一下「複製」以複製物件。
   - 選取物件，然後按一下「刪除」以刪除物件。
2. 設定可用的設定。
3. 按一下「儲存」。

新增/編輯 IP 位址/FQDN 物件

用途：新增或編輯位址物件，以設定 IPv4 位址、IPv6 位址或 FQDN 物件。

位置：「策略 > 身分識別物件 > IP 位址/FQDN > 新增/編輯」

步驟

1. 指定 IP 位址/FQDN 物件的名稱。

2. 選取物件類型。

   可用的類型：IPv4、IPv6 或 FQDN

   橋接模式或軟體切換

   如果 Cloud Edge 設備以「橋接模式」執行或做為「軟體切換」部署，則 Cloud Edge 支援 IPv6。

   - 您可以設定 IPv4 和 IPv6 位址物件。
   - FQDN 可以解析為 IPv4 或 IPv6 位址。

   路由模式

   如果 Cloud Edge 設備以「路由模式」運作，則 Cloud Edge 不支援 IPv6。

   - 您只能設定 IPv4 位址物件。
   - FQDN 必須解析為 IPv4 位址。

3. 指定位址物件做為 IP 位址（單一或逗點分隔）或 FQDN（單一或逗點分隔）。

   您可以指定 IP 位址物件做為單一位址、範圍，或做為類別網域間路由 (CIDR) 網路。

   範例：

   - `192.168.0.1`
   - `10.0.0.1-10.0.0.4`
   - `10.0.0.8/23`
   - `fd00:1:1111:200::1fff`
   - `fd00:1:1111:200::1000-fd00:1:1111:200::1fff`
   - `fd00:1:1111:200::1000/116`
   - `host.example.com`
   - `example.com`

- *.com
- *example.com
- *.example.com

注意

如上面的範例所示，FQDN 物件支援使用萬用字元 (*) 進行模糊比對。請注意，僅在 FQDN 開頭使用萬用字元，而不要在 FQDN 中間或結尾使用萬用字元。

4. 按一下「儲存」。

IP 位址/FQDN 物件參數

下表說明可設定的 IPv4 位址、IPv6 位址和 FQDN（完整網域名稱）物件參數。

表 6-6. 位址物件參數

參數	說明
物件名稱	指定可說明物件的名稱。當定義安全策略時，此名稱會顯示在位址清單中。名稱區分大小寫且必須是唯一名稱。僅限使用字母、數字、空格、連字號與底線。
類型	指定下列其中一個位址類型： • IPv4 • IPv6 • FQDN 對於在「橋接模式」和「軟體切換」部署中使用的物件，您可以設定 IPv4 和 IPv6 位址。此外，FQDN 可以解析為 IPv4 或 IPv6 位址。 對於在「路由模式」部署中使用的物件，您可以設定 IPv4 位址，且 FQDN 必須解析為 IPv4 位址。

參數	說明
位址	IPv4 位址： 使用下列標記指定 IP 位址或網路： • ip_address • ip_address_range • ip_address/bitmask 範例：192.168.1.1 或 192.168.1.1-192.168.1.10 或 192.168.80.0/24 IPv6 位址 使用下列標記指定 IPv6 位址或網路： • ipv6_address • ipv6_address_range • ipv6_address/bitmask (IPv6 CIDR) 範例： 2001:db8:123:1::1 或 2001:db8:123:1::1-2001:db8:123:1::10 或 2001:db8:123:1::/64 FQDN 使用下列標記指定 FQDN： • [domain].[tld] • [hostname].[domain].[tld] 注意 FQDN 物件支援使用萬用字元 (*) 進行模糊比對。請注意，僅在 FQDN 開頭使用萬用字元，而不要在 FQDN 中間或結尾使用萬用字元。 範例： • 精確 FQDN：example.com 或 host.example.com • 萬用字元 FQDN：*.com、*example.com 或 *.example.com 注意 僅當設定策略規則以比對來源/目標連線時，才能使用 FQDN 物件類型。

使用者驗證

驗證設定

定義終端使用者驗證的驗證來源和驗證快取設定。

- 透過代管使用者帳號、LDAP 帳號或 RADIUS 帳號進行使用者驗證。
- Cloud Edge 支援兩種驗證快取存留時間 (TTL) 選項：
  - 固定式 TTL（首次點擊）— 快取驗證使用者的最後時間。預設值：2 小時
  - 上次作用中 TTL（上次點擊）— 快取上次使用者與 Cloud Edge 互動的時間。預設值：2 小時

設定驗證設定

用途：將驗證設定用於驗證來源和驗證快取 TTL。

位置：「管理 > 使用者驗證 > 驗證設定」

步驟

1. 在「驗證來源」下方，選取下列其中一個選項：
   - 代管使用者

     使用者會以 Cloud Edge 中設定的認證登入。如需詳細資訊，請參閱代管使用者與群組 第 6-166 頁。
   - LDAP

     使用者會以 LDAP 驗證登入。如需詳細資訊，請參閱LDAP 設定 第 6-171 頁。

- RADIUS

  使用者會以 RADIUS 驗證登入。如需詳細資訊，請參閱 RADIUS 設定 第 6-173 頁。

2. 在「驗證快取」下，選取下列其中一項，然後選取 TTL 的時數：
   - 固定式 TTL（小時）
   - 上次作用中 TTL（小時）
3. 按一下「儲存」。

注意

- Cloud Edge 6.0 和更新版本的設備支援使用 LDAP 進行驗證。
- Cloud Edge 6.0 SP3 和更新版本的設備支援使用 RADIUS 進行驗證。

代管使用者與群組

在 Cloud Edge 雲端主控台上建立代管使用者帳號，即可讓使用者透過 VPN 或網頁驗證入口登入。可選擇性地將代管使用者組織為群組，以部署策略來影響指派給代管群組的所有代管使用者。VPN 與網頁驗證入口均由 Cloud Edge 雲端主控台所管理。

Cloud Edge 雲端主控台會將代管使用者與群組同步處理到同一家公司的所有設備。選擇性地針對此已同步處理的資訊設定策略並執行報告。

如果使用代管使用者和群組來進行驗證，關閉代管使用者帳號會讓使用者無法登入 VPN 與網頁驗證入口。

注意

對於不支援 VPN 的 Cloud Edge 設備型號，您可以使用代管使用者和群組透過網頁驗證入口來登入。

IPv6 流量不支援對使用者進行驗證。這包括任何依賴使用者驗證的功能，例如管理存取權、使用使用者進行安全性控制的策略、網頁驗證入口等。

管理代管使用者

用途：管理代管使用者以允許終端使用者存取設備所管理的資源。

位置：「管理 > 使用者驗證 > 代管使用者與群組 > 代管使用者」

步驟

1. 執行下列動作：
   - 按一下「新增」，可建立新代管使用者帳號。
   - 使用右上方的「搜尋」，可尋找使用者帳號。
   - 按一下代管使用者帳號名稱，可檢視或修改設定。
   - 選取代管使用者，然後按一下「啟動」，可允許該帳號登入 VPN 和網頁驗證入口。
   - 選取代管使用者，然後按一下「關閉」，可禁止該帳號登入 VPN 和網頁驗證入口。
   - 選取代管使用者，然後按一下「刪除」，可移除該使用者。

新增/編輯代管使用者

用途：新增代管使用者以允許使用者透過 VPN 或網頁驗證入口登入。

位置：「管理 > 使用者驗證 > 代管使用者 & 群組 > 代管使用者 > 新增/編輯使用者」

步驟

1. 啟動代管使用者。
2. 指定使用者詳細資料。
3. 將代管使用者指派給現有代管群組，或選擇性地將代管使用者指派給新的代管群組。

請參閱新增/編輯代管群組 第 6-169 頁。

4. 選取允許使用者變更網頁驗證入口或 VPN 入口網站密碼的核取方塊。

> **警告!**
> 如果多個使用者共用相同的帳號，請勿選取此核取方塊。否則，若密碼變更，部分使用者可能會遺失存取權。

5. 按一下「儲存」。

管理代管群組

用途：管理代管群組，以組織代管使用者以及更有效率地控制類似的代管使用者帳號。

位置：「管理 > 使用者驗證 > 代管使用者與群組 > 代管群組」

步驟

1. 執行下列動作：
   - 按一下「新增」，可建立新代管群組。
   - 使用右上方的「搜尋」，可尋找代管群組。
   - 按一下代管群組帳號名稱，可檢視或修改設定。
   - 選取代管群組，然後按一下「啟動」，可允許所有相關聯的代管使用者登入 VPN 和網頁驗證入口。
   - 選取代管群組，然後按一下「關閉」，可禁止所有相關聯的代管使用者登入 VPN 和網頁驗證入口。
   - 選取代管群組，然後按一下「刪除」，可移除該群組。

新增/編輯代管群組

用途：新增代管群組以組織代管使用者，並部署影響指派給代管群組的所有代管使用者的策略。

位置：「管理 > 使用者驗證 > 代管使用者 & 群組 > 代管群組 > 新增/編輯群組」

步驟

1. 指定代管群組詳細資料。
2. 按一下「儲存」。

匯入/匯出代管使用者與群組

用途：匯入或匯出使用者與群組，以簡化代管使用者/代管群組建立與更新，或建立組態設定的備份。

位置：「管理 > 使用者驗證 > 代管使用者與群組 > 匯入/匯出」

步驟

1. 執行下列動作：
   - 選取 CSV 檔案，然後按一下「匯入」來匯入代管使用者與群組。

     匯入時若發生衝突，可選擇性地選取核取方塊來覆寫現有的使用者與群組。將核取方塊保持為取消選取（預設值）可在出現重複時，保留現有的代管使用者與群組資訊。

     注意

     如需設定匯入檔案的詳細資料，請參閱準備匯入檔案 第 6-170 頁。
   - 按一下「匯出」，將代管使用者與群組匯出為 CSV 檔案。

注意

未指派代管使用者的代管群組將不會顯示在匯出的 CSV 檔案中。只有指派有代管使用者的代管群組才會匯出到 CSV 檔案。

準備匯入檔案

Cloud Edge 雲端主控台針對 CSV 檔案採用 UTF-8 編碼，以支援更多語言。某些試算表程式 (Microsoft Excel) 可能需要額外的組態設定，才能正確轉譯以 UTF-8 編碼的 CSV 檔案。

注意

趨勢科技建議使用 Google 試算表來準備代管使用者和群組的 CSV 檔案。

步驟

1. 採用下列格式建立 CSV 檔案。

```
user name, full name, email address, group, description, enable, password
juser, joe user, joeuser@example.com, group1, user's group, yes, asdg#2345
```

2. 在 Microsoft Excel 或其他試算表程式中開啟 CSV 檔案。
3. 移至「檔案 > 另存新檔」。
4. 在「檔案類型」下拉式功能表中，選取「CSV (逗號分隔) (*.csv)」。
5. 按一下「儲存」。
6. 如果使用 Microsoft Excel，請按一下「是」以確認。
7. 在記事本或其他文字編輯器中開啟 CSV 檔案。
8. 移至「檔案 > 另存新檔」。
9. 在「編碼」下拉式功能表中選取 UTF-8。
10. 按一下「儲存」。

LDAP 設定

Cloud Edge 6.0 和更新版本的設備支援使用輕量型目錄存取通訊協定 (LDAP) 來進行驗證。使用 LDAP 伺服器，透過 Cloud Edge 建立使用者特定或群組特定的政策很方便。使用者可以使用 LDAP 透過網頁驗證入口或 VPN 入口網站進行驗證。事件記錄檔、報告和通知會使用您的 LDAP 階層進行使用者識別。

重要

Cloud Edge G3 裝置不支援 LDAP 或 Radius。

Cloud Edge 支援在下列平台上使用 LDAP：

- Microsoft Windows 2012R2、Windows 2016 和 Windows 2019
- 開放式 LDAP

LDAP 驗證

使用 LDAP 設定來指定要與 Cloud Edge 整合的 LDAP 伺服器。Cloud Edge 會使用指定的 LDAP 伺服器執行下列動作：

- 在網頁驗證入口中驗證待識別的使用者
- 在 VPN 入口網站中驗證待識別的使用者
- 在策略規則設定中使用 LDAP 使用者或群組做為來源
- 新增或編輯報告時，在「報告者」欄位中使用 LDAP 使用者或群組

為了簡化使用者的 LDAP 組態設定，Cloud Edge 會針對設定 LDAP 驗證提供基本與進階的方法。

設定 LDAP 設定

用途：設定進行使用者驗證時所需的 LDAP 設定。

位置：「管理 > 使用者驗證 > LDAP 設定」

步驟

1. 選取下列其中一個選項：

基本	指定「網域名稱」、「使用者名稱」和「密碼」。如需詳細資訊，請參閱基本 LDAP 驗證 第 6-172 頁。
進階	指定用於與 LDAP 伺服器繫結的驗證伺服器、基準 DN、使用者名稱和密碼，以及新增 LDAP 伺服器與選取驗證方法。如需詳細資訊，請參閱進階 LDAP 驗證 第 6-173 頁。

重要

Cloud Edge G3 裝置不支援 LDAP 或 Radius。

2. 按一下「測試 LDAP 伺服器連線」。

注意

按一下「測試 LDAP 伺服器連線」按鈕後，系統會使用自動選取的設備測試連線。如果您要選取特定設備，請從「選擇要同步處理或測試的設備」旁的下拉式清單中進行選擇。

3. 按一下「儲存」。

基本 LDAP 驗證

Cloud Edge 為以下使用最廣的 LDAP 服務提供了簡單 LDAP 組態設定：Microsoft Active Directory (AD)。如果您使用 AD，請在 Cloud Edge 雲端主控台輸入以下基本資訊來設定使用者識別方法：網域名稱、使用者名稱和密碼。

藉由這些資訊，Cloud Edge 可使用 AD 自動探索工具取得必要資訊，包括：

- LDAP 伺服器位址
- 基底網域名稱
- 驗證資訊（Kerberos 領域/網域/KDC）

「進階 LDAP 驗證」欄位中會填入該等資訊。如果管理員判定自動探索到的結果不正確或無法運作，可以切換為「進階模式」並修改設定。

對於 LDAP 伺服器位址，自動探索工具會判定網域的所有網域控制站，然後 Cloud Edge 會選取並使用其中兩部最快的伺服器。

進階 LDAP 驗證

Cloud Edge 為熟悉 LDAP 的使用者提供進階驗證模式組態設定。

在進階模式組態設定中，使用者可以新增、刪除、移動及重新整理 LDAP 伺服器。

Cloud Edge 支援下列 LDAP 伺服器類型：

- MS Active Directory
- 開放式 LDAP

針對伺服器關係，Cloud Edge 僅支援上述伺服器進行「容錯移轉」。如果對主要伺服器的驗證失敗，Cloud Edge 會嘗試對次要伺服器進行驗證。

注意

Cloud Edge 僅支援相同網域內的多個 LDAP 伺服器進行容錯移轉。Cloud Edge 不支援位於多個網域的不同 LDAP 伺服器。

針對 LDAP 驗證方法，Cloud Edge 支援 MS Active Directory 和開放式 LDAP 採用下列 LDAP 驗證方法：

- 簡易
- Kerberos

針對基本和進階模式，請按一下「測試 LDAP 伺服器連線」按鈕來確認是否能夠對設定的 LDAP 伺服器進行驗證並回報結果。

RADIUS 設定

Cloud Edge 6.0 SP3 和更新版本的設備支援使用 RADIUS 進行驗證。使用者可以使用 RADIUS 透過網頁驗證入口或 VPN 入口網站執行驗證。您也可以在設

定中新增使用者和群組，然後使用 Cloud Edge 建立使用者特定或群組特定的策略。Cloud Edge 支援在下列平台上使用 RADIUS：

- Microsoft Windows 2012R2、Windows 2016 和 Windows 2019 上的網路策略伺服器。
- FreeRADIUS 3.0.13 或更新版本。

RADIUS 驗證

使用 RADIUS 設定來指定要與 Cloud Edge 整合的 RADIUS 伺服器。Cloud Edge 會使用指定的 RADIUS 伺服器執行下列作業：

- 在網頁驗證入口中驗證待識別的使用者
- 在 VPN 入口網站中驗證待識別的使用者
- 在策略規則設定中使用 RADIUS 使用者或群組做為來源
- 新增或編輯報告時，在「報告者」欄位中使用 RADIUS 使用者

您可以設定要執行 RADIUS 驗證的 RADIUS 伺服器和 RADIUS 使用者或群組。

設定 RADIUS 設定

用途：設定進行使用者驗證時所需的 RADIUS 設定。

位置：「管理 > 使用者驗證 > RADIUS 設定 > 一般設定」

步驟

1. 透過指定「主要 RADIUS 伺服器」、「通訊埠」和「密碼」，進行 RADIUS 設定。
2. 按一下「測試連線」以驗證連至 RADIUS 伺服器的連線。
3. 按一下「測試使用者認證」以測試 RADIUS 伺服器驗證功能是否正常運作。在 RADIUS 伺服器中指定使用者名稱和密碼，然後按一下「測試」。

注意

按一下「測試連線」按鈕後，系統會使用自動選取的設備測試連線。如果您要選取特定設備，請從「選擇要測試的設備」旁的下拉式清單中進行選擇。

4. 設定「次要 RAIUDS 伺服器」（選用）。
5. 指定「RADIUS 對應屬性」(「廠商特定/過濾 ID」)。

注意

如果選取「廠商特定」選項，則必須在 RADIUS 伺服器中設定「趨勢科技代碼 (6101)」做為廠商代碼。

6. 按一下「儲存」。

管理 RADIUS 使用者/群組

用途：管理 RADIUS 使用者/群組，以設定用於策略和報告的使用者/群組。

位置：「管理 > 使用者驗證 > RADIUS 設定 > RADIUS 使用者/群組」

步驟

1. 執行下列動作：
   - 按一下「新增」，以建立新的 RADIUS 使用者/群組。
   - 使用右上方的「搜尋」，以尋找 RADIUS 使用者/群組名稱。
   - 按一下 RADIUS 使用者/群組名稱，以檢視或修改說明。
   - 選取 RADIUS 使用者/群組名稱，然後按一下「刪除」，可移除該使用者/群組。

RADIUS 使用者和群組

您可以透過 RADIUS 伺服器來驗證使用者，但若要設定用於策略和報告的 RADIUS 使用者或群組，則必須在 Cloud Edge 雲端主控台中新增相同的使用者或群組。

如果使用者不想設定用於策略或報告的 RADIUS 使用者或群組，則只需要設定 RADIUS 伺服器設定。

Cloud Edge 不會將 RADIUS 使用者和群組與設備進行同步處理，而只會部署相關策略。

同步處理使用者帳號和群組

下列程序說明如何立即同步處理使用者帳號和群組。您可以設定策略並根據這項已同步處理的使用者和群組資訊產生報告。Cloud Edge 雲端主控台會每隔 8 小時自動從所有已註冊的設備同步處理使用者和群組。

同步處理的資訊包括 Cloud Edge 雲端主控台上設定的代管使用者和群組資訊。

步驟

1. 移至「管理 > 使用者驗證 > 使用者 ID 同步處理」。
2. 按一下「同步處理所有設備」。

   Cloud Edge 雲端主控台會同步處理所有已註冊設備上的使用者和群組資訊。

新增雲端主控台管理員帳號

Cloud Edge 雲端主控台使用者帳號可存取屬於同一公司的所有已註冊設備。預設會建立具有管理員權限的「管理員」帳號。

Cloud Edge 雲端主控台有兩種使用者帳號類型：

- 管理員
- 唯讀使用者

步驟

1. 移至「管理 > 使用者與帳號 > 帳號管理」。
2. 按一下「新增」，或按一下帳號的完整名稱進行變更。

   「新增/編輯帳號」畫面隨即出現。
3. 設定可用的設定。

選項	說明
完整名稱	輸入使用者的完整名稱。這會在使用者登入時顯示於 Cloud Edge 雲端主控台的右上方。
使用者名稱	輸入使用者的電子郵件信箱。使用者會輸入此電子郵件信箱來登入。 注意 建立使用者帳號後，使用者名稱即無法變更。
密碼	輸入使用者的密碼。 密碼必須至少 8 個字元，且必須包含至少一個大寫字母、一個小寫字母、一個數字，以及選擇性包含特殊字元。 秘訣 下列秘訣可協助您建立有效的密碼： • 在密碼中包含特殊字元 • 避免使用可以在任何語言的任何字典中找得到的單字 • 故意拼錯的單字 • 使用字組或單字組合
確認密碼	再次輸入使用者的密碼。

選項	說明
唯讀	選取此核取方塊來限制使用者的權限。如果未選取此核取方塊，則使用者的身分是「管理員」。 唯讀使用者只能執行下列操作： • 檢視「設備」、「策略」、「分析與報告」和「管理」標籤上的物件 • 在「資訊中心」中檢視和修改標籤和 Widget • 使用「變更使用者資料檔」畫面 • 按一下「報告」畫面中的「立即執行」按鈕

4. 按一下「儲存」。

在郵件用戶端上匯入 Cloud Edge CA 憑證

設定安全資料檔時，為了電子郵件的安全，您可以啟動安全通訊協定（SMTPS、POP3S 和 IMAPS）。使用安全電子郵件時，Cloud Edge 會充當私人憑證授權單位 (CA) 並動態產生傳送到郵件用戶端的數位憑證，以完成連線的安全通道。不過，預設 CA 並非由 Internet 上的知名（信任）CA 簽署。在這種情況下，郵件用戶端會一直產生快顯警告訊息，指出「您目前連線的伺服器使用的安全性憑證無法驗證」。

為了消除警告訊息並讓用戶端順利透過 SSL 或 startTLS 收發電子郵件，您可以在郵件用戶端上安裝 Cloud Edge CA 憑證。

本節包含下列程序：

- 匯出 CA 憑證 第 6-179 頁
- 匯入適用於 Microsoft Outlook 的 Cloud Edge CA 憑證 第 6-179 頁
- 匯入適用於 Mozilla Thunderbird 的 Cloud Edge CA 憑證 第 6-180 頁
- 匯入適用於 Mac OS 的 Cloud Edge CA 憑證 第 6-181 頁
- 將 Cloud Edge CA 憑證匯入 Android 裝置 第 6-182 頁

- 將 Cloud Edge CA 憑證匯入 iOS 裝置 第 6-183 頁

注意

本節未提供 Foxmail 的相關程序。這個版本的 Cloud Edge 不支援 Foxmail 的安全電子郵件掃瞄。

匯出 CA 憑證

您必須先匯出 Cloud Edge CA 憑證，然後才能將它安裝在郵件用戶端上。

步驟

1. 移至「管理 > 憑證管理」。
2. 若要匯出憑證，請按一下「匯出」。
3. 將憑證檔案 (`CloudEdge.crt`) 儲存到您的電腦。

匯入適用於 Microsoft Outlook 的 Cloud Edge CA 憑證

為了無縫解密 Microsoft Outlook 的安全電子郵件，您必須將 Cloud Edge CA 憑證匯入 Microsoft Windows 信任的根憑證授權單位的憑證存放區。

