GlobalProtect 管理者指南

Version 9.1

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

June 4, 2020

Table of Contents

GlobalProtect 概要

無論是在家裡檢查電子郵件還是在機場更新公司文件，多數員工如今都在公司的實體範圍外工作。隨著這類行動辦公的普及，雖能提升生產力與靈活性，但安全性風險卻也跟著水漲船高。每次使用者帶著他們的筆記型電腦或智慧型手機離開辦公室時，都會越過專為保護使用者與網路所設計的公司防火牆與相關原則。GlobalProtect™ 能將原先受實體限制所侷限的次世代防火牆原則一舉延伸至每位使用者，無論其身在何方，都能協助他們在漫遊時克服眼前的安全性挑戰。

以下幾節針對 Palo Alto Networks GlobalProtect 所供應的產品提供其概念性資訊，並說明 GlobalProtect 的元件與各種部署方案：

- 關於 GlobalProtect 元件
- GlobalProtect 支援的作業系統版本為何？
- GlobalProtect 支援什麼功能？
- 關於 GlobalProtect 授權

關於 GlobalProtect 元件

GlobalProtect 提供完整基礎結構讓您管理行動工作者，讓所有使用者不管使用什麼端點或身在何處，都能夠安全地進行存取。此基礎結構包含下列元件：

- GlobalProtect 入口網站
- GlobalProtect 閘道
- GlobalProtect App

GlobalProtect 入口網站

GlobalProtect 入口網站提供 GlobalProtect 基礎結構的管理功能。參與 GlobalProtect 網路的每個端點都會收到入口網站的設定資訊，包括可用閘道的相關資訊，以及連線到 GlobalProtect 閘道可能需要的任何用戶端憑證。此外，無論是 macOS 或是 Windows 端點，入口網站都能為其控制 GlobalProtect 應用程式軟體的行為和散佈（在行動端點上，GlobalProtect 應用程式透過 Apple App Store（iOS 端點）、Google Play（Android 端點）、Chromebooks 及 Microsoft Store（Windows 10 UWP 端點）散佈）。如果使用主機資訊設定檔 (HIP) 功能，入口網站也能定義要從主機收集的資訊種類，您完全可以依照需求自訂。在任何 Palo Alto Networks 新一代防火牆上的介面上，您都可以設定對 GlobalProtect 入口網站的存取。

GlobalProtect 閘道

GlobalProtect 閘道為 GlobalProtect 應用程式的流量提供強制執行的安全性功能。此外，如果已啟用 HIP 功能，閘道會從原始主機資料產生 HIP 報告，應用程式會提交此資訊並可將其用於強制執行原則。您可以設定不同的閘道類型，為遠端使用者提供強制執行的安全性功能及/或虛擬私人網路 (VPN) 存取，也可以為內部資源存取套用安全性原則。

在任何 Palo Alto Networks 新一代防火牆上的介面上，您都可以設定 GlobalProtect 閘道。您可以在同一個防火牆上執行閘道與入口網站，也可以在整個企業中擁有多個分散式閘道。

GlobalProtect App

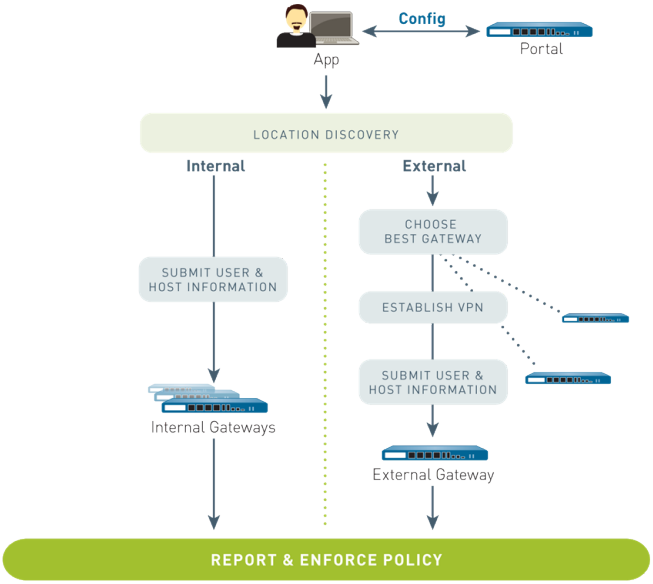
GlobalProtect 應用程式軟體在端點上執行，並可讓您透過已部署的 GlobalProtect 入口網站與閘道存取網路資源。

適用於 Windows 與 macOS 端點的 GlobalProtect 應用程式可從 GlobalProtect 入口網站部署。您可以在定義於入口網站上的用戶端組態中設定應用程式的行為，例如使用者可以看到的頁籤。詳情請參閱定義 GlobalProtect 代理程式組態、自訂 GlobalProtect 應用程式和部署 GlobalProtect 應用程式軟體。

適用於各種行動端點（iOS、Android 及 Windows UWP）的 GlobalProtect 應用程式可透過相關端點的官方商店取得—iOS 為 Apple App Store、Android 為 Google Play、Windows UWP 為 Microsoft Store。您也可以使用 AirWatch 部署 GlobalProtect 行動應用程式，AirWatch 是一個協力廠商行動端點管理系統。

如需更多詳細資訊，請參閱 GlobalProtect 支援的作業系統版本為何？

下圖說明 GlobalProtect 入口網站、閘道與應用程式如何一起合作，好讓所有使用者不管使用何種端點或身在何處都能夠安全地進行存取。



GlobalProtect 支援的作業系統版本為何？

常見的桌上型電腦、筆記型電腦、平板電腦和智慧型手機支援 GlobalProtect 應用程式。我們建議您在執行 PAN-OS 6.1 或更新版本上的防火牆上設定 GlobalProtect，並且您的一般使用者僅在端點上安裝支援的 GlobalProtect 應用程式版本。最低 GlobalProtect 應用程式版本隨作業系統而異；若要確定特定作業系統的最低 GlobalProtect 應用程式版本，請參見 Palo Alto Networks® 相容表中的下列主題：

- 我可以在哪裡安裝 GlobalProtect 應用程式？
- X-Auth IPSec 用戶端支援什麼？

GlobalProtect 應用程式的較早版本仍在作業系統和發布的 PAN-OS 上獲得支援。有關支援的最低 PAN-OS 版本，請參閱軟體更新網站上特定版本對應的 GlobalProtect 應用程式版本資訊。

關於 GlobalProtect 授權

如果您想使用 GlobalProtect 來透過單一或多個內部/外部閘道提供安全的遠端存取或虛擬私人網路 (VPN) 解決方案，那麼您無需任何 GlobalProtect 授權。但是，若要使用某些更進階的功能，例如 HIP 檢查和相關內容更新、GlobalProtect 行動應用程式支援或 IPv6 支援，則您必須購買年度 GlobalProtect 訂閱。此授權必須安裝在執行閘道的每個防火牆上，閘道負責：

- 執行 HIP 檢查
- 支援行動端點的 GlobalProtect 應用程式
- 支援 Linux 端點的 GlobalProtect 應用程式
- 提供 IPv6 連線
- 根據目的地網域、應用程式處理序名稱或 HTTP/HTTPS 視訊串流應用程式分割通道流量。

對於 GlobalProtect 無用戶端 VPN，您還必須從 GlobalProtect 入口網站在代管無用戶端 VPN 的防火牆上安裝 GlobalProtect 訂閱。您還需要 **GlobalProtect Clientless VPN**（**GlobalProtect** 無用戶端 **VPN**）動態更新才能使用此功能。

功能	需要訂閱？
單一外部閘道（Windows 與 macOS）	—
單一或多個內部閘道	—
多個外部閘道	—
物聯網 (IoT) 裝置	—
HIP 檢查	✓
基於端點機器憑證、端點序號及軟體和應用程式設定的代理程式組態 （只有在與 HIP 檢查一起使用時，才需要 GlobalProtect 訂閱）	✓
基於端點狀態的基於 HIP 的原則強制執行	✓
執行 Windows 和 macOS 的端點的應用程式	—
執行 iOS、Android、Chrome OS 及 Windows 10 UWP 的端點的行動應用程式	✓
執行 Linux 的端點的應用程式	✓
外部閘道 IPv6	✓
內部閘道 IPv6 （變更為預設行為—需要 GlobalProtect 應用程式 4.1.3 及以上版本，本例中無需 GlobalProtect 訂閱）	—
無用戶端 VPN	✓

功能	需要訂閱？
根據目的地網域、用戶端處理序和視訊串流應用程式分割通道	✓

如需在防火牆上安裝授權的相關資訊，請參閱啟動授權。

開始

若要使 GlobalProtect™ 能夠正常執行，您必須設定基礎結構，使其允許所有元件進行通訊。從基本層面來講，也就是設定 GlobalProtect 一般使用者將要與之連線以存取入口網站與閘道的介面與區域。由於 GlobalProtect 元件透過安全通道進行通訊，因此您必須為各種元件取得並部署所有必要的 SSL 憑證。以下幾節引導您設定 GlobalProtect 基礎結構：

- 為 GlobalProtect 建立介面與區域
- 在 GlobalProtect 元件之間啟用 SSL

為 GlobalProtect 建立介面與區域

您必須為您的 GlobalProtect 基礎結構設定下列介面與區域：

- **GlobalProtect** 入口網站—需要可供 GlobalProtect 應用程式連線的 Layer 3 介面或回送介面。如果入口網站與閘道位於同一個防火牆上，它們便可以使用相同介面。入口網站必須位於可從您網路外部存取的區域，例如 DMZ。
- **GlobalProtect** 閘道—閘道的介面與區域取決於您所設定之閘道為外部閘道或是內部閘道，如下所示：
  - 外部閘道—需要可供應用程式建立連線的 Layer 3 或回送介面與邏輯通道介面。Layer 3/回送介面必須位於外部區域，例如 DMZ。通道介面可與連線您的內部資源的界面處於同一區域（例如 **trust**）。為獲得加強的安全性和更好的可見性，您可以建立獨立的區域，如 **corp-vpn**。如果為通道介面建立不同的區域，您必須建立安全原則，以使流量能夠在 VPN 區域與信任區域之間流動。
  - 內部閘道—在您的信任區域中需要第 3 層或回送介面。您也可以建立通道介面以用於存取內部閘道，但並非必須這樣做。

如需使用回送介面來為不同連接埠與位址的 *GlobalProtect* 提供存取權的方法提示，請參閱是否可以將 GlobalProtect 入口網站頁面設定為可在任何連接埠存取？

如需入口網站與閘道的詳細資訊，請參閱關於 GlobalProtect 元件。

STEP 1 | 針對您計畫部署的每個入口網站與/或閘道設定一個 Layer 3 介面。

如果閘道與入口網站位於相同的防火牆，則您可以使這兩者使用同一個介面。

最佳作法是將入口網站與閘道設定為使用靜態 *IP* 位址。

在您已設定 *GlobalProtect* 入口網站或閘道的介面上，請勿附加允許 *HTTP*、*HTTPS*、*Telnet* 或 *SSH* 的介面管理設定檔，因為這會啟用從網際網路存取管理介面的存取權。請遵照保護管理存取權的最佳做法，來確保您可以保障防火牆的管理存取權，以防攻擊成功。

1. 選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet** 或 **Network**（網路）> **Interfaces**（介面）> **Loopback**（回送）然後選取您要為 GlobalProtect 設定的介面。在此範例中，我們將 **ethernet1/1** 設定為入口網站介面。
2. （僅限 Ethernet）將 **Interface Type**（介面類型）設定為 **Layer3**。
3. 在 **Config**（設定）頁籤上選取入口網站或閘道介面所屬的 **Security Zone**（安全性區域），如下所述：
   - 將入口網站與外部閘道置於不信任區域以供網路之外的主機存取，例如 **l3-untrust**。
   - 將內部閘道置於內部區域，例如 **l3-trust**。
   - 如果您尚未建立區域，請新增 **New Zone**（新區域）。在 [區域] 對話方塊中，定義新區域的 **Name**（名稱），然後按一下 **OK**（確定）。
4. 選取預設 **Virtual Router**（虛擬路由器）。
5. 為介面指派 IP 位址：
   - 對於 IPv4 位址，選取 **IPv4**，然後 **Add**（新增）要指派給介面的 IP 位址和網路遮罩，例如 203.0.11.100/24。
   - 對於 IPv6 位址，選取 **IPv6**，**Enable IPv6 on the interface**（在介面上啟用 **IPv6**），然後 **Add**（新增）要指派給介面的 IP 位址和網路遮罩，例如 2001:1890:12f2:11::10.1.8.160/80。

6. 按一下 **OK**（確定）儲存介面組態。

STEP 2 | 在裝載 GlobalProtect 閘道的防火牆上設定邏輯通道介面，該介面將會終止 GlobalProtect 應用程式所建立的 VPN 通道。

通道介面不需要 *IP* 位址，除非您需要動態路由。此外，如能將 *IP* 位址指定給通道介面，為連線問題進行疑難排解時將會很有用。

確定在 *VPN* 通道終止的區域中啟用 *User-ID*。

1. 選取 **Network**（網路）> **Interfaces**（介面）> **Tunnel**（通道），然後 **Add**（新增）通道介面。
2. 在 **Interface Name**（介面名稱）欄位中，輸入數值尾碼，例如 **.2**。
3. 在 **Config**（組態）頁籤中，選取 VPN 通道終止的 **Security Zone**（安全性區域），如下所示：
   - 若要使用您的信任區域作為通道的終止點，請從下拉式清單中選取該區域。
   - （建議）若要為另外建立一個區域終止 VPN，請新增 **New Zone**（新區域）。在區域對話方塊中，定義新區域的 Name（名稱）（例如 corp-vpn），**Enable User Identification**（啟用使用者識別），然後按一下 **OK**（確定）。
4. 將 **Virtual Router**（虛擬路由器）設定為 **None**（無）。
5. 為介面指派 IP 位址：
   - 對於 IPv4 位址，選取 **IPv4**，然後 **Add**（新增）要指派給介面的 IP 位址和網路遮罩，例如 203.0.11.100/24。
   - 對於 IPv6 位址，選取 **IPv6**，**Enable IPv6 on the interface**（在介面上啟用 **IPv6**），然後 **Add**（新增）要指派給介面的 IP 位址和網路遮罩，例如 2001:1890:12f2:11::10.1.8.160/80。
6. 按一下 **OK**（確定）儲存介面組態。

STEP 3 | 如果您已經建立另外的區域讓通道終止 VPN 連線，請建立安全性原則讓流量在 VPN 區域與您的信任區域之間流動。

例如，下列政策規則即可在 **corp-vpn** 區域與 **l3-trust** 區域之間實現流量。

	Name	Tags	Source				Destination		Application	Service	Action
			Zone	Address	User	HIP Profile	Zone	Address			
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 4 | **Commit**（提交）組態。

在 GlobalProtect 元件之間啟用 SSL

GlobalProtect 元件之間所有的互動都是透過 SSL/TLS 連線發生的。因此，在設定每個元件之前，您必須先產生及/或安裝必要憑證，以便您可以參考設定中的適當憑證。下列各節說明各種 GlobalProtect 憑證的支援憑證部署方法、說明及最佳做法指南，並提供產生與部署必要憑證的指示：

- 關於 GlobalProtect 憑證部署
- GlobalProtect 憑證最佳做法
- 將伺服器憑證部署至 GlobalProtect 元件

關於 GlobalProtect 憑證部署

透過以下三種基本方法，可以 為 GlobalProtect 元件部署伺服器憑證：

- （建議）組合協力廠商憑證與自我簽署的憑證—由於 GlobalProtect 應用程式將會在 GlobalProtect 設定之前存取入口網站，因此應用程式必須信任憑證才能建立 HTTPS 連線。
- 企業憑證授權—如果您已擁有自己的企業 CA，您可以使用此內部 CA 來針對每個 GlobalProtect 元件簽發憑證，然後再將其匯入到裝載您入口網站與閘道的防火牆上。端點必須連線至某些 GlobalProtect 服務，在此情況下，您還必須確保它們均已信任針對這些服務簽發憑證的根 CA 憑證。
- 自我簽署的憑證—您可以在入口網站產生自我簽署的 CA 憑證，並使用它來為所有 GlobalProtect 元件簽發憑證。不過，此解決方案相較於其他方法而言較不安全，因此不建議使用。如果您選擇此方法，一般使用者將會在第一次連線至入口網站時看到憑證錯誤。若要防止此錯誤發生，您可以透過手動方式或使用某種類型的集中式部署（例如 Active Directory 群組原則物件 (GPO)），將自我簽署的根 CA 憑證部署至所有端點。

GlobalProtect 憑證最佳做法

下表根據您要使用的功能摘要列出了您將需要的 SSL/TLS 憑證：

憑證	使用方式	發出程序/最佳作法
CA 憑證	用來簽署發出給 GlobalProtect 元件的憑證。	如果您計劃使用自我簽署憑證，請使用專用 CA 伺服器或 Palo Alto Networks 防火牆產生 CA 憑證，然後簽發由 CA 或中繼簽署的 GlobalProtect 入口網站和閘道憑證。
入口網站伺服器憑證	可讓 GlobalProtect 應用程式建立與入口網站的 HTTPS 連線。	• 此憑證在 SSL/TLS 服務設定檔中被識別。您可以透過在入口網站組態中選取其相關服務設定檔，來指派入口網站伺服器憑證。 • 從已知的協力廠商 CA 使用憑證。這是最安全的方法，而且可以確保使用者端點能夠建立與入口網站之間的信任關係，而不需要您部署根 CA 憑證。 • 如果您未使用已知的、公開 CA，您應匯出用於產生入口網站伺服器憑證的根 CA 憑證至所有運行 GlobalProtect 應用程式的端點。匯出此憑證防止一般使用者在初始入口網站登入時看到憑證警告。 • 憑證的通用名稱 (CN) 及主體別名 (SAN) 欄位，必須符合裝載入口網站之介面的 IP 位址或 FQDN。 • 一般而言，每個入口網站都必須擁有它自己的伺服器憑證。但是，如果在相同的介面上部署單一閘道與入口網站，則您必須為閘道和入口網站使用相同的憑證。

憑證	使用方式	發出程序/最佳作法
		• 如果您在相同的介面設定閘道與入口網站，我們也建議您對閘道與入口網站都使用相同的憑證設定檔與 SSL/TLS 服務設定檔。如果它們未使用相同的憑證設定檔與 SSL/TLS 服務設定檔，閘道設定會認為在 SSL 交握期間入口網站的設定比較重要。
閘道伺服器憑證	可讓 GlobalProtect 應用程式建立與閘道的 HTTPS 連線。	• 此憑證在 SSL/TLS 服務設定檔中被識別。您可以透過在閘道組態中選取其相關服務設定檔，來指派閘道伺服器憑證。 • 在防火牆或 CA 伺服器上產生 CA 憑證，並使用該 CA 憑證來產生所有閘道憑證。 • 憑證的 CN 及 SAN 欄位，必須符合您要用來設定閘道之介面的 FQDN 或 IP 位址。 • 入口網站可以根據組態將閘道根 CA 憑證散佈至 GlobalProtect 應用程式（入口網站組態代理程式頁籤中受信任的根 CA 清單）。但是，將閘道根 CA 憑證預先安裝在使用者受信任的憑證存放區或由公共 CA 簽發閘道憑證並不是必要的。 • 一般而言，每個閘道都必須擁有它自己的伺服器憑證。但是，如果在相同的介面上部署單一閘道與入口網站以供基本 VPN 存取，則您必須為兩個元件使用單一伺服器憑證。作為最佳做法，請使用公用 CA 簽署的憑證。 • 如果您在相同的介面設定閘道與入口網站，我們也建議您對閘道與入口網站都使用相同的憑證設定檔與 SSL/TLS 服務設定檔。如果它們未使用相同的憑證設定檔與 SSL/TLS 服務設定檔，閘道設定會認為在 SSL 交握期間入口網站的設定比較重要。

（選用）用戶端憑證	用來在 GlobalProtect 應用程式與閘道/入口網站之間實現 HTTPS 工作階段確立的相互驗證。這可確保只有具備有效用戶端憑證的端點可以驗證和連線網路	• 如需對用戶端憑證進行簡易部署，請將入口網站設定為在透過下列方法之一成功登入時將用戶端憑證部署至應用程式。
		  • 使用所有接收相同組態的 GlobalProtect 應用程式上的單一用戶端憑證。透過上傳憑證至入口網站並在入口網站代理程式組態中將其選取，指派 **Local**（本機）用戶端憑證。
		  • 使用簡單憑證註冊協定 (**SCEP**) 以啟用 GlobalProtect 入口網站，從而部署唯一的用戶端憑證至您的 GlobalProtect 應用程式。透過設定 SCEP 設定檔啟用，然後選取入口網站代理程式組態中的設定檔。
		• 當您為 GlobalProtect 端點：sha1、sha256、sha384 或 sha512 產生用戶端憑證時，使用下列摘要演算法之一。
		• 驗證一般使用者時，您可以使用其他機制將唯一用戶端憑證部署至每個端點。
		• 請考慮在沒有用戶端憑證的情況下先測試您的設定，並在確定其他設定均正確之後，再新增用戶端憑證。

憑證	使用方式	發出程序/最佳作法
（選用）電腦憑證	機器憑證是簽發給本機機器存放區或系統金鑰鏈中端點的用戶端憑證。各電腦憑證會識別主旨欄位（例如 CN=laptop1.example.com）內的端點，而非使用者。憑證確保僅受信任的端點可連線至閘道或入口網站。 透過預登入連線方法設定的使用者需要電腦憑證。	• 當您為 GlobalProtect 端點：sha1、sha256、sha384 或 sha512 產生用戶端憑證時，使用下列摘要演算法之一。 • 如果您要使用預先登入功能，必須在啟用 GlobalProtect 存取之前，先使用您自己的 PKI 基礎結構來將電腦憑證部署至每個端點。此方法對確保安全非常重要。 如需更多訊息，請參閱透過預登入遠端存取 VPN。

表格：GlobalProtect 憑證需求

如需用於在 GlobalProtect 端點、入口網站與閘道之間安全通訊的金鑰類型詳細資訊，請參閱 參考：GlobalProtect 應用程式加密功能 。

將伺服器憑證部署至 GlobalProtect 元件

以下表格顯示了將 SSL/TLS 憑證部署至 GlobalProtect 元件的最佳做法步驟：

- 從已知的協力廠商 CA 匯入伺服器憑證。

  針對 *GlobalProtect* 入口網站使用知名協力廠商 *CA* 的伺服器憑證。此作法確保一般使用者可以建立 *HTTPS* 連線，而不會直接看到關於不受信任憑證的警告。

  憑證的 *CN* 及 *SAN* 欄位（如果適用），必須符合您要用來設定入口網站的介面或協力廠商行動端點管理系統上裝置簽入介面的 *FQDN* 或 *IP* 位址。支援萬用字元比對功能。

  您匯入憑證之前，請確保憑證與金鑰檔案可從您的管理系統存取，而且您擁有用來解密私人金鑰的複雜密碼：

  1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證），然後 **Import**（匯入）新的憑證。
  2. 使用 **Local**（本機）憑證類型（預設值）。
  3. 輸入 **Certificate Name**（憑證名稱）。
  4. 輸入接收自 CA 的 **Certificate File**（憑證檔案）的路徑與名稱，或 **Browse**（瀏覽）以尋找檔案。
  5. 將 **File Format**（檔案格式）設定為 **Encrypted Private Key and Certificate (PKCS12)**（加密私人金鑰及憑證 **(PKCS12)**）。
  6. 在 **Key File**（金鑰檔案）欄位中輸入 PKCS#12 檔案的路徑與名稱，或 **Browse**（瀏覽）以尋找該檔案。
  7. 輸入用於加密私密金鑰的 **Passphrase**（複雜密碼），並重新輸入。
  8. 按一下 **OK**（確定）匯入憑證和金鑰。

- 建立用來針對 GlobalProtect 元件簽發自我簽署憑證的根 CA 憑證。

  在入口網站建立根 *CA* 憑證，並使用該憑證為閘道及選擇性針對用戶端簽發伺服器憑證。

  在部署自我簽署的憑證之前，您必須建立根 CA 憑證，用於為 GlobalProtect 元件簽署憑證：

1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證），然後 **Generate**（產生）新的憑證。
2. 使用 **Local**（本機）憑證類型（預設值）。
3. 輸入 **Certificate Name**（憑證名稱），例如 GlobalProtect_CA。憑證名稱不能包含空格。
4. 請勿選取 **Signed By**（簽署者）欄位中的值。無需選取 **Signed By**（簽署者），憑證自我簽署。
5. 啟用 **Certificate Authority**（憑證授權單位）選項。
6. 按一下 **OK**（確定）即可產生憑證。

- 使用入口網站上的根 CA，以建立自我簽署伺服器憑證。

請為您計劃部署的各閘道建立伺服器憑證，並選取協力廠商行動端點管理系統的管理介面（如果此為閘道擷取 *HIP* 報告的介面）。

在閘道伺服器憑證中，*CN* 和 *SAN* 欄位內的值必須一致。如果值不同，*GlobalProtect* 代理程式會偵測不符，並且不會信任憑證。如果您新增 *Host Name*（主機名稱）屬性，自我簽署的憑證將只包含 *SAN* 欄位。

或者，您可以使用簡單憑證註冊通訊協定 (SCEP) 以請求來自您企業的 CA 伺服器憑證。

1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證），然後 **Generate**（產生）新的憑證。
2. 使用 **Local**（本機）憑證類型（預設值）。
3. 輸入 **Certificate Name**（憑證名稱）。此名稱不能包含空格。
4. 在 **Common Name**（通用名稱）欄位中，輸入您要設定閘道的 FQDN（建議）或 IP 位址。
5. 在 **Signed By**（簽署者）欄位中，選取您建立的 GlobalProtect_CA。
6. 在憑證屬性區域，**Add**（新增）並定義用來唯一識別閘道的屬性。請記住，如果您新增 **Host Name**（主機名稱）屬性（會填入憑證的 SAN 欄位），則必須與您為 **Common Name**（通用名稱）定義的值完全符合。
7. 為伺服器憑證進行加密設定，包括加密 **Algorithm**（演算法）、金鑰長度（**Number of Bits**（位元數））、**Digest**（摘要）演算法和 **Expiration**（過期）（以天為單位）。
8. 按一下 **OK**（確定）即可產生憑證。