步驟

1. 將先前從 Cloud Edge 匯出的憑證檔案 (`CloudEdge.crt`) 複製到目標郵件用戶端電腦。
2. 在目標上，按兩下憑證檔案以將其開啟。
3. 按一下「安裝憑證」。

   「憑證匯入精靈」畫面隨即出現。

4. 選取「將所有憑證放入以下存放區」，然後按一下「瀏覽」。

   「選取憑證存放區」畫面隨即出現。

5. 選取「信任的根憑證授權單位」存放區，然後按一下「確定」。

6. 按「下一步」，然後在「安全性警告」頁面上選取「是」。

   如果顯示下列提示，表示憑證匯入成功：「匯入成功」。

7. 重新啟動 Microsoft Outlook。

   收發電子郵件不再產生憑證警告。

匯入適用於 Mozilla Thunderbird 的 Cloud Edge CA 憑證

為了無縫解密 Mozilla Thunderbird 的安全電子郵件，您必須將 Cloud Edge CA 憑證匯入 Thunderbird 信任的憑證授權單位的憑證存放區。

注意

本程序適用於 Thunderbird 45.7.1。不同 Thunderbird 版本的步驟可能不同。如有需要，請參閱您版本的 Thunderbird 文件。

步驟

1. 將先前從 Cloud Edge 匯出的憑證檔案 (`CloudEdge.crt`) 複製到目標郵件用戶端電腦。

2. 在目標上，開啟 Thunderbird 電子郵件應用程式，然後按一下「應用程式」功能表按鈕 (☰)。

3. 從下拉式功能表中選取「選項」。

   「選項」畫面隨即出現。

4. 選取「進階」，然後移至「憑證」標籤。

5. 按一下「檢視憑證」。

   「憑證管理員」畫面隨即出現。

6. 按一下「憑證機構」標籤。

7. 請點選「匯入」。

   「下載憑證」畫面隨即出現，在此畫面上會詢問您信任 Cloud Edge 憑證的用途。

8. 選取「信任此 CA 來識別網站」和「信任此 CA 來識別電子郵件使用者」。

9. 請點選「確定」。

10. 重新啟動 Thunderbird 應用程式並開啟「憑證管理員」畫面，確認 Cloud Edge 憑證已成功匯入到受信任的 CA 存放區。

匯入適用於 Mac OS 的 Cloud Edge CA 憑證

為了無縫解密 Mac OS 的安全電子郵件，您必須將 Cloud Edge CA 憑證匯入 Mac OS 信任的憑證授權單位的憑證存放區。

注意

本程序適用於 Mac OS El Capitan 10.11.6。不同 Mac OS 版本的步驟可能不同。如有需要，請參閱您版本的 Mac OS 文件。

執行本程序期間，系統可能會要求提供管理員認證來進行驗證。

步驟

1. 將先前從 Cloud Edge 匯出的憑證檔案 (`CloudEdge.crt`) 複製到目標 Mac OS 電腦。

2. 以滑鼠右鍵按一下 `CloudEdge.crt` 檔案。

3. 移至「開啟檔案的應用程式 > 鑰匙圈存取」。

「鑰匙圈」畫面隨即出現。

4. 在左窗格中，選取「系統」鑰匙圈。

   Cloud Edge 憑證列在右窗格中，但未受系統信任。

5. 在右窗格中，以滑鼠右鍵按一下 Cloud Edge 憑證項目，然後選取「取得資訊」。

   Cloud Edge 憑證資訊畫面隨即出現。

6. 展開「信任」資訊區段。

7. 在「使用此憑證時」下拉式功能表中，選取「一律信任」。

   此畫面列出的所有特定應用程式的值均會自動變更為「一律信任」。

8. 關閉畫面。

   「系統」鑰匙圈的右窗格顯示 Cloud Edge 憑證現在受到信任。

9. 重新啟動郵件用戶端。

   收發電子郵件不再產生憑證警告。

將 Cloud Edge CA 憑證匯入 Android 裝置

為了無縫解密 Android 裝置上的安全電子郵件，您必須將 Cloud Edge CA 憑證匯入信任的憑證存放區。

注意

安裝憑證的步驟會視 Android 裝置和版本而不同。如有需要，請參閱 Android 文件以取得詳細資訊。

若您不想安裝 Cloud Edge CA 憑證，可以移至電子郵件帳號的進階設定，並確認已勾選「接受所有憑證」。

步驟

1. 將先前從 Cloud Edge 匯出的憑證檔案 (`CloudEdge.crt`) 下載到目標 Android 裝置。

   存取和下載憑證的方法包括透過瀏覽器或透過電子郵件附件。

2. 在目標 Android 裝置上，移至「設定 > 安全性」。
3. 瀏覽並點選「由儲存空間安裝」。

   「開啟自」畫面隨即出現。

4. 選取「內部儲存空間」，然後選取「下載」資料夾。
5. 選取並安裝 Cloud Edge 憑證。
   - 使用預設憑證名稱。
   - 確認已選取「VPN 和應用程式」。
6. 移至「設定 > 安全性 > 信任的憑證」並選取「使用者憑證」標籤，確認已成功匯入 Cloud Edge 憑證。
7. 在 Android 裝置上重新啟動行動郵件用戶端。

將 Cloud Edge CA 憑證匯入 iOS 裝置

為了無縫解密 iOS 裝置上的安全電子郵件，您必須將 Cloud Edge CA 憑證匯入信任的憑證存放區。

注意

安裝憑證的步驟會視 iOS 版本而不同。如有需要，請參閱 iOS 文件以取得詳細資訊。

步驟

1. 使用電子郵件帳號傳送並下載您先前從 Cloud Edge 匯出的憑證檔案 (`CloudEdge.crt`)。

2. 按一下電子郵件中附加的憑證檔案。

   「安裝描述檔」畫面隨即開啟並提示您安裝憑證。

3. 點選「安裝」。

   由於這不是受信任的憑證，因此會顯示警告。

4. 點選「安裝」確認要安裝描述檔。

   「已安裝描述檔」確認畫面隨即開啟，其中顯示綠色的「已驗證」核取記號。

5. 點選「完成」關閉「已安裝描述檔」畫面。

6. 移至「設定 > 一般 > 資料檔」，確認已安裝 Cloud Edge 憑證。

   您必須立即啟動 Cloud Edge CA 憑證的完整信任。

7. 移至「設定 > 一般 > 關於本機 > 憑證信任設定」並將 Cloud Edge 撥至「開啟」，以啟動 Cloud Edge CA 憑證的完整信任。

8. 在 iOS 裝置上重新啟動行動郵件用戶端。

更新

若要確保擁有最新防護來抵禦最新風險，您有幾項病毒碼檔案元件可以更新。這些檔案包含已知安全威脅的二進位「特徵標記」或病毒碼。Cloud Edge 會使用這些病毒碼，在已知風險通過 Internet 設備時加以偵測。新的病毒碼檔案通常是每星期發行數個，而通訊協定與 IPS 特徵碼檔案的更新頻率則較不頻繁。

要讓 Cloud Edge 發揮最佳效果，就必須使用最新病毒碼檔案。特徵標記型病毒掃瞄的運作方式，是將已掃瞄檔案的二進位特徵與病毒碼檔案中的已知風險二進位特徵進行比較。趨勢科技經常會發行新版的病毒碼與間諜程式病毒碼來因應新識別出的風險。同樣地，當識別出新的網路釣魚 URL 時，也會發行新版的網路釣魚病毒碼。

Cloud Edge 使用「主動式更新」，這是趨勢科技的公用程式，能夠依要求或在背景更新病毒碼檔案與掃瞄引擎、間諜程式或可能的資安威脅程式病毒碼檔

案。「主動式更新」是許多趨勢科技產品都在使用的服務。「主動式更新」會連線到趨勢科技 Internet 更新伺服器，以便下載最新的病毒碼檔案與引擎。「主動式更新」不會中斷網路服務，亦不需要端點重新啟動。可依所排程的間隔定期取得更新，亦可依要求取得更新。

相關資訊

→ 可更新的元件

可更新的元件

若要確保擁有最新防護來抵禦最新風險，您有幾項引擎和病毒碼檔案元件可以更新。

病毒碼檔案包含已知安全威脅的二進位「"簽章"」或病毒碼。Cloud Edge 會使用這些病毒碼，在已知風險通過 Internet 設備時加以偵測。一些病毒碼檔案（例如病毒和雲端病毒碼檔案）通常是每週發行多次，而另一些病毒碼檔案（例如通訊協定和 IPS 特徵碼檔案）的更新頻率則較低。

垃圾郵件防護病毒碼和引擎

垃圾郵件病毒碼有助於 Cloud Edge 識別訊息和附件中的最新垃圾郵件。垃圾郵件防護引擎可偵測訊息和附件中的垃圾郵件。

C&C 資訊病毒碼

Command & Control (C&C) 資訊病毒碼為 Cloud Edge 提供增強的偵測與警訊功能，以減少進階持續性安全威脅和目標攻擊所造成的傷害。

IntelliTrap 病毒碼與例外

IntelliTrap 偵測技術會將趨勢科技病毒掃瞄引擎中的一項掃瞄選項搭配 IntelliTrap 病毒碼（用以找出潛在惡意檔案）和 IntelliTrap 例外病毒碼（當成允許清單）使用。Cloud Edge 會使用可用的 IntelliTrap 選項與病毒碼來偵測

惡意壓縮檔（例如壓縮檔中的 Bot）。病毒撰寫者通常會使用不同的檔案壓縮配置來規避病毒過濾機制。IntelliTrap 會以啟發式方式評估壓縮檔，協助減少 Bot 或任何其他惡意壓縮檔可能對網路造成的風險。

IPS 特徵碼

Cloud Edge 使用 IPS 特徵碼檔案來封鎖 IPS 弱點。如果比較幾個病毒碼後顯示網路連線存在弱點，Cloud Edge 會繼續進行所設定的處理行動。

間諜程式病毒碼

隨著暗中收集機密資訊的新隱藏型程式（可能的資安威脅程式）的誕生、散佈及獲發現，趨勢科技會收集其明顯特徵，並將這些資訊納入間諜程式/可能的資安威脅程式病毒碼檔案。

病毒掃瞄引擎與病毒碼

病毒掃瞄引擎會分析每個檔案的二進位特徵，然後將其與病毒碼檔案中的二進位資訊進行比較。如果相符，即判定檔案為惡意檔案。

本機雲端病毒碼

本機雲端病毒碼是雲端截毒掃瞄進階惡意程式掃瞄解決方案的本機部分。如果已啟動雲端截毒掃瞄，則 Cloud Edge 會將內容傳送至雲端截毒伺服器進行掃瞄。本機雲端病毒碼是雲端截毒掃瞄解決方案的處理常式部分。雲端病毒碼（位於雲端截毒伺服器）會經常更新，而本機雲端病毒碼每天更新一次。

排程更新

排程更新可確保 Cloud Edge 提供防範最新安全威脅的安全性。趨勢科技會經常發佈新版病毒碼和間諜程式病毒碼，以防範最新發現的安全威脅。

步驟

1. 移至「管理 > 排程更新」。
2. 按一下「開啟」以啟動排程更新。
   - 元件更新
   - 韌體與恢復出廠預設值版本更新

   注意

   自動恢復出廠預設值版本更新週期的排程與自動韌體更新週期共用同一個排程模式。
3. 選取執行更新的頻率。

   注意

   選取頻率時，指定的排程更新執行時間是 Cloud Edge 設備上的當地時間。
4. 按一下「儲存」。
5. 請等候幾分鐘，讓更新生效。
6. 按一下「全部部署」以使變更生效。

手動更新

排程更新可確保 Cloud Edge 提供防範最新安全威脅的安全性。趨勢科技會經常發佈新版病毒碼和間諜程式病毒碼，以防範最新發現的安全威脅。

步驟

1. 移至「 設備」。
2. 以滑鼠右鍵按一下設備，然後選取「更新」。

   「手動更新」畫面隨即出現。

3. 選取要更新的元件。
4. 按一下「更新」。

第 7 章

Cloud Edge 內部部署

本章說明如何在客戶網路中部署 Cloud Edge 設備，並提供基本管理作業的相關資訊。

部署

安全指導方針

遵循下列指導方針以確保一般安全性：

- 在安裝過程中及安裝後保持底座區域清潔無塵。
- 請勿穿戴可能勾住底座的寬鬆衣物或珠寶。請繫緊領帶或圍巾並捲起袖子。
- 在任何可能傷及雙眼的環境下作業時，請配戴護目鏡。
- 請勿執行任何可能傷及人員或使設備不安全的處理行動。
- 在安裝或拆卸底座或是靠近電源供應器工作時，請先關閉電源並拔下電源線，以中斷所有電源。
- 如果可能存在危險情況，請勿個人單獨為之。
- 請勿斷言電源已與電路斷開；務必隨時檢查電路。

包裝內容

當您拆封 Cloud Edge 設備包裝時，請務必核對其中的內容。您可以使用包裝隨附的快速使用卡片來核對內容。

部署模式

部署模式總覽

Cloud Edge 設備提供三種部署組態設定：路由模式、橋接模式，以及軟體切換（從「橋接模式」變化而來）。這些組態設定可控制 Cloud Edge 設備路由網路封包以及介面執行轉送決定的方式。

表 7-1. 部署模式

部署模式	用途
橋接模式	如果部署模式設為「橋接模式」，則您可以部署「橋接模式」或「軟體切換」組態設定。 橋接模式組態設定 Cloud Edge 裝置用做各種網路裝置（交換器、路由器、防火牆或端點）之間的第 2 層橋接器，可通透掃瞄雙向網路流量，但是在網路中不可見。 其所有介面均位於同一個子網路上。您只需為 橋接器介面 (br0) 設定能夠連線到 Internet 的 IP 位址即可。橋接器介面 (br0) 用於連線到 Cloud Edge 雲端主控台，以便提供 Cloud Message Scan 服務，並提供對其他雲端服務（例如趨勢科技主動式更新）的存取權。 「橋接模式」部署通常適用於位於現有防火牆或路由器後方的私人網路。 使用「橋接模式」不需要修改用戶端、路由器或交換器，是將 Cloud Edge 部署到現有網路拓撲的最簡便方式。 軟體切換組態設定 「軟體切換」是從「橋接模式」變化而來（模式切換設定為「橋接」）。 Cloud Edge 用做上游網路裝置（交換器、路由器或防火牆）與端點之間的軟體切換。Cloud Edge 設備會掃瞄所有通過的流量是否有惡意程式。 如同橋接模式，軟體切換的所有介面均位於同一個子網路上，而且您只需為 橋接器介面 (br0) 設定 IP 位址。橋接器介面 (br0) 提供 Internet 連線。不過，採用「軟體切換」部署時，除了上行通訊埠之外的所有通訊埠都會直接連線到端點（例如，用戶端、伺服器和 Wi-Fi 存取路由器）。 當 Cloud Edge 是在位於現有防火牆或路由器後方的私人網路上運作，並且您想要將端點直接連線到 Cloud Edge 設備時，通常會採用「軟體切換」部署。

部署模式	用途
	橋接模式（採用切換晶片組） 採用硬體切換晶片組的 Cloud Edge 設備提供更多優點。在「橋接模式」下，這款設備可用做具有 7 個 LAN 通訊埠的硬體切換，每個通訊埠皆可直接連線到端點（例如，用戶端、伺服器和 Wi-Fi 存取路由器）。 採用硬體切換晶片組的 Cloud Edge 設備，可為 Internet 流量提供全面的安全防護功能。此外，您可以設定內部網路流量的安全層級，包括「高」安全性、「標準」安全性或「高速」安全性。 當 Cloud Edge 是在位於現有防火牆或路由器後方的私人網路上運作，並且您想要將多個端點直接連線到 Cloud Edge 設備時，通常會將 Cloud Edge 設備部署為硬體切換。
路由模式	Cloud Edge 裝置用做私人網路與 Internet 之間的第 3 層路由裝置，在網路中可見。它可使用 NAT 隱藏私人網路的 IP 位址，並且具有流量串流掃瞄功能。 在「路由模式」下部署需要設定至少兩個網路介面：內部使用及外部使用各佔其一。所有介面均位於不同子網路，可讓您擁有一個能連線到公用 Internet 的 IP 位址。 每個連線到網路的介面必須設定對於該網路而言有效的 IP 位址。Cloud Edge 可在向目標網路傳送和接收封包並用做路由器之前執行網路位址轉譯。 在路由模式下，Cloud Edge 也會提供乙太網路上的點對點通訊協定 (PPPoE) 功能，以支援透過非對稱式數位用戶線路 (ADSL) 撥接到 ISP。 當 Cloud Edge 裝置部署為私人網路與公用網路之間的設備時，通常使用「路由模式」部署。 採用路由模式的無線網路 對於支援無線存取的 Cloud Edge 設備型號，您可以設定主要無線存取點和客體無線存取點。這款設備可對無線網路執行完整的安全掃瞄。 對於執行 Cloud Edge 6.0 SP1 或更新版本的 Cloud Edge 設備型號，當採用「路由模式」時，可以設定高可用性群組（HA 群組）來避免單點失敗，以提升網路可用性。

注意

採用「橋接模式」或「軟體切換」時，某些依賴第 3 層網路運作的設備功能將無法使用，例如 VPN 或 NAT。

上述三種部署組態設定都支援所有根據策略部署的安全功能，能保護您的網路安全無虞。

路由模式網路拓撲

在「路由模式」下，Cloud Edge 在網路中可見，用做了具有流量串流掃瞄功能的第 3 層路由裝置。

下圖展示 Cloud Edge 在「路由模式」下的典型網路拓撲：

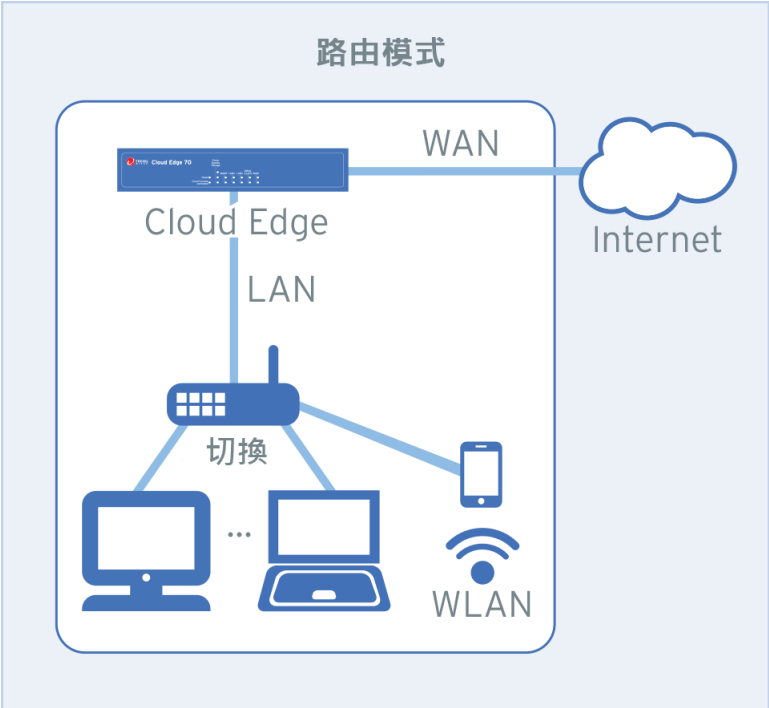


圖 7-1. 路由模式下的 Cloud Edge

在「路由模式」下，Cloud Edge 設備可用做私人網路與公用網路之間的第 3 層設備裝置並作為路由器運作。系統會為每個連接的介面指派一個 IP 位址。所有介面均位於不同子網路，可讓您擁有一個能連線到公用 Internet 的 IP 位址。Cloud Edge 可在向目標網路傳送及接收封包之前執行網路位址轉譯 (NAT)。

您必須將 WAN 介面連線到 Internet，Cloud Edge 設備才能向 Cloud Edge 雲端主控台註冊。Cloud Message Scan (CMS) 也會使用 WAN 連線在雲端中管理 Cloud Edge 以進行排程病毒碼更新，並善用趨勢科技™主動式雲端截毒技術™即時安全資訊的強大功能。

Cloud Edge 也會提供乙太網路上的點對點通訊協定 (PPPoE) 功能，以支援透過非對稱式數位用戶線路 (ADSL) 撥接到 ISP。

採用硬體切換晶片組的 Cloud Edge 設備

您可以使用與在設定所有其他 Cloud Edge 型號時所用的相同設定與組態設定，在「路由模式」下設定採用硬體切換晶片組的 Cloud Edge 設備。

採用路由模式的無線網路

下圖說明具有無線網路存取之 Cloud Edge 設備在「路由模式」下的典型網路拓撲：

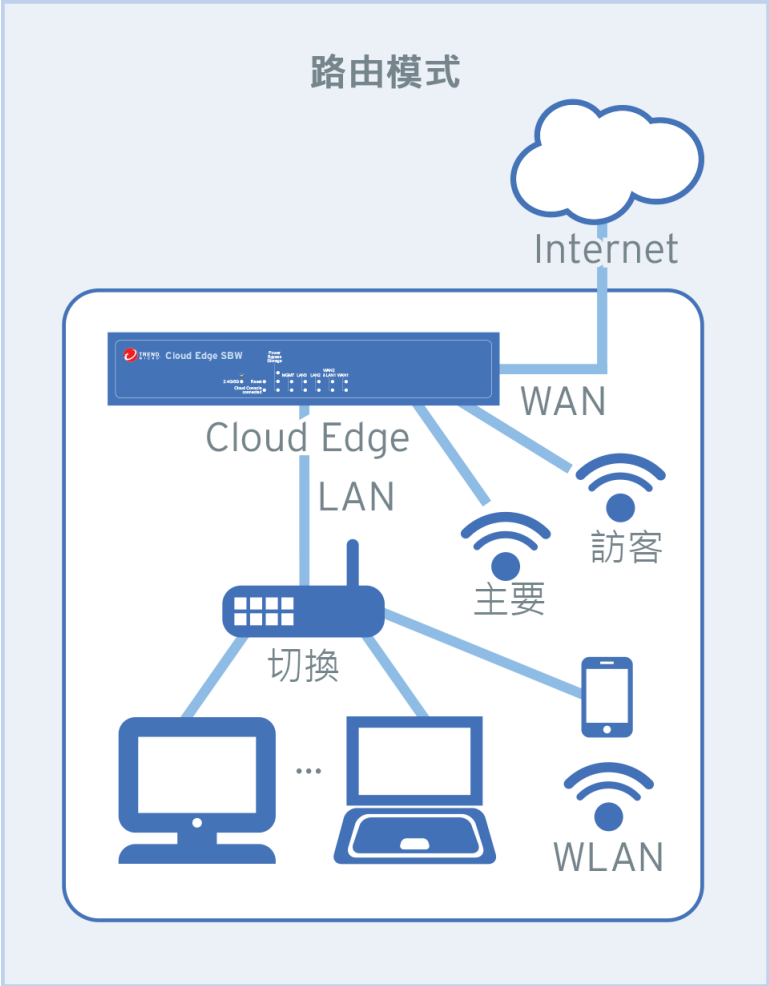


圖 7-2. 在「路由模式」下具有無線存取的 Cloud Edge

對於支援無線網路存取的 Cloud Edge 設備，您可以設定主要無線存取點和客體無線存取點。這款設備提供完整的無線網路安全防護功能。您可以使用 MAC 位址過濾來控制無線網路存取。您可以設定無線網路的其他服務（例如 DHCP 服務、頻寬控制、NAT 和 VPN）。

路由模式下的 HA 群組

對於執行 Cloud Edge 6.0 SP1 或更新版本的 Cloud Edge 設備型號，當採用「路由模式」時，可以設定高可用性群組（HA 群組）來避免單點失敗，以提升網路可用性。

您必須使用 Cloud Edge 雲端主控台來設定 HA 群組。如需有關此拓撲及如何設定此部署的相關資訊，請參閱建立 HA 群組 第 6-15 頁。

橋接模式網路拓撲

在「橋接模式」下，Cloud Edge 會擔任網路裝置（交換器、路由器或防火牆）之間的第 2 層橋接器。Cloud Edge 設備會掃瞄所有通過的流量是否有惡意程式。

下圖說明 Cloud Edge 在「橋接模式」下的典型網路拓撲：

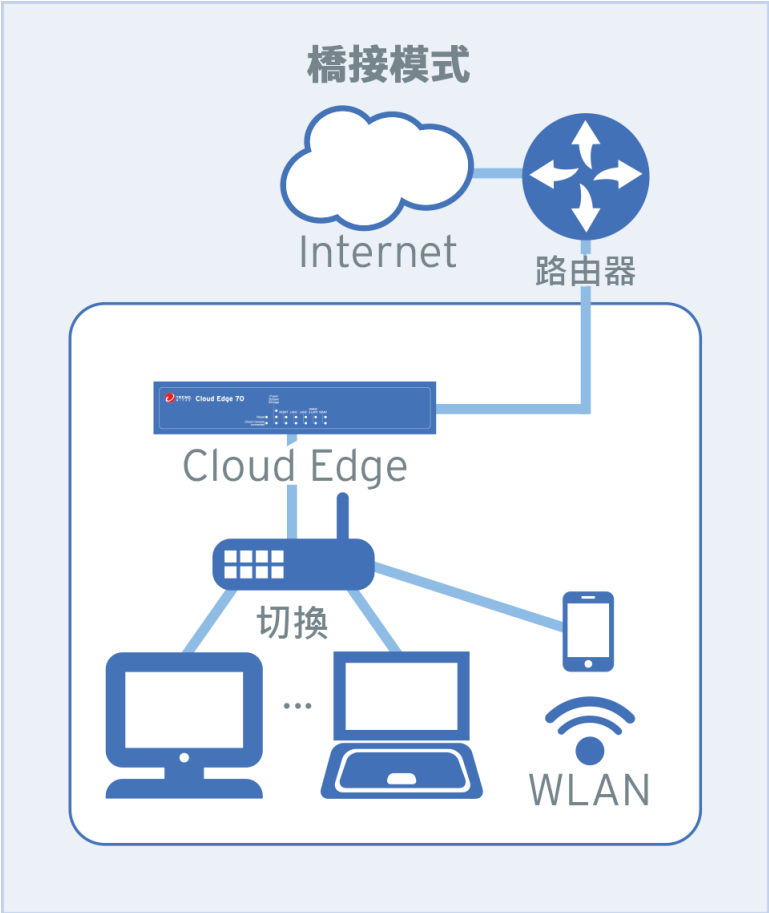


圖 7-3. 橋接模式下的 Cloud Edge

若要設定「橋接模式」，您必須將纜線連接到 WAN 介面和 LAN1 介面。與使用網路橋接器類似，WAN 與 LAN 介面必須位於同一個子網路。

由於「橋接模式」下的 Cloud Edge 設備是仰賴第 2 層網路運作，因此連接的介面不會獲指派 IP 位址。不過，您必須在 橋接器介面 (br0) 設定 IP 位址，來

向 Cloud Edge 雲端主控台註冊 Cloud Edge 設備。指派給 橋接器介面 (br0) 的 IP 位址用於執行雲端型 Cloud Message Scan (CMS)、管理 Cloud Edge 進行預約病毒碼更新，以及運用雲端中趨勢科技™主動式雲端截毒技術™的即時安全資訊強大功能。

當 Cloud Edge 是在位於現有防火牆或路由器後方的私人網路上運作時，請設定「橋接模式」，讓 Cloud Edge 能夠無阻礙地執行所有掃瞄功能。

軟體切換網路拓撲

在「軟體切換」組態設定中，Cloud Edge 用做網路裝置（交換器、路由器或防火牆）與端點之間的軟體切換。當 Cloud Edge 是在位於現有防火牆或路由器後方的私人網路上運作，並且您想要將端點直接連線到 Cloud Edge 設備時，請設定「軟體切換」部署。

設定為「軟體切換」時，Cloud Edge 設備會掃瞄所有通過它的流量是否有惡意程式。

下圖展示 Cloud Edge 採用「軟體切換」組態設定時的典型網路拓撲：

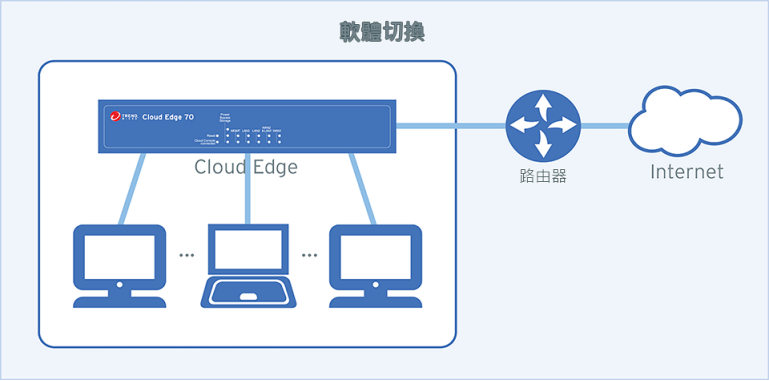


圖 7-4. 採用「軟體切換」組態設定的 Cloud Edge

- Cloud Edge 部署開關會設定為「橋接」；不過，您使用的部署步驟會將設備設定為「軟體切換」，而非透通橋接器。
- 若要將 Cloud Edge 設備設定為「軟體切換」，您必須將纜線連接至最少三個通訊埠。

  - WAN 介面與 LAN1 介面為必要項目。
  - 必須至少連線一個 LAN2 或 LAN3 通訊埠。
  - 如有需要，可以同時連線 LAN2 和 LAN3。
- 在連接纜線時，務必熟記網路拓撲。
  - 介面必須位於同一個子網路。
  - WAN 介面做為上行連線到路由器（直接或透過上游交換器）。
  - LAN1、LAN2 和 LAN3 通訊埠連線至內部網路上的端點。
- 由於「軟體切換」組態設定是仰賴第 2 層網路運作，因此連線的介面不會獲指派 IP 位址。
- 您必須在 橋接器介面 (br0) 設定 IP 位址，來向 Cloud Edge 雲端主控台註冊 Cloud Edge 設備。

  指派給 橋接器介面 (br0) 的 IP 位址用於執行雲端型 Cloud Message Scan (CMS)、管理 Cloud Edge 進行預約病毒碼更新，以及運用雲端中趨勢科技™主動式雲端截毒技術™的即時安全資訊強大功能。

橋接模式網路拓撲（採用切換晶片組）

採用硬體切換晶片組的 Cloud Edge 設備是一款功能完備的安全裝置，但也可在「橋接模式」下用做硬體切換。採用「橋接模式」時，設備會用做網路裝置（交換器、路由器或防火牆）與端點之間的硬體切換。這款設備的 LAN 通訊埠數目擴增至 8 個 (LAN1-LAN8)。LAN1-LAN7 可直接連線到端點。LAN8 用於旁路功能，且不能用於連線到端點。

下圖說明採用硬體切換晶片組的 Cloud Edge 設備在「橋接模式」下的典型網路拓撲：

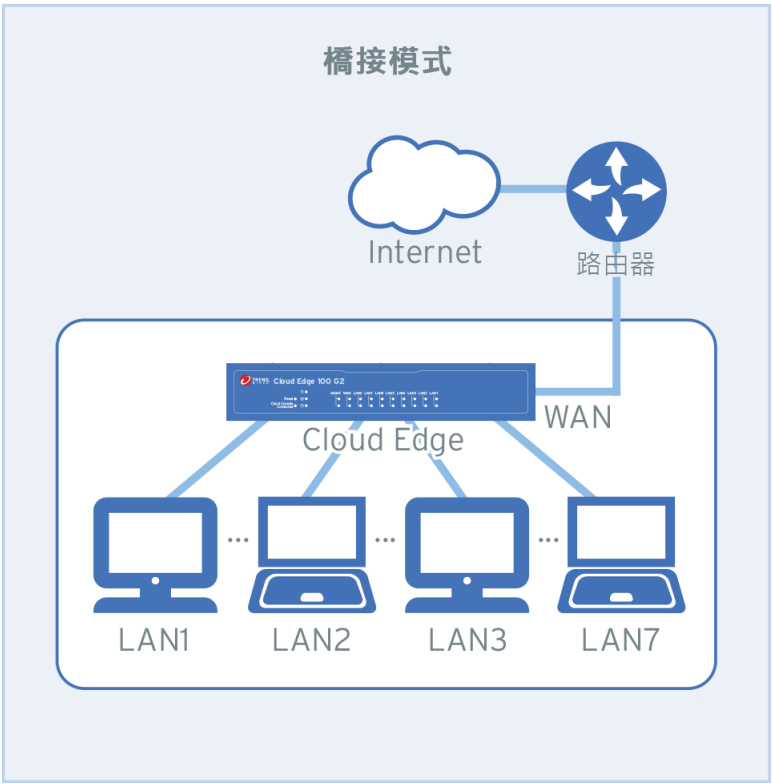


圖 7-5. 橋接模式下的採用硬體切換晶片組的 Cloud Edge

當 Cloud Edge 是在位於現有防火牆或路由器後方的私人網路上運作，並且您想要將最多 7 個端點直接連線到 Cloud Edge 設備時，請以「橋接模式」部署採用硬體切換晶片組的 Cloud Edge 設備。

設備會掃瞄通過 WAN 介面的所有流量，以提供完整的安全功能。

針對內部流量（LAN 到 LAN 流量）提供的安全性取決於您在設定設備時所選擇的安全模式。

若要設定「橋接模式」，您必須將纜線連接到 WAN 和 LAN1 介面。此外，您可以將纜線從 LAN2-LAN7 連接到內部端點。WAN 和 LAN 介面必須皆位於同一個子網路。

由於「橋接模式」下的設備是仰賴第 2 層網路運作，因此連接的介面不會獲指派 IP 位址。不過，您必須在虛擬 切換介面 (sw0) 設定 IP 位址，來向 Cloud Edge 雲端主控台註冊 Cloud Edge 設備。您也可以在 切換介面 (sw0) 設定其他切換相關設定。

指派給 切換介面 (sw0) 的 IP 位址用於執行雲端型 Cloud Message Scan (CMS)、管理 Cloud Edge 進行預約病毒碼更新，以及運用雲端中趨勢科技™主動式雲端截毒技術™的即時安全資訊強大功能。

即使 WAN 和 LAN1-LAN8 介面都是不具有 IP 位址的 L2 介面，您仍可設定一些與硬體切換組態設定相關的介面設定。

採用硬體切換晶片組之設備上的旁路通訊埠

採用硬體切換晶片組之 Cloud Edge 設備的某些通訊埠提供增強的旁路功能，即使在發生中斷掃描的事件（例如重新開機、系統問題和關閉電源）期間，仍可讓流量周遊設備。在設定採用硬體切換晶片組的 Cloud Edge 設備之前，請先瞭解旁路通訊埠的運作方式，以便針對特定業務需求選擇適用的通訊埠。

有兩種旁路模式：

- 旁路模式 1：

  設備會旁路 WAN 與 LAN1-LAN7 之間的所有流量。LAN8 在旁路期間不可用。開啟設備的電源後，在系統失敗、系統開機和升級期間等，「旁路模式 1」仍會運作（如果需要）。設備必須開啟電源，「旁路模式 1」才能運作。

  一旦關閉設備電源，「旁路模式 1」便無法運作。

  只有採用硬體切換晶片組的設備會實作此模式，其他 Cloud Edge 型號並未提供此旁路模式。

- 旁路模式 2：

  設備會旁路 WAN 與 LAN1 之間的流量。關閉設備的電源後，「旁路模式 2」仍會運作。

其他 Cloud Edge 型號亦提供此旁路動作。此外，採用硬體切換晶片組的 Cloud Edge 設備在開啟電源後，「旁路模式 2」將不會運作，因為運作的是「旁路模式 1」。

請參閱下表以判斷旁路功能在各種情境下的互動方式：

開啟電源

轉折點	→ DC 輸入	→ 開機	→ 安裝旁路模組	→ 初始化完成	
系統階段	DC 輸出	BIOS	作業系統啟動	初始化	正常
橋接模式	WAN 和 LAN1 旁路	WAN 和 LAN1-LAN7 旁路	WAN 和 LAN1-LAN7 旁路	WAN 和 LAN1-LAN7 旁路	關閉旁路/開啟掃瞄
路由模式	不旁路	不旁路	不旁路	不旁路	不旁路/開啟掃瞄

重新開機

轉折點	輸入重新開機指令	→ 重新啟動	→ 開機	→ 安裝旁路模組	→ 初始化完成	
系統階段	正常	準備	BIOS	作業系統啟動	初始化	正常
橋接模式	關閉旁路/開啟掃瞄	WAN 和 LAN1-LAN7 旁路	WAN 和 LAN1-LAN7 旁路	WAN 和 LAN1-LAN7 旁路	WAN 和 LAN1-LAN7 旁路	關閉旁路/開啟掃瞄
路由模式	不旁路/開啟掃瞄	不旁路	不旁路	不旁路	不旁路	不旁路/開啟掃瞄

核心嚴重錯誤

轉折點	嚴重錯誤	→ WDT 逾時（80 秒）	→ 重新啟動	→ 開機	→ 安裝旁路模組	→ 初始化完成

系統階段	正常	核心嚴重錯誤	關閉電源（0.2 秒）	BIOS	作業系統啟動	初始化	正常
橋接模式	關閉旁路/開啟掃瞄	WAN 和 LAN1-LAN7 旁路	WAN 和 LAN1 旁路	WAN 和 LAN1-LAN7 旁路	WAN 和 LAN1-LAN7 旁路	WAN 和 LAN1-LAN7 旁路	關閉旁路/開啟掃瞄
路由模式	不旁路/開啟掃瞄	不旁路	不旁路	不旁路	不旁路	不旁路	不旁路/開啟掃瞄

部署模式切換

Cloud Edge 設備提供三種部署類型：路由模式、橋接模式，以及軟體切換（一種特殊的「橋接模式」組態設定）。這些組態設定可控制 Cloud Edge 設備路由網路封包以及介面執行轉送決定的方式。

所有 Cloud Edge 設備型號的預設部署模式都是「橋接模式」。

Cloud Edge 設備背面的開關可控制部署模式。若要變更部署模式，請將開關移至想要的模式。變更部署模式後，必須手動重新啟動設備。

注意

如果要部署「軟體切換」組態設定，請將部署開關設定為「橋接」。這是因為「軟體切換」組態設定是從「橋接模式」變化而來的。

圖 7-6. 部署模式切換

注意

本手冊中顯示的圖片可能與您的 Cloud Edge 設備稍微有些不同。

注意

Cloud Edge 300 的背面沒有部署模式開關。若要變更部署模式，您必須使用內部部署主控台。如果要部署「軟體切換」組態設定，請選擇「橋接模式」。

預先部署檢查清單

筆記型電腦需求

表 7-2. 筆記型電腦需求

需求	詳細資料

具有乙太網路通訊埠的筆記型電腦	已安裝下列軟體的電腦：
	• Adobe™ Flash™ 10 或更新版本
	• 支援的 Web 瀏覽器
	  • Firefox™ 70 或更新版本
	  • Google™ Chrome 78 或更新版本
	  • Microsoft Edge™ (Chromium) 85 或更新版本

部署需求

表 7-3. 橋接模式需求

需求	詳細資料
乙太網路纜線（3 條）	連線至 MGMT 通訊埠（管理）及 WAN 和 LAN1 資料通訊埠。
IP 位址（1 個位址）	• 從您的網際網路服務提供者 (ISP) 取得用於連線到 WAN 的相關資訊：DHCP 或靜態。您將使用此資訊來設定採用硬體切換晶片組之設備的橋接器介面 (br0) 或切換介面 (sw0)。
DNS 設定	• 您的網路 DNS 伺服器 IP 位址。

表 7-4. 路由模式需求

需求	詳細資料
乙太網路纜線（3 條）	連線至 MGMT 通訊埠（管理）及 WAN 和 LAN1 資料通訊埠。 注意 在此組態設定中，LAN1 通訊埠用於連線到內部區域網路。 對於採用硬體切換晶片組的設備：您可將 LAN1 連線到內部端點。
IP 位址（2 個位址）	• 從您的網際網路服務提供者 (ISP) 取得用於連線到 WAN 的相關資訊：DHCP、靜態或 PPPoE。 • 取得內部 LAN1 連線的 IP 位址資訊（靜態） • 對於具有無線功能的設備：如果您在初始部署期間啟動了主要無線網路，則您需要第三個 IP 位址供無線網路介面使用。
DNS 設定	• 使用由 ISP 的 DHCP 指派的自動 DNS 設定，或取得您的網路 DNS 伺服器 IP 位址。

表 7-5. 軟體切換需求

需求	詳細資料
乙太網路纜線（4-5 條）	連線至 MGMT 通訊埠（管理）、WAN、LAN1、LAN2 和 LAN3（選擇性）。 • WAN 是連線至外部網路（直接或透過上游交換器）的上行。 • LAN1、LAN2 和 LAN3（選擇性）會連線至內部區域網路上的端點。 注意 「軟體切換」組態設定需要三個連線的介面。您必須連線 WAN 和 LAN1 以及至少一個其他 LAN 介面。

需求	詳細資料
IP 位址（1 個位址）	• 從您的網際網路服務提供者 (ISP) 取得用於連線到 WAN 的相關資訊：DHCP 或靜態。您將使用此資訊來將 橋接器介面 (br0)設定為 L3 介面。 注意 「軟體切換」組態設定中使用的其他介面會設定為 L2 介面，而您無法指派 IP 位址給這些介面。
DNS 設定	• 您的網路 DNS 伺服器 IP 位址。

注意

橋接模式和路由模式：若要將更多 LAN 通訊埠連線到其他內部網路或端點，可能需要額外的纜線和 IP 位址。

路由模式：可以將 LAN1 通訊埠設定為次要的備用 WAN 連線。在此情況下，您可將剩餘的 LAN 通訊埠設定為內部網路。如需詳細資訊，請參閱管理路由 第 7-79 頁。

安裝和初始組態設定

Trend Micro™ Cloud Edge 是新一代的 MSP（管理服務提供者）安全解決方案，結合了內部部署與雲端安全功能。在內部部署安裝 Cloud Edge 設備並進行初始組態設定，MSP 就可透過雲端來遠端管理您的網路。

步驟

1. 設定硬體。

   設定硬體 第 7-19 頁

2. 從 MGMT 通訊埠登入內部部署主控台。

   透過 MGMT 通訊埠登入內部部署主控台 第 7-21 頁

3. 執行初始組態設定。

執行初始組態設定 第 7-21 頁

4. 註冊設備（若尚未註冊）。

   註冊設備 第 7-38 頁

5. 執行其他組態設定，以符合業務需求。

   執行其他組態設定 第 7-40 頁

設定硬體

您必須先設定硬體，才能將 Cloud Edge 設備連線到 Cloud Edge 雲端主控台並向其註冊。

注意

在獲得指示之前，請勿開啟 Cloud Edge 設備的電源。

步驟

1. 切換背面的開關來選取部署模式。

   依預設，Cloud Edge 設備設定為「橋接模式」。

注意

本手冊中顯示的圖片可能與您的設備稍微有些不同。

注意

Cloud Edge 300 的背面沒有部署模式開關。若要變更部署模式，您必須使用內部部署主控台。預設為「橋接模式」。

2. 將設備接上電源。
3. 將設備連線至網路。
   a. 將設備的 WAN 通訊埠連線至廣域網路（即 Internet）。
   b. 將設備的 LAN1 通訊埠連線至內部區域網路，例如您的某一段網路。

      部署「軟體切換」組態設定或以「橋接模式」部署採用硬體切換晶片組的 Cloud Edge 設備時，請將 LAN1 連線至適當的端點。
4. 根據部署組態設定執行適當的處理行動。
   - 橋接模式：選擇性地將設備的剩餘 LAN 通訊埠連線至其他內部網路。
   - 橋接模式（採用切換晶片組）：選擇性地將設備的 LAN2-LAN7 通訊埠連線至內部網路上的端點。

     當採用硬體切換晶片組的設備處於「橋接模式」時，可在發生某些事件（例如升級、重新啟動、關閉電源和系統嚴重錯誤）期間提供獨特的旁路功能。旁路功能可用與否取決於使用的通訊埠。若要瞭解如何指派端點給每個通訊埠，請參閱採用硬體切換晶片組之設備上的旁路通訊埠 第 7-13 頁。
   - 軟體切換：將設備的 LAN2 通訊埠和 LAN3（選擇性）連線至其他端點。

     「軟體切換」組態設定需要至少三個連線的通訊埠。WAN 與 LAN1 為必要項目。連線剩餘的 LAN2 和 LAN3 通訊埠（其中一個或全部兩個皆可）。
   - 路由模式：選擇性地將設備的剩餘 LAN 通訊埠連線至其他內部網路。
5. 開啟設備的電源。