- 使用簡單憑證註冊通訊協定 (SCEP) 以請求來自您企業的 CA 伺服器憑證。

針對您計畫部署的每個入口網站與閘道設定獨立的 *SCEP* 設定檔。然後使用特定 *SCEP* 設定檔以建立各 *GlobalProtect* 元件的伺服器憑證。

在入口網站和閘道伺服器憑證中，*CN* 欄位值必須包括 *FQDN*（建議）或介面的 *IP* 位址，您可以在此計劃設定入口網站或閘道，且必須與 *SAN* 欄位一致。

為了符合美國聯邦資訊處理標準 *(FIPS)*，您還必須啟用 *SCEP* 伺服器和 *GlobalProtect* 入口網站之間的相互 *SSL* 驗證。（*FIPS-CC* 操作顯示於防火牆登入頁面及其狀態列。）

在您提交了組態後，入口網站嘗試透過 SCEP 設定檔內的設定請求 CA 憑證。如果成功，裝載入口網站的防火牆會儲存 CA 憑證，並在 **Device Certificates**（裝置憑證）清單中顯示。

1. 為各 GlobalProtect 入口網站或閘道設定 SCEP 設定檔：
    1. 輸入 **Name**（名稱），識別您部署伺服器憑證的 SCEP 設定檔和元件。如果此設定檔適用於具有多重虛擬系統功能的防火牆，請選取一個虛擬系統或 **Shared**（共用）作為設定檔可用的 **Location**（位置）。

2. （選用）設定 **SCEP Challenge**（**SCEP** 挑戰），這是 PKI 和各憑證請求的入口網站之間的回應機制。使用您從 SCEP 伺服器獲取的 **Fixed**（固定）挑戰密碼或 **Dynamic**（動態）密碼，入口網站-用戶端提交使用者名稱和您選取的 OTP 至 SCEP 伺服器。對於動態 SCEP 挑戰，這可以是 PKI 管理員的憑證。
3. 設定入口網站用於連線 PKI 中 SCEP 伺服器的 **Server URL**（伺服器 **URL**）（例如 **`http://10.200.101.1/certsrv/mscep/`**）。
4. 在 **CA-IDENT Name**（**CA-IDENT** 名稱）欄位中輸入字串（長度最大為 255 個字元），用以識別 SCEP 伺服器。
5. 輸入 SCEP 伺服器所產生之憑證使用的 **Subject**（主旨）名稱。主旨必須包含格式 CN=<`value`> 中的普通名稱 (CN) 金鑰，其中 <`value`> 是入口網站或閘道的 FQDN 或 IP 位址。
6. 選取 **Subject Alternative Name Type**（主旨替代名稱類型）：如要在憑證的主旨或主旨替代副檔名輸入電子郵件名稱，選取 **RFC 822 Name**（**RFC 822** 名稱）。您也可以輸入 **DNS Name**（**DNS** 名稱）以用於評估憑證，或 **Uniform Resource Identifier**（統一資源識別項）以識別來自用戶端獲得憑證的資源。
7. 設定其他加密設定，包括憑證簽署要求的金鑰長度（**Number of Bits**（位元數））和 **Digest**（摘要）演算法。
8. 設定憑證允許的用途，用於簽署（**Use as digital signature**（用作數位簽章））或加密（**Use for key encipherment**（用作金鑰加密））。
9. 若要確保入口網站連線至正確的 SCEP 伺服器，請輸入 **CA Certificate Fingerprint**（**CA** 憑證指紋）。從 Thumbprint（指紋）欄位的 SCEP 伺服器介面取得該指紋。
10. 啟用 SCEP 伺服器與 GlobalProtect 入口網站之間的手動 SSL 驗證。
11. 按一下 **OK**（確定）然後 **Commit**（提交）設定。

2. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證），然後按一下 **Generate**（產生）。
3. 輸入 **Certificate Name**（憑證名稱）。此名稱不能包含空格。
4. 選取 **SCEP Profile**（**SCEP** 設定檔）以用於自動化發佈伺服器憑證的程序，該程序由企業 CA 簽署至入口網站或閘道，然後按一下 **OK**（確定）以產生憑證。GlobalProtect 入口網站使用 SCEP 設定檔內的設定，以提交 CSR 至您的企業 PKI。

- 將匯入或生成的伺服器憑證指派至 SSL/TLS 服務設定檔。
  1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔），然後 **Add**（新增）新的 SSL/TLS 服務設定檔。
  2. 輸入 **Name**（名稱）以識別設定檔和選取您匯入或生成的伺服器 **Certificate**（憑證）。
  3. 定義允許與 GlobalProtect 元件之間通訊的 SSL/TLS 版本範圍（**Min Version**（最低版本）至 **Max Version**（最高版本））。

     若要提供最強大的安全性，請將 *Min Version*（最低版本）設定為 *TLSv1.2*。
  4. 按一下 **OK**（確定）以儲存 SSL/TLS 服務設定檔。
  5. **Commit**（提交）變更。

- 部署自我簽署的伺服器憑證。

  - 匯出由入口網站的根 *CA* 所簽發的自我簽署伺服器憑證，並將它們匯入至閘道。
  - 請務必為每個閘道簽發唯一的伺服器憑證。
  - 當指定自我簽署的憑證時，您必須將根 *CA* 憑證散佈至入口網站用戶端組態中的終端用戶端。

  從入口網站匯出憑證。

1. 選取 **Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證）。
2. 選取要部署的閘道憑證，然後按一下 **Export Certificate**（匯出憑證）。
3. 將 **File Format**（檔案格式）設定為 **Encrypted Private Key and Certificate (PKCS12)**（加密私人金鑰及憑證 **(PKCS12)**）。
4. 輸入用於加密私密金鑰的 **Passphrase**（密碼），並進行確認。
5. 按一下 **OK**（確定）下載 PKCS12 檔案至您選取的位置。

匯入閘道上的憑證：

1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證），然後 **Import**（匯入）憑證。
2. 輸入 **Certificate Name**（憑證名稱）。
3. **Browse**（瀏覽）以尋找並選取您在之前步驟中下載的 **Certificate File**（憑證檔案）。
4. 將 **File Format**（檔案格式）設定為 **Encrypted Private Key and Certificate (PKCS12)**（加密私人金鑰及憑證 **(PKCS12)**）。
5. 輸入您在從入口網站匯出私人金鑰時用來加密的 **Passphrase**（複雜密碼），並進行確認。
6. 按一下 **OK**（確定）匯入憑證和金鑰。
7. **Commit**（提交）閘道進行的變更。

驗證

GlobalProtect™ 入口網站和閘道必須先驗證一般使用者，才會讓其存取 GlobalProtect 資源。您必須在進行入口網站和閘道設定之前，設定驗證機制。以下幾節詳細介紹支援的驗證機制，以及如何設定：

- 關於 GlobalProtect 使用者驗證
- 設定外部驗證
- 設定用戶端憑證驗證
- 設定雙因素驗證
- 設定 strongSwan Ubuntu 與 CentOS 端點驗證
- 設定 GlobalProtect 以便進行多因素驗證通知
- 啟用 VSA 至 RADIUS 伺服器的提交
- 啟用群組對應

關於 GlobalProtect 使用者驗證

GlobalProtect 應用程式首次連線入口網站時，將提示使用者驗證入口網站。如果驗證成功，GlobalProtect 入口網站傳送 GlobalProtect 設定，其中包括應用程式可連線的閘道清單，以及可選擇連線至閘道的用戶端憑證。成功下載並快取設定之後，應用程式會嘗試連線至其中一個在組態中指定的閘道。由於這些元件提供對於您網路資源的存取，因此它們也需要一般使用者進行驗證。

入口網站及閘道所需的安全性層級因閘道保護的資源敏感度而有所不同。GlobalProtect 提供彈性驗證架構，可讓您選擇適用於每個元件的驗證設定檔及/或憑證設定檔。

- 支援的 GlobalProtect 驗證方法
- 應用程式如何知道要提供的認證為何？

支援的 GlobalProtect 驗證方法

下表描述了 GlobalProtect 對每個方法支援和提供使用指南的驗證方法。

- 本機驗證
- 外部驗證
- 用戶端憑證驗證
- 雙因素驗證
- 應用程式（不以瀏覽器為基礎）的多因素驗證
- 單一登入

本機驗證

使用者帳戶認證與驗證機制對於防火牆而言都屬於本機。此驗證機制無法調整，因為它需要每個 GlobalProtect 一般使用者都具備帳戶，因此只建議在非常小型的部署中使用。

外部驗證

外部 LDAP、Kerberos、TACACS+、SAML 或 RADIUS 服務（包括對於雙因素以權杖為基礎驗證機制的支援，例如一次性密碼 (OTP) 驗證）會執行使用者驗證功能。啟用外部驗證：

- 建立伺服器設定檔，帶有用於存取外部驗證服務的設定。
- 參考伺服器設定檔建立驗證設定檔。
- 在入口網站和閘道組態中指定用戶端驗證，並選取指定使用這些設定的端點 OS。

您可以為每個 GlobalProtect 元件使用不同的驗證設定檔。如需說明，請參閱 設定外部驗證。組態示例請參閱遠端存取 VPN（驗證設定檔）。

如果您將入口網站或閘道設為透過 *SAML* 驗證對使用者進行驗證，停用單一登出 *(SLO)* 後，執行 *GlobalProtect* 應用程式 *4.1.8* 或更早版本的使用者將無法選取 *Sign Out*（登出）應用程式。無論 *SLO* 啟用還是停用，執行 *GlobalProtect* 應用程式 *4.1.9* 或更新版本的使用者均可選取 *Sign Out*（登出）應用程式。

如果您將入口網站或閘道設為透過 *Kerberos* 驗證對使用者進行驗證，當使用者成功使用此驗證方法進行驗證後，將無法選取 *Sign Out*（登出）*GlobalProtect* 應用程式。

如果您未允許 *GlobalProtect* 應用程式 *Save User Credentials*（儲存使用者認證）（*Network*（網路）> *GlobalProtect* > *Portals*（入口網站）> *<portal-config>* > *Agent*（代理程式）> *<agent-config>* > *Authentication*（驗證））*LDAP*、*TACACS+* 或 *RADIUS* 進行驗證後，將無法選取 *Sign Out*（登出）應用程式。

用戶端憑證驗證

針對更高的安全性，您可以設定入口網站或閘道在授與對於系統的存取權之前，會使用用戶端憑證來取得使用者名稱及驗證使用者。

- 若要驗證使用者，憑證欄位之一，如主旨名稱欄位，必須識別使用者名稱。
- 若要驗證端點，憑證的主旨欄位必須識別設備類型，而非使用者名稱。（透過預登入連線方法，入口網站或閘道在使用者登入之前驗證端點。）

如果您將入口網站或閘道設為透過用戶端憑證驗證對使用者進行驗證，當使用者僅使用用戶端憑證成功驗證後，將無法選取 *Sign Out*（登出）*GlobalProtect* 應用程式。

對於指定用戶端憑證的代理程式組態設定檔，各使用者會接收到用戶端憑證。提供憑證的機制確定憑證是否對各使用者為唯一，或在該代理程式組態下，所有使用者的憑證均一致：

- 若要部署對各使用者和端點唯一的用戶端憑證，請使用 **SCEP**。當使用者先登入時，入口網站請求來自企業的 PKI 憑證。入口網站獲得獨立憑證並將其部署至端點。
- 若要部署相同的用戶端憑證至所有接收代理程式組態的使用者，部署防火牆的 **Local**（本機）憑證。

使用可選的憑證設定檔以確認端點呈現的帶連線請求的用戶端憑證。憑證設定當指定使用者名稱和使用者網域欄位內容；列出 CA 憑證；封鎖工作階段條件；並提供確定 CA 憑證撤銷狀態的方法。因為憑證是新工作階段中端點或使用者驗證的一部分，您必須在使用者初次登入入口網站前，將在憑證設定檔中使用的憑證預部署至端點。

憑證設定檔指定哪個憑證欄位包含使用者名稱。如果憑證設定檔指定 [Username Field] 中的 [主旨]，端點所出示的憑證必須包含通用名稱才能讓端點連線。如果憑證設定檔指定 [Subject-Alt with an Email] 或 [主體名稱] 作為 [Username Field]，端點出示的憑證必須包含對應欄位，當 GlobalProtect 應用程式向入口網站或閘道驗證時，會將其作為使用者名稱使用。

GlobalProtect 也支援通用存取卡 (CAC) 與智慧卡式驗證，其需依靠憑證設定檔。透過這些卡，憑證設定檔必須包含在智慧卡或 CAC 中發出憑證的根 CA 憑證。

如果您指定用戶端憑證驗證，則不應在入口網站設定中設定用戶端憑證，因為當使用者連線時，端點將會提供該憑證。如需如何設定用戶端憑證驗證的範例，請參閱 遠端存取 VPN（憑證設定檔）。

雙因素驗證

透過雙因素驗證，入口網站或閘道使用兩種機制驗證使用者，如一次性密碼和 Active Directory (AD) 登入認證。您可以透過設定與新增憑證設定檔和驗證設定檔至入口網站與/或閘道設定，來啟用雙因素驗證。

您可以設定入口網站和閘道，以使用那個相同的驗證方法或不同的驗證方法。無論如何，使用者必須透過元件要求的兩種機制成功驗證，才能存取網路資源。

如果憑證設定檔指定 **Username Field**（使用者名稱欄位）可獲取使用者名稱的使用者名稱欄位，外部驗證服務自動使用使用者名稱驗證設定中的使用者外部驗證服務。例如，如果憑證設定檔中的 **Username Field**（使用者名稱欄位）設定為 **Subject**（主旨），則憑證通用名稱欄位中的值將作為使用者名稱，在驗證伺服器嘗試驗證使用者時使用。如果您不想強制使用者使用憑證中的使用者名稱驗證，請確保將憑證設定檔中的 **Username Field**（使用者名稱欄位）設定為 **None**（無）。組態示例請參閱透過雙因素驗證遠端存取 VPN。

應用程式（不以瀏覽器為基礎）的多因素驗證

（僅限 Windows 和 macOS）對於可能需要其他驗證的敏感、非瀏覽器型的網路資源（例如，財務應用程式或軟體開發應用程式），GlobalProtect 應用程式可以通知並提示使用者執行即時與多重因素驗證，在存取這些資源會需要該驗證。

單一登入

（ 僅限 Windows ）當您啟用單一登入 (SSO) 時，GlobalProtect 應用程式會使用使用者的 Windows 登入認證以自動驗證 GlobalProtect 入口網站與閘道並建立連線。您也可設定應用程式以 封裝協力廠商認證 ，以確保 Windows 使用者可以使用協力廠商認證提供者驗證並連線。

如果您啟用單一登入，執行 *GlobalProtect* 應用程式 *4.1.9* 或更新版本的使用者在使用 *SSO* 成功驗證後，將無法選取 *Sign Out*（登出） 應用程式。

應用程式如何知道要提供的認證為何？

依預設，針對用於入口網站登入的閘道，GlobalProtect 應用程式會嘗試使用相同的登入認證。在閘道與入口網站使用相同驗證設定檔與/或憑證設定檔的最簡單情況下，應用程式將明顯連線至閘道。

基於應用程式組態，您也可以自訂 GlobalProtect 入口網站和閘道—內部、外部、或僅手動—需要不同人種（如唯一 OTP）。這讓 GlobalProtect 入口網站或閘道提示輸入唯一的 OTP，而不會提示提供驗證設定檔內指定的認證。

有兩種選項可以修改預設應用程式驗證行為，以讓驗證更強更快：

- 入口網站或閘道上的 Cookie 驗證
- 轉送至部份或所有閘道的認證

入口網站或閘道上的 *Cookie* 驗證

Cookie 驗證可簡化一般使用者的驗證流程，因為他們將不再需要登入入口網站與閘道，或輸入多個 OTP 以分別進行入口網站與閘道驗證。這透過最小化使用者必須輸入認證的次數，提高使用者的體驗。此外，Cookie 允許在使用者密碼過期後使用臨時密碼重新啟用 VPN 存取權。

您可以為入口網站和單個的閘道獨立進行 Cookie 驗證設定（例如，您可以在閘道上設置較短的 cookie 存留時間，以保護敏感資源）。在入口網站或閘道部署驗證 cookie 至端點後，入口網站和閘道均依靠相同 cookie 驗證使用者。當應用程式提供 cookie 時，入口網站或閘道根據設定的 cookie 存留時間評估 cookie 是否有效。如果 cookie 逾期，GlobalProtect 自動提示使用者驗證入口網站或閘道。當驗證成功時，入口網站或閘道發出取代驗證 cookie 至端點且有效時間重新開始計算。

請考慮下列範例，不保護敏感資訊的入口網站 cookie 存留時間可設定為 15 天，要保護敏感資訊的閘道 cookie 存留時間可設定為 24 小時。當使用者首次透過入口網站驗證時，入口網站會發出驗證 cookie。如果五天後，使用者嘗試連線至入口網站，驗證 cookie 仍將有效。但是，在五天後，使用者嘗試連線閘道，閘道將評估 cookie 存留時間並確定其已過期（5 天 > 24 小時）。代理程式將自動提示使用者透過閘道驗證，並在成功驗證後，收到替換驗證 cookie。新驗證 cookie 將在入口網站上以有效狀態存留 15 天，並在閘道上存留 24 小時。

如需如何使用此選項的範例，請參閱設定雙因素驗證。

轉送至部份或所有閘道的認證

透過雙因素驗證，您可以指定入口網站和/或閘道類型（內部、外部或僅手動），提示使用者獲取對應的認證。當入口網站與閘道需要不同的認證（不同 OTP 或完全不同的登入認證）時，此方法可加快驗證流程。對於您選取的各入口網站或閘道，應用程式不會轉送認證，以讓您為不同的 GlobalProtect 元件自訂安全性。您可以對入口網站與內部閘道擁有相同的安全性，同時需要第二個因素 OTP 或不同密碼才能存取提供對於大多數敏感資源存取權的閘道。

如需如何使用此選項的範例，請參閱設定雙因素驗證。

應用程式如何知道要提供的認證為何者？

在將 GlobalProtect 設定為使用用戶端憑證以在 macOS 或 Windows 端點進行驗證，GlobalProtect 必須出示有效用戶端憑證以與入口網站和/或閘道進行驗證。

若要確認用戶端憑證是否有效，其必須符合下列需求：

- 憑證核發單位為憑證授權單位 (CA)，該授權單位為您在入口網站和閘道設定中的憑證設定檔中所定義。
- 憑證指定用戶端驗證目的，這也是建立憑證時憑證管理所指定的項目。
- 憑證位於憑證存放區（如 GlobalProtect 入口網站代理程式設定中設定）。依預設，GlobalProtect 應用程式首先會在使用者存放區尋找有效的憑證。如果不存在，應用程式之後會在機器存放區尋找。因為優先尋找使用者存放區，若 GlobalProtect 應用程式在使用者存放區中找到憑證，就不會在機器存放區中尋找。若要讓 GlobalProtect 應用程式僅在一個憑證存放區中尋找憑證，請在適當的 GlobalProtect 入口網站代理程式設定中設定 **Client Certificate Store Lookup**（用戶端憑證存放區查閱）選項。
- 憑證與在 GlobalProtect 入口網站代理程式設定中指定的其他目的相符。若要指定其他目的，您必須識別憑證的物件識別碼 (OID) 並在適當的 GlobalProtect 入口網站代理程式設定中設定 **Extended Key Usage OID**（延伸的金鑰使用情況 **OID**）。OID 是一數值，其會指示要使用憑證的應用程式或服務，且當憑證授權單位 (CA) 將其建立時，該應用程式或服務會自動連接至憑證。如需更多指定一般或自訂 OID 的詳細資訊，請參閱依 OID 的憑證選取項目。

當只有一個用戶端憑證符合以上需求時，應用程式會自動使用該用戶端憑證以進行驗證。然而，當多個用戶端認證符合這些需求時，GlobalProtect 會提示使用者從端點上的有效用戶端憑證清單中選取用戶端憑證。GlobalProtect 只會在使用者第一次連線時要求他們選取用戶端憑證，使用者可能不會知道要選取哪一個憑證。若是如此，我們建議您依憑證目的（如 OID 所指示）和憑證存放區來縮小可用用戶端憑證的清單。如需可設定以自訂應用程式之這些與其他設定的其他資訊，請參閱自訂 GlobalProtect 代理程式。

設定外部驗證

以下工作流程說明如何設定 GlobalProtect 入口網站與閘道，從而使用外部驗證服務。支援的驗證服務包括 LDAP、Kerberos、RADIUS、SAML 及 TACACS+。

GlobalProtect 也支援本機驗證。若要使用本機驗證，建立一個本機使用者資料庫（*Device*（設備）> *Local User Database*（本機使用者資料庫）），其中包含您想要允許 *GlobalProtect* 存取的使用者和群組，然後參閱驗證設定檔內的資料庫。

如需更多訊息，請參閱 支援的 GlobalProtect 驗證方法 。

設定外部驗證的選項包含：

- 設定 LDAP 驗證
- 設定 SAML 驗證
- 設定 Kerberos 驗證
- 設定 RADIUS 或 TACACS+ 驗證

設定 LDAP 驗證

各組織經常將 LDAP 用作驗證服務和使用者資訊的中央儲存庫。其也可用來儲存應用程式使用者的角色資訊。

STEP 1 | 建立伺服器設定檔

伺服器設定檔識別外部驗證服務，並會指示防火牆連線至外部驗證服務及針對您的使用者存取驗證認證的方式。

如果您使用 *LDAP* 連線至 *Active Directory (AD)*，則必須為每個 *AD* 網域建立個別的 *LDAP* 伺服器設定檔。

1. 選取 **Device**（裝置）> **Server Profiles**（伺服器設定檔）> **LDAP**，然後 **Add**（新增）LDAP 伺服器設定檔。
2. 輸入 **Profile Name**（設定檔名稱），例如 **`GP-User-Auth`**。
3. 如果此設定檔適用於具有多重虛擬系統功能的防火牆，請選取一個虛擬系統或 **Shared**（共用）作為設定檔可用的 **Location**（位置）。
4. 按一下 **Server List**（伺服器清單）區域的 **Add**（新增），然後輸入連線至驗證伺服器所需的資訊，包括伺服器 **Name**（名稱）、**LDAP Server**（**LDAP** 伺服器）IP 位址（或 FQDN）及 **Port**（連接埠）。
5. 選取 LDAP 伺服器 **Type**（類型）。
6. 輸入 **Bind DN**（繫結 **DN**）與 **Password**（密碼）以讓驗證服務能驗證防火牆。
7. （選用）如果您希望端點使用 SSL 或 TLS 更安全的連線目錄伺服器，請啟用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全連線）選項（預設為已啟用）。端點使用的協定視乎伺服器連接埠而定：
   - 389（預設）—TLS（特別是裝置會使用 StartTLS 操作，用來升級連接至 TLS 的初始純文字連線。）
   - 636—SSL
   - 任何其他連接埠—裝置首先會嘗試使用 TLS。若目錄伺服器不支援 TLS，則裝置會回復使用 SSL。
8. （選用）為了獲得額外的安全，請啟用 **Verify Server Certificate for SSL sessions**（確認 **SSL** 工作階段的伺服器憑證）選項，讓端點確認目錄伺服器為 SSL/TLS 連線所呈現的憑證。若要啟用驗證，您也必須啟用 **Require SSL/TLS secured connection**（要求 **SSL/TLS** 安全連線）選項。為了順利確認，憑證必須滿足以下條件之一：

- 位於裝置憑證清單內：**Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（設備憑證）。若有必要，將憑證匯入至裝置。
- 憑證簽署者位於受信任的憑證授權單位清單中：**Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Default Trusted Certificate Authorities**（預設的受信任憑證授權單位）。

9. 按一下 **OK**（確定）來儲存伺服器設定檔。

STEP 2 | （選用）建立驗證設定檔。

驗證設定檔指定入口網站或閘道在驗證使用者時使用的伺服器設定檔。在入口網站或閘道上，您可以指定一個或多個驗證設定檔至一個或多個用戶端驗證設定檔。對於用戶端驗證設定檔內驗證設定檔如何支援細微使用者驗證的說明，請參閱設定 GlobalProtect 閘道和設定對 GlobalProtect 入口網站的存取。

若要允許使用者連線和自行變更其過期密碼，無須管理員介入，請考慮使用透過預登入遠端存取 VPN。

如果使用者的密碼過期，您可以指派臨時 *LDAP* 密碼以允許使用者登入 *GlobalProtect*。在此狀況中，可已使用臨時密碼來驗證入口網站，但可能無法登入閘道，因為無法重複使用同一個臨時密碼。若要防止此問題發生，請在入口網站組態中設定驗證取代（*Network*（網路）> *GlobalProtect* > *Portal*（入口網站）），以讓 *GlobalProtect* 應用程式使用 *Cookie* 驗證入口網站，使用臨時密碼驗證閘道。

1. 選取 **Device**（設備）> **Authentication Profile**（驗證設定檔），然後按一下 **Add**（新增）來新增設定檔。
2. 輸入設定檔的 **Name**（名稱）。
3. 將 **Authentication**（驗證）**Type**（類型）設定為 **LDAP**。
4. 選取您在步驟 1 中建立的 LDAP 驗證 **Server Profile**（伺服器設定檔）。
5. 輸入 **sAMAccountName** 作為**Login Attribute**（登入屬性）。
6. 設定 **Password Expiry Warning**（密碼到期警告），以指示要在密碼到期的多少天數前通知使用者。依預設會在密碼到期前七天通知使用者（範圍為 1-255）。由於使用者必須在到期前變更密碼，您必須提供一段足夠長的通知時間，確保您的使用者可以繼續存取 GlobalProtect。若要使用此功能，您必須在您的 LDAP 伺服器設定檔中指定下列 LDAP 伺服器類型之一：**active-directory**、**e-directory** 或 **sun**。

   除非啟用預登入，否則密碼過期時使用者將無法存取 GlobalProtect。
7. 指定 **User Domain**（使用者網域）和 **Username Modifier**（使用者名稱修改程式）。端點會合併 **User Domain**（使用者網域）和 **Username Modifier**（使用者名稱修改程式）值以修改使用者所輸入的網域/使用者名稱字串。端點會使用修改的字串來進行驗證，且會針對 User-ID 群組對應使用 **User Domain**（使用者網域）值。當驗證服務需要特殊格式的網域/使用者名稱字串，且您不想要依靠使用者正確輸入網域時，修改使用者匯入就顯得非常有用。您可以從下列選項中選取：
   - 若僅要傳送未修改的使用者輸入，請將 **User Domain**（使用者網域）保留空白（預設值）並將 **Username Modifier**（使用者名稱修改程式）設定為變數 **%USERINPUT%**（預設值）。
   - 若要在使用者輸入前面加上網域，請輸入 **User Domain**（使用者網域）並將 **Username Modifier**（使用者名稱修改程式）設定為 **%USERDOMAIN%\%USERINPUT%**。
   - 若要在使用者輸入附加網域，請輸入 **User Domain**（使用者網域）並將 **Username Modifier**（使用者名稱修改程式）設定為 **%USERINPUT%@%USERDOMAIN%**。

   若 *Username Modifier*（使用者名稱修改程式）包含 *%USERDOMAIN%* 變數，則 *User Domain*（使用者網域）值會取代任何使用者輸入的網域字串。如果 *User Domain*（使用者網域）為空，則表示該裝置移除了任何使用者輸入的網域字串。
8. 在 **Advanced**（進階）頁籤上，**Add**（新增）**Allow List**（允許清單）以選取允許以此設定檔進行驗證的使用者和使用者群組。**all**（所有）選項允許每位使用者以此設定檔進行驗證。依預設，清單無項目，意味著無使用者可驗證。

9. 按一下 **OK**（確定）。

STEP 3 | 提交組態。

按一下 **Commit**（交付）。

設定 SAML 驗證

安全性聲明標記語言 (SAML) 一個以 XML 為基礎、開放標準的資料格式可用來在廠商（特別是在識別提供者 (IdP) 和服務提供者）之間交換驗證與授權。SAML 是 OASIS 安全性服務技術委員會的產品。

STEP 1 | 建立伺服器設定檔

伺服器設定檔識別外部驗證服務，並會指示防火牆連線至外部驗證服務及針對您的使用者存取驗證認證的方式。

下列步驟說明如何從 IdP 匯入 SAML 中繼資料檔案，以便防火牆能夠自動建立伺服器設定檔並填入連線、註冊和 IdP 憑證資訊。如果 IdP 未提供中繼資料檔案，請選取 **Device**（裝置）> **Server Profiles**（伺服器設定檔）> **SAML Identity Provider**（**SAML** 識別提供者），然後手動 **Add**（新增）伺服器設定檔。

1. 從 IdP 匯出 SAML 中繼資料檔案到防火牆可存取的端點。

   關於如何匯出檔案的說明，請參閱 IdP 文件。
2. 選取 **Device**（裝置）> **Server Profiles**（伺服器設定檔）> **SAML Identity Provider**（**SAML** 識別提供者）。
3. **Import**（匯入）中繼資料檔案到防火牆。
4. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱），例如 **`GP-User-Auth`**。
5. **Browse**（瀏覽）中繼資料檔案。
6. （建議）選取**Validate Identity Provider Certificate**（驗證識別提供者憑證）（預設值），讓防火牆驗證 IdP 憑證。

   只有在您將伺服器設定檔指派給驗證設定檔並 **Commit**（交付）變更之後，才會進行驗證。防火牆將使用驗證設定檔中的憑證設定檔驗證憑證。
7. 輸入 **Maximum Clock Skew**（最大時鐘誤差），即在防火牆驗證 IdP 訊息時，IdP 與防火牆之間允許的系統時間差值（單位為秒）。預設值為 60 秒，範圍為 1 至 900 秒。若差值超過此值，則驗證失敗。
8. 按一下 **OK**（確定）來儲存伺服器設定檔。

STEP 2 | （選用）建立驗證設定檔。

驗證設定檔指定入口網站或閘道在驗證使用者時使用的伺服器設定檔。在入口網站或閘道上，您可以指定一個或多個驗證設定檔至一個或多個用戶端驗證設定檔。有關用戶端驗證設定檔內驗證設定檔如何支援細微使用者驗證的更多資訊，請參閱設定 GlobalProtect 閘道和設定對 GlobalProtect 入口網站的存取。

SAML 驗證支援透過 *GlobalProtect* 應用程式 *5.0* 及更新版本 使用預先登入的遠端存取 VPN。

1. 選取 **Device**（設備）> **Authentication Profile**（驗證設定檔），然後按一下 **Add**（新增）來新增驗證設定檔。
2. 輸入驗證設定檔的 **Name**（名稱）。
3. 將 **Authentication**（驗證）**Type**（類型）設定為 **SAML**。
4. 選取您在步驟 1 中建立的 SAML **IdP Server Profile**（**IdP** 伺服器設定檔）。
5. 設定下列選項以啟用防火牆與 SAML 識別提供者之間的憑證驗證。請參閱 SAML 2.0 驗證以瞭解詳細資訊。

- 防火牆用來簽署訊息的 **Certificate for Signing Requests**（用於簽署要求的憑證），防火牆會將該訊息傳送至 IdP。
- 防火牆將用於驗證 IdP 憑證的 **Certificate Profile**（憑證設定檔）。

6. 指定使用者名稱與管理角色格式。
   - 指定 **Username Attribute**（使用者屬性）和 **User Group Attribute**（使用者群組屬性）。

     不同於其他外部驗證類型，*SAML* 驗證設定檔沒有 *User Domain*（使用者網域）屬性。

   - （選用）如果您打算使用此設定檔來驗證您在 IdP 識別存放區中管理的管理帳戶，請指定 **Admin Role Attribute**（管理角色屬性）和 **Access Domain Attribute**（存取網域屬性）。
7. 在 **Advanced**（進階）頁籤上，**Add**（新增）**Allow List**（允許清單）以選取允許以此設定檔進行驗證的使用者和群組。**all**（所有）選項允許每位使用者以此設定檔進行驗證。依預設，清單無項目，意味著無使用者可驗證。

   請確定在 **Allow List**（允許清單）中的使用者名稱與傳回 SAML IdP 伺服器的使用者名稱相同。
8. 按一下 **OK**（確定）。

STEP 3 | **Commit**（提交）組態。

STEP 4 | （僅限 Chromebooks）為 Chromebooks 啟用 SAML SSO。

您可按照以下步驟在 Chromebooks 上為適用于 Android 的 GlobalProtect 應用程式設定 SAML SSO。

1. 登入至 Google 管理主控台並選取 **Security**（安全性）。
2. 選取 **Set up single sign-on (SSO)**（設定單一登入 **(SSO)**）。
3. （選用）如果您想要透過除 Google 以外的其他提供者設定 SSO，請選取 **Setup SSO with third party identity provider**（透過協力廠商識別提供者設定 **SSO**），並指定 **Sign-in page URL**（登入頁面 **URL**）和 **Sign-out page URL**（登出頁面 **URL**）並上載有效的 **Verification certificate**（驗證憑證）。
4. 在 GlobalProtect 中設定 SAML 識別提供者。
   1. 在 GlobalProtect 控制台中，選取 **Device**（裝置）> **Server Profiles**（伺服器設定檔）> **SAML Identity Provider**（ **SAML** 識別提供者）。
   2. 在 Google 管理控制台中比對您為 IdP 輸入的值。

設定 Kerberos 驗證

Erberos 是一電腦網路驗證通訊協定，可以使用票證來允許節點透過非安全性網路通訊來以安全的方式向彼此證明其身分。

Windows（*7*、*8* 和 *10*）與 *macOS (10.10* 和更新版本）端點支援 *Kerberos* 驗證。適用於 *macOS* 端點的 *Kerberos* 驗證需要的最低 *GlobalProtect* 應用程式版本為 *4.1.0*。

STEP 1 | 建立伺服器設定檔

伺服器設定檔識別外部驗證服務，並會指示防火牆連線至外部驗證服務及針對您的使用者存取驗證認證的方式。

1. 選取 **Device**（裝置）> **Server Profiles**（伺服器設定檔）> **Kerberos**，然後 **Add**（新增）Kerberos 伺服器設定檔。

2. 輸入 **Profile Name**（設定檔名稱），例如 **`GP-User-Auth`**。
3. 如果此設定檔適用於具有多重虛擬系統功能的防火牆，請選取一個虛擬系統或 **Shared**（共用）作為設定檔可用的 **Location**（位置）。
4. 在 **Servers**（伺服器）區域按一下 **Add**（新增），然後輸入下列資訊以連線至驗證伺服器：
   - 伺服器**Name**（名稱）
   - 輸入 **Kerberos Server**（**Kerberos** 伺服器）的 IP 位址或 FQDN
   - 連接埠
5. 按一下 **OK**（確定）來儲存伺服器設定檔。

STEP 2 | （選用）建立驗證設定檔。

驗證設定檔指定入口網站或閘道在驗證使用者時使用的伺服器設定檔。在入口網站或閘道上，您可以在一個或多個用戶端驗證設定檔中指定一個或多個驗證設定檔。有關用戶端驗證設定檔內驗證設定檔如何支援細微使用者驗證的資訊，請參閱設定 GlobalProtect 閘道和設定對 GlobalProtect 入口網站的存取。

若要允許使用者連線和自行變更其過期密碼，無須管理員介入，請考慮使用透過預登入遠端存取 VPN。

1. 選取 **Device**（設備）> **Authentication Profile**（驗證設定檔），然後按一下 **Add**（新增）來新增設定檔。
2. 輸入設定檔的 **Name**（名稱）然後選取 **Kerberos** 作為驗證 **Type**（類型）。
3. 選取您在步驟 1 中建立的 Kerberos 驗證 **Server Profile**（伺服器設定檔）。
4. 指定 **User Domain**（使用者網域）和 **Username Modifier**（使用者名稱修改程式）。端點會合併這些值，以修改使用者在登入期間輸入的網域/使用者名稱字串。端點會使用修改的字串來進行驗證，且會針對 User-ID 群組對應使用 **User Domain**（使用者網域）值。當驗證服務需要特殊格式的網域/使用者名稱字串，且您不想要依靠使用者正確輸入網域時，修改使用者匯入就顯得非常有用。您可以從下列選項中選取：
   - 若要傳送未修改的使用者輸入，請將 **User Domain**（使用者網域）保留空白（預設值），並將 **Username Modifier**（使用者名稱修改程式）設定為變數 **%USERINPUT%**（預設值）。
   - 若要在使用者輸入前面加上網域，請輸入 **User Domain**（使用者網域）並將 **Username Modifier**（使用者名稱修改程式）設定為 **%USERDOMAIN%\%USERINPUT%**。
   - 若要在使用者輸入附加網域，請輸入 **User Domain**（使用者網域）並將 **Username Modifier**（使用者名稱修改程式）設定為 **%USERINPUT%@%USERDOMAIN%**。

   若 *Username Modifier*（使用者名稱修改程式）包含 *%USERDOMAIN%* 變數，則 *User Domain*（使用者網域）值會取代任何使用者輸入的網域字串。如果 *User Domain*（使用者網域）為空，則表示該裝置移除了任何使用者輸入的網域字串。
5. 如果您的網路支援，請設定 Kerberos 單一登入 (SSO)。
   - 輸入 **Kerberos Realm**（**Kerberos** 領域）（最多 127 個字元）以指定使用者登入名稱的主機名稱部分。例如，使用者帳戶名稱 user@EXAMPLE.LOCAL 具有領域 EXAMPLE.LOCAL。
   - **Import**（匯入）一個 **Kerberos Keytab**（**Kerberos** 金鑰標籤）檔案。出現提示時，請 **Browse**（瀏覽）金鑰標籤檔案，然後按一下 **OK**（確定）。驗證期間，端點首先會嘗試使用金鑰標籤建立 SSO。若成功建立，且使用者嘗試的存取位於 **Allow List**（允許清單）中，則驗證會立即成功。否則，驗證程序會回復為使用特定驗證 **Type**（類型）的手動（使用者名稱/密碼）驗證。**Type**（類型）不一定為 Kerberos。若要變更此行為，讓使用者可以僅使用 Kerberos 驗證，在 GlobalProtect 入口網站代理程式組態中，設定 **Use Default Authentication on Kerberos Authentication Failure**（當 **Kerberos** 驗證失敗時使用預設驗證）為 **No**（否）。
6. 在 **Advanced**（進階）頁籤上，**Add**（新增）**Allow List**（允許清單）以選取允許以此設定檔進行驗證的使用者和使用者群組。**all**（所有）選項允許每位使用者以此設定檔進行驗證。依預設，清單無項目，意味著無使用者可驗證。
7. 按一下 **OK**（確定）。

STEP 3 | 提交組態。

按一下 **Commit**（交付）。

設定 RADIUS 或 TACACS+ 驗證

RADIUS 是一個用戶端/伺服器通訊協定和軟體，其能讓遠端存取伺服器與中央伺服器溝通，以驗證撥入使用者並授予其對要求系統或服務的存取權。TACACS+ 是一個完整建立的 UNIX 網路共有的驗證通訊協定，其可讓遠端存取伺服器將使用者登入密碼轉送至驗證伺服器以決定是否允許對特定系統的存取。

STEP 1 | 建立伺服器設定檔

伺服器設定檔識別外部驗證服務，並會指示防火牆連線至外部驗證服務及針對您的使用者存取驗證認證的方式。

如果您想要啟用 VSA 至 RADIUS 伺服器的提交，您必須建立一個 *RADIUS* 伺服器設定檔。

1. 選取 **Device**（裝置）> **Server Profiles**（伺服器設定檔），然後選取設定檔類型（**RADIUS** 或 **TACACS+**）。
2. **Add**（新增）新的 RADIUS 或 TACACS+ 伺服器設定檔。
3. 輸入 **Profile Name**（設定檔名稱），例如 **`GP-User-Auth`**。
4. 如果此設定檔適用於具有多重虛擬系統功能的防火牆，請選取一個虛擬系統或 **Shared**（共用）作為設定檔可用的 **Location**（位置）。
5. 設定下列 **Server Settings**（伺服器設定）：
   - 逾時 **(秒)**—在伺服器連線要求時間因為缺少來自驗證伺服器的回應而逾時的秒數。
   - 驗證通訊協定—用於連線至驗證伺服器的通訊協定。選項包括 **CHAP**、**PAP**、**PEAP-MSCHAPv2**、**PEAP with GTC**, or **EAP-TTLS with PAP**。

     如果您將 *PEAP-MSCHAPv2*（受保護的可擴展驗證通訊協定- *Microsoft* 挑戰握手驗證通訊協定版本 *2*）設定為驗證通訊協定，當遠端使用者在下一次登入時密碼過期或 *RADIUS/AD* 管理員要求變更密碼時，其可透過 *GlobalProtect* 應用程式變更 *RADIUS* 或 *Active Directory (AD)* 密碼。
   - （僅 RADIUS）**Retries**（重試）—在停止要求前防火牆嘗試連線至驗證伺服器的次數。
   - （僅 TACACS+）**Use single connection for all authentication**（對所有驗證使用單一連線）—允許所有 TACACS+ 驗證要求透過單一 TCP 工作階段（而不是每個要求的個別工作階段）而發生的選項。
6. 在 **Servers**（伺服器）區域按一下 **Add**（新增），然後輸入下列資訊以連線至驗證伺服器：
   - 名稱
   - **RADIUS** 或 **TACACS+ Server**（伺服器）（伺服器的 IP 位址或 FQDN）
   - **Secret**（密碼）（讓驗證服務能驗證防火牆的共用密碼）
   - 連接埠
7. 按一下 **OK**（確定）來儲存伺服器設定檔。

STEP 2 | （選用）建立驗證設定檔。

驗證設定檔指定入口網站或閘道在驗證使用者時使用的伺服器設定檔。在入口網站或閘道上，您可以在一個或多個用戶端驗證設定檔中指定一個或多個驗證設定檔。有關用戶端驗證設定檔內驗證設定檔如何支援細微使用者驗證的資訊，請參閱設定 GlobalProtect 閘道和設定對 GlobalProtect 入口網站的存取。

若要允許使用者連線和自行變更其過期密碼，無須管理員介入，請考慮使用透過預登入遠端存取 VPN。

1. 選取 **Device**（設備）> **Authentication Profile**（驗證設定檔），然後按一下 **Add**（新增）來新增設定檔。
2. 輸入設定檔的 **Name**（名稱）。
3. 選取 **Authentication**（驗證）**Type**（類型）（**RADIUS** 或 **TACACS+**）。
4. 選取您從下拉式選單的步驟 1 中建立的 RADIUS 或 TACACS+驗證 **Server Profile**（伺服器設定檔）。
5. （僅 RADIUS）如果您想要將此資訊包含在驗證設定檔中，請啟用 **Retrieve user group from RADIUS**（自 **RADIUS** 擷取使用者群組）。
6. 指定 **User Domain**（使用者網域）和 **Username Modifier**（使用者名稱修改程式）。端點會合併這些值，以修改使用者在登入期間輸入的網域/使用者名稱字串。端點會使用修改的字串來進行驗證，且會針對 User-ID 群組對應使用 **User Domain**（使用者網域）值。當驗證服務需要特殊格式的網域/使用者名稱字串，且您不想要依靠使用者正確輸入網域時，修改使用者匯入就顯得非常有用。您可以從下列選項中選取：
   - 若要傳送未修改的使用者輸入，請將 **User Domain**（使用者網域）保留空白（預設值）並將 **Username Modifier**（使用者名稱修改程式）設定為變數 **%USERINPUT%**（預設值）。
   - 若要在使用者輸入前面加上網域，請輸入 **User Domain**（使用者網域）並將 **Username Modifier**（使用者名稱修改程式）設定為 **%USERDOMAIN%\%USERINPUT%**。
   - 若要在使用者輸入附加網域，請輸入 **User Domain**（使用者網域）並將 **Username Modifier**（使用者名稱修改程式）設定為 **%USERINPUT%@%USERDOMAIN%**。

   若 *Username Modifier*（使用者名稱修改程式）包含 *%USERDOMAIN%* 變數，則 *User Domain*（使用者網域）值會取代任何使用者輸入的網域字串。如果 *User Domain*（使用者網域）為空，則表示該裝置移除了任何使用者輸入的網域字串。
7. 在 **Advanced**（進階）頁籤上，**Add**（新增）**Allow List**（允許清單）以選取允許以此設定檔進行驗證的使用者和使用者群組。**all**（所有）選項允許每位使用者以此設定檔進行驗證。依預設，清單無項目，意味著無使用者可驗證。
8. 按一下 **OK**（確定）。

STEP 3 | **Commit**（提交）組態。

設定用戶端憑證驗證

對於選用的用戶端憑證驗證，使用者出示用戶端憑證及連線請求至 GlobalProtect 入口網站或閘道。入口網站或閘道可使用公用或唯一的用戶端憑證，驗證使用者或端點是否屬於您的組織。

部署用戶端憑證的方法視乎您組織的安全性需求而定。

- 部署驗證的共用用戶端憑證
- 部署驗證的電腦憑證
- 部署驗證的使用者指定用戶端憑證

部署驗證的共用用戶端憑證

若要確定端點使用者是否屬於您的組織，您可以針對所有端點使用相同用戶端憑證，或產生不同憑證以使用特殊代理程式組態進行部署。使用此工作流程以簽發自我簽署用戶端憑證，並從入口網站進行部署。

STEP 1 | 產生憑證以部署多個 GlobalProtect 端點。

1. 建立用來針對 GlobalProtect 元件簽發自我簽署憑證的根 CA 憑證。
2. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證），然後 **Generate**（產生）新的憑證。
3. 將 **Certificate Type**（驗證類型）設定為 **Local**（本機）（預設）。
4. 輸入 **Certificate Name**（憑證名稱）。此名稱不能包含空格。
5. 輸入 **Common Name**（通用名稱）以將此憑證識別為應用程式憑證（例如，`GP_Windows_App`）。由於此憑證將使用相同代理程式設定部署至所有應用程式，因此不需要以唯一方式識別特定使用者或端點。
6. 在 **Signed By**（簽署者）欄位中，選取您的根 CA。
7. 選取 **OCSP Responder**（OCSP 回應程式）來驗證憑證的撤銷狀態。
8. 按一下 **OK**（確定）即可產生憑證。

STEP 2 | 設定雙因素驗證。

在 GlobalProtect 入口網站代理程式組態內的驗證設定，以啟用入口網站以透明方式將 **Local**（本機）用戶端憑證部署至防火牆，讓該應用程式可以接收組態。

部署驗證的電腦憑證

若要確認端點是否屬於您的組織，使用您自己的公開金鑰基礎結構 (PKI) 來將電腦憑證簽發並散佈至每個端點（建議）或產生自我簽署的電腦憑證以用於匯出。透過預登入方法，需要機器憑證且在 GlobalProtect 元件授予存取權限前，必須在端點上安裝。

若要確認端點屬於您的組織，還必須設定驗證設定檔，以驗證該使用者（請參閱雙因素驗證）。

使用下列工作流程來建立用戶端憑證，並手動部署至端點。如需更多資訊，請參閱關於 GlobalProtect 使用者驗證。如需組態範例，請參閱遠端存取 VPN（憑證設定檔）。

STEP 1 | 將用戶端憑證發出至 GlobalProtect 應用程式和端點。

這將啟用 GlobalProtect 入口網站和閘道，以驗證該端點屬於您的組織。

1. 建立用來針對 GlobalProtect 元件簽發自我簽署憑證的根 CA 憑證。
2. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證），然後按一下 **Generate**（產生）。
3. 輸入 **Certificate Name**（憑證名稱）。憑證名稱不能包含空格。
4. 在 **Common Name**（通用名稱）欄位中輸入將會顯示在憑證上的 IP 位址或 FQDN。

5. 從 **Signed By**（簽署者）下拉式清單中選取根 CA。
6. 選取 **OCSP Responder**（**OCSP** 回應程式）來驗證憑證的撤銷狀態。
7. 為憑證進行 **Cryptographic Settings**（加密設定），包括加密 **Algorithm**（演算法），金鑰長度（**Number of Bits**（位元數）），**Digest**（摘要）演算法（使用 sha1、sha256、sha384 或 sha512），以及憑證 **Expiration**（過期）（以天為單位）。

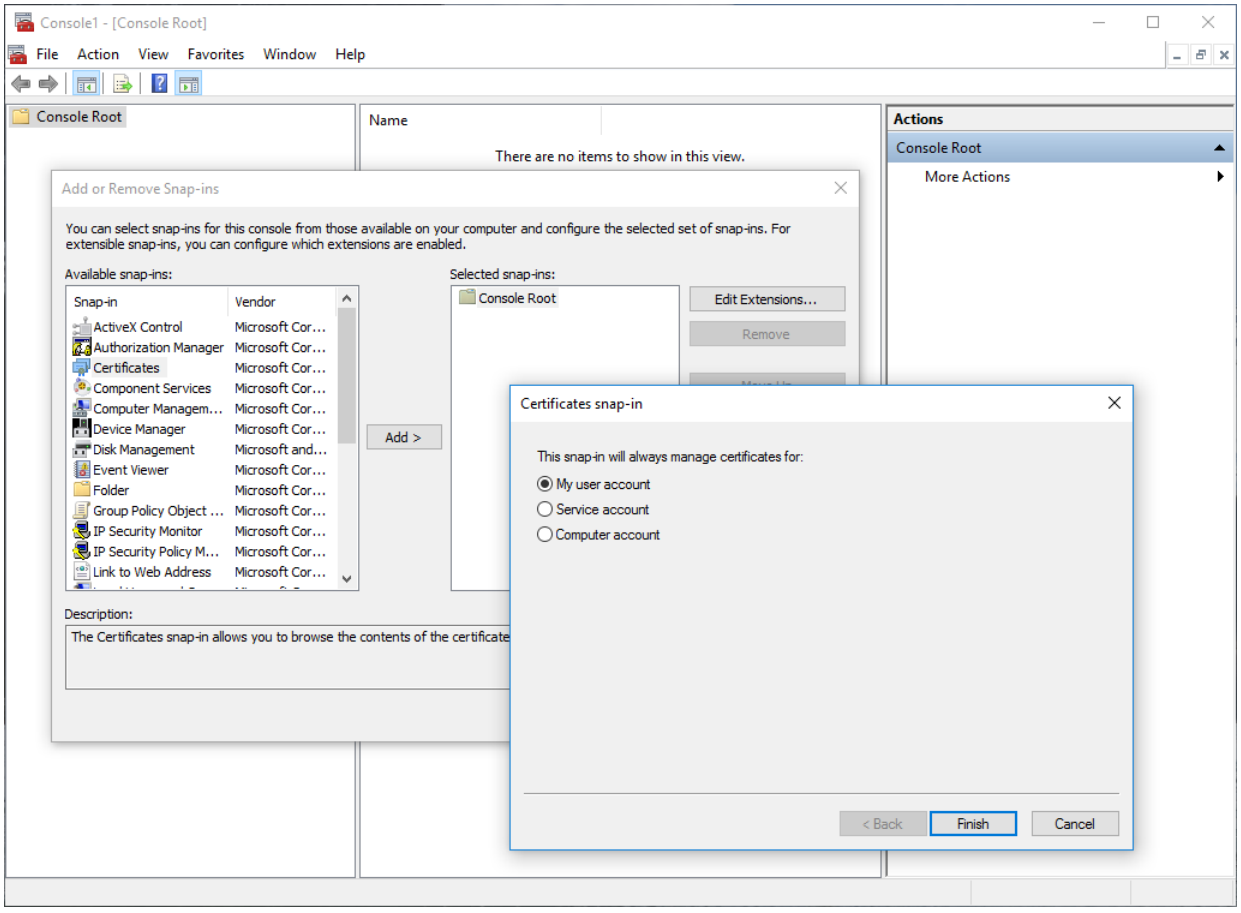
   若防火牆處於 FIPS-CC 模式，且金鑰產生演算法為 RSA，則 RSA 金鑰必須為 2,048 或 3072 位元。
8. 在 **Certificate Attributes**（憑證屬性）區域，**Add**（新增）並定義屬性來將端點識別為屬於您的組織。請記住，如果您新增 **Host Name**（主機名稱）屬性（會填入憑證的 SAN 欄位），則必須與您定義的 **Common Name**（通用名稱）值完全符合。
9. 按一下 **OK**（確定）即可產生憑證。