   如果 WAN 介面使用 DHCP 且設備已預先註冊，則該設備會自動連線至 Cloud Edge 雲端主控台。

接下來需執行的動作

如果 WAN 介面使用 PPPoE 或靜態 IP 位址，您必須登入 Cloud Edge 設備的內部部署主控台並設定 WAN 介面，才能讓設備連線到 Cloud Edge 雲端主控台。

透過 MGMT 通訊埠登入內部部署主控台

步驟

1. 使用乙太網路線，將電腦連接至 Cloud Edge 設備的 MGMT 通訊埠。
2. 設定電腦，以自動在用以連接 MGMT 通訊埠的乙太網路介面取得 IP 位址。
3. 開啟支援的 Web 瀏覽器。
4. 移至下列 URL：

   `https://192.168.252.1:8443`
5. 指定登入認證。

   預設管理員帳號認證：

   使用者名稱：`admin`

   密碼：`adminCloudEdge`
6. 按 ENTER 鍵或按一下「登入」。

   Cloud Edge 內部部署主控台的「快速設定」頁面隨即出現。

執行初始組態設定

第一次登入 Cloud Edge 內部部署主控台後，將自動開啟「快速設定」畫面。

趨勢科技建議您使用「快速設定」畫面來設定 WAN 上行設定及指定系統設定。

注意

僅當 Cloud Edge 設備未註冊或離線時，才會自動顯示「快速設定」畫面。若要在裝置上線時檢視「快速設定」畫面，請按一下畫面右上方的「快速設定」連結。

根據選擇的部署模式，執行下列其中一項初始組態設定。

- 橋接模式的初始組態設定 第 7-22 頁
- 橋接模式（採用切換晶片組）的初始組態設定 第 7-25 頁
- 軟體切換的初始組態設定 第 7-27 頁
- 路由模式的初始組態設定 第 7-30 頁
- 路由模式（無線）的初始組態設定 第 7-33 頁

您可以從「快速設定」畫面執行測試，以確認部署組態設定：

- 測試以確認部署組態設定 第 7-37 頁

相關資訊

→ 部署模式總覽
→ 部署模式切換

橋接模式的初始組態設定

請使用「「快速設定」畫面」來設定 Cloud Edge 設備的基本「橋接模式」部署設定。設定基本部署設定後，您可以使用內部部署主控台來設定其他設定。

步驟

1. 登入 Cloud Edge 內部部署主控台。
2. 在「上行組態設定」區段中，指定下列詳細資料來設定 橋接器介面 (br0) 的網路資訊：

選項	說明
部署模式	已設定為「橋接模式」的唯讀欄位。 部署模式的設定方式是將設備背面的部署模式開關撥動到「橋接」。請參閱部署模式切換 第 7-15 頁。 注意 針對 Cloud Edge 300 設備，您可以使用這個選項來將部署模式變更為「橋接模式」。
類型	選取「橋接」。
「介面 1」與「介面 2」	只有在「橋接模式」下才會顯示這些欄位，且因為所有介面都是第 2 層介面，所以無法設定這些欄位。您無法指派 IP 位址給第 2 層介面。
模式	使用下列其中一項將 IP 位址指派給 橋接器介面 (br0)： • DHCP • 靜態：指定「IPv4 位址」、「IPv4 網路遮罩」與「IPv4 預設設備」。 注意 Cloud Edge 設備必須能夠使用指派的 IP 位址存取 Internet 資源。
主要 DNS	指定 DNS 伺服器的 IP 位址。如果您在「模式」欄位中選取「靜態」，則此為必要設定。
次要 DNS 第三級 DNS	選擇性地指定次要與第三級 DNS 伺服器的 IP 位址。

3. 在「系統設定」區段中，為 Cloud Edge 設備設定主機名稱以及時間與位置設定。

選項	說明
主機名稱	指定主機名稱。

選項	說明
啟動 NTP 伺服器	如果您想與 NTP 伺服器進行同步處理，請選取此選項，然後在「NTP 伺服器」欄位中新增 NTP 伺服器 IP 位址。
手動設定時間	如果要手動設定時間，請選取此選項，然後在「本機時間」欄位以下列格式指定目前時間：`yyyy-mm-dd hh:mm:ss`。例如，`2015-01-16 13:03:28`。
「位置」和「城市」	選取離 Cloud Edge 設備最近的位置與城市，來設定適當的時區。 如果「位置」/「城市」不是「亞洲」/「東京」，則時區資訊將會從 Cloud Edge 雲端主控台同步到設備向其註冊之公司的時區。

4. 按一下「開始組態設定測試」來驗證網路上行組態設定。

   如需詳細資訊，請參閱測試以確認部署組態設定 第 7-37 頁。

   注意

   如果裝置未在初始組態設定之前註冊，則註冊測試和相依性服務檢查將不會成功。這是正常情況。在註冊之後，您可以返回「快速設定」畫面並重新執行組態設定測試，以確認註冊狀態並驗證相依性服務測試是否成功。

5. （選用）如果測試耗時過久，您可以按一下「停止組態設定測試」，即可在測試完成前將其停止。

   建議您完成此測試，以確保所有組態設定和服務皆正常運作。

6. 按一下「儲存並註冊」。

   注意

   Cloud Edge 設備成功向 Cloud Edge 雲端主控台完成註冊後，按鈕文字會變更為「儲存設定」。

橋接模式（採用切換晶片組）的初始組態設定

請使用「「快速設定」畫面」來設定採用硬體切換晶片組之 Cloud Edge 設備的基本「橋接模式」部署設定。設定基本部署設定後，您可以使用內部部署主控台來設定包括硬體切換設定在內的其他設定。

注意

若要設定特定 切換介面 (sw0) 設定，請務必使用 Cloud Edge 雲端主控台。

步驟

1. 登入 Cloud Edge 內部部署主控台。
2. 在「上行組態設定」區段中，指定下列詳細資料來設定 切換介面 (sw0) 的網路資訊：

選項	說明
部署模式	已設定為「橋接模式」的唯讀欄位。 部署模式的設定方式是將設備背面的部署模式開關撥動到「橋接」。請參閱部署模式切換 第 7-15 頁。
內部網路安全模式	已設定為「高安全性」的唯讀欄位。 這是初始預設設定。完成初始設定後，您可以使用 Cloud Edge 雲端主控台變更內部網路安全模式請參閱每一種內部網路安全模式提供的安全防護 第 6-58 頁
介面	已設定為「WAN、LAN1–LAN8」的唯讀欄位。 WAN、LAN1-LAN8 L2 介面會自動包含在硬體切換組態設定中，您無法將其移除或關閉，也不能變更為 L3 介面。

選項	說明
模式	使用下列其中一項將 IP 位址指派給 切換介面 (sw0)： • DHCP • 靜態：指定「IPv4 位址」、「IPv4 網路遮罩」與「IPv4 預設設備」。 注意 Cloud Edge 設備必須能夠使用指派的 IP 位址存取 Internet 資源。
主要 DNS	指定 DNS 伺服器的 IP 位址。如果您在「模式」欄位中選取「靜態」，則此為必要設定。
次要 DNS 第三級 DNS	選擇性地指定次要與第三級 DNS 伺服器的 IP 位址。

3. 在「系統設定」區段中，為 Cloud Edge 設備設定主機名稱以及時間與位置設定。

選項	說明
主機名稱	指定主機名稱。
啟動 NTP 伺服器	如果您想與 NTP 伺服器進行同步處理，請選取此選項，然後在「NTP 伺服器」欄位中新增 NTP 伺服器 IP 位址。
手動設定時間	如果要手動設定時間，請選取此選項，然後在「本機時間」欄位以下列格式指定目前時間：`yyyy-mm-dd hh:mm:ss`。例如，`2015-01-16 13:03:28`。
「位置」和「城市」	選取離 Cloud Edge 設備最近的位置與城市，來設定適當的時區。 如果「位置」/「城市」不是「亞洲」/「東京」，則時區資訊將會從 Cloud Edge 雲端主控台同步到設備向其註冊之公司的時區。

4. 按一下「開始組態設定測試」來驗證網路上行組態設定。

如需詳細資訊，請參閱測試以確認部署組態設定 第 7-37 頁。

注意

如果裝置未在初始組態設定之前註冊，則註冊測試和相依性服務檢查將不會成功。這是正常情況。在註冊之後，您可以返回「快速設定」畫面並重新執行組態設定測試，以確認註冊狀態並驗證相依性服務測試是否成功。

5. （選用）如果測試耗時過久，您可以按一下「停止組態設定測試」，即可在測試完成前將其停止。

   建議您完成此測試，以確保所有組態設定和服務皆正常運作。

6. 按一下「儲存並註冊」。

注意

Cloud Edge 設備成功向 Cloud Edge 雲端主控台完成註冊後，按鈕文字會變更為「儲存設定」。

軟體切換的初始組態設定

若要為具有「軟體切換」組態設定的 Cloud Edge 設備執行初始基本設定，必須先使用內部部署主控台設定一些特定設定，然後使用「「快速設定」畫面」完成初始組態設定。設定基本設定後，您可以使用內部部署主控台來設定其他設定。

重要

部署模式開關必須設定為「橋接」，才能設定「軟體切換」組態設定。請參閱部署模式切換 第 7-15 頁。

步驟

1. 登入 Cloud Edge 內部部署主控台。

   「快速設定」畫面隨即開啟。由於必須使用內部部署主控台來設定特定的初始「軟體切換」設定，因此現在必須開啟內部部署主控台。

2. 按一下畫面右上方的「Cloud Edge 內部部署主控台」連結。

   「Cloud Edge 內部部署主控台」畫面隨即開啟。

3. 移至「網路 > 橋接」。

4. 在「名稱」欄中，按一下「br0」。

   「新增/編輯橋接」畫面隨即開啟。

5. 指定下列項目：

選項	說明
類型	將類型從「橋接」變更為「軟體切換」。 選取「軟體切換」後，會出現不同的可用選項。「介面 1」和「介面 2」欄位會取代為「切換介面」欄位。
切換介面	選取要包含在「軟體切換」組態設定中的介面。 • 「切換介面」欄位隨即出現，並預先選取了「WAN」和「LAN1」。您無法取消選取它們。 由於組態設定必須至少有三個介面，因此您必須再選取至少一個介面。選取「LAN2」或「LAN3」，或兩者皆選。 • 這些是 L2 介面。您無法指派 IP 位址給這些介面。
模式	使用下列其中一項將 IP 位址指派給 橋接器介面 (br0)： • DHCP • 靜態：指定「IPv4 位址」、「IPv4 網路遮罩」與「IPv4 預設設備」。 注意 Cloud Edge 設備必須能夠使用指派的 IP 位址存取 Internet 資源。

6. 按一下「套用」。

7. 按一下右上角的「快速設定」。

   「快速設定」畫面隨即開啟。

8. 在「上行組態設定」區段中，指定下列項目來設定 橋接器介面 (br0) 的 DNS：

選項	說明
主要 DNS	指定 DNS 伺服器的 IPv4 位址。如果您在「模式」欄位中選取了「靜態」，則此為必要設定。
次要 DNS 第三級 DNS	選擇性地指定次要與第三級 DNS 伺服器的 IPv4 位址。

注意

在「「快速設定」畫面」中，「部署模式」、「類型」和「介面」欄位均為唯讀。

9. 在「系統設定」區段中，為 Cloud Edge 設備設定主機名稱以及時間與位置設定。

選項	說明
主機名稱	指定主機名稱。
啟動 NTP 伺服器	如果您想與 NTP 伺服器進行同步處理，請選取此選項，然後在「NTP 伺服器」欄位中新增 NTP 伺服器 IP 位址。
手動設定時間	如果要手動設定時間，請選取此選項，然後在「本機時間」欄位以下列格式指定目前時間：`yyyy-mm-dd hh:mm:ss`。例如，`2015-01-16 13:03:28`。
「位置」和「城市」	如有需要，請選取離 Cloud Edge 設備最近的位置與城市，來設定適當的時區。 如果「位置」/「城市」不是「亞洲」/「東京」，則時區資訊將會從 Cloud Edge 雲端主控台同步到設備向其註冊之公司的時區。

10. 按一下「開始組態設定測試」來驗證網路上行組態設定。

如需詳細資訊，請參閱測試以確認部署組態設定 第 7-37 頁。

注意

如果裝置未在初始組態設定之前註冊，則註冊測試和相依性服務檢查將不會成功。這是正常情況。在註冊之後，您可以返回「快速設定」畫面並重新執行組態設定測試，以確認註冊狀態並驗證相依性服務測試是否成功。

11. （選用）如果測試耗時過久，您可以按一下「停止組態設定測試」，即可在測試完成前將其停止。

    建議您完成此測試，以確保所有組態設定和服務皆正常運作。

12. 按一下「儲存並註冊」。

注意

Cloud Edge 設備成功向 Cloud Edge 雲端主控台完成註冊後，按鈕文字會變更為「儲存設定」。

路由模式的初始組態設定

請使用「「快速設定」畫面」，來設定 Cloud Edge 設備的基本「路由模式」部署設定。設定基本部署設定後，您可以使用內部部署主控台來設定其他設定。

步驟

1. 登入 Cloud Edge 內部部署主控台。
2. 在「上行組態設定」區段中，指定下列詳細資料來設定連線 Internet 的 WAN 介面的網路資訊：

選項	說明
部署模式	已設定為「路由模式」的唯讀欄位。 部署模式的設定方式是將設備背面的部署模式開關撥動到「路由」。請參閱部署模式切換 第 7-15 頁。 注意 針對 Cloud Edge 300 設備，您可以使用這個選項來將部署模式變更為「路由模式」。
WAN 介面	這是已設定為 WAN 的唯讀欄位，且只有在 Cloud Edge 設備部署為「路由模式」時才能使用。無法在「「快速設定」畫面」中修改此欄位。
模式	使用下列其中一項將 IP 位址指派給 WAN 介面： • DHCP • PPPoE：指定使用者名稱與密碼。只有在「路由模式」下才可使用此選項。 • 靜態：指定「IPv4 位址」、「IPv4 網路遮罩」與「IPv4 預設設備」。 注意 Cloud Edge 設備必須能夠使用指派的 IP 位址存取 Internet 資源。
主要 DNS	指定 DNS 伺服器的 IP 位址。如果您在「模式」欄位中選取「靜態」，則此為必要設定。
次要 DNS 第三級 DNS	選擇性地指定次要與第三級 DNS 伺服器的 IP 位址。

3. 在「系統設定」區段中，為 Cloud Edge 設備設定主機名稱以及時間與位置設定。

選項	說明
主機名稱	指定主機名稱。

選項	說明
啟動 NTP 伺服器	如果您想與 NTP 伺服器進行同步處理，請選取此選項，然後在「NTP 伺服器」欄位中新增 NTP 伺服器 IP 位址。
手動設定時間	如果要手動設定時間，請選取此選項，然後在「本機時間」欄位以下列格式指定目前時間：`yyyy-mm-dd hh:mm:ss`。例如，`2015-01-16 13:03:28`。
「位置」和「城市」	選取離 Cloud Edge 設備最近的位置與城市，來設定適當的時區。 如果「位置」/「城市」不是「亞洲」/「東京」，則時區資訊將會從 Cloud Edge 雲端主控台同步到設備向其註冊之公司的時區。

4. 按一下「開始組態設定測試」來驗證網路上行組態設定。

   如需詳細資訊，請參閱測試以確認部署組態設定 第 7-37 頁。

   注意

   如果裝置未在初始組態設定之前註冊，則註冊測試和相依性服務檢查將不會成功。這是正常情況。在註冊之後，您可以返回「快速設定」畫面並重新執行組態設定測試，以確認註冊狀態並驗證相依性服務測試是否成功。

5. （選用）如果測試耗時過久，您可以按一下「停止組態設定測試」，即可在測試完成前將其停止。

   建議您完成此測試，以確保所有組態設定和服務皆正常運作。

6. 按一下「儲存並註冊」。

   注意

   Cloud Edge 設備成功向 Cloud Edge 雲端主控台完成註冊後，按鈕文字會變更為「儲存設定」。

7. 使用內部部署主控台設定 LAN1 介面。

   a. 按一下「「快速設定」畫面」右上角的「Cloud Edge 內部部署主控台」連結。

b. 移至「網路 > 介面」。

c. 按一下 LAN1 介面來編輯設定。

d. 從「類型」下拉式清單中選取「L3」，然後設定 IP 位址設定。

- DHCP：需要時指定 MTU/MSS。
- 靜態：手動輸入 IPv4（「IPv4 位址」、「IPv4 網路遮罩」）的位址資訊，並選擇性地輸入設備位址。如有需要，請指定「MTU/MSS」。

e. 按一下「套用」。

8. 可選擇性地使用 Cloud Edge 雲端主控台設定其他 LAN 介面。

路由模式：編輯網路介面 第 6-48 頁

路由模式（無線）的初始組態設定

請使用「「快速設定」畫面」，來設定具有無線網路存取之 Cloud Edge 設備的基本「路由模式」部署設定。設定基本部署設定後，您可以使用內部部署主控台來設定包括無線網路設定在內的其他設定。

注意

若要設定無線網路存取控制設定，請務必使用 Cloud Edge 雲端主控台。

步驟

1. 登入 Cloud Edge 內部部署主控台。
2. 在「上行組態設定」區段中，指定下列詳細資料來設定連線 Internet 的 WAN 介面的網路資訊：

選項	說明
部署模式	已設定為「路由模式」的唯讀欄位。 部署模式的設定方式是將設備背面的部署模式開關撥動到「路由」。請參閱部署模式切換 第 7-15 頁。
WAN 介面	這是已設定為 WAN 的唯讀欄位，且只有在 Cloud Edge 設備部署為「路由模式」時才能使用。無法在「快速設定」中修改此欄位。
模式	使用下列其中一項將 IP 位址指派給 WAN 介面： • DHCP • PPPoE：指定使用者名稱與密碼。只有在「路由模式」下才可使用此選項。 • 靜態：指定「IPv4 位址」、「IPv4 網路遮罩」與「IPv4 預設設備」。 注意 Cloud Edge 設備必須能夠使用指派的 IP 位址存取 Internet 資源。
主要 DNS	指定 DNS 伺服器的 IP 位址。如果您在「模式」欄位中選取「靜態」，則此為必要設定。
次要 DNS 第三級 DNS	選擇性地指定次要與第三級 DNS 伺服器的 IP 位址。

3. 在「無線設定」區段中，指定下列詳細資料來設定 Cloud Edge 設備的無線網路存取：

選項	說明
啟動無線 AP	選取此選項可啟動無線網路存取。 此選項會啟動主要無線網路，但不會啟動客體無線網路。
頻率	選取「2.4 GHz」或「5 GHz」選項。

選項	說明
SSID	輸入要指派給無線網路的 SSID。 預設 SSID 是 `CloudEdge-XXYY` (2.4 GHz) 或 `CloudEdge-GUEST-XXYY` (5 GHz) XXYY 代表設備之產品序號的前四個數字。
安全設定	選取「開啟」或「WPA-PSK[TKIP]+WPA2-PSK[AES]」選項。 還有其他安全設定選項可供使用。完成初始設定後，您可以使用內部部署主控台來修改包括安全設定在內的無線網路組態設定。 趨勢科技建議您針對無線網路使用安全性選項，而不要使用「開啟」選項。

4. 在「系統設定」區段中，為 Cloud Edge 設備設定主機名稱以及時間與位置設定。

選項	說明
主機名稱	指定主機名稱。
啟動 NTP 伺服器	如果您想與 NTP 伺服器進行同步處理，請選取此選項，然後在「NTP 伺服器」欄位中新增 NTP 伺服器 IP 位址。
手動設定時間	如果要手動設定時間，請選取此選項，然後在「本機時間」欄位以下列格式指定目前時間：`yyyy-mm-dd hh:mm:ss`。例如，`2015-01-16 13:03:28`。
「位置」和「城市」	選取離 Cloud Edge 設備最近的位置與城市，來設定適當的時區。 如果「位置」/「城市」不是「亞洲」/「東京」，則時區資訊將會從 Cloud Edge 雲端主控台同步到設備向其註冊之公司的時區。

5. 按一下「開始組態設定測試」來驗證網路上行組態設定。

   如需詳細資訊，請參閱測試以確認部署組態設定 第 7-37 頁。

> **注意**
>
> 如果裝置未在初始組態設定之前註冊，則註冊測試和相依性服務檢查將不會成功。這是正常情況。在註冊之後，您可以返回「快速設定」畫面並重新執行組態設定測試，以確認註冊狀態並驗證相依性服務測試是否成功。

6. （選用）如果測試耗時過久，您可以按一下「停止組態設定測試」，即可在測試完成前將其停止。

   建議您完成此測試，以確保所有組態設定和服務皆正常運作。

7. 按一下「儲存並註冊」。

> **注意**
>
> Cloud Edge 設備成功向 Cloud Edge 雲端主控台完成註冊後，按鈕文字會變更為「儲存設定」。

8. 使用內部部署主控台設定 LAN1 介面

   a. 按一下「「快速設定」畫面」右上角的「Cloud Edge 內部部署主控台」連結。

   b. 移至「網路 > 介面」。

   c. 按一下 LAN1 介面來編輯設定。

   d. 從「類型」下拉式清單中選取「L3」，然後進行 IP 位址設定。

      - DHCP：視需要指定「MTU/MSS」。
      - 靜態：手動輸入 IPv4（「IPv4 位址」、「IPv4 網路遮罩」）的位址資訊，並選擇性地輸入設備位址。視需要指定「MTU/MSS」。

   e. 按一下「套用」。

9. 可選擇性地使用 Cloud Edge 雲端主控台設定其他 LAN 介面。

   a. 登入 Cloud Edge 雲端主控台。

   登入雲端主控台 第 6-2 頁

b. 視需要設定介面。

路由模式：編輯網路介面 第 6-48 頁

路由模式：編輯無線網路介面 第 6-49 頁

測試以確認部署組態設定

完成初始部署組態設定後，Cloud Edge 可以執行一系列測試，以確認設備可以連線到 Internet、確認設備是已註冊狀態，以及確認各種必要服務皆可使用。如果某個測試失敗，將不會執行後續測試。您必須修正任何導致測試失敗的問題，然後重新執行測試。

下列測試將會依序執行：

順序	測試	說明	若發生以下情況，則測試失敗...
1	WAN 檢查	檢查 WAN 和 LAN1 介面狀態（上線或離線）。	兩個介面皆離線。
2	DNS 檢查	檢查 DNS 組態設定。 檢查 DNS 要求是否成功。	未設定 DNS。 一個 DNS 檢查失敗。
3	WAN 路由器檢查	檢查路由器組態設定。 檢查是否可以成功連線到外部網站。	沒有到 WAN 的路由。 Cloud Edge 無法連線到外部網站。
4	註冊狀態檢查	檢查註冊狀態。	設備未註冊。