STEP 2 | 在端點的個人憑證存放區中安裝憑證。

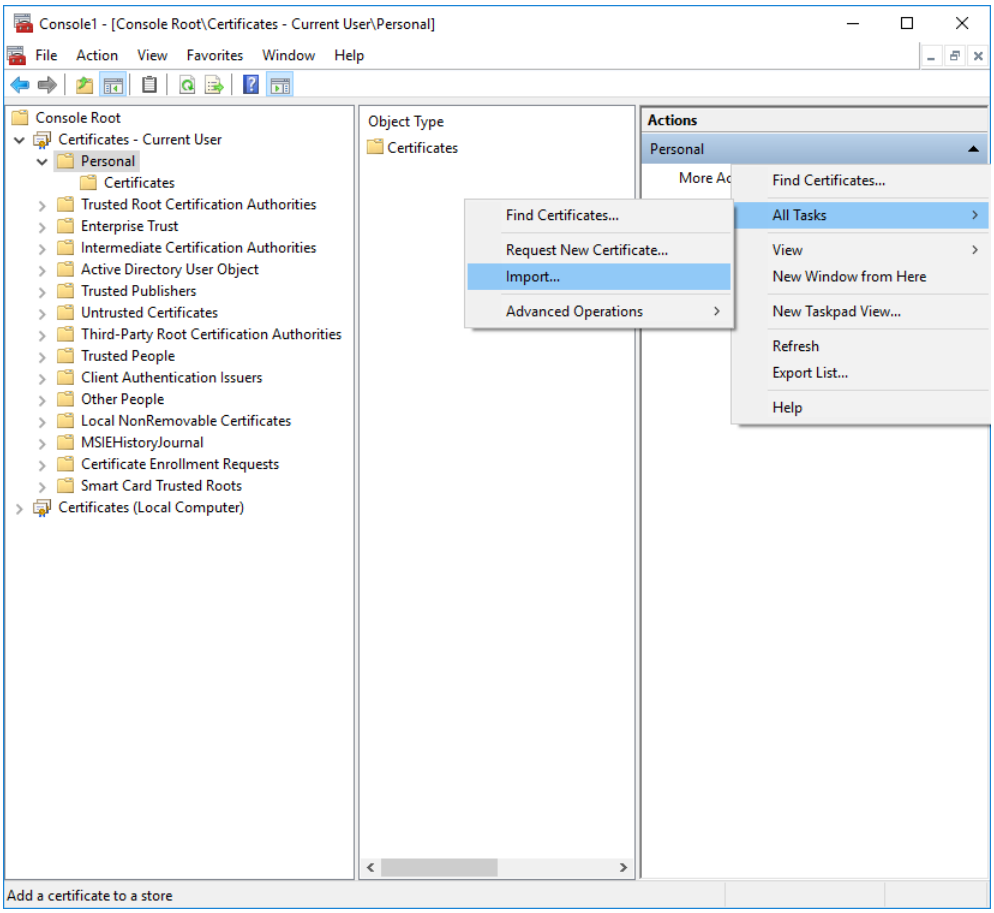
如果您使用唯一使用者憑證或電腦憑證，在初次入口網站/閘道連線之前，您必須將每個憑證安裝在端點的個人憑證存放區中。將電腦憑證安裝到 Windows 的本機電腦憑證存放區以及 macOS 的系統金鑰鏈中。將使用者憑證安裝到 macOS 上的 Windows 與 Keychain 的目前使用者憑證存放區。

例如，若要使用 Microsoft 管理主控台在 Windows 系統安裝憑證：

1. 從命令提示中，輸入 `mmc` 來啟動 Microsoft 管理主控台。
2. 選取 **File**（檔案）> **Add/Remove Snap-in**（新增/移除嵌入式管理單元）。
3. 從 **Available snap-ins**（可用嵌入式管理單元）清單中，選取 **Certificates**（憑證），然後根據您匯入的憑證類型，**Add**（新增）並選取下列憑證嵌入式管理單元之一：
   - **Computer account**（電腦帳戶）—如果您要匯入電腦憑證，請選取此選項。
   - **My user account**（我的使用者帳戶）—如果您要匯入使用者憑證，請選取此選項。



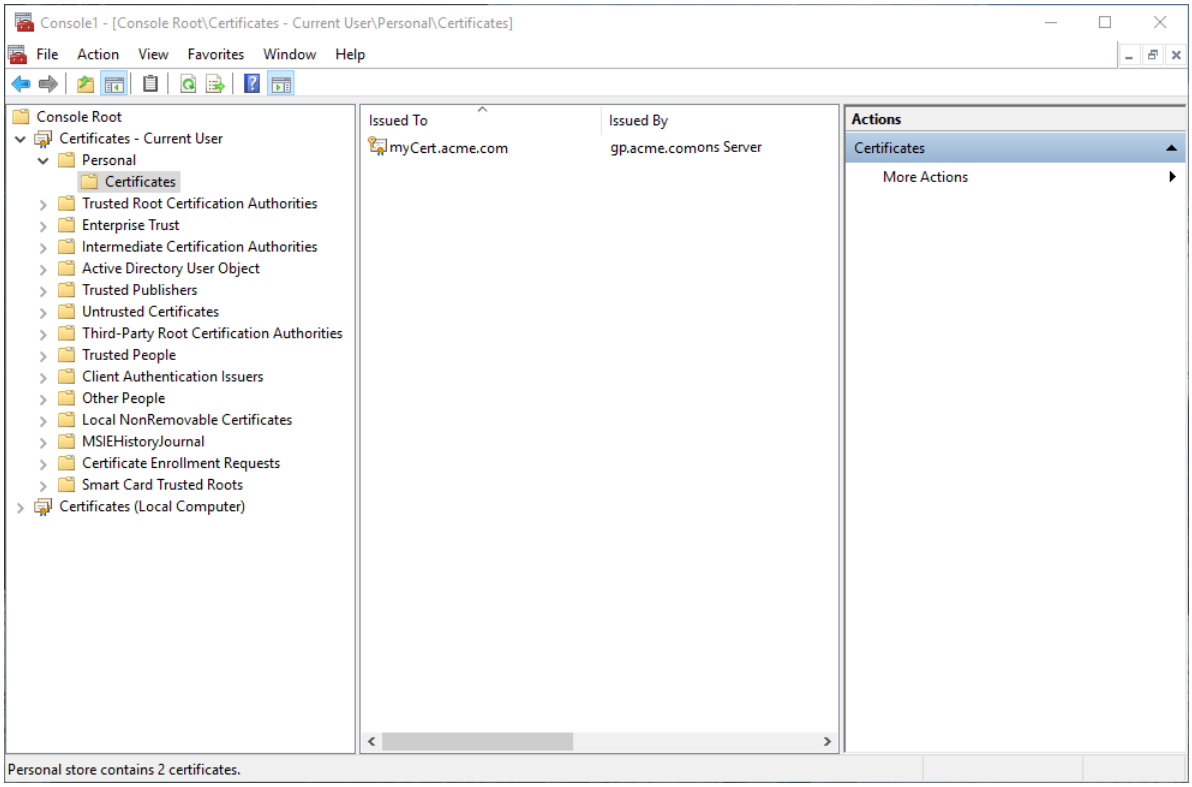
4. 從 **Console Root**（主控台根）中，展開 **Certificates**（憑證），然後選取 **Personal**（個人）。
5. 在 **Actions**（動作）欄中，選取 **Personal**（個人）> **More Actions**（其他動作）> **All Tasks**（所有工作）> **Import**（匯入），然後依照憑證匯入精靈中的步驟來匯入您從 CA 收到的 PKCS 檔案。



6. **Browse**（瀏覽）至並選取要匯入的 .p12 憑證檔案（選取 **Personal Information Exchange**（個人資訊交換）作為要瀏覽的檔案類型），並輸入您用來加密私人金鑰的 **Password**（密碼）。將 **Certificate store**（憑證存放區）設定為 **Personal**（個人）。

STEP 3 | 確認憑證已新增至個人憑證存放區。

從 **Console Root**（主控台根）導覽至個人憑證存放區（**Certificates**（憑證）> **Personal**（個人）> **Certificates**（憑證）：



STEP 4 | 將用來簽發用戶端憑證的根 CA 憑證匯入至防火牆。

只有由外部 CA 簽發用戶端憑證時，例如公開 CA 或企業 PKI，此步驟才為必要。如果您使用自我簽署的憑證，根 CA 則已由入口網站/閘道所信任。

1. 下載用來簽發用戶端憑證的根 CA 憑證（Base64 格式）。
2. 從產生用戶端憑證的 CA 匯入根 CA 憑證至防火牆：
    1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證），然後按一下 **Import**（匯入）。
    2. 將 **Certificate Type**（驗證類型）設定為 **Local**（本機）（預設）。
    3. 輸入作為用戶端 CA 憑證識別的 **Certificate Name**（憑證名稱）。
    4. **Browse**（瀏覽）至並選取從 CA 下載的 **Certificate File**（憑證檔案）。
    5. 將 **File Format**（檔案格式）設定為 **Base64 Encoded Certificate (PEM)**（**Base64 編碼憑證 (PEM)**），然後按一下 **OK**（確定）。
    6. 在 **Device Certificates**（裝置憑證）頁籤上，選取您剛才匯入的憑證以開啟憑證資訊。
    7. 選取 **Trusted Root CA**（信任根 **CA**），然後按一下 **OK**（確定）。

STEP 5 | 建立用戶端憑證設定檔。

1. 選取 **Device**（設備）> **Certificates**（憑證）> **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔）以 **Add**（新增）新的憑證設定檔。
2. 輸入設定檔 **Name**（名稱）。
3. 選取 **Username Field**（使用者名稱欄位）值，來指定憑證中的哪個欄位將包含使用者的識別資訊。

    如果您計劃設定入口網站或閘道，以僅透過憑證驗證使用者，您必須指定 **Username Field**（使用者名稱欄位）。這讓 GlobalProtect 可以透過憑證關聯使用者名稱。

    如果您計劃為雙因素驗證設定入口網站或閘道，可以將預設值設為 **None**（無），或若要新增其他安全層，指定一個使用者名稱。如果您指定使用者名稱，您的外部驗證服務確認用戶端憑證中的使用者名稱與使用者名稱要求驗證相符。這樣可確保使用者是接收憑證的使用者。

使用者無法變更包含在憑證中的使用者名稱。

4. 在 **CA Certificates**（**CA** 憑證）區域，按一下 **Add**（新增）。選取您在步驟 4 中從 **CA Certificates**（**CA** 憑證）下拉式清單匯入的受信任的根 CA 憑證，然後按一下 **OK**（確定）。

STEP 6 | 儲存組態。

Commit（提交）變更。

部署驗證的使用者指定用戶端憑證

若要驗證個別使用者—您必須將唯一的用戶端憑證發出給每個 GlobalProtect 使用者，並在啟用 GlobalProtect 之前先將他們部署至端點。若要自動化使用者指定用戶端憑證的產生和部署，您可以設定 GlobalProtect 入口網站，將其用作企業 PKI 中 SCEP 伺服器的簡易憑證註冊通訊協定 (SCEP) 用戶端。

SCEP 在該企業 PKI 中動態運作，以便在入口網站請求時產生使用者指定憑證，並將憑證傳送至入口網站。入口網站然後以透明方式部署憑證至應用程式。當使用者請求存取時，應用程式可以出示用戶端憑證以向入口網站或閘道驗證。

GlobalProtect 入口網站或閘道會使用關於端點和使用者的識別資訊，以評估是否允許使用者存取。如果主機 ID 位於裝置封鎖清單上，或工作階段與任何憑證設定檔內指定的封鎖選項相符，GlobalProtect 將封鎖存取權。如果由於無效的基於 SCEP 的用戶端憑證導致驗證失敗，GlobalProtect 應用程式會嘗試根據驗證設定檔內的設定向入口網站驗證，並擷取憑證。如果應用程式無法從入口網站擷取憑證，端點將無法連線。

STEP 1 | 建立 SCEP 設定檔。

1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **SCEP**，然後 **Add**（新增）新的 SCEP 設定檔。
2. 輸入用來識別 SCEP 設定檔的 **Name**（名稱）。
3. 如果此設定檔適用於具有多重虛擬系統功能的防火牆，請選取一個虛擬系統或 **Shared**（共用）作為設定檔可用的 **Location**（位置）。

STEP 2 | （選用）為使基於 SCEP 的憑證產生更安全，在 PKI 與各憑證要求的入口網站之間設定 SCEP 質詢回應機制。

在您設定此機制後，其操作不可見，不必進行進一步輸入。

為了符合美國為了符合聯邦資訊處理標準 (FIPS)，請使用 **Dynamic**（動態）**SCEP** 挑戰 ，並指定一個使用 HTTPS 的 **Server URL**（伺服器 **URL**）（請參閱步驟 7）。

選取下列其中一個 **SCEP** 挑戰選項：

- **None**（無）— （預設）SCEP 伺服器在簽發憑證之前，不會質詢入口網站。
- **Fixed**（固定）— 輸入從 PKI 基礎結構的 SCEP 伺服器中取得的註冊質詢 **Password**（密碼）。
- **Dynamic**（動態）—輸入 **Username**（使用者名稱）和您選取的 **Password**（密碼）（可能是 PKI 管理員的認證）以及入口網站用戶端提交這些認證的 SCEP **Server URL**（伺服器 **URL**）。認證用於向 SCEP 伺服器驗證，以透明方式產生用於每次憑證要求的入口網站 OTP 密碼。(您可以看到螢幕在註冊挑戰密碼是欄位中重新整理後，此 OTP 將根據每個憑證要求變更）。PKI 以透通方式將每個新密碼傳輸至入口網站，其接著使用該密碼用於憑證要求。

STEP 3 | 指定 SCEP 伺服器與入口網站之間的連線設定，以啟用入口網站來請求和接收用戶端憑證。

您可以透過在憑證 **Subject**（主旨）名稱中指定權杖，來包含關於端點或使用者的其他資訊。

在對 SCEP 伺服器的 CSR **Subject**（主旨）欄位中，入口網站會包含權杖值作為 **CN** 和主機 ID 作為 **SerialNumber**。主機 ID 會依端點類型而有所不同：GUID (Windows)、介面的 MAC 位址 (macOS)、Android ID（Android 端點）、UDID（iOS 端點）或 GlobalProtect 指派的唯一名稱 (Chrome)。

1. 在 **Configuration**（組態）區域，輸入入口網站用於連線 PKI 中 SCEP 伺服器的 **Server URL**（伺服器 **URL**）（例如 `http://10.200.101.1/certsrv/mscep/`）。
2. 輸入 **CA-IDENT Name**（**CA-IDENT** 名稱）（長度最大為 255 個字元），用以識別 SCEP 伺服器。
3. 輸入 SCEP 伺服器所產生之憑證使用的 **Subject**（主旨）名稱。主旨必須是一個格式為 <**attribute**>=<**value**> 的辨別名稱，且必須包含通用名稱 (CN) 屬性 (CN=<**variable**>)。CN 支援下列動態權杖：
   - `$USERNAME`—使用此權杖讓入口網站能向特定使用者要求憑證。若要使用此變數，您也必須啟用群組對應。使用者輸入的使用者名稱必須與使用者群組對應表格中的名稱相符。
   - `$EMAILADDRESS`—使用此權杖以要求與特定電子郵件地址關聯的憑證。若要使用此變數，您也必須啟用群組對應並在伺服器設定檔的 **Mail Domains**（郵件網域）區域中設定 **Mail Attributes**（郵件屬性）。若 GlobalProtect 無法辨識使用者的電子郵件地址，便會產生唯一的 ID 並以該值填入 CN。
   - `$HOSTID`—若要僅為端點要求憑證，請指定主機 ID 權杖。當使用者嘗試登入入口網站時，端點會傳送識別資訊，其中包括其主機 ID 值。

   當 GlobalProtect 入口網站將 SCEP 設定推送至應用程式時，主旨名稱的 CN 部分會取代為憑證擁有者的實際值（使用者名稱、主機 ID 或電子郵件地址）（例如，**`O=acme,CN=johndoe`**）。
4. 選取 **Subject Alternative Name Type**（主旨替代名稱類型）：
   - **RFC 822 Name**（**RFC 822** 名稱）—在憑證的主旨或主旨替代副檔名輸入電子郵件名稱。
   - **DNS Name**（**DNS** 名稱）—輸入用於評估憑證的 DNS 名稱。
   - **Uniform Resource Identifier**（統一資源識別項）—輸入應用程式從中取得憑證的資源名稱。
   - **None**（無）—請勿指定憑證的屬性。

STEP 4 | （選用）進行憑證 **Cryptographic Settings**（密碼設定）。

- 選取憑證的 **Number of Bits**（位元數）（金鑰長度）。

  如果防火牆處於 FIPS-CC 模式，則金鑰產生演算法為 RSA。RSA 金鑰必須為 2,048 位元或更大。
- 選取 **Digest for CSR**（**CSR** 摘要），這會指出憑證簽署請求 (CSR) 的摘要演算法：憑證簽署要求 (CSR)：sha1、sha256、sha384 或 sha512。

STEP 5 | （選用）設定允許使用的憑證（簽署或加密）。

- 若要使用此憑證進行簽署，請選取 **Use as digital signature**（用作數位簽章）核取方塊。此選項可讓端點使用憑證中的私密金鑰來驗證數位特徵碼。
- 若要使用此憑證進行加密，請選取 **Use for key encipherment**（用作金鑰加密）核取方塊。此選項可讓應用程式使用憑證中的私密金鑰來加密透過 HTTPS 連線（使用 SCEP 伺服器核發的憑證建立連線）交換的資料。

STEP 6 | （選用）若要確保入口網站連線至正確的 SCEP 伺服器，請輸入 **CA Certificate Fingerprint**（**CA** 憑證指紋）。從 SCEP 伺服器介面的 **Thumbprint**（指紋）欄位取得該指紋。

1. 為 SCEP 伺服器管理員 UI 輸入 URL（例如 **`http://<hostname or IP>/CertSrv/mscep_admin/`**）。
2. 複製指紋並在 **CA Certificate Fingerprint**（**CA** 憑證指紋）欄位中輸入。

STEP 7 | 啟用 SCEP 伺服器與 GlobalProtect 入口網站之間的手動 SSL 驗證。這需要符合美國美國聯邦資訊處理標準 (FIPS)。

FIPS-CC 操作顯示於防火牆登入頁面及其狀態列。

選取 SCEP 伺服器的根 **CA Certificate**（**CA** 憑證指紋）。選取 **Client Certificate**（用戶端憑證）來選取性地在 SCEP 伺服器與 GlobalProtect 入口網站之間啟用相互 SSL 驗證。

STEP 8 | 儲存並提交組態。

1. 按一下 **OK**（確定）以儲存設定。
2. **Commit**（提交）組態。

入口網站嘗試使用 SCEP 設定檔中的設定請求 CA 憑證，並將其儲存至托管入口網站的防火牆。如果成功，CA 憑證將顯示在 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）中。

STEP 9 | （選用）如果在儲存 SCEP 設定檔之後，入口網站無法取得憑證，您可以手動透過入口網站產生憑證簽署請求 (CSR)。

1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證），然後 **Generate**（產生）新的憑證。
2. 選取 **SCEP** 作為 **Certificate Type**（憑證類型）。
3. 輸入 **Certificate Name**（憑證名稱）。此名稱不能包含空格。
4. 選取 **SCEP Profile**（**SCEP** 設定檔），用以提交 CSR 至企業 PKI。
5. 按一下 **OK**（確定），以提交請求並產生憑證。

STEP 10 | 設定雙因素驗證。

指派 SCEP 設定檔 GlobalProtect 入口網站代理程式組態以啟用入口網站要求和部署用戶端憑證至接收此組態的應用程式。

設定雙因素驗證

如果您需要強驗證保護敏感資產，或符合法規要求，如 PCI、SOX 或 HIPAA，設定 GlobalProtect 以使用（用雙因素驗證計劃的）驗證服務。雙因素驗證架構需要兩項內容：一般使用者知道的內容（例如 PIN 或密碼）以及一般使用者擁有的內容（硬體或軟體權杖/OTP、智慧卡或憑證）。您也可以透過外部驗證服務的組合、用戶端和憑證設定檔，啟用雙因素驗證。

以下主題提供如何在 GlobalProtect 中設定雙因素驗證的範例：

- 透過憑證和驗證設定檔啟用雙因素驗證
- 使用一次性密碼 (OTP) 啟用雙因素驗證
- 使用智慧卡啟用雙因素驗證
- 使用軟體權杖應用程式啟用雙因素驗證

透過憑證和驗證設定檔啟用雙因素驗證

以下工作流程顯示了如何設定 GlobalProtect，以要求使用者同時向憑證設定檔與驗證設定檔進行驗證。使用者必須成功使用這兩種方法驗證才能連線至入口網站/閘道。如需此設定的詳細資訊，請參閱使用雙因素驗證的遠端存取 VPN。

STEP 1 | 建立驗證伺服器設定檔。

驗證伺服器設定檔會指示防火牆連線至外部驗證服務及針對您的使用者擷取驗證認證的方式。

如果您使用 *LDAP* 連線至 *Active Directory (AD)*，則必須為每個 *AD* 網域建立個別的 *LDAP* 伺服器設定檔。

1. 選取 **Device**（裝置）> **Server Profiles**（伺服器設定檔），然後選取設定檔類型（**LDAP**、**Kerberos**、**RADIUS** 或 **TACACS+**）。
2. **Add**（新增）新伺服器設定檔。
3. 輸入 **Profile Name**（設定檔名稱），例如 `gp-user-auth`。
4. （僅限 LDAP）選取 LDAP 伺服器 **Type**（類型）（**active-directory**、**e-directory**、**sun** 或 **other**（其他））。
5. 在 **Servers**（伺服器）或 **Servers List**（伺服器清單）區域按一下 **Add**（新增）（根據伺服器設定檔類型），然後輸入下列資訊以連線至驗證服務：
   - 伺服器的 **Name**（名稱）
   - **Server**（伺服器）FQDN 的 IP 位址
   - 連接埠
6. （僅限 RADIUS、TACACS+ 與 LDAP）指定下列設定，以允許防火對驗證服務進行驗證：
   - RADIUS 和 TACACS+ —新增伺服器項目時輸入共用 **Secret**（密碼）。
   - LDAP—輸入 **Bind DN**（繫結 **DN**）與 **Password**（密碼）。
7. （僅限 LDAP）如果您希望端點使用 SSL 或 TLS 更安全的連線目錄伺服器，啟用選項以 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全連線）（預設為已啟用）。端點使用的協定視乎 **Server list**（伺服器清單）中的伺服器 **Port**（連接埠）而定：
   - 389（預設）—TLS（特別是端點會使用 StartTLS 操作，用來升級連接至 TLS 的初始純文字連線）。
   - 636—SSL。
   - 任何其他連接埠—端點首先會嘗試使用 TLS。若目錄伺服器不支援 TLS，則端點使用 SSL。
8. （僅限 LDAP）為了獲得額外的安全，請啟用選項以 **Verify Server Certificate for SSL sessions**（確認 **SSL** 工作階段的伺服器憑證），讓端點確認目錄伺服器為 SSL/TLS 連線所呈現的憑證。若要啟用此驗

證，您也必須啟用選項以 **Require SSL/TLS secured connection**（需要 SSL/TLS 安全連線）。為了成功驗證，必須符合下列狀況之一：

- 憑證位於裝置憑證清單內：**Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（設備憑證）。如有必要，將憑證匯入端點中。
- 憑證簽署者位於受信任的憑證授權單位清單中：**Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Default Trusted Certificate Authorities**（預設的受信任憑證授權單位）。

9. 按一下 **OK**（確定）來儲存伺服器設定檔。

STEP 2 | 建立識別驗證使用者服務的驗證設定檔。您稍後可以選擇在入口網站和閘道上指派設定檔選項。

1. 選取 **Device**（設備）> **Authentication Profile**（驗證設定檔），然後按一下 **Add**（新增）來新增設定檔。
2. 輸入設定檔的 **Name**（名稱）。
3. 選取 **Authentication**（驗證）**Type**（類型）。
4. 選取在步驟 1 中建立的 **Server Profile**（伺服器設定檔）。
5. （僅限 LDAP）輸入 **sAMAccountName** 作為**Login Attribute**（登入屬性）。
6. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 3 | 建立入口網站用於比對這些來自使用者端點之用戶端憑證的用戶端憑證設定檔。

當設定雙因素驗證，以使用用戶端憑證時，外部驗證服務使用使用者名稱值以驗證用戶端憑證中的使用者（如指定）。這樣可確保登入的使用者實際上正是接收憑證的使用者。

1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔），然後 **Add**（新增）新的憑證設定檔。
2. 輸入設定檔的 **Name**（名稱）。
3. 選取下列其中一個 **Username Field**（使用者名稱欄位）值：
   - 如果您想要用戶端憑證驗證個別使用者，選取識別使用者的憑證欄位。
   - 如果您要從入口網站部署用戶端憑證，請選取 **None**（無）。
   - 如果您要設定與預先登入連線方法搭配使用的憑證設定檔，請選取 **None**（無）。
4. **Add**（新增）您要指定給設定檔的 **CA Certificates**（**CA** 憑證），然後進行下列設定：
   1. 選取 **CA certificate**（**CA** 憑證），受信任的根 CA 憑證或來自 SCEP 伺服器的 CA 憑證。如有必要，匯入憑證。
   2. （選用）輸入 **Default OCSP URL**（預設 **OCSP URL**）。
   3. （選用）選取 **OCSP Verify Certificate**（**OCSP** 確認憑證）憑證。
   4. （選用）輸入用於簽署憑證之範本的 **Template Name**（範本名稱）。
5. （選用）選取下列選項以指定何時封鎖使用者要求工作階段：
   1. 憑證狀態未知。
   2. GlobalProtect 元件未在 **Certificate Status Timeout**（憑證狀態逾時）規定的秒數內擷取憑證狀態。
   3. 用戶端憑證主體中的序號屬性，與 GlobalProtect 應用程式向端點報告的主機 ID 不相符。
   4. 憑證已過期。
6. 按一下 **OK**（確定）。