順序	測試	說明	若發生以下情況，則測試失敗...
5	Cloud Edge 雲端服務檢查，包括下列項目： • 主動式更新 • 雲端掃瞄 • 雲端郵件掃瞄 • 電子郵件信譽評等 • 記錄檔上傳 • 網頁信譽評等 • 雲端截毒掃瞄 • Machine Learning	已檢查所有服務。	每個服務會個別檢查，且每個服務會個別標示為成功或失敗。 如果所有服務檢查全都失敗，整體相依性檢查便會失敗。

註冊設備

如果您尚未使用 Cloud Edge 雲端主控台註冊 Cloud Edge 設備，必須先註冊才能部署安全策略。

步驟

1. 登入 Cloud Edge 雲端主控台。
2. 在 Cloud Edge 雲端主控台中，移至「設備」。
3. 按一下「註冊新設備」。
4. 指定設備設定。

選項	說明
顯示名稱	指定新設備顯示在 Cloud Edge 雲端主控台中的名稱。
型號	指定 Cloud Edge 設備硬體的型號。

選項	說明
產品序號	指定 Cloud Edge 設備的產品序號。產品序號位於設備本身或設備包裝上。產品序號由 12 位英數字元組成，並由連字號分隔（範例：4C80-9315-3A0B）。

5. 按一下「儲存」。

   註冊作業可能需要數分鐘才能完成。

   在註冊之後，Cloud Edge 雲端主控台會將策略部署到設備。在註冊完成後，您可以透過 Cloud Edge 雲端主控台資訊中心 Widget、記錄檔分析，以及根據 Cloud Edge 設備傳送之即時流量產生的報告，來檢視記錄檔統計資料。

6. 確認是否成功註冊。

   驗證註冊 第 6-14 頁。

確認註冊

趨勢科技建議在註冊每個設備後都加以確認。下列程序說明如何使用 Cloud Edge 內部部署主控台檢查設備已正確向 Cloud Edge 雲端主控台註冊。

步驟

1. 登入 Cloud Edge 內部部署主控台。
2. 執行下列其中一個動作：
   - 瀏覽至「資訊中心 > 系統資訊 (Widget)」，然後查看「雲端管理狀態」下的資訊。
   - 瀏覽至「管理 > 裝置管理 > 雲端管理（標籤）」，然後確認所顯示的資訊。
3. 依照確認連線 第 7-40 頁中的程序確認連線。

確認連線

確認連線並測試您的部署，以確定 Cloud Edge 設備已向 Cloud Edge 雲端主控台註冊，並且可以根據策略來正確路由傳送流量。

步驟

1. 檢閱下表來瞭解 LED 燈狀態。

LED 燈	狀態
不亮燈	Cloud Edge 設備無法與 Internet 通訊。
持續亮綠燈	Cloud Edge 設備已向 Cloud Edge 雲端主控台註冊且正在與之通訊。
閃綠燈	Cloud Edge 設備未向 Cloud Edge 雲端主控台註冊或無法與之通訊。

2. 如果 Cloud Edge 註冊成功，請嘗試從內部端點存取 Internet。

   當您可以存取 Internet 時，即表示 Cloud Edge 成功。

   注意

   如果您無法確認部署，請聯絡趨勢科技。

執行其他組態設定

您可以執行其他組態設定步驟來滿足業務需求。根據下列每個步驟中的指示使用 Cloud Edge 內部部署主控台或 Cloud Edge 雲端主控台。

步驟

1. 對於具有無線網路功能的 Cloud Edge 設備，設定該設備的無線設定。
   - 無線網路組態設定（包含設定客體無線網路）：（內部部署主控台）：

管理無線網路 第 7-60 頁

- 無線存取控制：（Cloud Edge 雲端主控台）：

  設定無線網路的存取控制 第 6-102 頁

- 無線介面組態設定（Cloud Edge 雲端主控台）：

  路由模式：編輯網路介面 第 6-48 頁

2. 針對已連線網路上的用戶端，將介面設定為用做 DHCP 伺服器。
   - WAN 或 LAN1 介面（內部部署主控台）：

     修改 DHCP 服務設定 第 7-87 頁

   - 其他 LAN 介面或 MGMT 介面（Cloud Edge 雲端主控台）：

     編輯 DHCP 設定 第 6-67 頁

     對於具有無線網路存取功能的 Cloud Edge 設備，您可以設定主要無線網路和客體無線網路的 DHCP。
3. 新增以策略為基礎的路由（內部部署主控台）。
   - 新增以策略為基礎的路由 第 7-82 頁
4. 新增靜態路由（Cloud Edge 雲端主控台）。
   - 新增靜態路由 第 6-75 頁
5. 設定 Cloud Edge 設備介面的 NAT（Cloud Edge 雲端主控台）。
   - 新增目標 NAT 規則 第 6-79 頁
   - 新增來源 NAT 規則 第 6-81 頁
   - 變更 NAT 規則優先順序 第 6-81 頁
6. 設定內部部署主控台逾時設定（內部部署主控台）。
   - 設定內部部署主控台逾時 第 7-91 頁
7. 管理 Cloud Edge 設備的管理存取權（Cloud Edge 雲端主控台）。

- 啟動管理存取權 第 7-93 頁

8. 為 WAN 和 LAN1 介面設定監控主機（內部部署主控台）。
   - 在介面上設定監控主機 第 7-58 頁

管理

管理網路設定

您可以管理用以處理及識別網路流量的網路設定。

管理網路介面

向 Cloud Edge 雲端主控台註冊 Cloud Edge 設備之前，您可以從 Cloud Edge 內部部署主控台檢視並修改所有自動偵測到的網路介面。

註冊設備後，您可以使用 Cloud Edge 內部部署主控台檢視或修改下列介面的組態設定：

注意

註冊之後，必須使用 Cloud Edge 雲端主控台設定 MGMT 介面。

- 橋接模式：橋接器介面 (br0)
  - 使用「橋接模式」時，虛擬 橋接器介面 (br0) 是唯一可用的 L3 介面。
  - 設定此介面時，您可以使用靜態或 DHCP IPv4 定址。

    橋接器介面 (br0) 不支援 PPPoE。

- 橋接器介面 (br0) 不支援 VLAN。

> **注意**
>
> 您可以編輯實體介面的某些 L2 設定（例如 MTU）。請使用內部部署主控台來編輯 WAN 和所有 LAN L2 介面。

- 橋接模式（採用切換晶片組）：切換介面 (sw0)
  - 使用「橋接模式」時，虛擬 切換介面 (sw0) 是唯一可用的 L3 介面。
  - 設定此介面時，您可以使用靜態或 DHCP IPv4 定址。

    切換介面 (sw0) 不支援 PPPoE。
  - 切換介面 (sw0) 不支援 VLAN。
  - WAN 和 LAN1-LAN8 介面會自動新增到切換組態設定中。
    - 您無法從切換組態設定中移除上述任何一個介面，也無法將其變更為 L3 介面。
    - 您可以關閉 LAN2-LAN7 介面。
    - 您無法關閉 WAN、LAN1 或 LAN8 介面。
    - 您可以將端點連線到 LAN1-LAN7 介面。

      您不應將端點連線到 LAN8 介面，因為該介面用於旁路功能。

> **注意**
>
> 您可以編輯實體介面的某些 L2 設定，例如 MTU 和流量控制。請使用內部部署主控台來編輯 WAN 和 LAN1-LAN8 介面。

- 軟體切換：橋接器介面 (br0)
  - 部署「軟體切換」組態設定時，虛擬 橋接器介面 (br0) 是唯一可用的 L3 介面。
  - 設定此介面時，您可以使用靜態或 DHCP IPv4 定址。

    橋接器介面 (br0) 不支援 PPPoE。

- 您必須新增至少三個 L2 介面來用做軟體切換。

  您必須新增 WAN 和 LAN1。您可以在「軟體切換」組態設定中新增 LAN2 和 LAN3（其中一個或全部兩個皆可）。

  您可以在「軟體切換」組態設定中新增 L3 介面。Cloud Edge 會在 L3 介面新增到軟體切換後自動將其變更為 L2 介面。

  當設備最初以「路由模式」部署，但稍後變更為「橋接模式」並部署為「軟體切換」時，就會發生這種狀況。在此情況下，現有的 L3 介面必須先新增至切換組態設定中，然後才能轉換為 L2 介面。

注意

您可以編輯實體介面的某些 L2 設定（例如 MTU）。請使用內部部署主控台來編輯 WAN 和所有 LAN L2 介面。

- 路由模式：WAN 和 LAN1
  - 您可以在 WAN 或 LAN1 介面上設定靜態、DHCP 和 PPPoE IPv4 定址。

    注意

    如果 LAN1 介面是用做備用 WAN 連線，則有可能使用 PPPoE。

  - WAN 介面提供 Internet 連線。
  - LAN1 介面可設定做為第二個 WAN 介面以提供備用 Internet 連線，也可以設定做為 LAN 介面以連線至內部網路。

    如需有關雙 WAN 組態設定的詳細資訊，請參閱在多個 ISP/WAN 環境之間進行自動容錯移轉 第 7-82 頁。

注意

您可以使用內部部署主控台來編輯 WAN 與 LAN1。若要編輯其他介面，請務必使用 Cloud Edge 雲端主控台。

您可以使用內部部署主控台將 L3 VLAN 新增到 WAN 和 LAN1 介面；不過，執行 Cloud Edge 6.0 和更新版本的設備不支援 L2 VLAN。

支援的網路介面組態設定

Cloud Edge 設備支援下列網路 L3 介面組態設定：

- 靜態 IP 位址（靜態）
  - 路由模式：所有 L3 介面皆支援
  - 路由模式：無線網路介面支援
  - 橋接模式和軟體切換：橋接器介面 (br0) 支援
  - 橋接模式（採用切換晶片組）：切換介面 (sw0) 支援
  - 所有模式：MGMT 通訊埠支援
- 動態主機設定通訊協定 (DHCP)
  - 路由模式：WAN 或 LAN1 L3 介面支援
  - 橋接模式和軟體切換：橋接器介面 (br0) 支援
  - 橋接模式（採用切換晶片組）：切換介面 (sw0) 支援
  - 所有模式：MGMT 通訊埠不支援
- 乙太網路點對點通訊協定 (PPPoE)
  - 路由模式：WAN 和 LAN1 L3 介面支援
  - 橋接模式和軟體切換：橋接器介面 (br0) 不支援
  - 橋接模式（採用切換晶片組）：切換介面 (sw0) 不支援
  - 所有模式：MGMT 通訊埠不支援

有關變更為軟體切換部署的資訊

以下是您在將 Cloud Edge 設備變更為「軟體切換」部署時應瞭解的一些資訊。

- 可以將除了管理介面 (MGMT) 以外的所有介面新增至軟體切換。需要三個介面。WAN 與 LAN1 為必要項目。您可以新增 LAN2 或 LAN3 做為第三個介面。如有需要，您可以新增 LAN2 或 LAN3 到「軟體切換」。

- WAN 和 LAN1 介面的防故障存取：
  - 即使部署為「軟體切換」的設備是以多埠橋接器的型態運作，Cloud Edge 仍會使用 WAN 和 LAN1 介面提供防故障存取。
  - WAN 和 LAN1 介面用做旁路通訊埠，可支援透過 LAN1 通訊埠進行存取，即使設備處於離線狀態亦然。依賴 Internet 相關裝置應透過 LAN1 介面連線。
- 對於新增至「軟體切換」組態設定的任何介面：
  - 介面會自動啟動。
  - 任何 L3 介面都會自動變更為 L2。
  - 會關閉介面上的 DHCP 服務。
  - 會刪除任何相關的 SNAT 規則。
  - 您無法將屬於軟體切換一部分的 L2 介面變更為 L3 介面。
  - 您無法關閉屬於軟體切換一部分的 L2 介面。
- 在進行「軟體切換」設定時，適用下列規則：
  - 您只能變更已新增至軟體切換的 L2 介面的 MTU 和頻寬設定。

    您可以變更軟體切換 MTU（預設值為 1438）和通訊埠 MTU（預設值為 1504）。Cloud Edge 會阻止您將軟體切換 MTU 設定為大於通訊埠 MTU。
  - 您必須使用內部部署主控台來設定「軟體切換」部署。
- 以下情況適用於「軟體切換」部署的郵件掃瞄：
  - 在「橋接模式」下，Cloud Edge 只會對 WAN 介面與 LAN1 介面之間的流量執行郵件掃瞄，

    而不會對 LAN 介面之間的流量執行郵件掃瞄。
  - 採用「軟體切換」部署時，Cloud Edge 會對 WAN 介面與所有 LAN 介面之間的流量執行郵件掃瞄，

    並且會對 LAN 介面之間的流量執行郵件掃瞄。

- 在「軟體切換」部署與「路由模式」部署之間切換時，請謹記以下幾點：
  - 如果將組態設定從「軟體切換」變更為「路由模式」，則「軟體切換」組態設定將會遺失。
  - 如果將組態設定從「路由模式」變更為「軟體切換」，則 LAN2 和 LAN3 組態設定和相關的 NAT 規則都會遺失。

啟動或關閉介面

Cloud Edge 設備的特定介面可能會隨部署模式的不同而預設為啟動或關閉。在特定組態設定中，您可能無法關閉某些介面。

注意

不論在任何一種部署模式下，您皆無法關閉 MGMT 通訊埠。

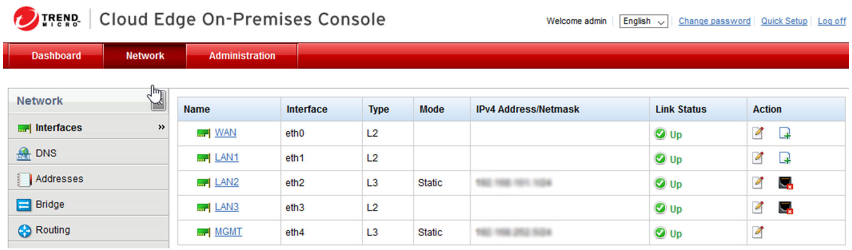


圖 7-7. 範例：處於路由模式的 Cloud Edge 70

請從 Cloud Edge 內部部署主控台啟動或關閉介面。

- 路由模式：LAN2 和 LAN3 介面預設會啟動。

  您可以隨時關閉或重新啟動這些介面。
- 橋接模式：LAN2 和 LAN3 介面預設會關閉。

  您可以隨時啟動或關閉這些介面。
- 軟體切換：將 LAN2 和 LAN3 新增為軟體切換介面時，會自動啟動它們。

  如果介面屬於「軟體切換」組態設定的一部分，則您無法關閉該介面。

注意

Cloud Edge 300 設備沒有 LAN3 介面。

採用硬體切換晶片組的 Cloud Edge 設備

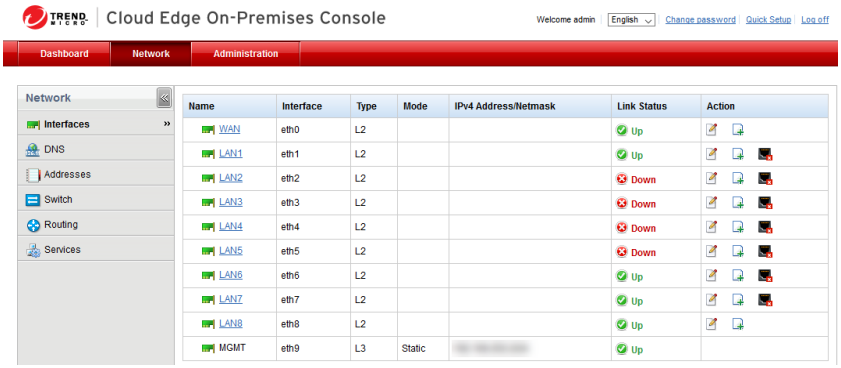


圖 7-8. 範例：處於橋接模式的 Cloud Edge 100 G2

依預設，所有通訊埠均為啟動狀態。您無法關閉 WAN、LAN8 或 MGMT 介面。

- 路由模式

  您可以關閉 LAN1-LAN7 介面。

- 橋接模式

  WAN 和 LAN1-LAN8 介面會自動選取做為硬體切換的通訊埠。您無法從硬體切換組態設定移除這些通訊埠；不過，您可以關閉 LAN1-LAN7 介面。

具有無線網路功能的 Cloud Edge 設備

您無法從「介面」頁面啟動或關閉無線網路介面。

當您啟動無線存取時，系統會自動啟動主要無線網路，而當您啟動客體無線網路時，系統會自動啟動客體無線網路。如果您關閉相應的無線網路，系統會自動關閉無線網路介面。

步驟

1. 從 Cloud Edge 內部部署主控台，移至「網路 > 介面」。
2. 執行下列其中一項作業：
   a. 針對您想要啟動的介面，按一下「啟動」圖示 ( )。
   b. 針對您想要關閉的介面，按一下「關閉」圖示 ( )。

為橋接模式/軟體切換編輯網路介面

您可以對處於「橋接模式」或「軟體切換」組態設定的 Cloud Edge 設備，設定實體 L2 介面的 MTU。請務必使用內部部署主控台來進行此程序。

注意

如需瞭解為「橋接模式」（採用切換晶片組）設定實體介面時要遵循的程序，請參閱編輯橋接模式（採用切換晶片組）的網路介面 第 7-50 頁。

如需瞭解為「路由模式」設定實體介面時要遵循的程序，請參閱編輯路由模式的網路介面 第 7-54 頁。

步驟

1. 移至「網路 > 介面」。
2. 按一下您要編輯的 L2 介面的名稱。

   「新增/編輯介面」畫面隨即開啟。
3. 對於「MTU」，輸入所需的 MTU。

   範圍為 576 到 1504。在實體介面上設定的 MTU，與在 橋接器介面 (br0) 上設定的 MTU 各自獨立。在 橋接器介面 (br0) 上設定的 MTU，不能低於在實體介面上設定的 MTU。
4. 按一下「套用」。

編輯橋接模式（採用切換晶片組）的網路介面

處於「橋接模式」時，您可以設定採用硬體切換晶片組之 Cloud Edge 設備的實體 L2 介面（WAN、LAN1-LAN8）。請務必使用內部部署主控台來進行此程序。您可以根據介面和內部網路安全模式設定諸如 MTU、風暴控制和流量控制等設定。

當採用硬體切換晶片組的設備處於「橋接模式」時，可在發生某些事件（例如升級、重新啟動、關閉電源和系統嚴重錯誤）期間提供獨特的旁路功能。旁路功能可用與否取決於使用的介面。若要瞭解如何指派端點給每個介面，請參閱採用硬體切換晶片組之設備上的旁路通訊埠 第 7-13 頁。

注意

如需瞭解為「橋接模式」或「軟體切換」設定實體 L2 介面時要遵循的程序，請參閱為橋接模式/軟體切換編輯網路介面 第 7-49 頁。

如需瞭解為「路由模式」設定實體 L3 介面時要遵循的程序，請參閱編輯路由模式的網路介面 第 7-54 頁。

步驟

1. 移至「網路 > 介面」。
2. 按一下「名稱」下的 WAN 介面，然後進行 MTU 設定。

選項	說明
類型	唯讀欄位。您無法變更「類型」，且無法從切換組態設定中移除 WAN 介面。
MTU	指定 576 到 1504 之間的值。您無法針對 WAN 介面設定 Jumbo 框架。 MTU 是 WAN 介面上唯一的可編輯欄位。

3. 在「名稱」下，按一下您要編輯的 L2 介面 (LAN1-LAN8) 的名稱，然後設定可編輯的介面設定。

   高安全性模式和標準模式

選項	說明
類型	唯讀欄位。您無法變更「類型」，且無法從切換組態設定中移除 WAN 介面。
MTU	範圍：576 到 9216；預設值為 1504 在實體介面上設定的 MTU，與在 切換介面 (sw0) 上設定的 MTU 各自獨立。在 切換介面 (sw0) 上設定的 MTU，不能低於在實體介面上設定的 MTU。
風暴控制閾值	以整數指定閾值 (Mbps)。
風暴控制模式	選取要套用風暴控制的封包類型： • 多點傳送 • 廣播

高速模式

注意

您無法在「高速」模式下修改 MTU。MTU 預設接受 Jumbo 框架。

選項	說明
類型	唯讀欄位。您無法變更「類型」，且無法從切換組態設定中移除 WAN 介面。
流量控制	選取「啟動」以啟動流量控制。
風暴控制閾值	以整數指定閾值 (Mbps)。
風暴控制模式	選取要套用風暴控制的封包類型： • 未知單點傳送 • 多點傳送 • 廣播

4. 按一下「套用」。

介面設定的清單：橋接模式（採用切換晶片組）

在為採用硬體切換晶片組的 Cloud Edge 設備設定實體介面（WAN、LAN1-LAN8）之前，請先檢閱每一種內部網路安全模式（高安全性、標準和高速）的可用設定。您必須使用內部部署主控台來設定 WAN、LAN1-LAN8 介面。

如需有關每一種模式提供之網路安全防護的詳細資訊，請參閱每一種內部網路安全模式提供的安全防護 第 6-58 頁。

高安全性模式

設定	說明
類型	設定為「L2」。 「橋接模式」下的唯讀欄位。您無法變更「類型」，且無法從切換組態設定中移除 WAN/LAN1-LAN8 介面。
MTU	您可以為「高安全性」模式和「標準」模式設定此項。 LAN1-LAN8 支援 Jumbo 框架。 範圍：576 到 9216；預設值為 1504。 注意 WAN MTU 範圍為 576 到 1504。
風暴控制閾值	您可以為所有安全模式設定此項。 閾值會分別套用到每一種風暴控制類型。例如，當設定為 20 時，多點傳送閾值和廣播閾值會各自設定為 20。
風暴控制模式：多點傳送	您可以為所有安全模式設定此項。
風暴控制模式：廣播	您可以為所有安全模式設定此項。

標準模式

設定	說明
類型	設定為「L2」。 「橋接模式」下的唯讀欄位。您無法變更「類型」，且無法從切換組態設定中移除 WAN/LAN1-LAN8 介面。

設定	說明
MTU	您可以為「高安全性」模式和「標準」模式設定此項。 LAN1-LAN8 支援 Jumbo 框架。 範圍：576 到 9216；預設值為 1504。 注意 WAN MTU 範圍為 576 到 1504。
風暴控制閾值	您可以為所有安全模式設定此項。 閾值會分別套用到每一種風暴控制類型。例如，當設定為 20 時，多點傳送閾值和廣播閾值會各自設定為 20。
風暴控制模式：多點傳送	您可以為所有安全模式設定此項。
風暴控制模式：廣播	您可以為所有安全模式設定此項。

高速模式

設定	說明
類型	設定為「L2」。 「橋接模式」下的唯讀欄位。您無法變更「類型」，且無法從切換組態設定中移除 WAN/LAN1-LAN8 介面。
MTU	設定為「高速」模式時，此欄位不會顯示。 您無法變更採用「高速」模式之 LAN 的 MTU；不過，LAN1-LAN8 的 MTU 預設接受 Jumbo 框架。WAN MTU 範圍為 576 到 1504。
流量控制	此設定僅適用於「高速」模式。
風暴控制閾值	您可以為所有安全模式設定此項。 閾值會分別套用到每一種風暴控制類型。例如，當設定為 20 時，未知單點傳送閾值、多點傳送閾值和廣播閾值會各自設定為 20。
風暴控制模式：未知單點傳送	此設定僅適用於「高速」模式。

設定	說明
風暴控制模式：多點傳送	您可以為所有安全模式設定此項。
風暴控制模式：廣播	您可以為所有安全模式設定此項。

注意

MGMT 介面是從 Cloud Edge 雲端主控台設定的。

當您以「路由模式」部署採用硬體切換晶片組的設備時，設定設備的方式可採用與設定所有其他已設為「路由模式」之 Cloud Edge 型號的相同方式。

編輯路由模式的網路介面

在註冊處於「路由模式」的 Cloud Edge 設備之前，您可以使用內部部署主控台來設定所有 L3 實體介面。向 Cloud Edge 雲端主控台註冊 Cloud Edge 設備後，您僅可從內部部署主控台編輯 WAN 和 LAN1 實體介面。

注意

如需瞭解為「橋接模式」或「軟體切換」設定實體介面時要遵循的程序，請參閱為橋接模式/軟體切換編輯網路介面 第 7-49 頁。

如需瞭解為「橋接模式」（採用切換晶片組）設定實體介面時要遵循的程序，請參閱編輯橋接模式（採用切換晶片組）的網路介面 第 7-50 頁。

步驟

1. 移至「網路 > 介面」。
2. 按一下介面的名稱。
3. 根據介面模式設定介面設定。

   WAN 和 LAN1 介面可使用靜態、DHCP 或 PPPoE 定址。

   - 針對靜態位址，請設定適用的參數：

選項	說明
類型	選取 L3。
模式	選取「靜態」。
MTU	指定 576 到 1500 之間的值。
MSS	選取「覆寫」並指定 536 到 1460 之間的值。 注意 MSS 值不能大於 (MTU - 40)。
IPv4 位址	指定 IPv4 位址（範例：`10.10.10.23`）。
IPv4 網路遮罩	指定 IPv4 子網路遮罩（範例：`255.255.254.0`）。
IPv4 預設設備	指定 IPv4 預設設備（範例：`10.10.10.1`）。只有 WAN 組態設定才需要此設定。

- 針對 DHCP，請設定適用的參數：

選項	說明
類型	選取 L3。
模式	選取 DHCP。
MTU	指定 576 到 1500 之間的值。
MSS	選取「覆寫」並指定 536 到 1460 之間的值。 注意 MSS 值不能大於 (MTU - 40)。

- 針對 PPPoE 設定下列參數：

注意
使用 PPPoE 時，您無法設定 MTU 或 MSS。

選項	說明
類型	選取 L3。
模式	選取 PPPoE。
使用者名稱	指定網際網路服務提供者提供的使用者名稱。 注意 您最多可以指定三個 ISP 帳號。如果主要 ISP 帳號無法使用，Cloud Edge 會使用次要 ISP 帳號或第三級 ISP 帳號自動連線到網路。通過此連線的服務一經還原，Cloud Edge 即會切換回主要 ISP 帳號。
密碼	指定網際網路服務提供者提供的密碼。
PPPoE 進階設定	指定下列項目： • 隨選閒置時間（秒）：此設定可讓 Cloud Edge 設備在處於離線狀態長達指定的時間後，中斷 Internet 連線。如果 Cloud Edge 設備因離線而終止 Internet 連線，則此裝置會在您嘗試存取 Internet 時恢復連線。 此選項預設為關閉。 • 連線逾時（秒）：此設定可讓 Cloud Edge 設備定期檢查 Internet 連線。如果 Internet 連線無法使用，設備將自動重新建立連線。 此選項可讓設備持續保持 Internet 連線，即使連線閒置也是一樣。由於會始終保持連線，因此此選項可將 Internet 連線回應時間降到最低。 此設定的預設值為 30（秒）。

4. 如果設備尚未註冊，請為介面設定管理存取權。

   選取要允許的管理服務和流量（內部部署主控台、Ping、SSH、SNMP）。您可以使用選取的服務從內部網路管理 Cloud Edge 設備。啟動內部部署主控台管理服務可提供登入存取權，讓授權的使用者能夠存取內部部署主控台。

注意

只有當 Cloud Edge 設備未註冊時，才可從內部部署主控台設定管理存取權。註冊設備後，此欄位為唯讀，您必須從 Cloud Edge 雲端主控台設定管理存取權。

雖然您可以在 Cloud Edge 設備的 WAN 介面上啟動管理服務，但不建議您這麼做。您應該僅在內部介面上啟動管理服務與流量。

5. 在「監控設定」區段下，指定您要 Cloud Edge 監控的主機（IP 位址或網域名稱）。

   如果 Cloud Edge 設備無法存取主機，它會終止目前的連線，然後使用設定的下一個 ISP 帳號來建立連線。如果任何主機皆無法使用，Cloud Edge 會關閉與介面相關聯的靜態路由或以策略為基礎的路由。不過，當主要連線恢復時，Cloud Edge 就會終止作用中連線，然後重新建立主要連線。

   如需詳細資訊，請參閱使用監控主機來判定路由是否可用 第 7-57 頁。

6. 在「頻寬設定」區段下，指定下列項目：

   - 下游：通過通訊埠的下載速度上限。預設值為空白。
   - 上游：通過通訊埠的上傳速度上限。預設值為空白。

   如需詳細資訊，請參閱使用介面頻寬設定來限制流量 第 7-58 頁。

7. 按一下「套用」。

8. 確認更新出現在「網路 > 介面」的介面清單中。

使用監控主機來判定路由是否可用

監控主機

Cloud Edge 會檢查 WAN 是否正常運作中，方法是從每個輸出介面 Ping 對應的監控 IP 位址或主機名稱。如果無法連接監控主機，則會關閉任何與該介面相關聯的靜態路由或策略型路由。如果流量符合另一條路由，則會將該流量路由至其他靜態路由或策略型路由。如果流量不符合另一條路由，則會將該流量經由預設設備路由傳送或是捨棄。

- 若要設定監控主機，請參閱在介面上設定監控主機 第 7-58 頁。
- 若要設定預設設備，請參閱新增靜態路由 第 6-75 頁。
- 若要設定策略型路由，請參閱新增策略型路由 第 7-82 頁。

如需有關自動容錯移轉的詳細資訊，請參閱多個 ISP/WAN 環境的自動容錯移轉 第 7-82 頁。

在介面上設定監控主機

步驟

1. 移至「網路 > 介面」。

   注意

   向 Cloud Edge 雲端主控台註冊 Cloud Edge 設備之前，您可在所有介面上設定監控主機。註冊後，則僅能針對 WAN 和 LAN1 介面設定監控主機。

2. 按一下介面的名稱。
3. 按一下「監控設定」。

   「監控設定」區段隨即開啟。

4. 選取「啟動介面監控」。
5. 新增主機 IP 位址來監控介面。
6. 按一下「套用」。

使用介面頻寬設定來限制流量

設定介面頻寬設定，以設定下游與上游流量的門檻值上限。頻寬控制策略不得超過介面頻寬門檻值。依預設，Cloud Edge 不會限制頻寬。可為每個介面設定不同的門檻值。

當介面頻寬設定配置錯誤時，可能會發生網路壅塞。趨勢科技建議您將介面頻寬設定為該介面所允許的門檻值上限，然後再設定頻寬控制策略來決定哪個流量擁有較高的優先順序。

若要進行介面頻寬設定，請移至「網路 > 介面」。如需詳細資訊，請參閱 Cloud Edge 內部部署主控台主題編輯路由模式的網路介面 第 7-54 頁。

注意

向 Cloud Edge 雲端主控台註冊 Cloud Edge 設備之前，您可以對所有「路由模式」介面進行頻寬設定。註冊設備後，則僅能針對 WAN 或 LAN1 介面進行頻寬設定。

管理 VLAN

VLAN 的運作方式

虛擬區域網路 (VLAN) 是由一組端點、伺服器和其他網路裝置組成，不論所在位置如何，彼此的通訊就如在同一個 LAN 區段內。即使分散各地並連線到許多網路區段，端點和伺服器仍可以屬於相同的 VLAN。

VLAN 以邏輯而非實體方式隔開裝置。每個 VLAN 均視為一個廣播網域。VLAN 1 中的裝置可以與 VLAN 1 中的其他裝置連線，但無法與其他 VLAN 中的裝置連線。VLAN 中各裝置之間的通訊獨立於實體網路之外。

VLAN 隔開裝置的方式是對 VLAN 中裝置傳送和接收的所有封包增加 `802.1Q` VLAN 標籤。VLAN 標籤是 4 位元組框架延伸，其中包含 VLAN 識別碼以及其他資訊。

新增/編輯 VLAN 子介面

您可以將 L3 VLAN 子介面新增到接收標記為 VLAN 之封包的 Cloud Edge eth0 和 eth1 介面。您必須為每個 L3 VLAN 子介面設定唯一的 IPv4 位址和網路遮罩。如有需要，您可以編輯 VLAN 介面。

注意

您無法將 VLAN 子介面新增到無線介面。

步驟

1. 在新增 VLAN 子介面之前，請先檢閱有關如何藉由 Cloud Edge 設備運作 VLAN 的重要資訊。

   如何在 VLAN 中部署 Cloud Edge 第 6-59 頁

2. 移至「網路 > 介面」。
3. 執行適當的處理行動：
   - 若要新增 VLAN，請按一下「處理行動」欄中的 VLAN 新增組態設定圖示 ()。
   - 若要編輯 VLAN，請按一下「VLAN」區段中的 VLAN 名稱。
4. 指定 VLAN 設定。
   - 名稱：為 VLAN 介面命名。
   - 類型：會自動顯示 L3 VLAN，並且為唯讀。

     不支援 L2 VLAN。
   - 模式：選取「DHCP」或「靜態」。

     如果選取靜態，請指定「IPv4 位址」和「IPv4 網路遮罩」。
   - VLAN ID：指定 VLAN ID，其必須與此 VLAN 介面所接收封包的 VLAN ID 相符。

     每個 VLAN 介面的 VLAN ID，都必須與連接 VLAN 介面之 IEEE 802.1Q 相容路由器或交換器所新增的 VLAN ID 相符。VLAN ID 可以是 1 和 4094 之間的任何數字（0 和 4095 為保留數字）。

     您無法變更現有 VLAN 介面的 VLAN ID。

管理無線網路

請使用 Cloud Edge 內部部署主控台來管理無線網路。

無線網路總覽

您可以為受支援的 Cloud Edge 設備設定主要無線網路和客體無線網路。您應瞭解可以運用哪些方式來部署及設定無線網路，以及哪些設備功能可供無線網路使用。

一般資訊

您可以在設定無線網路時使用下列一般資訊：

- 只有「路由模式」才支援無線網路。

  如果您從「橋接模式」變更為「路由模式」，無線網路設定會採用預設設定。

- 主要無線網路和客體無線網路均預設為關閉。
- 依預設，如果啟動了客體無線網路，則客體無線網路上的用戶端將無法存取主要無線網路或內部區域網路上的資源。

  您可以視需要啟動本機存取。在允許訪客存取內部資源之前，您應謹慎考量安全性問題。

- 支援 2.4 GHz 或 5 GHz 網路頻率（擇一而用）。

  預設運作頻率為 2.4 GHz。

- 支援 20 個無線用戶端連線。

無線網路設定與組態設定

您可以使用下列方法來為 Cloud Edge 設備設定無線網路：

- 請從「「快速設定」畫面」執行主要無線網路的基本設定。
- 完成初始設定後，您可以在下列位置管理無線網路組態設定：
  - Cloud Edge 內部部署主控台：設定一般設定、主要無線網路，以及客體無線網路。
  - Cloud Edge 雲端主控台：設定無線網路存取控制設定，以及管理無線用戶端連線。

> **注意**
>
> 您可以從 Cloud Edge 雲端主控台檢視客體和無線網路組態設定，但必須使用內部部署主控台才能變更組態設定。

無線網路介面組態設定

您可以編輯無線網路介面：

- 請從 Cloud Edge 雲端主控台設定及檢視無線介面的相關資訊。
- 您可以從「介面」頁面為主要和客體無線介面設定靜態 IP 位址。

  無線介面不支援 VLAN。

  > **注意**
  >
  > 如果無線介面未啟動，雖然可以在「介面」頁面中看到該無線介面，但其介面狀態會顯示為離線。

- 使用「設備資訊」頁面檢視無線介面狀態和統計資料的相關資訊。

  如果未啟動主要無線網路或客體無線網路的無線網路，相應介面的介面狀態將是「離線」。

無線網路與相關的網路功能

您可以為無線網路設定相關功能（例如，管理存取權、靜態路由、DHCP 存取、NAT、頻寬控制、VPN 及端點防護）：

- 使用 Cloud Edge 雲端主控台啟動管理存取權。

  您可以啟動主要無線網路和客體無線網路的管理存取權，惟啟動客體無線網路的存取權需謹慎為之。

- 從 Cloud Edge 雲端主控台設定靜態路由。
- 從 Cloud Edge 雲端主控台設定 DHCP 服務。
  - 您可以設定主要無線網路和客體無線網路的 DHCP 服務。
  - 不論相應的客體無線網路或主要無線網路處於啟動還是關閉狀態，無線介面都會顯示在「DHCP」頁面上。

DHCP 服務會依預設啟動，並擁有預設的 IP 位址集區。

- 從 Cloud Edge 雲端主控台設定 NAT。
  - 您可以設定主要無線網路和客體無線網路的 NAT。
  - 不論相應的客體無線網路或主要無線網路處於啟動還是關閉狀態，無線介面都會顯示在「NAT」頁面上。

    目標 NAT 規則：選擇無線介面做為入口介面。

    來源 NAT 規則：選擇無線介面做為出口介面。
- 設定頻寬控制。
  - 您可以設定頻寬控制，以納入主要無線網路和客體無線網路。
  - 若要對來自無線網路的流量套用頻寬控制，請使用「任意」做為來源或目標頻寬控制參數，或是設定選取的位址物件，這些物件包含來自要套用頻寬控制之無線網路的 IP 位址。
- 從 Cloud Edge 雲端主控台設定 VPN 存取。
  - 您可以設定主要無線網路和客體無線網路的使用者 VPN 或 Site-to-Site VPN。
  - 若要在無線網路上建立 VPN，請建立並使用其中包含所需無線網路 IP 位址的網路物件。

    必須啟動無線網路（主要或客體），才能在該無線網路上建立 VPN。
- 您可以設定網路存取控制（端點防護）。

  在您為選定設備設定「WFBSS 端點防護」和「可疑用戶端的端點防護」後，無線網路上的用戶端即會受到防護。

無線網路與 Cloud Edge 安全

無線網路會受到 Cloud Edge 安全防護的保護（可使用 Cloud Edge 雲端主控台加以設定）：

- 策略物件

  設定策略物件時，可以使用無線網路 IP 位址或 MAC 位址。

- 策略

  請使用來源參數或目標參數，來納入位址物件（其中包含主要無線網路和客體無線網路）或透過無線網路登入的使用者和群組。

- HTTPS 檢查規則

  請使用解密來源參數或目標參數，來納入位址物件（其中包含主要無線網路和客體無線網路）或透過無線網路登入的使用者和群組。

- 核可/封鎖清單

  已設定的核可清單和封鎖清單會套用至無線網路流量。

- 安全資料檔

  針對 Cloud Edge 設備選取的安全資料檔會套用至無線網路流量。

- 通知

  當無線網路流量發生違規時，系統會傳送通知。

稽核與診斷支援

系統會對無線網路組態設定進行稽核，並且為無線網路提供某些診斷功能。

- Cloud Edge 雲端主控台稽核記錄：啟動無線網路後，稽核記錄即會登載有關無線組態設定變更的項目。
- Cloud Edge 內部部署主控台診斷：
  - 在無線介面（wlan0 和 wlan1）上或針對無線通訊協定 (wifi0) 執行封包擷取。

    如果未啟動無線網路（主要或客體），其相應的網路介面將不會顯示在封包擷取頁面上。

  - 「診斷」檔案收集的「基本設定與事件記錄檔」類別包含無線網路的相關資訊。
  - 健全狀況檢查提供主要和客體無線介面狀態的相關資訊。

設定一般無線網路設定

根據您的無線網路需求，設定一般無線網路設定。有些一般無線設定適用於主要無線網路，而有些設定則同時適用於主要無線網路和客體無線網路，下列程序中將會註明。

步驟

1. 移至「網路 > 無線 > 無線設定 > 一般設定」。
2. 選取「啟動主要無線網路」。

   此設定僅適用於主要無線網路。預設為關閉。

   選取此選項不會啟動客體無線網路。您必須從「客體網路」標籤啟動客體無線網路。
3. 設定下列項目：
   - 頻率：選取您的無線網路頻率。

     此設定同時適用於主要無線網路和客體無線網路。

     Cloud Edge 無線網路能以 2.4 GHz 或 5.0 GHz 頻率運作。這款設備無法同時以兩種頻率運作。預設運作頻率為 2.4 GHz。
   - 啟動 SSID 廣播：如果您想要廣播主要無線網路的 SSID，請選取此選項。

     此設定僅適用於主要無線網路。

     啟動此選項後，Cloud Edge 設備會廣播主要無線網路的 SSID，讓附近的用戶端可以在「可用的無線網路」畫面上看到該網路。預設為啟動。
   - SSID：指定主要無線網路的存取點名稱。

     此設定僅適用於主要無線網路。

     預設 SSID 如下：

     - 2.4 GHz：CloudEdge-XXYY

- 5 GHz：CloudEdge-5G-XXYY

> **注意**
>
> XXYY 代表 Cloud Edge 設備之產品序號的前四個字元。為了取得最佳的安全性，您應該輸入預設值以外的字元來做為 SSID。

- 通道：指定通道號碼。

  此設定同時適用於主要無線網路和客體無線網路。

  通道數目視選擇的頻率和所在國家/地區而有所不同。預設值為「自動」。

- 模式：指定模式。

  此設定同時適用於主要無線網路和客體無線網路。

  2.4 GHz：選項包括「11bgn 混合」和「11bg 混合」

  5 GHz：選項包括「僅 11a」、「11a/n 混合」和「11a/n/ac 混合」

- 安全性：指定您想要採用的安全類型。

  此設定僅適用於主要無線網路。

  - 如果選取「開啟」，則無需設定其他安全設定。
  - 如果選取「WPA-PSK[TKIP]」、「WPA2-PSK[AES]」或「WPA-PSK[TKIP]+WPA2-PSK[AES]」安全類型，則還必須指定「預先共用金鑰」。

    > **注意**
    >
    > 僅當選取「11bg 混合」(2.4 GHz) 或「僅 11a」(5 GHz) 模式時，「WPA-PSK[TKIP]」安全設定才可用。

  - 如果選取「WPA/WPA2 Enterprise」安全類型，則還必須指定「Radius 伺服器 IP 位址」、「Radius 伺服器通訊埠」和「Radius 伺服器密碼」。

4. （選用）選取「WPA/WPA2 Enterprise」後，按一下「測試」並輸入要在連線到 Radius 伺服器時使用的使用者名稱和密碼，以確認 Cloud Edge 可以成功連線。
5. 在「進階設定」區段下，設定下列進階無線設定：

   進階設定同時適用於主要無線網路和客體無線網路。

   - DTIM 間隔：指定 DTIM 間隔。範圍為 1 到 255。預設值為 `3`。
   - 指標間隔：指定指標間隔（毫秒）。範圍為 100 到 1000。預設值為 `100`。
   - 簡短前序編碼：按一下「啟動」或「關閉」可啟動或關閉此選項。
   - RTS 閾值：指定 RTS 閾值（介於 0 到 2347 個位元組之間）。預設值為 `2347` 個位元組。
   - 啟動短 GI：按一下「啟動」或「關閉」可啟動或關閉此選項。
   - 傳輸功率：指定無線網路存取點的傳輸功率百分比。範圍為 1 到 100。預設值為 `100`。

   注意

   僅當您選擇的網路頻率為 2.4 GHz 時，「簡短前序編碼」、「RTS 閾值」和「啟動短 GI」等欄位才可用。

6. 按一下「儲存」。

設定客體無線網路設定

根據您的無線網路需求，設定客體無線網路設定。

步驟

1. 移至「網路 > 無線 > 無線設定 > 客體網路」。
2. 選取「啟動客體網路」。

   根據預設，系統不會啟動客體無線網路。

注意

必須先啟動主要無線網路，然後才能啟動客體無線網路

3. 啟動要用於客體網路的選項：

   - 啟動 SSID 廣播

     啟動此選項後，Cloud Edge 設備會廣播客體網路的 SSID，讓附近的用戶端可以在「可用的無線網路」畫面上看到客體無線網路。預設為啟動。

   - 啟動存取區域網路

     啟動此選項後，客體無線網路上具有適當權限的使用者皆可存取內部區域網路上的資源。預設為關閉。

4. 指定客體無線網路的 SSID。

   預設 SSID 如下：

   - 2.4 GHz：CloudEdge-GUEST-XXYY
   - 5 GHz：CloudEdge-5G-GUEST-XXYY

注意

XXYY 代表 Cloud Edge 設備之產品序號的前四個字元。為了取得最佳的安全性，您應該輸入預設值以外的字元來做為 SSID。

5. 在「安全設定」下，指定要用於客體無線網路的安全類型。

   - 如果選取「開啟」，則無需設定其他安全設定。
   - 如果選取「WPA-PSK[TKIP]」、「WPA2-PSK[AES]」或「WPA-PSK[TKIP]+WPA2-PSK[AES]」安全類型，則還必須指定「預先共用金鑰」。

     注意

     僅當在「一般設定」標籤中選取「11bg 混合」(2.4 GHz) 或「僅 11a」(5 GHz) 模式時，「WPA-PSK[TKIP]」安全設定才可用。

- 如果選取「WPA/WPA2 Enterprise」安全類型，則還必須指定「Radius 伺服器 IP 位址」、「Radius 伺服器通訊埠」和「Radius 伺服器密碼」。

6. （選用）選取「WPA/WPA2 Enterprise」後，按一下「測試」並輸入要在連線到 Radius 伺服器時使用的使用者名稱和密碼，以確認 Cloud Edge 可以成功連線。
7. 按一下「儲存」。