STEP 4 | （選用）將用戶端憑證發出至 GlobalProtect 用戶端和端點。

若要以透明方式部署用戶端憑證，設定您的入口網站以散佈共用用戶端憑證至您的端點或設定入口網站以使用 SCEP 請求和部署唯一的每個使用者的用戶端憑證。

1. 使用您的企業 PKI 或公開 CA 將用戶端憑證發出給每個 GlobalProtect 使用者。
2. 針對預先登入連線方法，在端點的個人憑證存放區中安裝憑證。

STEP 5 | 儲存 GlobalProtect 設定。

按一下 **Commit**（交付）。

使用一次性密碼 (OTP) 啟用雙因素驗證

使用工作流程，透過一次性密碼 (OTP) 在入口網站和閘道上設定雙因素驗證。當使用者要求存取時，入口網站或閘道提示使用者輸入 OTP。驗證服務會將 OTP 作為權杖傳送到使用者的 RSA 裝置。

設定雙因素驗證計劃與設定其他驗證類型類似。雙因素驗證計劃需要您設定：

- 伺服器設定檔（通常用於雙因素驗證的 RADIUS 服務）被指派至驗證設定檔。
- 用戶端驗證設定檔包含這些元件使用服務的驗證設定檔。

依預設，應用程式將會提供用來登入入口網站與閘道的相同認證。對於 OTP 驗證，此行為將會導致驗證初始時在閘道失敗，而且由於延遲的關係，也會導致提示使用者登入，使用者的 OTP 可能會到期。若要防止這一情形，您必須設定提示需要 OTP 的入口網站和閘道，而不是根據應用程式組態使用相同的認證。

您也可以透過設定驗證取代，減少提示使用者提供 OTP 的頻率。這將啟用入口網站和閘道，以產生和接受安全加密 cookie，從而在特定時間內驗證使用者。入口網站和/或閘道在 cookie 過期前，不要求新的 OTP，從而減少了使用者必須提供 OTP 的次數。

STEP 1 | 在您設定後端 RADIUS 服務以產生 OTP 的權杖，並確保使用者有必要的裝置（如硬體權杖）後，請設定 RADIUS 伺服器以與防火牆互動。

如需特定指示，請參閱您 RADIUS 伺服器的文件集。在大多數情況下，您都需要在 RADIUS 伺服器上設定驗證代理程式與用戶端組態，以實現防火牆與 RADIUS 伺服器之間的通訊。您也必須針對要用於加密防火牆與 RADIUS 伺服器間工作階段的共用密碼予以定義。

STEP 2 | 在裝載閘道與/或入口網站的各防火牆上，建立一個 RADIUS 伺服器設定檔。（針對小型部署，一道防火牆可以裝載入口網站和閘道。）

1. 選取 **Device**（設備）> **Server Profiles**（伺服器設定檔）> **RADIUS**。
2. **Add**（新增）新設定檔。
3. 輸入 RADIUS 設定檔的 **Profile Name**（設定檔名稱）。
4. 在 **Servers**（伺服器）區域中，**Add**（新增）一個 RADIUS 實例，然後輸入：
   - 用來識別此 RADIUS 伺服器的描述性 **Name**（名稱）。
   - **RADIUS Server**（**RADIUS** 伺服器）的 IP 位址。
   - 用來加密防火牆與 RADIUS 伺服器之間工作階段的共用 **Secret**（密碼）
   - RADIUS 伺服器將接聽驗證要求的 **Port**（連接埠）號碼（預設為 1812）
5. 按一下 **OK**（確定）來儲存設定檔。

STEP 3 | 建立驗證設定檔。

1. 選取 **Device**（設備）> **Authentication Profile**（驗證設定檔），然後按一下 **Add**（新增）來新增設定檔。
2. 輸入設定檔的 **Name**（名稱）。此名稱不能包含空格。
3. 選取 **RADIUS** 作為驗證服務 **Type**（類型）。
4. 選取您建立用來存取 RADIUS 伺服器的 **Server Profile**（伺服器設定檔）。
5. 輸入 **User Domain**（使用者網域）名稱。防火牆會使用此值來比對驗證的使用者與允許清單項目，也會將其用於 User-ID 群組對應。
6. 選取 **Username Modifier**（使用者名稱修改程式）來修改 RADIUS 伺服器所預期的使用者名稱/網域格式。

7. 按一下 **OK**（確定）來儲存驗證設定檔。

STEP 4 | 指派驗證設定檔至 GlobalProtect 入口網站和/或閘道。

您可以為入口網站和閘道設定多個用戶端驗證組態。對於各用戶端驗證組態，您可以指定驗證設定檔，以套用於特定 OS 的端點。

此步驟說明如何將驗證設定檔新增至入口網站或閘道組態。如需設定這些元件的其他詳細資訊，請參閱 GlobalProtect 入口網站與 GlobalProtect 閘道。

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）或 **Gateways**（閘道）。
2. 選取現有入口網站或閘道組態，或 **Add**（新增）一個。如果您在新增新的入口網站或閘道，請指定其名稱、位置和網路參數。
3. 在 **Authentication**（驗證）頁籤上，選取 **SSL/TLS service Profile**（**SSL/TLS** 服務設定檔）或 **Add**（新增）一個新設定檔。
4. **Add**（新增）新的 **Client Authentication**（用戶端驗證）組態，然後進行下列設定：
   - 用戶端驗證組態的 **Name**（名稱）。
   - 此組態適用的端點 **OS**。
   - 您在建立驗證設定檔中建立的 **Authentication Profile**（驗證設定檔）。
   - （選用）自訂 **Username Label**（使用者名稱標籤）。
   - （選用）自訂 **Password Label**（密碼標籤）。
   - （選用）自訂 **Authentication Message**（驗證訊息）。
5. 按一下 **OK**（確定）來儲存組態。

STEP 5 | （選用）設定入口網站或閘道，每次使用者登入時提示輸入使用者名稱和密碼，或僅輸入密碼。透過 OTP 的雙因素驗證不支援儲存密碼，因為使用者每次登入時必須輸入一個動態密碼。

此步驟描述了在入口網站代理程式組態中進行密碼設定的方法。如需其他詳細資訊，請參閱自訂 GlobalProtect 應用程式。

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後選取現有入口網站組態。
2. 在 GlobalProtect 入口網站組態對話方塊上，選取 **Agent**（代理程式）。
3. 選取現有代理程式組態或 **Add**（新增）一個。
4. 在 **Authentication**（驗證）頁籤上，將 **Save User Credentials**（儲存使用者認證）設定為 **Save Username Only**（僅儲存使用者名稱）或 **No**（否）。此設定讓 GlobalProtect 在您接下來步驟中選取各元件時，提示使用者輸入動態密碼。
5. 按兩下 **OK**（確定）儲存組態。

STEP 6 | 選取 GlobalProtect 元件—閘道入口網站和類型—提示輸入動態密碼，如 OTP。

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後選取現有入口網站組態。
2. 在 GlobalProtect 入口網站組態對話方塊上，選取 **Agent**（代理程式）。
3. 選取現有代理程式組態或 **Add**（新增）一個。
4. 在 **Authentication**（驗證）頁籤上，選取 **Components that Require Dynamic Passwords (Two-Factor Authentication)**（需要動態密碼的元件（雙因素驗證））。當被選取時，入口網站和/或閘道的類型提示輸入 OTP。

   請勿為任何使用 *SAML* 驗證的元件選取 *Components that Require Dynamic Passwords (Two-Factor Authentication)*（需要動態密碼元件（雙因素驗證））選項。
5. 按兩下 **OK**（確定）儲存組態。

STEP 7 | 如果啟用了單一登入 (SSO)，將其停用。由於代理程式組態指定 RADIUS 作為驗證服務，因此不支援 Kerberos SSO。

此步驟描述了如何停用 SSO。如需更多詳細資訊，請參閱定義 GlobalProtect 代理程式組態。

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後選取現有入口網站組態。
2. 在 GlobalProtect 入口網站組態對話方塊上，選取 **Agent**（代理程式）。
3. 選取現有代理程式組態或 **Add**（新增）一個。
4. 在 **App**（應用程式）頁籤上，將 **Use Single Sign-on (Windows Only)**（使用單一登入（僅 **Windows**））設定為 **No**（否）。
5. 按兩下 **OK**（確定）儲存組態。

STEP 8 | （選用）若要最小化使用者必須提供認證的次數，設定驗證取代。

依預設，入口網站或閘道透過驗證設定檔和選用的憑證設定檔驗證使用者。透過驗證取代，入口網站或閘道使用其部署至端點的加密 cookie 驗證使用者。Cookie 有效時，使用者可登入，無需輸入常規認證或 OTP。如需更多資訊，請參閱在入口網站或閘道上的 Cookie 驗證。

必須封鎖 *cookie* 未過期的端點存取時（例如端點遺失或被盜），您可以將該裝置新增到封鎖清單以封鎖端點存取。

如需更多詳細資訊，請參閱 GlobalProtect 入口網站 與 GlobalProtect 閘道。

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）或 **Gateways**（閘道）。
2. 選取現有入口網站或閘道組態，或 **Add**（新增）一個。
3. 根據是否要設定入口網站或閘道，請選取下列選項之一：
   - **GlobalProtect** 入口網站組態—在 GlobalProtect 入口網站組態對話方塊上，選取 **Agent**（代理程式 > *<agent-config>* > **Authentication**（驗證）。
   - **GlobalProtect** 閘道組態—在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Client Settings**（用戶端設定）> *<client-setting>* > **Authentication Override**（驗證取代）。
4. 進行下列 **Authentication Override**（驗證取代）設定：
   - 驗證取代的 **Name**（名稱）。
   - **Generate cookie for authentication override**（為驗證取代產生 **cookie**）—啟用入口網站或閘道，以產生加密的端點指定 cookie。使用者成功驗證後，入口網站或閘道發出驗證 cookie 至端點。
   - **Accept cookie for authentication override**（接受驗證取代 **cookie**）—讓入口網站或閘道透過有效的、加密 cookie 驗證使用者。端點提供有效的 Cookie 後，入口網站或閘道可驗證透過入口網站或閘道加密的 Cookie，解密 Cookie，接著驗證使用者。

     GlobalProtect 應用程式必須知道連線使用者的使用者名稱才能比對和擷取來自使用者端點的驗證 *cookie*。應用程式擷取 *cookie* 後，會將其傳送至入口網站或閘道以進行使用者驗證。

     （僅限 *Windows*）如果您在门户网站代理配置中将“使用单一登录”选项设置为“是”（已启用*SSO*）（*Network*（網路）> *GlobalProtect* > *Portals*（入口網站）> *<portal-config>* > *Agent*（代理程式）> *<agent-config>*. > *App*（應用程式），*GlobalProtect* 應用程式將使用 *Windows* 使用者名稱擷取使用者的本機驗證 *cookie*。如果您將 *Use Single Sign-On*（使用單一登入）選項設為 *No*（否）（*SSO* 已停用），則必須允許 *GlobalProtect* 應用程式 儲存使用者認證 才能擷取使用者的驗證 *cookie*。將 *Save User Credentials*（儲存使用者認證）選項設為 *Yes*（是）以儲存使用者名稱和密碼，或設為 *Save Username Only*（僅儲存使用者名稱）以僅儲存使用者名稱。

     （ 僅限 *macOS*）由於 *macOS* 端點不支援單一登入，因此必須允許 *GlobalProtect* 應用程式 *Save User Credentials*（儲存使用者認證）才能擷取使用者的驗證 *cookie*。將 *Save User Credentials*（儲存使用者認證）選項設為 *Yes*（是）以儲存使用者名稱和密碼，或設為 *Save Username Only*（僅儲存使用者名稱）以僅儲存使用者名稱。

- **Cookie Lifetime**（**Cookie** 存留時間）—指定 Cookie 有效的小時數、天數或週數。閘道的存留時間一般為 24 小時—以保護敏感資訊—入口網站為 15 天。小時範圍為 1–72；週範圍為 1–52；天數範圍為 1–365。在入口網站或閘道的 cookie 超時後（以先到為準），入口網站或閘道提示使用者驗證並加密一個新的 cookie 遞送至端點。
- **Certificate to Encrypt/Decrypt Cookie**（用於加密/解密 **Cookie** 的憑證）—指定 RSA 憑證，以用於加密與解密 Cookie。您必須在入口網站和閘道上使用相同的憑證。

  最佳做法是，設定 *RSA* 憑證以使用您的網路支援的最強摘要演算法。

  入口網站和閘道使用 RSA 加密填補計劃 PKCS#1 V1.5 以產生 Cookie（透過憑證的公開金鑰）並解密 Cookie（透過憑證的私密金鑰）。

5. 按兩下 **OK**（確定）儲存組態。

STEP 9 | **Commit**（提交）組態。

STEP 10 | 確認組態。

從執行 GlobalProtect 應用程式的端點，嘗試連線至您啟用 OTP 驗證的閘道或入口網站。您應該會看到類似下文的提示：

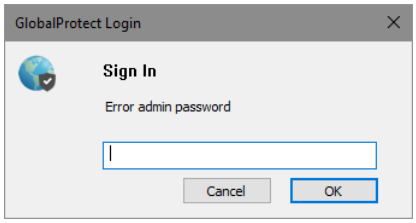


圖 1: OTP 快顯提示

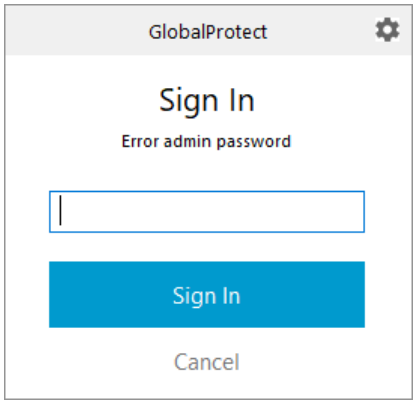


圖 2: GlobalProtect 狀態面板上的 **OTP** 提示

使用智慧卡啟用雙因素驗證

如果您想要讓一般使用者使用智慧卡或通用存取卡 (CAC) 進行驗證，您必須將發出包含在 CAC 或智慧卡中憑證的根 CA 憑證匯入至入口網站和閘道。然後您可以建立包含該根 CA 的憑證設定檔，並將其套用至您的入口網站與/或閘道設定，以便能夠在驗證程序中使用智慧卡。

STEP 1 | 設定您的智慧卡基礎結構。

此程序假設您已將智慧卡與智慧卡讀卡機部署給一般使用者。

如需特定指示，請參閱驗證提供者軟體的文件集。

在大多數情況下，智慧卡基礎結構設定涉及針對一般使用者與參與伺服器的產生憑證，在本例中也就是 GlobalProtect 入口網站與/或閘道。

STEP 2 | 匯入發出包含在一般使用者智慧卡中之用戶端憑證的根 CA 憑證。

確定可從管理系統存取憑證，然後完成下列步驟：

1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證），然後 **Import**（匯入）新的憑證。
2. 輸入 **Certificate Name**（憑證名稱）。
3. 輸入從 CA 所收到 **Certificate File**（憑證檔案）的路徑與名稱，或按一下 **Browse**（瀏覽）以找到該檔案。
4. 從 **File Format**（檔案格式）下拉式清單中選取 **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**），然後按一下 **OK**（確定）來匯入憑證。

STEP 3 | 在您要使用 CAC 或智慧卡驗證的每個入口網站/閘道上建立憑證設定檔。

如需其他憑證設定檔欄位的詳細資訊，例如使用 *CRL* 或 *OCSP*，請參閱線上說明。

1. 選取 **Device**（裝置）> **Certificates Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。
2. 選取現有憑證設定檔或 **Add**（新增）一個。
3. 輸入憑證設定檔的 **Name**（名稱）。
4. 選取 PAN-OS 用來比對 User-ID 其 IP 位址的憑證憑證 **Username Field**（使用者名稱欄位）—您可以選取 **Subject**（主旨）以使用通用名稱、**Subject Alt**（主旨替代）：電子郵件 以使用電子郵件地址，或 主旨替代：**Principal Name**（主體名稱）以開啟主體名稱。
5. 在 **CA Certificates**（**CA** 憑證）區域中，**Add**（新增）您在步驟 2 中匯入到憑證設定檔的受信任根 CA 憑證。出現提示時，請選取 **CA Certificate**（**CA** 憑證），然後按一下 **OK**（確定）。
6. 按一下 **OK**（確定）來儲存憑證設定檔。

STEP 4 | 指派憑證設定檔至入口網站或閘道。此步驟說明如何將憑證設定檔新增至入口網站或閘道組態。如需設定這些元件的詳細資訊，請參閱 GlobalProtect 入口網站與 GlobalProtect 閘道。

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）或 **Gateways**（閘道）
2. 選取現有入口網站或閘道組態，或 **Add**（新增）一個。
3. 在 GlobalProtect 閘道組態對話方塊上，選取 **Authentication**（驗證）。
4. 選取您剛剛建立的 **Certificate Profile**（憑證設定檔）。
5. 按一下 **OK**（確定）來儲存組態。

STEP 5 | **Commit**（提交）組態。

STEP 6 | 確認組態。

從執行 GlobalProtect 應用程式的端點，嘗試連線至您已設定啟用智慧卡驗證的閘道或入口網站。系統提示時，插入您的智慧卡並確認您可以成功向 GlobalProtect 驗證。

使用軟體權杖應用程式啟用雙因素驗證

如果您的組織使用的是軟體權杖（軟權杖），例如 RSA SecurID，來實作雙因素驗證，使用者必須先開啟其軟體權杖應用程式並輸入其 PIN 才能取得密碼，然後在 GlobalProtect 應用程式的 **Password**（密碼）欄位輸入密碼。這一兩步程序使得登入程序複雜化。

為了簡化登入程序並改善使用者體驗，GlobalProtect 提供了無縫的軟權杖驗證。使用者在 GlobalProtect **Password**（密碼）欄位輸入 RSA PIN， 且 GlobalProtect 從 RSA 擷取密碼並透過連線繼續，使用者無需採取額外的步驟開啟 RSA 應用程式。

此功能支援以下三種 RSA 模式：PinPad 樣式（PIN 與權杖代碼整合）、Fob 樣式（PIN 後接權杖代碼）與無 Pin 模式。對於 PinPad 與 Fob 樣式，使用者會在 **Password**（密碼）欄位輸入 PIN，且 GlobalProtect 會擷取密碼。在無 Pin 模式下，Password（密碼）欄位會以灰色顯示且使用者會輸入其使用者名稱。

此功能支援安裝 *GlobalProtect™* 應用程式 *5.1* 及更新版本的 *Windows* 裝置。

STEP 1 | 在用戶端 Windows 裝置上變更登錄機碼以實現無縫的軟權杖驗證。

您必須在用戶端 Windows 裝置上變更 Windows 登錄才能實現無縫的軟權杖驗證。GlobalProtect 應用程式只會在初始化時擷取此登錄項目一次。

1. 開啟 Windows 登錄編輯器並選取 **HKEY_LOCAL_MACHINE** > **SOFTWARE**（軟體） > **PALO Also Networks** > **GlobalProtect** > **Settings**（設定）。
2. 將 **auth-api** 值變更為 **yes**。

由於已在用戶端機器中將 *auth-api* 設為 *yes*，因此您應透過基於 *RSA* 的驗證來設定入口網站與閘道。由於 *GlobalProtect* 將嘗試擷取密碼，因此不支援其他驗證設定檔。

由於入口網站與閘道使用 *RSA* 驗證，我們建議您在閘道上啟用基於 *cookie* 的驗證。當 *GlobalProtect* 嘗試取得閘道的密碼時，為入口網站擷取的權杖可能仍在使用中，且由於密碼已被使用，驗證可能會失敗。因此，我們建議您在入口網站上產生驗證取代 *cookie* 並在閘道上接受 *cookie*。

STEP 2 | 使用基於 RSA 的驗證設定入口網站與閘道。

STEP 3 | 在 GlobalProtect 入口網站上啟用基於 cookie 的驗證。

指定 GlobalProtect 取代現有驗證將允許 GlobalProtect 以新建立的密碼取代現有密碼。

1. 選取 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站） > *<portal-config>*；然後選取 **Agent**（代理程式）頁籤。
2. **Add**（新增）代理程式組態或選取現有組態。
3. 選取 **Generate cookie for authentication override**（產生 **Cookie** 以供驗證取代）。

STEP 4 | 啟用 GlobalProtect 閘道以接受驗證取代 cookie。

1. 選取 **Network**（網路） > **GlobalProtect** > **Gateways**（閘道），然後按一下 **Agent**（代理程式）頁籤。
2. 選取 **Client Settings**（用戶端設定），然後選取 GlobalProtect 用戶端組態或新增一個。
3. 選取 **Authentication Override**（驗證取代）；然後，選取 **Accept cookie for authentication override**（接受驗證取代 **cookie**）。

STEP 5 | 選取 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站） > *<portal-config>*；然後選取 **Authentication**（驗證）頁籤。

STEP 6 | **Add**（新增）用戶端驗證設定檔或選取現有設定檔；然後，選取 **Automatically retrieve passcode from SoftToken application**（從 **SoftToken** 應用程式自動擷取密碼）。

設定 strongSwan Ubuntu 與 CentOS 端點驗證

若要將 GlobalProtect 存取延伸到 strongSwan Ubuntu 與 CentOS 端點，請為這些端點設定驗證。

若要檢視在 *Ubuntu Linux* 與 *CentOS* 上支援 *strongSwan* 的 *GlobalProtect* 最小版本，請參閱GlobalProtect 支援的作業系統版本為何？。

如要連線至 GlobalProtect 閘道，使用者必須成功驗證。以下工作流程顯示了如何啟用 strongSwan 端點驗證的示例。如需關於 strongSwan 的完整資訊，請參閱 strongSwan wiki。

- 透過憑證設定檔啟用驗證
- 透過驗證設定檔啟用驗證
- 透過雙因素驗證啟用驗證

透過憑證設定檔啟用驗證

下列工作流程顯示了如何透過憑證設定檔啟用 strongSwan 用戶端驗證的方法。

STEP 1 | 為 GlobalProtect 閘道設定 IPsec 通道，以與 strongSwan 用戶端進行通訊。

1. 選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）。
2. 選取現有閘道或 **Add**（新增）一個。
3. 在 GlobalProtect 閘道組態對話方塊的 **Authentication**（驗證）頁籤中，選取您要用於進行驗證的 **Certificate Profile**（憑證設定檔）。
4. 選取 **Agent**（用戶端）> **Tunnel Settings**（通道設定）以啟用 **Tunnel Mode**（通道模式），並指定下列設定以設定通道：
   - 選取此核取方塊可 **Enable X-Auth Support**（啟用 **X-Auth** 支援）。
   - 如果已設定 **Group Name**（群組名稱）和 **Group Password**（群組密碼），將其移除。
   - 按一下 **OK**（確定）以儲存設定。

STEP 2 | 確認 IPsec 通道設定檔 (**`ipsec.conf`**) **`conn %`** 預設區段內的預設連線設定，為 strongSwan 用戶端正確定義。

`ipsec.conf` 檔案通常可以在 `/etc` 資料夾內找到。

此程序中的組態為以下版本進行了測試和確認：

- *PAN-OS 6.1* 的 *Ubuntu 14.0.4* 帶 *strongSwan 5.1.2* 和 *CentOS 6.5* 帶 *strongSwan 5.1.3*。
- *PAN-OS 7.0* 的 *Ubuntu 14.0.4* 帶 *strongSwan 5.2.1*。

如果您使用不同版本的 *strongSwan*，此程序中的組態可用於參考。如需詳細資訊，請參閱 strongSwan wiki。

將 `ipsec.conf` 檔案 `conn %default` 區段內的下列設定修改為以下建議設定。

```
ikelifetime=20m reauth=yes rekey=yes keylife=10m rekeymargin=3m rekeyfuzz=0%
 keyingtries=1 type=tunnel
```

STEP 3 | 修改 strongSwan 用戶端的 IPsec 設定檔 (**`ipsec.conf`**) 和 IPsec 密碼檔案 (**`ipsec.secrets`**) 以使用建議設定。

`ipsec.secrets` 檔案通常可以在 `/etc` 資料夾內找到。

使用 strongSwan 用戶端使用者名稱作為憑證的通用名稱。

將 `ipsec.conf` 檔案中的以下項目修改成建議設定。

```
conn <connection name> keyexchange=ikev1 authby=rsasig ike=aes-sha1-
modp1024,aes256 left=<strongSwan/Linux-client-IP-address> leftcert=<client
 certificate with the strongSwan client username used as the certificate's
 common name> leftsourceip=%config leftauth2=xauth right=<GlobalProtect-
Gateway-IP-address> rightid="CN=<Subject-name-of-gateway-certificate>"
 rightsubnet=0.0.0.0/0 auto=add
```

將 `ipsec.conf` 檔案中的以下項目修改成建議設定。

```
:RSA <private key file> "<passphrase if used>"
```

STEP 4 | 開始 strongSwan IPsec 服務並連線至您想要 strongSwan 用戶端在驗證 GlobalProtect 閘道時使用的 IPsec 通道。

使用 `config <name>` 變數來命名通道組態。

- Ubuntu：

```
ipsec start ipsec up <name>
```

- CentOS：

```
strongSwan start strongswan up <name>
```

STEP 5 | 確認通道設定正確，且 VPN 至 strongSwan 用戶端和 GlobalProtect 閘道的連線已建立。

1. 確認特定連線的詳細狀態資訊（透過指定連線）或來自 strongSwan 用戶端的所有連線的狀態資訊。
   - Ubuntu：

     ```
     ipsec statusall [<connection name>]
     ```

   - CentOS：

     ```
     strongswan statusall [<connection name>]
     ```

2. 選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）。在 **Info**（資訊）列中，選取閘道為 strongSwan 用戶端連線設定的 **Remote Users**（遠端使用者）。strongSwan 用戶端應在 **Current Users**（目前使用者）下列出。

透過驗證設定檔啟用驗證

下列工作流程顯示了如何透過驗證設定檔啟用 strongSwan 用戶端驗證的方法。驗證設定檔會指定在驗證 strongSwan 用戶端時要使用哪一個伺服器設定檔。