疑難排解無線網路

檢視無線網路的疑難排解資訊。

步驟

1. 移至「網路 > 無線 > 無線設定 > 疑難排解」
2. 使用記錄檔來對無線網路進行疑難排解。
3. 按一下頁面右上角的「重新整理」圖示，以更新顯示的記錄項目。

   顯示的記錄數目上限為 100。

管理 DNS

您可以檢視和編輯 Cloud Edge 設備的網域名稱伺服器 (DNS) 伺服器設定。

由於使用 DHCP 或 PPPoE 存取 Internet 的環境可能會從 ISP 動態取得 DNS 組態設定，因此您可能不需要在這些環境中進行 DNS 設定。

DNS 最佳做法建議

主動式雲端截毒技術 (SPN) 使用雲端服務，並且依賴 DNS 查詢進行查詢。為了確保能快速回應並最大程度地降低延遲，Cloud Edge 裝置必須設定 DNS 伺服器。您最多可以設定三個 DNS 伺服器。

DNS 伺服器必須能夠支援 Cloud Edge 所發出的大量 DNS 要求。一般來說，在 Cloud Edge 建置其本機 DNS 快取前，瀏覽一個 URL 會發出兩個 DNS 要求。請確保您的 DNS 伺服器安裝在資源與效能充足的伺服器上，以處理額外的 DNS 數量。

為了降低延遲，每個 DNS 伺服器應具備快速網路卡，並安裝在快速網路交換器上。

相較於 ISP 提供的安裝在公司網路外的 DNS 伺服器，趨勢科技建議您使用內部 DNS 伺服器。一般來說，ISP DNS 伺服器延遲性較高，且不支援來自單一 IP 位址的大量 DNS 查詢。許多 ISP DNS 伺服器具有節流機制，可限制每秒 DNS 要求數，並會影響 Cloud Edge 的網頁信譽評等服務 (WRS) 效能。

若要改善網路回應時間和效能，請將 DNS 伺服器放置在盡可能靠近 Cloud Edge 裝置的位置，以消除裝置之間不必要的網路躍點。

WRS 與 URL 過濾要求會透過 HTTP 通訊埠 80 發出。請勿在防火牆中封鎖這些通訊埠的 Cloud Edge 管理 IP 位址。

設定 DNS 設定

步驟

1. 移至「網路 > DNS」。
2. 設定適用的 DNS 伺服器 IPv4 位址。

   注意

   如果 Cloud Edge 從網際網路服務提供者動態取得 DNS，則「繼承 DNS 資訊」區段會出現並顯示唯讀 DNS 資訊。

3. 按一下「套用」。

管理位址物件

位址物件決定內部網路中允許的 IP 位址範圍。依預設，Cloud Edge 會使用「預設內部位址」位址物件，其中包含所有的內部 IP 位址範圍（10.0.0.0/8、

172.16.0.0/12、192.168.0.0/16）。在設定以策略為基礎的路由時，也會使用位址物件。

- 您可以在 Cloud Edge 內部部署主控台上移至「網路 > 位址」，來檢視及編輯已設定的 IPv4 位址物件。
- 在設備註冊後，您就無法使用 Cloud Edge 內部部署主控台的「網路 > 位址」頁面來新增或刪除位址物件。
- 您可以使用 Cloud Edge 雲端主控台新增、編輯及刪除要在網路設定和以策略為基礎的路由中使用的 IPv4 位址物件。

注意

在「路由」下建立以策略為基礎的規則時，您可以新增 IPv4 位址物件。對於在設定以策略為基礎的路由時新增的位址物件，您稍後可以從「網路 > 位址」頁面編輯它們。

IP 位址物件參數

下表說明從 Cloud Edge 內部部署主控台新增或編輯 IPv4 物件時的可設定參數。從內部部署主控台設定策略路由規則時，可以使用這些 IPv4 位址物件。

表 7-6. 位址物件參數

參數	說明
物件名稱	指定可說明位址的名稱。定義以策略為基礎的路由規則時，此名稱會顯示在位址清單中。名稱區分大小寫且必須是唯一名稱。僅限使用字母、數字、空格、連字號與底線。
類型	IPv4
位址	使用下列標記指定 IP 位址或網路： • `ip_address` • `ip_address_range` • `ip_address/bitmask` 範例：192.168.1.1 或 192.168.1.1-192.168.1.10 或 192.168.80.0/24

檢視位址物件

步驟

- 移至「 網路 > 位址」 。

編輯位址物件

您可以使用 Cloud Edge 內部部署主控台來編輯現有 IPv4 位址物件的 IP 位址。

有一個預設 IPv4 位址物件「“預設內部位址”」設定為使用 IP 位址 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16。

步驟

1. 移至「 網路 > 位址」 。
2. 按一下您要編輯的位址物件的名稱。
3. 編輯 IP 位址。

   編輯 IPv4 位址物件的設定時，Cloud Edge 支援單一 IP 位址（'-' 作為範圍標記）以及 IP 位址/網路遮罩 (192.168.1.1/24)。

   範例： `192.168.0.1,10.0.0.1-10.0.0.4,192.168.1.1/24`
4. 按一下「確定」 。
5. 確認修改的位址物件在「網路 > 位址」的清單中顯示 IP 位址修改。

> **注意**
>
> 您可以在「網路位址」頁面上編輯 IPv4 位址物件，但無法新增。但是，在「路由」下建立以策略為基礎的規則時，您可以新增 IPv4 位址物件。設定以策略為基礎的路由時新增的位址物件稍後可以使用此程序進行編輯。

管理橋接/切換設定

您可以從 Cloud Edge 內部部署主控台檢視及管理「橋接模式」/「軟體切換」部署的 橋接器介面 (br0)，或「橋接模式」（採用切換晶片組）的切換介面 (sw0)。

步驟

1. 根據 Cloud Edge 設備型號執行適當的動作。
   a. 移至「網路 > 橋接」。
   b. 移至「網路 > 切換」。
2. 在「名稱」下，執行適當的動作。
   a. 按一下「br0」。
   b. 按一下採用硬體切換晶片組之設備的「sw0」。
3. 執行下列動作：
   - 檢視 橋接器介面 (br0) 或 切換介面 (sw0) 設定的摘要。
   - 按一下 橋接器介面 (br0) 或 切換介面 (sw0) 名稱，以檢視其他詳細資訊或編輯設定。

接下來需執行的動作

使用 Cloud Edge 雲端主控台設定 切換介面 (sw0) 的內部網路安全模式設定。

若要變更安全模式或編輯模式設定，請登入 Cloud Edge 雲端主控台，然後移至「設備 > （選取的設備） > 網路 > 介面」頁面。

請參閱設定切換介面 (sw0) 設定 第 6-54 頁。

設定橋接器介面 (br0)

您可以對處於「橋接模式」的選定設備的 橋接器介面 (br0) 進行設定。橋接器介面 (br0) 是一個虛擬介面，您必須從 Cloud Edge 內部部署主控台來設定它。

注意

如需瞭解為「軟體切換」設定 橋接器介面 (br0) 時要遵循的程序，請參閱設定軟體切換的橋接器介面 (br0) 第 7-75 頁。

如需瞭解在採用硬體切換晶片組的 Cloud Edge 設備上為「橋接模式」設定切換介面 (sw0)時要遵循的程序，請參閱下列內容：

- 設定切換介面 (sw0) 第 7-77 頁（從 Cloud Edge 內部部署主控台）
- 設定切換介面 (sw0) 設定 第 6-54 頁（從 Cloud Edge 雲端主控台）

步驟

1. 移至「網路 > 橋接」。
2. 按一下「名稱」下的「br0」。

   新增/編輯橋接 畫面隨即開啟。
3. 對於「類型」，請選取「橋接」。

   「介面 1」和「介面 2」欄位均為唯讀，並預設為 L2 介面（分別預先選取了 WAN [L2] 和 LAN1 [L2]）。
4. 設定可編輯的介面設定。

   橋接器介面 (br0) 可以使用靜態或 DHCP 定址。

   - 針對靜態位址，請設定適用的參數：

選項	說明
模式	選取「靜態」。
MTU	指定 576 到 1500 之間的值。
IPv4 位址	指定 IPv4 位址（範例：`10.10.10.23`）。
IPv4 網路遮罩	指定 IPv4 子網路遮罩（範例：`255.255.254.0`）。
IPv4 預設設備	指定 IPv4 預設設備（範例：`10.10.10.1`）。只有 WAN 組態設定才需要此設定。

- 針對 DHCP，請設定適用的參數：

選項	說明
模式	選取 DHCP。
MTU	指定 576 到 1500 之間的值。

5. 如果設備尚未註冊，請為 橋接器介面 (br0) 設定管理存取權。

   選取要允許的管理服務和流量（內部部署主控台、Ping、SSH、SNMP）。您可以使用選取的服務從內部網路管理 Cloud Edge 設備。啟動內部部署主控台管理服務可提供登入存取權，讓授權的使用者能夠存取內部部署主控台。

   注意

   只有當 Cloud Edge 設備未註冊時，才可從內部部署主控台設定管理存取權。註冊設備後，此欄位為唯讀，您必須從 Cloud Edge 雲端主控台設定管理存取權。

6. 在「進階設定」下，選擇性地選取「啟動跨距樹狀目錄通訊協定」。

   Cloud Edge 會使用跨距樹狀目錄通訊協定來偵測並防止設備所在的網路產生迴圈。Cloud Edge 無法偵測下游網路或下游裝置上發生的迴圈。

7. 在「進階設定」下，選擇性地選取「啟動連結中斷檢測」。

8. 按一下「套用」。

設定軟體切換的橋接器介面 (br0)

您可以對部署為「軟體切換」（從「橋接模式」變化而來）的選定設備的 橋接器介面 (br0) 進行軟體切換設定。橋接器介面 (br0) 是一個虛擬介面，您必須從 Cloud Edge 內部部署主控台來設定它。

- 採用「軟體切換」部署時，Cloud Edge 設備部署模式開關會設定為「橋接」，並且您可以為 橋接器介面 (br0) 設定與執行基本「橋接模式」部署時所用的相同 IP 位址設定。

- 此外，您必須額外新增至少三個實體介面做為軟體切換的 L2 介面。WAN 與 LAN1 為必要通訊埠。您可以新增 LAN2 和 LAN3 做為第三個軟體切換介面。如有需要，您可以新增 LAN2 和 LAN3 通訊埠。

注意

如需瞭解為「橋接模式」設定 橋接器介面 (br0) 時要遵循的程序，請參閱設定橋接器介面 (br0) 第 7-73 頁。

如需瞭解在採用硬體切換晶片組的 Cloud Edge 設備上為「橋接模式」設定切換介面 (sw0)時要遵循的程序，請參閱下列內容：

- 設定切換介面 (sw0) 第 7-77 頁（從 Cloud Edge 內部部署主控台）
- 設定切換介面 (sw0) 設定 第 6-54 頁（從 Cloud Edge 雲端主控台）

步驟

1. 移至「網路 > 橋接」。
2. 按一下「名稱」下的「br0」。

   新增/編輯橋接 畫面隨即開啟。
3. 對於「類型」，請選取「軟體切換」。

   在設定「軟體切換」部署時使用的其他參數會變成可用。
4. 在「切換介面」下，選取要包含在軟體切換中的實體介面。
   - 「WAN[L2]」和「LAN1[L2]」是必要項目，因此會以唯讀選取項目狀態預先選取。
   - 您必須在「LAN2[L2]」或「LAN3[L2]」兩項中選擇至少一項。您可以同時選擇「LAN2[L2]」和「LAN3[L2]」。
5. 選擇用於設定 橋接器介面 (br0) 的「模式」。

   選擇「靜態」或「DHCP」。
6. （選用）變更軟體切換的「MTU」。

   預設值為 1438。範圍為 576-1500。

您也可以修改 Cloud Edge 設備上實體介面的 MTU。針對軟體切換設定的 MTU 不能大於實體介面上所設定的 MTU。

7. 如果「模式」是「靜態」，請設定適用的 IPv4 介面設定。

選項	說明
IPv4 位址	指定 IPv4 位址（範例：`10.10.10.23`）。
IPv4 網路遮罩	指定 IPv4 子網路遮罩（範例：`255.255.254.0`）。
IPv4 預設設備	指定 IPv4 預設設備（範例：`10.10.10.1`）。只有 WAN 組態設定才需要此設定。

8. 如果設備尚未註冊，請為 橋接器介面 (br0) 設定管理存取權。

   選取要允許的管理服務和流量（內部部署主控台、Ping、SSH、SNMP）。您可以使用選取的服務從內部網路管理 Cloud Edge 設備。啟動內部部署主控台管理服務可提供登入存取權，讓授權的使用者能夠存取內部部署主控台。

   注意

   只有當 Cloud Edge 設備未註冊時，才可從內部部署主控台設定管理存取權。註冊設備後，此欄位為唯讀，您必須從 Cloud Edge 雲端主控台設定管理存取權。

9. 在「進階設定」下，選擇性地選取「啟動跨距樹狀目錄通訊協定」。

   Cloud Edge 會使用跨距樹狀目錄通訊協定來偵測並防止設備所在的網路產生迴圈。Cloud Edge 無法偵測下游網路或下游裝置上發生的迴圈。

10. 按一下「套用」。

設定切換介面 (sw0)

您可以對處於「橋接模式」之採用硬體切換晶片組的選定 Cloud Edge 設備的切換介面 (sw0) 進行設定。切換介面 (sw0) 是一個虛擬介面，您可以從 Cloud Edge 內部部署主控台來設定它。

注意

如需瞭解為「橋接模式」設定 橋接器介面 (br0) 時要遵循的程序，請參閱設定橋接器介面 (br0) 第 7-73 頁。

如需瞭解為「軟體切換」設定 橋接器介面 (br0) 時要遵循的程序，請參閱設定軟體切換的橋接器介面 (br0) 第 7-75 頁。

步驟

1. 移至「網路 > 切換」。
2. 按一下「名稱」下的「sw0」。

   新增/編輯切換 畫面隨即開啟。

   - 「名稱」欄位為唯讀並已設定為「sw0」。
   - 「內部網路安全模式」欄位為唯讀並已設定為「高安全性」。

     您可以使用 Cloud Edge 雲端主控台來變更內部網路安全模式。
3. 針對「模式」，請選取「DHCP」或「靜態」。
4. 如果模式為「靜態」，請輸入 IPv4 位址、IPv4 網路遮罩和 IPv4 預設閘道。
5. 您可以視需要設定「MTU」。

   指定 576 到 1500 之間的值。預設值為 1438。
6. 如果設備尚未註冊，請為 切換介面 (sw0) 設定管理存取權。

   選取要允許的管理服務和流量（內部部署主控台、Ping、SSH、SNMP）。您可以使用選取的服務從內部網路管理 Cloud Edge 設備。啟動內部部署主控台管理服務可提供登入存取權，讓授權的使用者能夠存取內部部署主控台。

   注意

   只有當 Cloud Edge 設備未註冊時，才可從內部部署主控台設定管理存取權。註冊設備後，此欄位為唯讀，您必須從 Cloud Edge 雲端主控台設定管理存取權。

7. （僅限「高安全性」模式和「標準」模式）：在「進階設定」下，您可以視需要執行下列操作：

   a. 選取「啟動跨距樹狀目錄通訊協定」。

      Cloud Edge 會使用跨距樹狀目錄通訊協定來偵測並防止設備所在的網路產生迴圈。Cloud Edge 無法偵測下游網路或下游裝置上發生的迴圈。

   b. 選取「IGMP 窺探 (IGMP Snooping)」。

8. 按一下「套用」。

接下來需執行的動作

從 Cloud Edge 雲端主控台進行其他 切換介面 (sw0) 設定（例如「內部網路安全」模式）。

請參閱設定切換介面 (sw0) 設定 第 6-54 頁。

管理路由

Cloud Edge 設備是網路中的安全裝置，所有封包傳輸都會通過它們。您必須熟悉一些基本路由概念，才能正確設定 Cloud Edge 設備。

Cloud Edge 設備具有預先定義的預設靜態路由。當網路流量與任何以策略為基礎的路由規則或已設定的靜態路由皆不相符時，系統會使用預先定義的靜態路由作為 IPv4 預設設備（靜態路由至 0.0.0.0/0），然後套用至所有流量。

除了預先定義的預設靜態路由外，您也可以設定下列組態設定來控制路由流量的方式：

- 以 IPv4 策略為基礎的路由（若要手動控制流量在您環境中的路由方式）
- IPv4 靜態路由
- 每個介面上的 IPv4 預設設備

重要

您必須設定至少一個預設設備來與 Cloud Edge 雲端主控台連線。

Cloud Edge 會選取路由並根據指定的規則動態更新其路由資料表。這樣一組規則可讓 Cloud Edge 決定將封包傳送到目標的最佳路由或路徑。

注意

Cloud Edge 不支援 IPv6 路由。

有關路由的設定位置資訊

您可以使用下列資訊來設定路由，以控制流量在 Cloud Edge 設備上的路由方式：

- 以 IPv4 策略為基礎的路由

  您必須使用 Cloud Edge 內部部署主控台來設定以策略為基礎的路由。如需詳細資訊，請移至新增以策略為基礎的路由 第 7-82 頁。

- IPv4 靜態路由

  您必須使用 Cloud Edge 雲端主控台來設定靜態路由。若要設定靜態路由（包括設備的預設路由），請移至新增靜態路由 第 6-75 頁。

- 每個介面上的 IPv4 預設設備

  若要使用 Cloud Edge 內部部署主控台設定 WAN 或 LAN1 介面上的預設設備，請參閱編輯路由模式的網路介面 第 7-54 頁。

  若要使用 Cloud Edge 雲端主控台設定其他 LAN 介面和 MGMT 介面上的預設設備，請移至路由模式：編輯網路介面 第 6-48 頁。

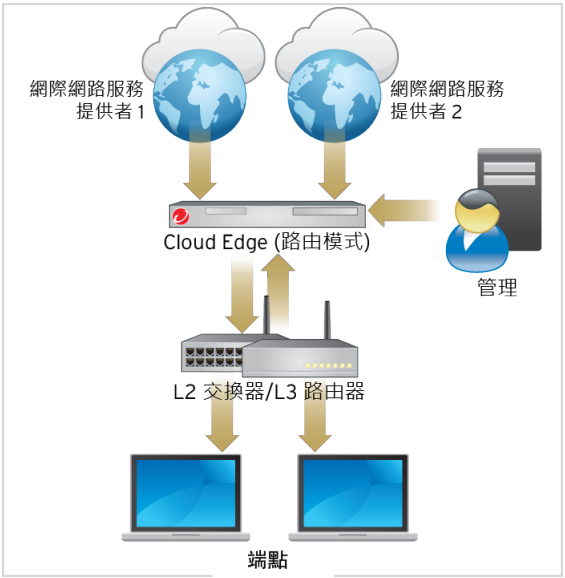
關於以策略為基礎的路由管理

在現今的高效能網路中，組織需要能夠自由地根據本身定義的策略實作封包轉送和路由，同時無須考量傳統路由通訊協定的問題。靜態和動態路由是以流量目標進行路由，而以策略為基礎的路由則提供了標記封包的機制，讓某些類型的流量得以進行差異化路由。以目標為基礎的路由技術難以變更特定流量的路由行為。以策略為基礎的路由又稱為「智慧型路由」，可讓您根據目標網路以外的多項不同條件指定路由行為，包括來源介面、來源或目標位址或服務類型。

假設某間公司在各據點之間有兩個連結，一個是高頻寬低延遲的昂貴連結，另一個則是低頻寬、延遲較高且費用較低的連結。若使用傳統路由通訊協定，就會根據連結的頻寬和/或延遲（使用 EIGRP 或 OSPF）特性計算得到的矩陣節省率，透過較高頻寬的連結傳送絕大部分的流量。以策略為基礎的路由則會將較高優先順序的流量透過高頻寬/低延遲連結進行路由，而透過低頻寬/高延遲連結傳送所有其他流量。

透過以策略為基礎的路由，Cloud Edge 可以路由來自多個 ISP 和 WAN 的流量。下圖顯示如何使用 L2 交換器為兩個 ISP 設定 Cloud Edge。

圖 7-9. 以策略為基礎的路由範例



如果其中一個介面的監控 IP 位址無法使用，與該介面相關的所有以策略為基礎的路由都會關閉。符合以策略為基礎的路由規則的所有流量會透過預設設備路由。若要設定監控 IP 位址，請移至監控主機 第 7-57 頁。如果設定多個預設設備，則會使用循環配置資源選取方式從這些設備路由輸出流量。

在多個 ISP/WAN 環境之間進行自動容錯移轉

當某個 ISP 或 WAN 連線失敗時，Cloud Edge 支援在多個 WAN/ISP 連結之間進行自動容錯移轉。Cloud Edge 會每十 (10) 秒檢查一次連線。如果 Cloud Edge 偵測不到連線，Cloud Edge 會持續每兩 (2) 秒檢查一次。在連續四 (4) 次連線嘗試失敗後，即會開始進行自動容錯移轉。如果稍後建立連線，則連結會自動還原。

當容錯移轉進行時，請執行下列操作：

- 檢視系統事件記錄檔
- 查看路由資料表以確認實際流量路由

注意

如需有關監控主機的詳細資訊，請參閱監控主機 第 7-57 頁。

新增以策略為基礎的路由

如果您想要手動控制流量在環境中的路由方式，可以設定以 IPv4 策略為基礎的路由。

步驟

1. 移至「網路 > 路由 > 策略路由」。
2. 按一下「新增」。
3. 選擇性地啟動規則。
4. 指定長度為 1 到 32 個字元，且包含字母、數字或底線的策略名稱。
5. 輸入說明（選用）。
6. 在「來源位址」下，選取下列其中一個參數：
   - 任意：包含所有來源位址。（預設）
   - 選取的位址：顯示先前設定的來源位址選項清單以及「新增」圖示 ()，以便視需要新增 IPv4 位址物件。

若要設定新的 IP 位址物件，請移至新增策略路由的新 IPv4 位址物件 第 7-83 頁。

7. 從「來源介面」下拉式方塊中選取適當的來源介面。
8. 在「目標位址」下，選取下列其中一個參數：
   - 任意：包含所有目標位址。（預設）
   - 選取的位址：顯示先前設定的目標位址選項清單以及「新增」圖示 ()，以便視需要新增 IPv4 位址物件。

     若要設定新的 IP 位址物件，請移至新增策略路由的新 IPv4 位址物件 第 7-83 頁。
9. 在「服務類型」下，選取下列其中一個參數：
   - 任意：包括所有服務
   - 已選取：僅包括選取的服務
10. 選取出口介面。
11. 針對具有靜態 IP 位址的介面，請指定下一個躍點。
12. 選擇性地啟動網路偽裝。

注意

如果內部 IP 位址必須轉址為出口介面的 IP 位址，請選取「啟動網路偽裝」。

13. 按一下「確定」。

新增策略路由的新 IPv4 位址物件

當您為以策略為基礎的路由設定規則時，可以新增 IPv4 位址物件。

注意

將位址物件新增到策略路由規則時，無法設定 IPv6 位址物件。

步驟

1. 移至「網路 > 路由 > 策略路由」，然後按一下「新增」以開啟「新增策略路由規則」視窗。
2. 在「新增策略路由規則」視窗的「來源位址」或「目標位址」中，選取「選取的位址」。
3. 按一下「新增」。

   「新增/編輯位址物件」畫面隨即開啟。
4. 指定位址物件的名稱。
5. IPv4 是唯一的選項且在「通訊協定」清單方塊中已預先選取。
6. 指定 IP 位址或 CIDR 網路（單一或逗點分隔）。

   進行 IPv4 位址物件的設定時，Cloud Edge 支援單一 IP 位址（'-' 作為範圍標記）以及 IP 位址/網路遮罩 (192.168.1.1/24)。

   範例： 192.168.0.1,10.0.0.1-10.0.0.4,192.168.1.1/24
7. 按一下「確定」。

路由資料表

在原廠預設組態設定中，Cloud Edge 路由資料表包含一個靜態 IPv4 預設路由。透過定義其他 IPv4 靜態路由，可新增路由資訊到路由資料表。資料表可能包含數個路由到相同目標的不同路由，這表示這些路由中指定的下一個躍點路由器的 IPv4 位址或與這些路由相關聯的 Cloud Edge 介面可能不同。

Cloud Edge 會評估路由資料表中的資訊，然後選取到目標的最佳路由，通常是 Cloud Edge 設備與最接近之下一個躍點路由器之間的最短距離。在某些情況下，如果最佳路由不可用，則會選擇距離較長的路由。Cloud Edge 會在裝置的轉送資料表（裝置之路由資料表的子集）中安裝可用的最佳路由。系統會根據轉送資料表中的資訊轉送封包。

注意

Cloud Edge 不支援 IPv6 路由。

檢視路由資料表

步驟

1. 移至「網路 > 路由 > 路由資料表」。
2. 檢視 IPv4 路由。

路由資料表指標

下表說明路由資料表指標。

代碼	定義
K	核心路由
C	已連線
S	靜態

管理 DHCP 與 DDNS 服務

Cloud Edge 設備支援動態主機組態設定通訊協定 (DHCP) 與動態 DNS (DDNS) 服務。

動態主機設定通訊協定 (DHCP)

您可以對 Cloud Edge 設備上的一個或多個 LAN 介面啟動動態主機組態設定通訊協定 (DHCP) 服務。每個啟動了 DHCP 服務的介面均做為 DHCP 伺服器，可指派 IPv4 位址和其他網路設定（例如，預設設備和 DNS (IPv4) 設定）給內部用戶端。

還可以為每個 DHCP 伺服器進行 DCHP 進階伺服器設定（IPv4 位址靜態對應與 DHCP 租用時間）。

如果設有 DHCP 服務的介面收到 DHCP 要求，Cloud Edge 會自動回應這些要求。

- 若要使用 Cloud Edge 內部部署主控台設定 DHCP 服務，請參閱修改 DHCP 服務設定 第 7-87 頁。
- 若要使用 Cloud Edge 雲端主控台設定 DHCP 服務，請參閱編輯 DHCP 設定 第 6-67 頁。

動態 DNS (DDNS)

動態 DNS (DDNS) 會自動即時更新 Internet DNS 名稱伺服器，以將主機名稱的作用中 DNS 組態設定、IPv4 位址與其他資訊保持最新。

您可以在 Cloud Edge 設備的 WAN 介面設定 DDNS 服務。您必須使用 Cloud Edge 雲端主控台來設定動態 DNS。如需詳細資訊，請參閱動態 DNS 第 6-71 頁。

檢視 DHCP 服務與設定

步驟

1. 移至「網路 > 服務 > DHCP」。
2. 在資料表中，檢視與任何 DHCP 服務相關聯的參數：

選項	說明
名稱	DHCP 服務的名稱（範例：LAN1）。
IP 位址/網路遮罩	指派給介面的 IPv4 位址和子網路遮罩。
啟動	圖示表示服務的狀態：已啟動（綠色/開啟）或已關閉（紅色/關閉）。
IP 集區	DHCP 服務可出租給用戶端的適用 IPv4 位址範圍。
選項	DNS 伺服器 IPv4 位址、設備 IPv4 位址和租用時間。只有當 DHCP 伺服器使用指定的 DNS 時，才會顯示 DNS IPv4 位址。

選項	說明
處理行動	按一下圖示可編輯 DHCP 服務設定。

修改 DHCP 服務設定

步驟

1. 視需要檢閱下列資訊：
   - DHCP 的部署模式資訊 第 6-68 頁
   - 預設 DHCP IP 位址集區 第 6-69 頁
2. 移至「網路 > 服務 > DHCP」。
3. 執行下列其中一項作業：
   - 在「名稱」欄，按一下要修改之 DHCP 伺服器的名稱。
   - 在「處理行動」欄，按一下要修改的 DHCP 服務所在列的編輯圖示 ()。
4. 設定 DHCP 設定。

   請參閱預設 DHCP IP 位址集區 第 6-69 頁以瞭解下列各項的相關資訊：
   - 有關您可將其設定為 DHCP 伺服器之介面的部署模式特定資訊。
   - 哪些 IP 位址已依預設指派給各 IP 位址集區。

選項	說明
啟動 DHCP	選取以啟動服務。
IP 位址/網路遮罩	指派給介面的 IPv4 位址和子網路遮罩。
偏好的 DNS	選取偏好的 DNS 方法。

選項	說明
	• 選取「使用系統 DNS 設定」，可使用「網路 > DNS」中所設定的設備系統 DNS。 • 選取「使用介面 IP 位址」，可使用介面 IPv4 位址做為 DNS。 • 選取「使用指定的 DNS 伺服器」，可手動設定 IPv4 位址做為 DNS 設定。
設備	系統會自動根據介面 IPv4 位址和網路遮罩設定填入 DHCP 伺服器設備。您可以選擇性變更 IPv4 設備位址。
IP 位址範圍的起點與終點	指定 IPv4 位址範圍，可建立 DHCP 組態設定適用的 IP 位址集區。 注意 Cloud Edge 不支援 IPv6 位址集區。

5. 設定「進階設定」。

選項	說明
租用時間	對於「租用時間」，調整所租用的 IPv4 位址與網路遮罩不再有效的時間與日期。 指定天數、小時數或分鐘數。例如，如果您僅指定時數，則會限制只能在這個時數內使用租用。

靜態對應	您可以使用靜態對應，手動將靜態 IPv4 位址繫結至特定 MAC 位址。
	
	對於「靜態對應」，指定 MAC 位址/IPv4 位址對應。您可以輸入多個對應。範例：
	
	`00:0C:29:A9:69:25 對應至 192.168.2.1`
	`00-FF-8A-B9-5A-49 對應至 192.168.1.1`

6. 按一下「套用」。
7. 在「網路 > 服務 > DHCP」中，確認設定已變更。

執行管理工作

您可以從 Cloud Edge 設備內部部署主控台執行下列管理工作：

- 選擇使用英文或簡體中文語言設定
- 設定全域系統設定
  - 設定主機名稱和時間設定
  - 管理使用者存取 Cloud Edge 內部部署主控台的方式
  - 設定 Proxy 伺服器設定
- 管理 Cloud Edge 裝置設定
- 執行更新
- 檢視裝置記錄檔
- 執行維護工作
- 執行診斷測試並檢視健全狀況檢查資訊
- 瞭解如何聯絡客服部門

切換語言設定

Cloud Edge 內部部署主控台提供英文和日文語言支援。

步驟

1. 展開 Cloud Edge 內部部署主控台右上角的下拉式清單方塊。
2. 選取適用語言。

管理全域系統設定

您可以管理 Cloud Edge 設備的全域系統設定，例如主機名稱以及時間與日期設定。其他進階設定包括設定 Cloud Edge 內部部署主控台的作業階段逾時和指定 Proxy 伺服器設定。

設定主機名稱與時間設定

您可以從 Cloud Edge 內部部署主控台或使用 Cloud Edge 設備的「快速設定」畫面，為 Cloud Edge 設備設定主機名稱和時間與日期設定。

步驟

1. 登入 Cloud Edge 內部部署主控台。
2. 執行下列其中一個動作：

選項	說明
使用 Cloud Edge 內部部署主控台	移至「管理 > 系統設定 > 一般」標籤。
使用「快速設定」畫面	按一下 Cloud Edge 內部部署畫面右上方的「快速設定」連結，然後移至「系統設定」區段。

3. 設定下列項目：

選項	說明
主機名稱	指定主機名稱。
啟動 NTP 伺服器	如果要與 NTP 伺服器同步處理，請選取此選項，然後在「NTP 伺服器」欄位新增伺服器 IP 位址。
手動設定時間	如果要手動設定時間，請選取此選項，然後在「本機時間」欄位以下列格式指定目前時間：`yyyy-mm-dd hh:mm:ss`。例如：`2015-01-16 13:03:28`
「位置」和「城市」	選取離 Cloud Edge 設備最近的位置與城市，來設定適當的時區。

4. 執行適當的動作。
   - 如果您使用了「一般」標籤，請按一下「套用」。
   - 如果您使用了「快速設定」畫面，請按一下「儲存設定」。

注意

如果 Cloud Edge 設備未向 Cloud Edge 雲端主控台註冊，則按鈕文字為「儲存並註冊」。

進行內部部署主控台設定

Cloud Edge 內部部署主控台設定包括下列選項：

- 閒置逾時：依預設，如果五分鐘內沒有活動發生，Cloud Edge 設備會中斷管理作業階段的連線。建議使用此閒置逾時，以防有人從登入了 Cloud Edge 的電腦使用 Cloud Edge 內部部署主控台，卻又置之不理。您可以視需要調整閒置逾時。
- 憑證：您可以瀏覽至 Cloud Edge 內部部署主控台的 SSL 憑證並加以選取。

設定內部部署主控台逾時

步驟

1. 移至「管理 > 系統設定 > 主控台設定」標籤。
2. 在「閒置逾時」區段，設定所需的作業階段逾時。
3. 按一下「套用」。

進行內部部署主控台憑證設定

步驟

1. 移至「管理 > 系統設定 > 主控台設定」標籤。
2. 在「憑證設定」區段，新增憑證設定。
   - SSL 憑證

- SSL 密碼

3. 按一下「套用」。

設定 Proxy 伺服器設定

您可以設定 Cloud Edge 設備使用 HTTP Proxy 伺服器進行產品更新、使用授權更新、網頁信譽評等查詢和 Cloud Message Scan (CMS)。

步驟

1. 移至「管理 > 系統設定 > Proxy 伺服器設定」標籤。
2. 選取「使用 HTTP Proxy 伺服器」核取方塊。
3. 指定 HTTP Proxy 伺服器 IPv4 位址與通訊埠號碼。
4. 如有必要，請指定伺服器所需的使用者名稱和密碼。
5. 按一下「套用」。

裝置管理

您可以設定裝置管理設定，以遠端管理及監控 Cloud Edge 設備。您也可以提供 Cloud Edge CLI 的存取點。

對管理存取權進行管理

您可以使用 Cloud Edge 設備的內部部署主控台來設定設備，以允許或封鎖用來遠端管理及監控 Cloud Edge 設備的特定類型管理服務（內部部署主控台、Ping、SSH 和 SNMP）。啟動內部部署主控台管理服務可提供登入存取權，讓授權的使用者能夠存取內部部署主控台。

您可以視需要在每個 L3 介面上啟動或關閉各服務。

注意

雖然可以在 WAN 介面上啟動管理服務，但為了取得最佳的安全性，您應該在內部介面上啟動管理服務與流量，以便只能從位於 Cloud Edge 設備後的裝置管理 Cloud Edge 設備。

啟動 SNMP 後，您必須移至「管理 > 裝置管理 > SNMP 設定」來進行 SNMP 設定。在選取的介面上啟動及設定 SNMP 支援後，使用者就可以使用 SNMP 管理程式取得支援的物件資訊。

對於具有無線網路功能的 Cloud Edge 設備，您可以啟動其主要無線網路或客體無線網路的管理存取權。在允許客體無線網路的管理存取權時，請務必注意安全問題。

啟動管理存取權

Cloud Edge 設備支援使用內部部署主控台、Ping、SSH 和 SNMP 進行管理存取。啟動管理存取權可允許使用選取的通訊協定進行遠端存取。

在 Cloud Edge 設備註冊後，您必須使用 Cloud Edge 雲端主控台來啟動或關閉使用內部部署主控台、Ping、SSH 或 SNMP 服務進行管理存取。

步驟

1. 登入 Cloud Edge 雲端主控台。
2. 移至「設備 > （設備名稱） > 管理存取權」。
3. 在表格下的欄位中，指定允許遠端存取設備的 IPv4 位址。

   管理存取權不支援使用 IPv6。

   注意

   此設定決定可遠端存取設備的 IPv4 位址範圍。支援單一 IPv4 位址，並可使用 '-' 符號作為範圍標記。將 IPv4 位址與網路遮罩的格式設定為 `192.168.1.1/24`。若未指定任何項目，將允許所有 IPv4 位址。

4. 選取要為介面啟動的服務。
   - 內部部署主控台

內部部署主控台服務可提供 Cloud Edge 設備內部部署主控台的存取權。

- Ping
- SSH
- SNMP

5. 按一下「儲存」。

接下來需執行的動作

啟動 SNMP 存取權後，您必須使用 Cloud Edge 設備內部部署主控台來設定 SNMP 設定。

請參閱設定 SNMP 設定 第 7-94 頁

設定 SNMP 設定

您必須使用 Cloud Edge 內部部署主控台進行 SNMP 設定。

步驟

1. 登入 Cloud Edge 內部部署主控台。
2. 移至「管理 > 裝置管理 > SNMP 設定」。
3. 選取「啟動 SNMP」核取方塊。
4. 指定 SNMP 設定。

選項	說明
電子郵件信箱	指定聯絡人的電子郵件信箱。
位置	聯絡人的位置，例如「中國辦事處 IT 室」。
社群名稱	指定從 Cloud Edge 擷取資訊時所需的社群字串（預設值：public）。

注意

可在 SNMP 管理程式中檢視 Cloud Edge 設備之聯絡人的電子郵件信箱與位置資訊。

如果已啟動 SNMP 管理功能，使用者可以使用 SNMP 管理程式管理裝置。只有當指定的社群字串是有效的 v2 社群字串時，SNMP 管理程式才能管理設備。

Web Shell

「Web Shell」標籤可讓您存取 Cloud Edge 命令列介面 (CLI) 進行進階組態設定。強烈建議在趨勢科技支援人員的指導下使用 CLI，以避免出現組態設定錯誤。

診斷

您可以執行診斷測試，然後檢視健全狀況檢查結果來疑難排解問題，並辨識出哪些 Cloud Edge 裝置元件是健全狀況良好或健全狀況不佳。您也可以收集並下載診斷檔案。

- 執行封包擷取
- 執行流量追蹤
- 收集並下載檔案
- 檢視健全狀況檢查資訊

檢視健全狀況檢查資訊

您可以從內部部署主控台檢視設備的健全狀況相關資訊。

步驟

1. 登入 Cloud Edge 內部部署主控台。

2. 移至「管理 > 診斷 > 健全狀況檢查」。
3. 檢視設備健全狀況的相關資訊，包括下列項目：

區段	項目	說明
硬體資訊	產品序號	唯讀項目
	Cloud Edge 裝置類型	唯讀項目 裝置類型是 Cloud Edge 型號。
	Cloud Edge 韌體版本	唯讀項目
系統資源	系統溫度	顯示目前狀態
	系統磁碟使用率	
	資料磁碟使用率	
網路介面狀態	所有網路介面的清單	狀態：上線或離線 包含主要網路的狀態。 還包含支援無線網路功能之 Cloud Edge 設備的客體無線網路狀態。
服務狀態	自動註冊模組	狀態：執行中或錯誤
	DHCP 服務	狀態：執行中、錯誤或關閉
	活動訊號模組	狀態：執行中、錯誤或無
	L2TP VPN 服務	狀態：執行中、錯誤、關閉或無
	記錄檔上傳模組	狀態：執行中或錯誤
	郵件掃瞄服務	狀態：執行中或錯誤
	NTP 服務	狀態：執行中、錯誤或關閉
	掃瞄服務	狀態：執行中或錯誤

區段	項目	說明
	系統監控模組	狀態：執行中或錯誤
	Site-to-Site VPN 服務	狀態：執行中、錯誤、關閉或無
	SSL VPN 服務	狀態：執行中、錯誤、關閉或無
	使用者驗證模組	狀態：執行中或錯誤

還原軟體修補程式

步驟

1. 在內部部署主控台中，移至「管理 > 更新 > 軟體修補程式」。
2. 選取您要還原的已套用修補程式，然後按一下「還原」。

原廠設定

還原原廠設定會將 Cloud Edge 設備重設為預設網路設定，並清除所有記錄檔和資料庫資訊。

還原原廠設定的使用案例：

- Cloud Edge 設備硬碟已滿。
- 在不同客戶位置使用 Cloud Edge 設備。
- 當客戶不再使用 Cloud Edge 設備時，將資料移除以滿足符合性需求。

還原原廠設定

警告!

還原原廠設定會刪除儲存在 Cloud Edge 設備中的所有記錄檔和資料庫資訊。這些資訊無法還原。

步驟

1. 關閉 Cloud Edge 設備的電源。
2. 按住位於背面的重設按鈕。

   重設按鈕位於 Cloud Edge 設備背面的 AC 電源插座和 USB 通訊埠之間。
3. 重新開啟 Cloud Edge 設備的電源。
4. 放開重設按鈕，直到設備上的黃色 LED 指示燈重新開始閃爍。

   黃色 LED 指示燈會閃爍約 2 分鐘。當 Cloud Edge 設備重新啟動時，即已還原原廠設定。

第 8 章

技術支援

瞭解下列主題：

疑難排解資源

聯絡技術支援之前，請考慮造訪下列趨勢科技線上資源。

使用支援入口網站

趨勢科技支援入口網站是全年無休的線上資源，包含有關常見和不常見問題的最新資訊。

步驟

1. 移至「https://success.trendmicro.com/tw/business-support」。
2. 從可用產品中進行選取，或請點選適當的按鈕來搜尋解決方案。
3. 使用「搜尋支援」方塊搜尋可用的解決方案。
4. 如果未找到解決方案，請點選「聯絡支援」，然後選取所需的支援類型。

秘訣

若要線上提交支援案例，請造訪下列 URL：

https://success.trendmicro.com/tw/sign-in

趨勢科技支援工程師會在 24 小時或更短時間內調查案例並對其進行回應。

安全威脅百科全書

現今的大多數惡意程式都包含混合安全威脅（合併了兩種或更多種技術），以略過電腦安全通訊協定。趨勢科技會使用建立自訂防範策略的產品來抵禦此複雜惡意程式。安全威脅百科全書提供了多種混合性安全威脅的名稱和癥狀的完整清單，包括已知惡意程式、垃圾郵件、惡意 URL 和已知弱點。

移至 https://www.trendmicro.com/vinfo/tw/threat-encyclopedia/malware/ 以瞭解更多資訊：

- 目前正在使用中或「擴散中」的惡意程式和惡意可攜式程式碼。
- 用於形成完整網頁攻擊過程的關聯安全威脅資訊頁面
- 有關目標攻擊和安全威脅的 Internet 安全威脅諮詢
- 網頁攻擊和線上趨勢資訊
- 每週惡意程式報告

聯絡趨勢科技

可以透過電話或電子郵件聯絡趨勢科技代表：

地址	趨勢科技股份有限公司 台北市敦化南路二段 198 號 8 樓
電話	(886) 2-23789666
網站	https://www.trendmicro.com
電子郵件信箱	企業授權用戶技術專線 Web mail：http://www.trend.com.tw/corpmail/

- 全球客戶服務據點：

  https://www.trendmicro.com/us/about-us/contact/index.html

  與台灣趨勢科技聯絡：

  http://www.trendmicro.tw/tw/about-us/contact/index.html

- 趨勢科技產品文件：

  https://docs.trendmicro.com/zh-tw/home.aspx

加速支援要求

為了提高解決問題的速度，現已提供下列資訊：

- 問題模擬的步驟
- 裝置或網路資訊
- 電腦品牌、型號以及連接的任何其他硬體或裝置
- 記憶體大小和可用硬碟空間
- 作業系統和 Service Pack 版本
- 安裝的用戶端版本
- 產品序號或啟動碼
- 安裝環境的詳細說明
- 已接收的任何錯誤訊息的確切文字

將可疑內容傳送到趨勢科技

有多個選項可供將可疑內容傳送到趨勢科技，以便進一步分析。

電子郵件信譽評等服務

查詢特定 IP 位址的信譽評等，並指定一個訊息轉移用戶端，以將其包含在全域核可清單中：

https://servicecentral.trendmicro.com/en-us/ers/

請參閱下列「常見問題集」項目，將訊息範例傳送給趨勢科技：

https://success.trendmicro.com/tw/solution/1112106

檔案信譽評等服務

收集系統資訊並將可疑檔案內容提交到趨勢科技：

https://success.trendmicro.com/tw/solution/1059565

記錄案例編號以供追蹤。

網頁信譽評等服務

查詢疑似網路釣魚網站的 URL 的安全分級和內容類型，或其他所謂「病媒」（間諜程式和惡意程式等 Internet 威脅的蓄意來源）：

https://global.sitesafety.trendmicro.com/

如果指定的分級不正確，請傳送重新分類要求到趨勢科技。

其他資源

除了解決方案和支援外，線上還提供許多其他實用資源，可讓您保持最新狀態、瞭解創新以及最新的安全趨勢。

下載專區

有時，趨勢科技可能會針對報告的已知問題發行修補程式，或是發行適用於特定產品或服務的升級。如果要瞭解是否有適用的修補程式，請移至：

https://downloadcenter.trendmicro.com/index.php?regs=tw

如果未套用修補程式（修補程式已過期），請開啟 Readme 檔以判斷其是否與您的環境相關。Readme 檔還包含安裝說明。

文件意見反應

趨勢科技始終力求改善其文件。如果您對本文件或趨勢科技的任何文件有任何疑問、意見或建議，請透過 https://docs.trendmicro.com/en-us/survey.aspx 聯絡我們。

索引

十四畫

趨勢科技股份有限公司
台北市敦化南路二段 198 號 8 樓
電話：(886) 2-23789666　傳真：(886) 2-23780993
Web mail: http://www.trend.com.tw/corpmail/

www.trendmicro.com
Item Code: APTM09748/230625