STEP 1 | 為 GlobalProtect 閘道設定 IPsec 通道，以用於與 strongSwan 用戶端進行通訊。

1. 選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）。
2. 選取現有閘道或 **Add**（新增）一個。
3. 在 GlobalProtect 閘道組態對話方塊的 **Authentication**（驗證）頁籤中，選取您要使用的 **Authentication Profile**（驗證設定檔）。

4. 選取 **Agent**（用戶端）> **Tunnel Settings**（通道設定）以啟用 **Tunnel Mode**（通道模式），並指定下列設定以設定通道：
   - 選取此核取方塊可 **Enable X-Auth Support**（啟用 **X-Auth** 支援）。
   - 如未設定，請輸入 **Group Name**（群組名稱）和 **Group Password**（群組密碼）。
   - 按一下 **OK**（確定）以儲存通道設定。

STEP 2 | 確認 IPsec 通道設定檔 (**`ipsec.conf`**) **`conn %`** 預設區段內的預設連線設定，為 strongSwan 用戶端正確定義。

`ipsec.conf` 檔案通常可以在 `/etc` 資料夾內找到。

此程序中的組態為以下版本進行了測試和確認：
- *PAN-OS 6.1* 的 *Ubuntu 14.0.4* 帶 *strongSwan 5.1.2* 和 *CentOS 6.5* 帶 *strongSwan 5.1.3*。
- *PAN-OS 7.0* 的 *Ubuntu 14.0.4* 帶 *strongSwan 5.2.1*。

如果您使用不同版本的 *strongSwan*，此程序中的組態可用於參考。如需詳細資訊，請參閱 strongSwan wiki。

在 `ipsec.conf` 檔案 `conn %default` 區段內，設定下列建議設定：

```
ikelifetime=20m reauth=yes rekey=yes keylife=10m rekeymargin=3m rekeyfuzz=0%
 keyingtries=1 type=tunnel
```

STEP 3 | 修改 strongSwan 用戶端的 IPsec 設定檔 (**`ipsec.conf`**) 和 IPsec 密碼檔案 (**`ipsec.secrets`**) 以使用建議設定。

`ipsec.secrets` 檔案通常可以在 `/etc` 資料夾內找到。

使用 strongSwan 用戶端使用者名稱作為憑證的通用名稱。

在 `ipsec.conf` 檔案內設定下列建議設定：

```
conn <connection name> keyexchange=ikev1 ikelifetime=1440m keylife=60m
 aggressive=yes ike=aes-sha1-modp1024,aes256 esp=aes-sha1 xauth=client
 left=<strongSwan/Linux-client-IP-address> leftid=@#<hex of Group Name
 configured in the GlobalProtect gateway> leftsourceip=%modeconfig
 leftauth=psk rightauth=psk leftauth2=xauth right=<gateway-IP-address>
 rightsubnet=0.0.0.0/0 xauth_identity=<LDAP username> auto=add
```

在 `ipsec.secrets` 檔案內設定下列建議設定：

```
: PSK <Group Password configured in the gateway> <username> :XAUTH “<user
 password>”
```

STEP 4 | 開始 strongSwan IPsec 服務並連線至您想要 strongSwan 用戶端在驗證 GlobalProtect 閘道時使用的 IPsec 通道。

- Ubuntu：

```
ipsec start ipsec up <name>
```

- CentOS：

```
strongSwan start strongswan up <name>
```

STEP 5 | 確認通道設定正確，且 VPN 至 strongSwan 用戶端和 GlobalProtect 閘道的連線已建立。

1. 確認特定連線的詳細狀態資訊（透過指定連線）或來自 strongSwan 用戶端的所有連線的狀態資訊。
   - Ubuntu：

     ```
     ipsec statusall [<connection name>]
     ```

   - CentOS：

     ```
     strongswan statusall [<connection name>]
     ```

2. 選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）。在 **Info**（資訊）列中，選取閘道為 strongSwan 用戶端連線設定的 **Remote Users**（遠端使用者）。strongSwan 用戶端應在 **Current Users**（目前使用者）下列出。

透過雙因素驗證啟用驗證

使用雙因素驗證時，strongSwan 用戶端必須成功使用憑證設定檔與驗證設定檔來成功驗證，才能連線至 GlobalProtect 閘道。下列工作流程顯示了如何透過雙因素驗證啟用 strongSwan 用戶端驗證的方法。

STEP 1 | 為 GlobalProtect 閘道設定 IPsec 通道，以用於與 strongSwan 用戶端進行通訊。

1. 選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）。
2. 選取現有閘道或 **Add**（新增）一個。
3. 在 GlobalProtect 閘道組態對話方塊的 **Authentication**（驗證）頁籤中，選取您要使用的 **Certificate Profile**（憑證設定檔）和 **Authentication Profile**（驗證設定檔）。
4. 選取 **Agent**（用戶端）> **Tunnel Settings**（通道設定）以啟用 **Tunnel Mode**（通道模式），並指定下列設定以設定通道：
   - 選取此核取方塊可 **Enable X-Auth Support**（啟用 **X-Auth** 支援）。
   - 如果已設定 **Group Name**（群組名稱）和 **Group Password**（群組密碼），將其移除。
   - 按一下 **OK**（確定）以儲存通道設定。

STEP 2 | 確認 IPsec 通道設定檔 (**`ipsec.conf`**) **`conn %`** 預設區段內的預設連線設定，為 strongSwan 用戶端正確定義。

`ipsec.conf` 檔案通常可以在 `/etc` 檔案夾內找到。

此程序中的組態為以下版本進行了測試和確認：

- *PAN-OS 6.1* 的 *Ubuntu 14.0.4* 帶 *strongSwan 5.1.2* 和 *CentOS 6.5* 帶 *strongSwan 5.1.3*。
- *PAN-OS 7.0* 的 *Ubuntu 14.0.4* 帶 *strongSwan 5.2.1*。

如果您使用不同版本的 *strongSwan*，此程序中的組態可用於參考。如需詳細資訊，請參閱 strongSwan wiki。

在 `ipsec.conf` 檔案內設定下列建議設定：

```
ikelifetime=20m reauth=yes rekey=yes keylife=10m rekeymargin=3m rekeyfuzz=0%
 keyingtries=1 type=tunnel
```

STEP 3 | 修改 strongSwan 用戶端的 IPsec 設定檔 (**ipsec.conf**) 和 IPsec 密碼檔案 (**ipsec.secrets**) 以使用建議設定。

ipsec.secrets 檔案通常可以在 /etc 資料夾內找到。

使用 strongSwan 用戶端使用者名稱作為憑證的通用名稱。

在 ipsec.conf 檔案內設定下列建議設定：

```
conn <connection name> keyexchange=ikev1 authby=xauthrsasig ike=aes-sha1-
modp1024 esp=aes-sha1 xauth=client left=<strongSwan/Linux-client-IP-address>
 leftcert=<client-certificate-without-password> leftsourceip=%config
 right=<GlobalProtect-gateway-IP-address> rightid=%anyCN=<Subject-name-of-
gateway-cert>" rightsubnet=0.0.0.0/0 leftauth2=xauth xauth_identity=<LDAP
 username> auto=add
```

在 ipsec.secrets 檔案內設定下列建議設定：

```
<username> :XAUTH "<user password>" ::RSA <private key file> "<passphrase if
 used>"
```

STEP 4 | 開始 strongSwan IPsec 服務並連線至您想要 strongSwan 用戶端在驗證 GlobalProtect 閘道時使用的 IPsec 通道。

- Ubuntu：

```
ipsec start  ipsec up <name>
```

- CentOS：

```
strongSwan start strongswan up <name>
```

STEP 5 | 確認通道設定正確，且 VPN 至 strongSwan 用戶端和 GlobalProtect 閘道的連線已建立。

1. 確認特定連線的詳細狀態資訊（透過指定連線）或來自 strongSwan 用戶端的所有連線的狀態資訊。
   - Ubuntu：

     ```
     ipsec statusall [<connection name>]
     ```

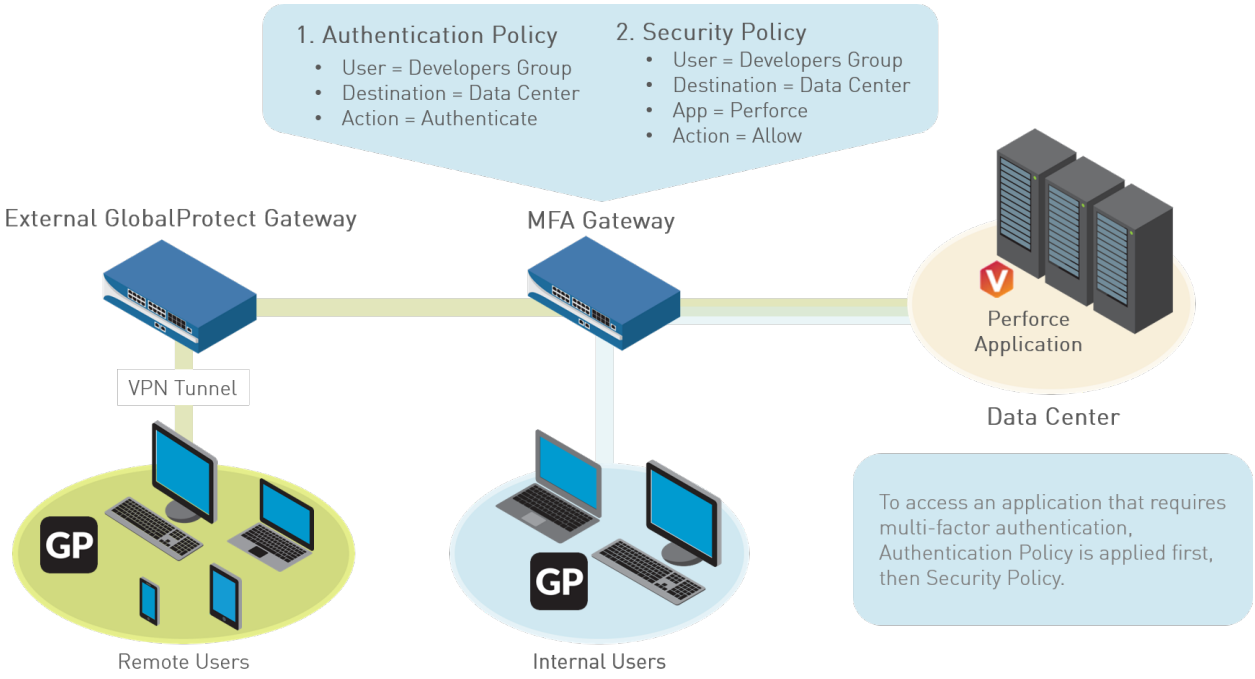
   - CentOS：

     ```
     strongswan statusall [<connection name>]
     ```

2. 選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）。在 **Info**（資訊）列中，選取閘道為 strongSwan 用戶端連線設定的 **Remote Users**（遠端使用者）。strongSwan 用戶端應在 **Current Users**（目前使用者）下列出。

設定 GlobalProtect 以便進行多因素驗證通知

為了保護關鍵應用程式，並阻止攻擊者使用被盜取的憑證在整個網路中水平擴散，您可以設定以原則為基礎的多因素驗證 (MFA)。這可以確保每個使用者在存取高度敏感的服務和應用程式之前，會回應不同類型（因素）的多重驗證挑戰。



如果使用者工作階段與驗證原則相符，則應用程式或服務的類型將決定有關驗證挑戰的使用者體驗通知：

- （僅限 Windows 或 macOS 端點）不以瀏覽器為基礎的應用程式—若要促進在 Windows 或 macOS 端點上對非 HTTP 應用程式的 MFA 通知（例如 Perforce），需要 GlobalProtect 應用程式。當工作階段與驗證原則規則相符時，防火牆會透過嵌入的 URL 連結到驗證入口網站頁面，向 GlobalProtect 應用程式發送 UDP 通知。GlobalProtect 應用程式即會以快顯通知向使用者顯示此訊息。
- 以瀏覽器為基礎的應用程式—以瀏覽器為基礎的應用程式不需要 GlobalProtect 對使用者顯示通知訊息。當防火牆將工作階段視為 Web 瀏覽流量時（根據 App-ID），防火牆會自動對使用者出示驗證原則規則中指定的驗證入口網站頁面（以前稱為被控制的入口網站）。如需詳細資訊，請參閱設定多因素驗證。

若要將 GlobalProtect 設定為針對不以瀏覽器為基礎的應用程式顯示 MFA 通知，請使用下方工作流程：

STEP 1 | 設定 GlobalProtect 之前，請先在防火牆上設定多因素驗證。

如果使用 *GlobalProtect* 的雙因素驗證來驗證閘道或入口網站，則需要使用 *RADIUS* 伺服器設定檔。如果使用 *GlobalProtect* 來通知使用者關於驗證原則比對（*UDP* 訊息），則多因素驗證伺服器設定檔已足夠。

若要使用多因素驗證來保護敏感資源，最簡單的解決方案是將防火牆與已在網路中建立的 MFA 廠商整合。當您的 MFA 結構準備就緒時，您就可以開始設定驗證原則的元件。如需詳細資訊，請參閱設定多因素驗證。

- 啟用被控制的入口網站來記錄驗證時間戳記，並更新使用者對應。
- 建立伺服器設定檔，該設定檔會定義防火牆如何連線到驗證使用者的服務。
- 將伺服器設定檔指派給會指定驗證參數的驗證設定檔。
- 設定安全性原則規則，該規則允許使用者存取需要驗證的資源。

STEP 2 | （僅限外部閘道）若要 GlobalProtect 支援外部閘道上的多因素驗證，您必須為防火牆上的進入通道介面設定回應頁面：

1. 選取 **Device**（裝置）> **Response Pages**（回應頁面）> **MFA Login Page**（MFA 登入頁面）。
2. 選取然後 **Export**（匯出）**Predefined**（預先定義的）範本至您選取的位置。
3. 在端點上，使用 HTML 編輯器來自訂下載的回應頁面，並使用唯一檔案名稱儲存該頁面。
4. 返回防火牆上的 **MFA Login Page**（MFA 登入頁面）對話方塊，**Import**（匯入）自訂頁面，**Browse**（瀏覽）並選取 **Import File**（匯入檔案），選取 **Destination**（目的地）（虛擬系統或共用位置）。按一下 **OK**（確定），然後按一下 **Close**（關閉）。

STEP 3 | （僅限外部閘道）啟用 **Response Pages**（回應頁面）作為在 **Interface Mgmt**（介面管理）設定檔上允許使用的服務：

1. 選取 **Network**（網路）> **Network Profiles**（網路設定檔）> **Interface Mgmt**（介面管理），然後選取設定檔。
2. 在 **Permitted Services**（允許的服務）區域中，選取 **Response Pages**（回應頁面），然後按下 **OK**（確定）。

STEP 4 | （僅限外部閘道）將 **Interface Mgmt**（介面管理）設定檔附加至通道介面：

1. 選取 **Network**（網路）> **Interfaces**（介面）> **Tunnel**（通道），以及您要用來使用回應頁面的通道介面。
2. 選取 **Advanced**（進階），然後選取您在上一步設定的 **Interface Mgmt**（介面管理）設定檔作為 **Management Profile**（管理設定檔）。

STEP 5 | （僅限外部閘道）在與通道介面關聯的區域上（**Network**（網路）> **Zones**（區域）> **<tunnel-zone**）**Enable User Identification**（啟用使用者識別）。

STEP 6 | 設定 GlobalProtect 用戶端，以支援不以瀏覽器為基礎的應用程式多因素驗證通知。

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後選取入口網站組態（或 **Add**（新增）入口網站）。
2. 選取 **Agent**（代理程式），然後選取現有的代理程式組態或 **Add**（新增）新的代理程式組態。
3. 在 **App**（應用程式）頁籤上選取以下選項：
   - 將 **Enable Inbound Authentication Prompts from MFA Gateways**（從 **MFA** 閘道啟用輸入驗證提示）設為 **Yes**（是）。若要支援多重要素驗證 (MFA)，GlobalProtect 應用程式必須收到從閘道傳來的 UDP 驗證提示並進行確認。選取 **Yes**（是）可讓 GlobalProtect 應用程式收到提示並進行確認。依預設，此值設為 **No**（否），代表 GlobalProtect 會封鎖來自閘道的 UDP 驗證提示。
   - 在 **Network Port for Inbound Authentication Prompts (UDP)**（輸入驗證提示的網路連接埠 **(UDP)**）欄位，請指定連接埠號碼，以供 GlobalProtect 應用程式從 MFA 閘道接收輸入 UDP 驗證提示。預設連接埠為 4501。若要變更連接埠，請指定 1 到 65535 的數字。
   - 在 **Trusted MFA Gateways**（受信任的 **MFA** 閘道）欄位中，為 GlobalProtect 應用程式將信任進行多因素驗證的重新導向 URL 指定閘道位址和連接埠編號（僅針對非預設連接埠，例如 6082）。當 GlobalProtect 應用程式收到 UDP 驗證提示，其中包含目的地為特定網路連接埠的重新導向 URL 時，GlobalProtect 僅在重新導向 URL 受信任時才顯示驗證訊息。
   - 設定 **Default Message for Inbound Authentication Prompts**（輸入驗證提示的預設訊息）。當使用者嘗試存取需要額外驗證的資源時，GlobalProtect 會收到一個包含輸入驗證提示的 UDP 封包，並顯示此訊息。該 UDP 封包也包含您在設定多因素驗證中所指定的驗證入口網站頁面 URL。GlobalProtect 會自動將 URL 附加到訊息。例如，若要顯示此主題開頭所示的通知，請輸入下列訊息：

     您已嘗試存取需要另外驗證的受保護資源。請繼續進行驗證，到：
4. 儲存代理程式變更（按兩下 **OK**（確定）），然後 **Commit**（提交）您的變更。

啟用 VSA 至 RADIUS 伺服器的提交

當與入口網站或閘道通訊時，GlobalProtect 端點傳送包含端點 IP 位址、作業系統 (OS)、主機名稱、使用者網域和 GlobalProtect 應用程式版本的資訊。您可以啟用防火牆，在驗證階段將此資訊作為 Vendor-Specific Attributes (VSA) 傳送至 RADIUS 伺服器（依預設，防火牆不會傳送 VSA）。RADIUS 管理員隨後將基於這些 VSA 執行管理工作。例如，RADIUS 管理員可能使用 OS 屬性定義原則，授權 Microsoft Windows 使用者的定期密碼驗證和 Google Android 使用者的一次性密碼 (OTP) 驗證。

此程序的必要條件如下所示：

- 將 Palo Alto 網路 RADIUS 字典匯入您的 RADIUS 伺服器。
- 設定 RADIUS 伺服器設定檔並將其指派至驗證設定檔。如需詳細資訊，請參閱設定外部驗證。
- 指派驗證設定檔至 GlobalProtect 入口網站或閘道。如需詳細資訊，請參閱設定對 GlobalProtect 入口網站的存取或設定 GlobalProtect 閘道。

STEP 1 | 登入防火牆 CLI

STEP 2 | 為您想要傳送的各 VSA 輸入命令：

```
username@hostname> set authentication radius-vsa-on client-source-
ip username@hostname> set authentication radius-vsa-on client-os
 username@hostname> set authentication radius-vsa-on client-hostname
 username@hostname> set authentication radius-vsa-on user-domain
 username@hostname> set authentication radius-vsa-on client-gp-version
```

如果您稍後想要停止讓防火牆傳送特定 *VSA*，請執行相同命令，但使用 ***radius-vsa-off*** 選項代替 ***radius-vsa-on***。

啟用群組對應

由於代理程式或應用程式如在您的一般使用者系統上執行，則使用者均需要成功驗證才能獲得 GlobalProtect 的存取權，因此各 GlobalProtect 使用者的身分識別均為已知。不過，如果您要想能夠根據群組成員資格定義 GlobalProtect 組態與/或安全原則，防火牆必須從您的目錄伺服器擷取群組清單與對應成員清單。這就叫做群組對應。

若要啟用此功能，您必須建立 LDAP 伺服器設定檔，其中包括指示防火牆連接與驗證目錄伺服器的方式，以及搜尋目錄是否有使用者與群組資訊的方式。防火牆連線至 LDAP 伺服器之後，會擷取群組對應，在定義代理程式組態與安全原則時，您將能夠選取群組。防火牆支援各種 LDAP 目錄伺服器，其中包括 Microsoft Active Directory (AD)、Novell eDirectory 和 Sun ONE 目錄伺服器。

使用下列程序連接至 LDAP 目錄以啟用防火牆並擷取使用者對群組的對應資訊：

STEP 1 | 建立 LDAP 伺服器設定檔，指定如何連線至防火牆應連線以取得群組對應資訊的目錄。

1. 選取 **Device**（設備）> **Server Profiles**（伺服器設定檔）> **LDAP**，然後按一下 **Add**（新增）。
2. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。
3. 如果此設定檔適用於具有多重虛擬系統功能的防火牆，請選取一個虛擬系統或 **Shared**（共用）作為設定檔可用的 **Location**（位置）。
4. 針對每個 LDAP 伺服器（最多四個），**Add**（新增）並輸入 **Name**（名稱）（以識別伺服器）、伺服器 IP 位址（**LDAP Server**（**LDAP** 伺服器）欄位），以及伺服器 **Port**（連接埠）（預設為 389）。
5. 從下拉式清單選取伺服器 **Type**（類型）：**active-directory**、**e-directory**、**sun** 或 **other**（其他）。
6. 如果您希望裝置使用 SSL 或 TLS 以求更安全地連線到目錄伺服器，請選取 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全連線）核取方塊（預設為已選取）。裝置使用的協定視乎伺服器 **Port**（連接埠）而定：
   - 389（預設）—TLS（特別是裝置會使用 StartTLS 操作，用來升級連接至 TLS 的初始純文字連線。）
   - 636—SSL
   - 任何其他連接埠—裝置首先會嘗試使用 TLS。若目錄伺服器不支援 TLS，則裝置會回復使用 SSL。
7. 為了獲得額外的安全，請選取 **Verify Server Certificate for SSL sessions**（確認 **SSL** 工作階段的伺服器憑證）核取方塊（預設為不選取），讓裝置確認目錄伺服器為 SSL/TLS 連線所出示的憑證。若要啟用此驗證，您也必須選取 **Require SSL/TLS secured connection**（要求 **SSL/TLS** 安全連線）核取方塊。為了順利確認，憑證必須滿足以下條件之一：
   - 位於裝置憑證清單內：**Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（設備憑證）。如有必要，將憑證匯入裝置中。
   - 憑證簽署者位於受信任的憑證授權單位清單中：**Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Default Trusted Certificate Authorities**（預設的受信任憑證授權單位）。
8. 按一下 **OK**（確定）。

STEP 2 | 將 LDAP 伺服器設定檔新增至 User-ID 群組對應設定。

1. 選取 **Device**（裝置）> **User Identification**（使用者識別）> **Group Mapping Settings**（群組對應設定），然後 **Add**（新增）新的群組對應組態。
2. 選取 **Server Profile**（伺服器設定檔）。
3. 輸入群組對應組態的 **Name**（名稱）。
4. 選取您剛剛建立的 **Server Profile**（伺服器設定檔）。
5. 指定 **Update Interval**（更新間隔）（秒），過了此間隔後，防火牆將啟動與 LDAP 目錄伺服器的連線，以取得針對此防火牆原則中使用的群組所進行的任何更新（範圍是 60 到 86,400 秒）。
6. 確保伺服器設定檔為 **Enabled**（已啟用）以啟用群組對應。

STEP 3 | （選用）允許 GlobalProtect 從目錄伺服器擷取序號。

GlobalProtect 能夠識別連線中的端點的狀態，並根據端點序號的存在強制執行 HIP 型安全性原則。如果端點受管理，您可將端點的序號繫結至目錄伺服器中端點的機器帳戶。然後，當防火牆從目錄伺服器擷取群組對應資訊時，可以預先擷取這些受管理端點的序號。

1. 從群組對應組態中，選取 **Server Profile**（伺服器設定檔）。
2. 啟用 **Fetch list of managed devices**（擷取受管理的裝置清單）選項。

STEP 4 | （選用）指定用於識別使用者與使用者群組的屬性。

1. 從群組對應組態中，選取 **User and Group Attributes**（使用者與群組屬性）。
2. 在使用者屬性區域，指定用於識別個別使用者的 **Primary Username**（主要使用者名稱）、**E-Mail**（電子郵件）及 **Alternate Username 1-3**（替代使用者名稱 **1-3**）。
3. 在群組屬性區域，指定用於識別使用者群組的 **Group Name**（群組名稱）、**Group Member**（群組成員）及 **E-Mail**（電子郵件）。

STEP 5 | （選用）限制原則規則中可選取的群組。

根據預設，如果未指定群組，則所有群組都可在原則規則中使用。

1. 從目錄服務中新增現有的群組：
   1. 從群組對應組態中，選取 **Group Include List**（群組包含清單）。
   2. 在可用群組清單中，選取您希望在原則規則中顯示的群組，並按一下新增 (⊕) 圖示，以將群組移至包含的群組清單。
2. 如果您的原則規則要以不符合現有使用者群組的使用者屬性作為基礎，請根據 LDAP 篩選器建立自訂群組：
   1. 從群組對應組態中，選取 **Custom Group**（自訂群組）。
   2. **Add**（新增）新的自訂群組。
   3. 輸入群組 **Name**（名稱）；此名稱在現行防火牆或虛擬系統的群組對應組態中必須是唯一的。如果該 **Name**（名稱）與現有 AD 群組網域的辨別名稱 (DN) 具有相同的值，防火牆將在該名稱的所有參照中使用自訂群組（例如在原則和日誌中）。
   4. 指定 **LDAP Filter**（**LDAP** 篩選器），最長 2,048 個 UTF-8 字元，然後按一下 **OK**（確定）。防火牆不會驗證 LDAP 篩選器。

若要最佳化 *LDAP* 搜尋並盡可能降低對 *LDAP* 目錄伺服器的效能影響，請使用索引屬性並縮小搜尋範圍以包含您因原則或可見度所需的使用者與群組物件。或者，您可以根據 *LDAP* 篩選器建立自訂群組。

STEP 6 | Commit（提交）您的變更。

按一下 **OK**（確定）與 **Commit**（提交）。

GlobalProtect 閘道

- GlobalProtect 閘道概念
- 設定 GlobalProtect 閘道的先決工作
- 設定 GlobalProtect 閘道
- 在 GlobalProtect 閘道上分割通道流量

GlobalProtect 閘道概要

由於傳遞給應用程式的 GlobalProtect 入口網站組態包括端點可連線的閘道清單，因此建議先設定閘道，再設定入口網站。

GlobalProtect 閘道可以將閘道設定為提供兩個主要功能：

- 針對連線至閘道的 GlobalProtect 應用程式強制執行安全原則。您也可以針對增強的安全原則精細度在閘道啟用 HIP 收集。如需啟用 HIP 檢查的詳細資訊，請參閱主機資訊。
- 提供對於內部公司網路的虛擬私人網路 (VPN) 存取。VPN 存取則透過裝載閘道的防火牆上端點與通道介面之間的 IPsec 或 SSL 通道提供。

您也可以在部署於 *AWS* 雲端的 *VM-Series* 防火牆上設定 *GlobalProtect* 閘道。透過將 *VM-Series* 防火牆部署在 *AWS* 雲端中，您可以快速、輕鬆地在任何地區中部署 *GlobalProtect* 閘道，無須設定此基礎結構時通常需要的費用或 *IT* 物流。如需詳細資訊，請參閱 使用案例：將 VM-Series 防火牆作為 AWS 中的 GlobalProtect 閘道 。

GlobalProtect 閘道概念

這些章節提供的資訊是關於在多個閘道組態中的閘道連線優先順序與 GlobalProtect 閘道的 MIB 支援。

- 閘道類型
- 多個閘道組態中的閘道優先順序
- GlobalProtect MIB 支援

閘道類型

GlobalProtect 閘道為 GlobalProtect 應用程式的流量提供強制執行的安全性功能。此外，如果已啟用主機資訊設定檔 (HIP) 功能，閘道會從原始主機資料產生 HIP 報告，端點會提交此資訊並可將其用於強制執行原則。

在任何 Palo Alto Networks 新一代防火牆上設定 GlobalProtect 閘道。您可以在同一個防火牆上執行閘道與入口網站，也可以在整個企業中擁有多個分散式閘道。

GlobalProtect 支援下列閘道類型：

- 內部—這是在內部網路上設定為 GlobalProtect 閘道的介面，可套用安全性原則以存取內部資源。當與 User-ID 與/或 HIP 檢查搭配使用時，便可使用內部閘道來提供安全而準確的方法，從而根據使用者與/或裝置狀態識別並控制流量。內部閘道在需要關鍵資源之驗證存取權的敏感環境中非常有用。您可以在通道模式或非通道模式下設定內部閘道。GlobalProtect 應用程式在執行內部主機偵測以判斷端點位置後會連線至內部閘道。
- 外部閘道（自動探索）—外部閘道位於公司網路外部，並為遠端使用者提供安全性增強程式和/或虛擬私人網路 (VPN) 存取。依預設，GlobalProtect 應用程式會自動根據您指派至閘道、來源區域和回應時間的優先順序連線至**Best Available**（現有最佳）外部閘道（請參閱多個閘道設定中的閘道優先順序）。
- 外部閘道（手動）—手動外部閘道位於公司網路外部，並為遠端使用者提供安全性增強程式和/或虛擬私人網路 (VPN) 存取。自動探索外部閘道與手動外部閘道間的差異是 GlobalProtect 應用程式在使用者起始連線時僅連線至手動外部閘道。您也可以為手動外部閘道設定不同驗證要求。若要設定手動閘道，您必須在定義 GlobalProtect 代理程式組態時將閘道辨識為 **Manual**（手動）。

多個閘道組態中的閘道優先順序

若要為您的行動工作者啟用安全存取，且無論其位於何處，您可以策略性地部署其他 Palo Alto Networks 新一代的防火牆並設定其作為 GlobalProtect 閘道。若要確定您的應用程式連線的偏好閘道，新增閘道至入口網站代理程式組態並指派各閘道連線優先順序。請參閱定義 GlobalProtect 代理程式組態。

如果 GlobalProtect 入口網站代理程式組態包含多個閘道，應用程式將嘗試與其代理程式組態中所列出的所有閘道通訊。然後，應用程式將使用優先順序與回應時間來決定要連線的目標閘道。使用 GlobalProtect 應用程式 4.0.2 與更舊版本時，僅當高優先順序閘道的回應時間大於所有閘道平均回應時間時，應用程式將連線至低優先順序閘道。

例如，為 gw1 和 gw2 考慮下列回應時間：

名稱	優先順序	回應時間
gw1	最高	80 ms
gw2	高	25 毫秒

應用程式確定最高優先順序的閘道回應時間（較大數字）大於兩個閘道的平均回應時間 (52.5 ms)，從而連線至 gw2。此範例中，應用程式儘管有較高的優先順序，仍未連線到 gw1，因為 80 ms 的回應時間高於二者的平均值。

現在，考慮為 gw1、gw2 和協力廠商閘道 gw3 的回應時間：

名稱	優先順序	回應時間
gw1	最高	30 毫秒
gw2	高	25 毫秒
gw3	中	50 毫秒

此範例中，所有閘道的平均回應時間為 35 ms。應用程式將評估哪個閘道的回應比平均回應時間快，並可看到 gw1 和 gw2 都有較快的回應時間。應用程式將連線擁有更高優先順序的閘道。此範例中，應用程式會連線到 gw1，因為 gw1 具有所有閘道中最高的優先順序，且回應時間低於平均值。

除了閘道優先順序之外，您還可以新增一個或多個來源區域至外部閘道組態。GlobalProtect 會辨識來源區域，並只允許使用者連線到針對該區域所設定的閘道。在選取閘道時，會先考慮使用來源閘道，然後才是閘道優先順序。

在 GlobalProtect 應用程式 4.0.3 與更舊版本中，GlobalProtect 應用程式會為指派為最高、高與中等優先順序之閘道的優先順序設在指派為低與最低優先順序的閘道之前，而不考慮回應時間。GlobalProtect 應用程式會將任何指派為低或最低優先順序的閘道增加至閘道清單中。此會確保應用程式先嘗試連線至您設定為高優先順序的閘道。

GlobalProtect MIB 支援

Palo Alto Networks 端點支援標準和企業管理資訊庫 (MIB) 讓您可以監控端點的實體狀態、使用統計資料、設陷和其他有用的資訊。大部分 MIB 使用物件群組，透過簡易網路管理通訊協定 (SNMP) 架構來描述端點的特性。您必須將這些 MIB 載入到您的 SNMP 管理員以監控 MIB 中定義的物件（端點統計資料和設陷）（如需詳細資訊，請參閱 PAN-OS 8.1 管理者指南中的使用 SNMP 管理程式以探索 MIB 和物件）。

PAN-COMMON-MIB—與企業 MIB 一起被包含在內—使用 panGlobalProtect 物件群組。下表描述了組成 panGlobalProtect 物件群組的物件。

object	說明
panGPGWUtilizationPct	GlobalProtect 閘道使用率（以百分比顯示）
panGPGWUtilizationMaxTunnels	允許的最大通道數
panGPGWUtilizationActiveTunnels	使用中連線連線數

使用這些 SNMP 物件以監控 GlobalProtect 閘道的使用率和根據需要變更。例如，如果使用中的通道數達到 80% 或高於允許的最大通道數量，您應考慮新增其他的閘道。

設定 GlobalProtect 閘道的先決工作

您必須先完成下列工作，才能開始設定 GlobalProtect 閘道：

- 為您打算用來設定各閘道的防火牆建立介面（與區域）。針對需要通道連線的閘道，您必須設定實體介面與虛擬通道介面。請參閱為 GlobalProtect 建立介面與區域。
- 設定 GlobalProtect 應用程式所需的閘道伺服器憑證和 SSL/TLS 服務設定檔，以與閘道之間建立 SSL 連線。請參閱在 GlobalProtect 元件之間啟用 SSL。
- 定義將用來驗證 GlobalProtect 使用者的驗證設定檔與/或憑證設定檔。請參閱驗證。

設定 GlobalProtect 閘道

在完成必要工作之後，請設定 GlobalProtect 閘道 。

STEP 1 | 新增閘道。

1. **Add**（新增）新的閘道（**Network**（網路） > **GlobalProtect** > **Gateways**（閘道））。
2. 為閘道 **Name**（命名）。

   閘道名稱不能包含空格，且對於每個虛擬系統來說是唯一的。命名的最佳做法是將可協助使用者與管理者識別閘道的位置或其他描述性資訊包含其中。
3. （ 選用 ）選取閘道所屬的虛擬系統 **Location**（位置）。

STEP 2 | 指定允許端點連線至閘道的網路資訊。

如果其尚未存在，請 為閘道建立網路介面 。

在您設定的介面上，請勿附加允許 *HTTP*、*HTTPS*、*Telnet* 或 *SSH* 的介面管理設定檔，因為這會啟用從網際網路存取管理介面的存取權。請遵照 保護管理存取權的最佳做法 ，來確保您可以保障防火牆的管理存取權，以防攻擊成功。

1. 選取端點用來與閘道通訊的 **Interface**（介面）。
2. 指定用於閘道 Web 服務的 **IP Address Type**（**IP** 位址類型）和 **IP Address**（**IP** 位址）。
   - 您可以將 **IP Address Type**（**IP** 位址類型）設定為 **IPv4 Only**（僅限 **IPv4**）、**IPv6 Only**（僅限 **IPv6**），或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。如果您的網路支援雙堆疊組態（也就是會同時執行 IPv4 和 IPv6），請使用 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。
   - IP 位址必須與 IP 位址類型相容。例如，`172.16.1.0`（適用於 IPv4）或 `21DA:D3:0::2F3b`（適用於 IPv6）。對於雙堆疊組態，輸入 IPv4 和 IPv6 位址。

STEP 3 | 為閘道指定其驗證一般使用者的方式。

如果閘道的 SSL/TLS 服務設定檔尚未存在，請 為 GlobalProtect 元件部署伺服器憑證 。

如果驗證設定檔或憑證設定檔尚未存在，請使用 驗證設定工作 來為閘道設定這些設定檔。

進行下列任何閘道 **Authentication**（驗證）設定（**Network**（網路） > **GlobalProtect** > **Gateways**（閘道） > *<gateway-config>* > **Authentication**（驗證））：

- 若要保障閘道與 GlobalProtect 應用程式間的通訊安全，為閘道選取 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。

  若要提供最強大的安全性，請將 *SSL/TLS* 服務設定檔的 *Min Version*（最低版本）設定為 *TLSv1.2*。
- 若要使用本機使用者資料庫或外部驗證服務（例如 LDAP、Kerberos、TACACS+、SAML 或 RADIUS，包括 OTP）驗證使用者，請透過下列設定 **Add**（新增）**Client Authentication**（用戶端驗證）組態：
  - 指定用於識別用戶端驗證組態的 **Name**（名稱）。
  - 識別此組態套用的 **OS**（作業系統）類型。依預設，組態會套用到 **Any**（任一）作業系統。
  - 選取或新增一個 **Authentication Profile**（驗證設定檔）以驗證要存取閘道的端點。
  - 輸入要用於閘道登入的自訂 **Username Label**（使用者名稱標籤）（例如，電子郵件地址 **(username@domain**）。
  - 輸入要用於閘道登入的自訂 **Password Label**（密碼標籤）（例如，雙因素權杖式驗證的密碼）。
  - 輸入 **Authentication Message**（驗證訊息）幫助一般使用者理解登入期間使用到哪些認證。訊息長度最多為 256 個字元（預設為 `Enter login credentials`）。

- 選取下列選項之一以定義使用者是否可以使用認證與/或用戶端憑證對閘道進行驗證：
  - 若要要求使用者同時使用認證與用戶端憑證對閘道進行驗證，請將 **Allow Authentication with User Credentials OR Client Certificate**（允許使用使用者憑證或用戶端憑證進行驗證）選項設定為 **No (User Credentials AND Client Certificate Required)**（否（需要使用者認證與用戶端憑證））（預設）。
  - 若要允許使用者使用認證或用戶端憑證對閘道進行驗證，請將 **Allow Authentication with User Credentials OR Client Certificate**（允許使用使用者憑證或用戶端憑證進行驗證）選項設定為 **Yes (User Credentials OR Client Certificate Required)**（是（需要使用者認證或用戶端憑證））。

    當您將此選項設為 **Yes**（是）時，閘道首先會檢查端點以取得用戶端憑證。如果端點沒有用戶端憑證或您沒有為用戶端驗證組態設定憑證設定檔，則端點使用者可以使用其使用者認證對閘道進行驗證。
- 若要根據用戶端憑證或智慧卡/CAC 驗證使用者，請選取對應的 **Certificate Profile**（憑證設定檔）。您必須使用簡易憑證註冊通訊協定 (SCEP) 預部署用戶端憑證或部署驗證用使用者指定用戶端憑證。
  - 如果您想要求使用者使用其使用者認證與用戶端憑證對閘道進行驗證，則必須指定 **Certificate Profile**（憑證設定檔）與驗證設定檔
  - 如果您要允許使用者使用其使用者認證或用戶端憑證對閘道進行驗證，且為使用者驗證指定了 **Authentication Profile**（驗證設定檔），則 **Certificate Profile**（憑證設定檔）為選用項目。
  - 如果您要允許使用者使用其使用者認證或用戶端憑證對閘道進行驗證，但沒有為使用者驗證選取 **Authentication Profile**（驗證設定檔），則 **Certificate Profile**（憑證設定檔）為必選項目。
  - 如果您未設定任何與特定作業系統相符的 **Authentication Profile**（驗證設定檔），則 **Certificate Profile**（憑證設定檔）為必選項目。

    如果您允許使用者使用使用者認證或用戶端憑證對閘道進行驗證，則不要選取 *Username Field*（使用者名稱欄位）設為 *None*（無）的 *Certificate Profile*（憑證設定檔）。
- 若要使用雙因素驗證，請選取 **Authentication Profile**（驗證設定檔）與 **Certificate Profile**（憑證設定檔）。使用者必須成功使用這兩種方法驗證才能獲得存取權限。

  （僅限 *Chrome*）如果您將閘道設為使用用戶端與 *LDAP* 進行雙因素驗證，執行 *Chrome OS 47* 或更新版本的 *Chromebook* 會收到選取用戶端憑證的過多提示。若要防止收到過多提示，請設定原則以在 *Google* 管理控制台中指定用戶端憑證，然後將該原則部署至受管理的 *Chromebook*：

  1. 登入至 Google 管理控制台，選取 *Device management*（裝置管理）> *Chrome management*（*Chrome* 管理）> *User settings*（使用者設定）。
  2. 在 *Client Certificates*（用戶端憑證）區段中，輸入下列 *URL* 模式以 *Automatically Select Client Certificate for These Sites*（自動為這些網站選取用戶端憑證）：

     ```
     {"pattern": "https://[*.]","filter":{}}
     ```
  3. 按一下 *Save*（儲存）。*Google* 管理控制台在幾分鐘內即可將原則部署至所有裝置。

STEP 4 | 啟用通道，然後設定通道參數。

如果是外部閘道，通道參數是必需的，內部閘道則為選用

若要強制使用 *SSL-VPN* 通道模式，請停用（清除）*Enable IPSec*（啟用 *IPSec*）選項。依預設，只有在端點無法建立 *IPSec* 通道時才會使用 *SSL-VPN*。

只有 *IPSec* 通道支援延伸驗證（*X* 驗證）。

如果您 *Enable X-Auth Support*（啟用 *X* 驗證支援），*GlobalProtect IPSec Crypto* 設定檔將不使用。

如需支援的密碼演算法詳細資訊，請參閱 GlobalProtect 應用程式加密功能。

1. 在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Tunnel Settings**（通道設定）。
2. 啟用 **Tunnel Mode**（通道模式）以啟用分割通道。
3. 選取您在 為閘道建立網路介面 時定義的 **Tunnel Interface**（通道介面）。
4. （ 選用 ）指定可同時存取閘道以進行驗證、HIP 更新和 GlobalProtect 應用程式更新的使用者人數上限（**Max User**（最大使用者數））。當欄位為空時將顯示值範圍並根據平台而有所不同。
5. **Enable IPSec**（啟用 **IPSec**），然後選取 **GlobalProtect IPSec Crypto**（**GlobalProtect IPSec** 加密）設定檔以保證 GlobalProtect 應用程式與閘道之間的 VPN 通道安全。**default**（預設）設定檔會使用 AES-128-CBC 加密和 sha1 驗證。

   IPSec 不支援 *Windows 10 UWP* 端點。

   您還可建立 **New GlobalProtect IPSec Crypto**（新的 **GlobalProtect IPSec** 加密）設定檔（**GlobalProtect IPSec Crypto**（**GlobalProtect IPSec** 加密）下拉式清單），然後進行下列設定：

   1. 指定用來識別設定檔的 **Name**（名稱）。
   2. **Add**（新增）**Authentication**（驗證）和 **Encryption**（加密）演算法，讓 VPN 端點可用於交涉防護通道內資料的金鑰：
      - **Encryption**（加密）—如果您不確定 VPN 端點的支援情況，您可以按照安全程度由上至下，新增多個加密演算法，具體如下：**aes-256-gcm**, **aes-128-gcm**, **aes-128-cbc**.端點交涉最強演算法，建立通道。
      - **Authentication**（驗證）—選取驗證演算法 (**sha1**) 以提供資料完整性和驗證保護。儘管設定檔需要驗證演算法，此設定僅套用於 AES-CBC 加密 (**aes-128-cbc**)。如果您使用 AES-GCM 加密演算法（**aes-256-gcm** 或 **aes-128-gcm**），設定將被忽略，因為這些加密可提供原生 ESP 完整性保護。
   3. 按一下 **OK**（確定）來儲存設定檔。
6. （選用）如果任何端點必須使用協力廠商 VPN（例如在 Linux 上執行的 VPNC 用戶端）連線至閘道，請 **Enable X-Auth Support**（啟用 **X** 驗證支援）。如果您啟用 X 驗證，且端點需要，您必須提供 **Group**（群組）名稱與 **Group Password**（群組密碼）。依預設，當用來建立 IPSec 通道的金鑰到期時，使用者不需要重新驗證。若需要重新驗證使用者，請停用 **Skip Auth on IKE Rekey**（跳過對 **IKE** 重設金鑰的驗證）選項。

   若要針對 *strongSwan* 端點 *Enable X-Auth Support*（啟用 *X* 驗證支援），您還必須停用 *Skip Auth on IKE Rekey*（跳過對 *IKE* 重設金鑰的驗證），因為這些端點在 *IKE SA* 交涉期間需要進行重新驗證。此外，您還必須新增 `closeaction=restart` 設定至 *strongSwan IPSec* 組態檔案的 `conn %default` 區段。（如需 *StrongSwan IPSec* 組態的詳細資訊，請參閱 設定 strongSwan Ubuntu 與 CentOS 端點驗證。）

   雖然 *iOS* 與 *Android* 端點都支援 *X* 驗證存取，但它所提供的這些端點上的 *GlobalProtect* 功能卻很有限。請改為使用 *GlobalProtect* 應用程式，簡化 *GlobalProtect* 在 *iOS* 和 *Android* 端點上提供的所有安全性功能集存取。適用於 *iOS* 的 *GlobalProtect* 可在 *Apple App Store* 找到。適用於 *Android* 的 *GlobalProtect* 可在 *Google Play* 找到。

STEP 5 | （ 僅限通道模式 ）為您的用戶端設定組態指定選取準則。

閘道會使用選取準則來決定要將哪個設定遞送至所連線的 GlobalProtect 應用程式。如果您擁有多個組態，請必須確保這些設定排序正確。閘道只要找到符合項目（基於 **Source User**（來源使用者）、**OS**（作業系統）及 **Source Address**（來源位址）），便會向使用者傳遞相關組態。因此，較具體的設定必須位於較一般性設定的前方。查看步驟 13 為用戶端設定組態清單排序提供說明。

1. 在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Client Settings**（用戶端設定）。
2. 選取現有用戶端設定組態或 **Add**（新增）一個。
3. 設定下列 **Config Selection Criteria**（設定選取準則）：
   - 若要部署此組態以指定使用者或使用者群組，請 **Add**（新增）**Source User**（來源使用者）（或使用者群組）。若要在預先登入模式下將此組態僅部署至使用應用程式的使用者，請在 **Source User**（來源使用者）下拉式清單中選取 **pre-logon**（預先登入）；若要將此組態部署至所有使用者，請選取 **any**（任何）。

     若要將組態部署至特定群組，您必須先依照 啟用群組對應 所述將使用者對應至群組。
   - 若要根據端點的作業系統來部署此組態，請 **Add**（新增）**OS**（作業系統）（例如 Android 或 Chrome）。若要將此組態部署至所有作業系統，請選取 **Any**（任何）。
   - 若要根據使用者位址部屬該組態，請 **Add**（新增）來源 **Region**（區域）或本機 **IP Address**（**IP** 位址）（IPv4 和 IPv6）。若要將該組態部屬至所有使用者位置，請勿指定 **Region**（區域）或 **IP Address**（**IP** 位址）。
4. 按一下 **OK**（確定）儲存組態選取準則。

STEP 6 | （僅限通道模式）設定驗證取代設定至啟用閘道，以產生和接受安全、加密的 cookie 驗證使用者。此功能允許使用者在指定時間內（例如每 24 小時），僅需要提供一次登入認證。

依預設，閘道透過驗證設定檔和選用的憑證設定檔驗證使用者。當啟用驗證取代時，GlobalProtect 快取成功的登入結果，並使用 cookie 驗證使用者，而不提示使用者提供認證。如需更多資訊，請參閱在入口網站或閘道上的 Cookie 驗證。如果需要用戶端憑證，端點也必須提供有效的憑證以獲得存取權限。

必須封鎖 *cookie* 未過期的裝置存取時（例如裝置遺失或被盜），您可以將該裝置新增到封鎖清單以立即 封鎖端點存取 。

1. 在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Client Settings**（用戶端設定）。
2. 選取現有用戶端設定組態或 **Add**（新增）一個。
3. 進行下列 **Authentication Override**（驗證取代）設定：
   - **Name**（名稱）—識別名稱。
   - **Generate cookie for authentication override**（為驗證取代產生 **cookie**）—啟用閘道以產生加密、特定端點的 cookie 並簽發驗證 cookie 至端點。
   - **Accept cookie for authentication override**（接受用於驗證覆寫的 **Cookie**）—啟用閘道以透過有效的加密 Cookie 驗證使用者。應用程式提供有效的 Cookie 後，閘道可驗證透過入口網站或閘道加密的 Cookie，解密 Cookie，接著驗證使用者。

     GlobalProtect 應用程式必須知道連線使用者的使用者名稱才能比對和擷取來自使用者端點的驗證 *cookie*。應用程式擷取 *cookie* 後，會將其傳送至入口網站或閘道以進行使用者驗證。

     （僅限 *Windows*）如果您在入口網站代理程式組態（*Network*（網路）> *GlobalProtect* > *Portals*（入口網站）> *<portal-config>* > *Agent*（代理程式）> *<agent-config>*。 > *App*（應用程式），*GlobalProtect* 應用程式將使用 *Windows* 使用者名稱擷取使用者的本機驗證 *cookie*。如果您將 *Use Single Sign-On*（使用單一登入）選項設為 *No*（否）（*SSO* 已停用），則必須允許 *GlobalProtect* 應用程式 儲存使用者認證 才能擷取使用者的驗證 *cookie*。將 *Save User Credentials*（儲

存使用者認證）選項設為 *Yes*（是）以儲存使用者名稱和密碼，或設為 *Save Username Only*（僅儲存使用者名稱）以僅儲存使用者名稱。

- **Cookie Lifetime**（**Cookie** 存留時間）—指定 Cookie 有效的小時數、天數或週數（預設為 24 小時）。小時範圍為 1 至 72；週範圍為 1 至 52；天數範圍為 1 至 365。Cookie 到期後，使用者必須重新輸入登入認證，閘道隨後會對新 Cookie 加密以傳送至應用程式。此值可與您為入口網站設定的 **Cookie Lifetime**（**Cookie** 存留時間）一致或不同。
- **Certificate to Encrypt/Decrypt Cookie**（用於加密/解密 **Cookie** 的憑證）—選取 RSA 憑證，以用於加密與解密 Cookie。您必須在入口網站和閘道上使用相同的憑證。

最佳做法是，設定 *RSA* 憑證以使用您的網路支援的最強摘要演算法。

入口網站和閘道使用 RSA 加密填補計劃 PKCS#1 V1.5 以產生 Cookie（使用公開憑證金鑰）並解密 Cookie（使用私密憑證金鑰）。

STEP 7 | （僅限通道模式 — 選用）設定用戶端層級 IP 集區，用於將 IPv4 或 IPv6 位址指定到連線至閘道之端點上的虛擬網路介面卡。

您必須僅在用戶端層級（*Network*（網路）> *GlobalProtect* > *Gateways*（閘道）> *<gateway-config>* > *GlobalProtect Gateway Configuration*（*GlobalProtect* 閘道設定）> *Agent*（代理程式）> *Client Settings*（用戶端設定）> *<client-setting>* > *Configs*（設定）> *IP Pools*（*IP* 集區））或閘道層級（*Network*（網路）> *GlobalProtect* > *Gateways*（閘道）> *<gateway-config>* > *GlobalProtect Gateway Configuration*（*GlobalProtect* 閘道設定）> *Agent*（代理程式）> *Client IP Pool*（用戶端 *IP* 集區））。

在非通道模式下的內部閘道設定中，不需要 *IP* 集區和分割通道設定，因為應用程式會使用指定給實體網路介面卡的網路設定。

不支援設定閘道 *IP* 位址集區時，使用位址物件。

1. 在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Client Settings**（用戶端設定）。
2. 選取現有用戶端設定組態或 **Add**（新增）一個。
3. 設定下列任何 **IP Pools**（**IP** 集區）設定：
   - 若要為需要靜態 IP 位址的端點指定驗證伺服器 IP 位址集區，請啟用 **Retrieve Framed-IP-Address attribute from authentication server**（從驗證伺服器擷取 **Framed-IP-Address** 屬性）選項，然後將子網路或 IP 位址範圍 **Add**（新增）至 **Authentication Server IP Pool**（驗證伺服器 **IP** 集區）。通道建立後，遠端使用者電腦上會建立一個介面，帶有與驗證伺服器 Framed-IP 屬性相符的子網絡或 IP 範圍內的位址。

     驗證伺服器 *IP* 位址集區必須大到足以支援所有同時連線。*IP* 位址指派是靜態的，即使在使用者中斷連線之後，也會保留該位址。
   - 若要指定用於將 IPv4 或 IPv6 位址指定到連線至閘道之端點的 **IP Pool**（**IP** 集區），請 **Add**（新增）IP 位址子網路/範圍。您可新增 IPv4 或 IPv6 子網路或範圍，或兩者的組合。

     若要確保適當地路由回閘道，您必須使用不同於指定到閘道上現有 IP 集區（如適用）和實際邊線至 LAN 之端點的 IP 位址範圍。我們建議您使用私人 IP 定址結構。
4. 按一下 **OK**（確定）來儲存 IP 集區組態。

STEP 8 | （僅限通道模式 — 選用）停用分割通道以確保所有流量（包括本機子網路流量）均通過 VPN 通道進行檢查與原則執行。

STEP 9 | （僅限通道模式）（選用）根據存取路由設定分割通道設定。

STEP 10 | （僅限通道模式 — 選用）根據目的地網域設定分割通道設定。

STEP 11 | （僅限通道模式）（選用）根據應用程式設定分割通道設定。

STEP 12 | （僅限通道模式 — 選用）為用戶端設定組態進行 DNS 設定。

如果您在用戶端設定組態中至少設定一個 *DNS* 伺服器或 *DNS* 尾碼（*Network*（網路）> *GlobalProtect* > *Gateways*（閘道）> *<gateway-config>* > *Agent*（代理程式）> *Client Settings*（用戶端設定）> *<client-settings-config>* > *Network Services*（網路服務））， 閘道會將 *DNS* 伺服器與 *DNS* 尾碼的組態傳送至端點。當您設定全域（閘道層級）*DNS* 伺服器與 *DNS* 尾碼時，也會發生此情況。

如果您未在用戶端設定組態中設定任何 *DNS* 伺服器或 *DNS* 尾碼，閘道會將全域 *DNS* 伺服器與 *DNS* 尾碼傳送至端點（若已設定）（*Network*（網路）> *GlobalProtect* > *Gateways*（閘道）> *<gateway-config>* > *Agent*（代理程式）> *Network Services*（網路服務））。

1. 在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Client Settings**（用戶端設定）。
2. 選取現有用戶端設定組態或 **Add**（新增）一個。
3. 設定下列任何 **Network Services**（網路服務）設定：
   - 指定 **DNS Server**（**DNS** 伺服器）的 IP 位址，以此用戶端設定組態的 GlobalProtect 應用程式會向此 IP 位址傳送 DNS 查詢。您可以新增最多 10 個 DNS 伺服器，以逗號分隔每個 IP 位址。
   - 遇到端點無法解析的不合格主機名稱時，指定端點應在本機使用的 **DNS Suffix**（**DNS** 尾碼）。

STEP 13 | （僅限通道模式）安排閘道代理程式組態，以將適當的組態部署至每個 GlobalProtect 應用程式。

當應用程式連線時，閘道會將封包中的來源資訊與您已定義的代理程式組態進行比較（**Agent**（代理程式）> **Client Settings**（用戶端設定））。藉助安全性規則評估，閘道會從清單頂端開始尋找符合項。找到符合項目時，會將對應的設定傳遞給應用程式。

- 若要將組態清單中的閘道組態向上移，請選取該組態和 **Move Up**（上移）。
- 若要將組態清單中的閘道組態向下移，請選取該組態和 **Move Down**（下移）。

STEP 14 | （僅限通道模式—選用）設定全域 IP 位址集區，用於將 IPv4 或 IPv6 位址指定到連線至閘道之所有端點上的虛擬網路介面卡。

此選項可讓您在閘道層級定義 IP 集區，而無需在閘道組態中為每個用戶端設定定義 IP 集區，從而簡化設定。

您必須僅在閘道層級（*Network*（網路）> *GlobalProtect* > *Gateways*（閘道）> *<gateway-config>* > *Agent*（代理程式）> *Client IP Pool*（用戶端 *IP* 集區））或用戶端層級（*Network*（網路）> *GlobalProtect* > *Gateways*（閘道）> *<gateway-config>* > *Agent*（代理程式）> *Client Settings*（用戶端設定）> *<client-setting>* > *IP Pools*（*IP* 集區））設定 *IP* 集區。

不支援設定閘道 *IP* 位址集區時，使用位址物件。

1. 在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Client IP Pool**（用戶端 **IP** 集區）。

2. **Add**（新增）IP 位址子網路/範圍，用於將 IPv4 或 IPv6 位址指定到連線至閘道的所有端點。您可新增 IPv4 或 IPv6 子網路或範圍，或兩者的組合。

   若要確保適當地路由回閘道，您必須使用不同於指定到閘道上現有 IP 集區（如適用）和實際邊線至 LAN 之端點的 IP 位址範圍。我們建議您使用私人 IP 定址結構。

STEP 15 | （僅限通道模式）指定端點的網路組態設定。

在非通道模式下的內部閘道設定中，不需要網路設定，因為 *GlobalProtect* 應用程式會使用指定給實體網路卡的網路設定。

在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Network Services**（網路服務）然後進行以下任何網路組態設定：

- 如果防火牆具有設定為 DHCP 用戶端的介面，您可以將 **Inheritance Source**（繼承來源）設定至該介面，而且將會為 GlobalProtect 應用程式指定與 DHCP 用戶端相同的設定。您還可以啟用核取方塊，以從繼承來源 **Inherit DNS Suffixes**（繼承 **DNS** 尾碼）。
- 手動指定 **Primary DNS**（主要 **DNS**）伺服器、**Secondary DNS**（次要 **DNS**）伺服器、**Primary WINS**（主要 **WINS**）伺服器、**Secondary WINS**（次要 **WINS**）伺服器及 **DNS Suffix**（**DNS** 尾碼）。您可以透過以逗號分隔每個尾碼來輸入多個 DNS 尾碼（最多 100 個）。

DNS Suffix（*DNS* 尾碼）不能包含任何非 *ASCII* 字元。

STEP 16 | （選用）修改端點的預設逾時設定。

在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Connection Settings**（連線設定）然後在逾時組態區域進行以下設定：

- 修改單一閘道登入工作階段的最大 **Login Lifetime**（登入存留時間）（預設登入存留時間為 30 天）。在這段存留時間內，閘道只要在 **Inactivity Logout**（非使用狀態登出）時間內收到來自端點的 HIP 檢查，使用者即可保持登入。在此時間之後，登入工作階段自動結束。
- 修改 **Inactivity Logout**（非使用狀態登出）時間以指定非作用中工作階段自動登出後的時間（預設為 3 小時）。如果閘道未在指定期間內收到來自端點的 HIP 檢查，使用者將登出 GlobalProtect。
- 修改 **Disconnect on Idle**（閒置時中斷連線）設定以指定閒置使用者登出 GlobalProtect 後的分鐘數（預設為 180 分鐘）。如果 GlobalProtect 應用程式未在設定的期間內透過 VPN 通道路由流量，使用者將登出 GlobalProtect。此設定僅適用於使用依需求連線方法連線至 GlobalProtect 的應用程式。

STEP 17 | （選用）設定 SSL VPN 通道的自動還原。

如果 GlobalProtect 連線因網路不穩定或端點狀態的變更而中斷，您可透過設定 SSL VPN 通道的自動還原，來允許或防止 GlobalProtect 應用程式自動為特定閘道重新建立 VPN 通道。

1. 在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Client Settings**（用戶端設定）。
2. 設定下列選項之一，以驗證 cookie 使用限制：
   - 若要防止 GlobalProtect 應用程式自動為此閘道重新建立 VPN 通道，請 **Disable Automatic Restoration of SSL VPN**（停用 **SSL VPN** 的自動還原）。
   - 若要允許 GlobalProtect 應用程式自動為此閘道重新建立 VPN 通道，請停用（清除）**Disable Automatic Restoration of SSL VPN**（停用 **SSL VPN** 的自動還原）選項（預設）。

STEP 18 | （選用）為驗證 cookie 設定來源 IP 位址執行。

您可設定 GlobalProtect 入口網站或閘道，以僅在端點的 IP 位址與為其發佈 cookie 的原始來源 IP 位址或特定網路 IP 位址範圍相符時，才從端點接收 cookie。您可使用 CIDR 子網路遮罩（例如 /24 或 /32）定義網路 IP 位址範圍。例如，如果驗證 cookie 最初發佈給公共來源 IP 位址為 201.109.11.10 的端點，且網路 IP 位址範圍的子網路遮罩設為 /24，驗證 cookie 隨後會在公共來源 IP 位址在 201.109.11.0/24 網路 IP 位址範圍內的端點上有效。

1. 在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Client Settings**（用戶端設定）。
2. 在驗證 cookie 使用限制區段中，**Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override)**（限制驗證 **cookie** 的使用（用於自動還原 **VPN** 通道或驗證覆寫）），然後設定下列條件之一：
   - 如果您選取 **The original Source IP for which the authentication cookie was issued**（為其發佈驗證 **cookie** 的原始來源 **IP**），只有當嘗試使用 cookie 之端點的公共來源 IP 位址與最初為其發佈 cookie 之端點的公共來源 IP 位址相同時，驗證 cookie 才有效。
   - 如果您選取 **The original Source IP network range**（原始來源 **IP** 網路範圍），只有當嘗試使用 cookie 之端點的公共來源 IP 位址在指定網路 IP 位址範圍內時，驗證 cookie 才有效。輸入 **Source IPv4 Netmask**（來源 **IPv4** 網路遮罩）或 **Source IPv6 Netmask**（來源 **IPv6** 網路遮罩）以定義驗證 cookie 有效的網路 IP 位址範圍之子網路遮罩（例如，**32** 或 **128**）。

STEP 19 | （僅限通道模式）從 VPN 通道排除 HTTP/HTTPS 視訊串流流量。

STEP 20 | （選用）定義當主機資訊設定檔用於 (HIP) 強制執行安全性規則時，一般使用者會看到的通知訊息。

只有當您建立主機資訊設定檔，並將它們新增到安全性原則時，才適用此步驟。如需設定 HIP 功能以及建立 HIP 通知訊息的詳細資訊，請參閱 主機資訊。

1. 在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **HIP Notification**（**HIP** 通知）。
2. 選取現有 HIP 通知組態或 **Add**（新增）一個。
3. 進行下列設定：
   - 選取此訊息適用的 **Host Information**（主機資訊）物件或設定檔。
   - 當對應的 HIP 設定檔已照原則進行比對或未比對時，根據您是否要顯示此訊息，選取 **Match Message**（符合訊息）或 **Not Match Message**（不符合訊息），然後 **Enable**（啟用）通知。您可根據您正在比對的物件與原則的目的，來為相符與非相符實例建立訊息。您也可以針對 **Match Message**（符合訊息）啟用 **Include Mobile App List**（包括行動應用程式清單）選項，指示哪些應用程式會觸發 HIP 相符。
   - 選取是否要將訊息顯示為 **System Tray Balloon**（系統匣球形文字說明）或 **Pop Up Message**（快顯訊息）。
   - 輸入並格式化訊息的文字（**Template**（範本）），然後按一下 **OK**（確定）。
   - 針對每個要定義的訊息重複這些步驟。

STEP 21 | 儲存閘道組態。

1. 按一下 **OK**（確定）以儲存設定。
2. **Commit**（提交）變更。

STEP 22 | （選用）若要設定 GlobalProtect 應用程式以在一般使用者連線時顯示識別此閘道位置的標籤，請指定設定此閘道的防火牆之實體位置。

當一般使用者遇到異常行為時（例如網路效能低），可向支援或服務台專業人員提供此位置資訊，以取得疑難排解協助。其還可使用此位置資訊來確定自己與閘道的距離。根據此距離，其可評估是否需要切換至較近的閘道。

如果您未指定閘道位置，*GlobalProtect* 應用程式將顯示空白位置欄位。

- 在 **CLI** 中 —使用下列 CLI 命令指定設定閘道之防火牆的實體位置：

```
<username@hostname> set deviceconfig setting global-protect
 location <location>
```

- 在 **XML API** 中—使用下列 XML API 指定設定閘道之防火牆的實體位置：
  - 裝置 —設定閘道之防火牆的名稱
  - 位置 —設定閘道之防火牆的位置

```
curl -k -F file=@filename.txt -g 'https://<firewall>/api/?
key=<apikey>&type=config&action=set&xpath=/config/devices/
entry[@name='<device-name>']/deviceconfig/setting/global-
protect&element=<location>location-string</location>'
```

在 GlobalProtect 閘道上分割通道流量

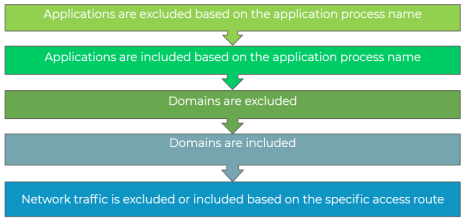
根據存取路由、目的地網域、應用程式及 HTTP/HTTPS 視訊串流應用程式設定分割通道流量。

藉助 *GlobalProtect* 訂閱，您可執行或套用分割通道規則至 *Windows* 與 *macOS* 端點。

分割通道功能讓您能夠節省頻寬並路由流量至：

- 通道企業 SaaS 與公共雲端應用程式，實現全面的 SaaS 應用程式可視性及控制，以避免在無法透過通道傳送所有流量的環境中與影子 IT 相關的風險。
- 在 VPN 通道外傳送對延遲敏感的流量（例如 VoIP），同時所有其他流量透過 VPN 傳送以由 GlobalProtect 閘道進行檢查及原則執行。
- 從 VPN 通道排除 HTTP/HTTPS 視訊串流流量。視訊串流應用程式（例如 YouTube 與 Netflix）會消耗大量頻寬。透過從 VPN 通道排除低風險視訊串流流量，您可以減少閘道上的頻寬消耗。

分割通道規則將按以下順序套用至 Windows 和 macOS 端點：



請參閱以下各節，了解如何在閘道上設定分割通道流量：

- 基於存取路由設定分割通道
- 基於網域和應用程序設定分割通道
- 排除來自 GlobalProtect VPN 通道的視訊流量

基於存取路由設定分割通道

若未包含或排除路由，則每個要求都會透過 VPN 通道傳送（無分割通道）。您可包含或排除透過 VPN 通道傳送的特定目的地 IP 子網路流量。透過 VPN 通道傳送的路由可以被定義為包含在通道中的路由，或從通道中排除的路由，或兩者都有。例如，您可以設定分割通道，讓遠端使用者在無須透過 VPN 通道的情況下存取網際網路。較特定的路由會優先於較不特定的路由。

將分割通道流量定義為包含存取路由時，這些路由是閘道推送至遠端使用者端點的路由，從而指定使用者端點可透過 VPN 連線傳送哪些流量。將分割通道流量定義為排除存取路由時，這些路由會透過端點上的實體介面卡傳送，而不是透過虛擬介面卡透過 GlobalProtect VPN 通道傳送（通道）。透過按存取路由排除分割通道流量，您可將延遲敏感或消耗高頻寬的流量傳送到 VPN 通道之外，同時所有其他流量透過 VPN 傳送，以便由 GlobalProtect 閘道檢查及執行原則。

本機路由優先於閘道傳送的路由。當您啟用分割通道時，使用者可直接連線至 proxy 與本機資源（例如本機印表機），無需透過 VPN 通道傳送任何本機子網路流量。透過停用分割通道，您可在使用者連線至 GlobalProtect 時，強制所有流量通過 VPN 通道進行檢查和原則執行。根據啟用還是停用直接存取本機網路，考慮下列 IPv4 與 IPv6 流量行為。

表 1: IPv4 流量行為

本機子網路 IPv4 流量	無本機網路直接存取已啟用		無本機網路直接存取已停用	
	建立通道前	建立通道後	建立通道前	建立通道後
新傳入流量	允許流量透過實體介面卡在本機子網路傳送。	流量透過 VPN 通道傳送。	允許流量透過實體介面卡在本機子網路傳送。	允許流量透過實體介面卡在本機子網路傳送。
新傳出流量	允許流量透過實體介面卡在本機子網路傳送。	流量透過 VPN 通道傳送。	允許流量透過實體介面卡在本機子網路傳送。	允許流量透過實體介面卡在本機子網路傳送。
現有流量	允許流量透過實體介面卡在本機子網路傳送。	流量已終止。	允許流量透過實體介面卡在本機子網路傳送。	允許流量透過實體介面卡在本機子網路傳送。

表 2: IPv6 流量行為

本機子網路 IPv46 流量	無本機網路直接存取已啟用		無本機網路直接存取已停用	
	建立通道前	建立通道後	建立通道前	建立通道後
新傳入流量	允許流量透過實體介面卡在本機子網路傳送。	允許流量透過實體介面卡在本機子網路傳送。	允許流量透過實體介面卡在本機子網路傳送。	允許流量透過實體介面卡在本機子網路傳送。
新傳出流量	允許流量透過實體介面卡在本機子網路傳送。	允許流量透過實體介面卡在本機子網路傳送。	允許流量透過實體介面卡在本機子網路傳送。	允許流量透過實體介面卡在本機子網路傳送。
現有流量	允許流量透過實體介面卡在本機子網路傳送。	允許流量透過實體介面卡在本機子網路傳送。	允許流量透過實體介面卡在本機子網路傳送。	允許流量透過實體介面卡在本機子網路傳送。

按照下列步驟根據存取路由設定分割通道。

STEP 1 | 開始之前

1. 設定 GlobalProtect 閘道。
2. 選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> *<gateway-config>*以修改現有閘道或新增一個。

STEP 2 | 啟用分割通道。

1. 在 **GlobalProtect** 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Tunnel Settings**（通道設定）以啟用 **Tunnel Mode**（通道模式）。
2. 為 GlobalProtect 應用程式設定通道參數。

STEP 3 | （僅限通道模式）停用分割通道以確保所有流量（包括本機子網路流量）均通過 VPN 通道進行檢查與原則執行。

1. 在 **GlobalProtect** 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Client Settings**（用戶端設定）> *<client-setting-config>*以選取現有用戶端設定組態或新增一個。
2. 選取 **Split Tunnel**（分割通道）> **Access Route**（存取路由），然後啟用 **No direct access to local network**（無本機網路直接存取）選項。

如果啟用此選項，分割通道流量將停用，且使用者將無法在連線 *GlobalProtect* 時直接傳送流量至 *proxy* 或本機資源。

STEP 4 | （僅限通道模式）根據存取路由設定分割通道設定。

當 GlobalProtect 應用程式建立擁有閘道的通道時，分割通道設定將指定到端點上的虛擬網路卡。

避免將同一個存取路由同時指定為包含和排除存取路由，這會造成設定錯誤。

您可透過指定目的地子網路或（**IP Netmask**（**IP** 網路遮罩）類型）位址物件路由某些流量，以包含在通道中或從通道中排除。

1. 在 **GlobalProtect** 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Client Settings**（用戶端設定）> *<client-setting-config>*以選取現有用戶端設定組態或新增一個。
2. 進行下列任何基於存取路由的 **Split Tunnel**（分割通道）設定（**Split Tunnel**（分割通道）> **Access Route**（存取路由））：
   - （選用）在 **Includes**（包含）區域，**Add**（新增）目的地子網路或（**IP** 網路遮罩類型）位址物件，僅將以您的 LAN 為目標的流量路由至 GlobalProtect。您可以包含 IPv6 或 IPv4 子網路。

     在 PAN-OS 8.0.2 及更新版本中，可使用最多 100 個存取路由在分割通道閘道組態中包含流量。與 GlobalProtect 應用程式 4.1.x 或更新版本結合，可使用最多 1,000 個存取路由。
   - （選用）在 **Excludes**（排除）區段，**Add**（新增）您想要應用程式排除的目的地子網路或（**IP Netmask**（**IP** 網路遮罩）類型）位址物件。排除的路由應比包含的路由更明確，否則可能會排除掉超出原有預期的流量。您可以排除 IPv6 或 IPv4 子網路。防火牆在分割通道閘道組態中支援最多 100 個排除存取路由。與 GlobalProtect 應用程式 4.1 及更新版本結合，可使用最多 200 個排除存取路由。

     您無法在 *Chromebooks* 上排除執行 *Android* 之端點的存取路由。*Chromebooks* 只支援 *IPv4* 路由。
3. 按一下 **OK**（確定）儲存分割通道組態。

STEP 5 | 儲存閘道組態。

1. 按一下 **OK**（確定）以儲存設定。
2. **Commit**（提交）變更。

基於網域和應用程序設定分割通道

根據目的地網域與連接埠（選用）或應用程式設定分割通道以包含所有流量（IPv4 與 IPv6）時，所有進入該特定網域或應用程式的流量均透過 VPN 通道傳送，進行檢查與原則執行。例如，您可使用 ***Salesforce.com** 目的地網域允許所有 Salesforce 流量透過 VPN 通道傳送。透過在 VPN 通道中包含所有 Salesforce 流量，您可提供對整個 Salesforce 網域及子網域的安全存取。您可設定分割通道，無需指定目的地 IP 位址子網路，從而將分割通道功能延伸至帶有動態公共 IP 位址的網域和應用程式，例如 SaaS 與公共雲端應用程式。

根據目的地網域與連接埠（選用）或應用程式設定分割通道以排除流量（IPv4 與 IPv6）時，該特定應用程式或網域的所有流量均在不檢查的情況下直接傳送至端點上的實體介面卡。例如，您可使用 **C:\Program Files (x86)\Skype\Phone\Skype** 應用程式進程名稱從 VPN 通道排除所有 Skype 流量。

僅 *Windows 7 Service Pack 2* 及更新版本和 *macOS 10.10* 及更新版本的端點支援此功能。

按照下列步驟設定分割通道，以根據目的地網域或程式進程名稱包含或排除流量。

STEP 1 | 開始之前

1. 設定 GlobalProtect 閘道。
2. 選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> *<gateway-config>*以修改現有閘道或新增一個。

STEP 2 | 啟用分割通道。

1. 在 **GlobalProtect** 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Tunnel Settings**（通道設定）以啟用 **Tunnel Mode**（通道模式）。
2. 為 GlobalProtect 應用程式設定通道參數。

STEP 3 | （僅限通道模式）根據目的地網域設定分割通道設定。當 GlobalProtect 應用程式建立擁有閘道的通道時，這些設定將指定到端點上的虛擬網路卡。

您無法根據目的地網域設定分割通道，因為此分割通道設定與 *macOS* 端點上的 *Sophos* 不相容。若要避免此不相容問題，

1. 在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Client Settings**（用戶端設定）> *<client-setting-config>*以選取現有用戶端設定組態或新增一個。
2. （選用）**Add**（新增）您要使用目的地網域和連接埠透過 VPN 連線路由至 GlobalProtect 的 SaaS 或公共雲端應用程式（**Split Tunnel**（分割通道）> **Domain and Application**（網域和應用程式）> **Include Domain**（包含網域））。您可新增最多 200 個項目至清單。例如，新增 *.gmail.com 以允許所有 Gmail 流量通過 VPN 通道。
3. （選用）**Add**（新增）您要使用目的地網域和連接埠從 VPN 通道排除的 SaaS 或公共雲端應用程式（**Split Tunnel**（分割通道）> **Domain and Application**（網域和應用程式）> **Include Domain**（排除網域））。您可新增最多 200 個項目至清單。例如，新增 *.target.com 以從 VPN 通道排除所有 Target 流量。
4. 按一下 **OK**（確定）儲存分割通道設定。

STEP 4 | （僅限通道模式）根據應用程式設定分割通道設定。

Safari 流量無法新增至 *macOS* 站點上基於應用程式的分割通道規則。

您可使用環境變量根據 *Windows* 和 *macOS* 端點上的應用程式設定分割通道。

1. 在 GlobalProtect 閘道組態對話方塊中，選取 **Agent**（代理程式）> **Client Settings**（用戶端設定）> *<client-setting-config>*以選取現有用戶端設定組態或新增一個。
2. （選用）**Add**（新增）您要使用應用程式處理序名稱透過 VPN 連線路由至 GlobalProtect 的 SaaS 或公共雲端應用程式（**Split Tunnel**（分割通道）> **Domain and Application**（網域和應用程式）> **Include Client Application Process Name**（包含用戶端應用程式處理序名稱））。您可新增最多 200 個項目至清單。例如，新增 Applications/RingCentral for Mac.app/Contents/MacOS/Softphone 以允許所有基於 RingCentral 的流量通過 macOS 端點上的 VPN 通道。

3. （選用）**Add**（新增）您要使用應用程式處理序名稱從 VPN 通道排除的 SaaS 或公共雲端應用程式（**Split Tunnel**（分割通道）> **Domain and Application**（網域和應用程式）> **Exclude Client Application Process Name**（排除用戶端應用程式處理序名稱））。您可新增最多 200 個項目至清單。例如，新增 **`/Applications/Microsoft Lync.app/Contents/MacOS/Microsoft Lync`** 以從 VPN 通道排除所有 Microsoft Lync 應用程式流量。
4. 按一下 **OK**（確定）儲存分割通道設定。

STEP 5 | 儲存閘道組態。

1. 按一下**OK**（確定）儲存閘道組態。
2. **Commit**（提交）您的變更。

排除來自 GlobalProtect VPN 通道的視訊流量

您可設定分割通道，以排除透過 VPN 通道傳送至特定網域的 HTTP/HTTPS 視訊串流流量。這會讓視訊流量直接透過端點上的實體介面傳送。防火牆上的 App-ID 功能可以在流量分割通道之前識別視訊串流。透過從 VPN 通道排除低風險視訊串流流量（如 YouTube 與 Netflix），您可以減少閘道上的頻寬消耗。

下列視訊串流應用程式的所有視訊流量類型都會被重新導向：

- YouTube
- Dailymotion
- Netflix

如果您從 VPN 通道排除任何其他視訊串流應用程式，僅會重新導向這些應用程式的下列視訊流量類型：

- MP4
- WebM
- MPEG

按照以下步驟設定分割通道，以從 VPN 通道排除視訊串流流量。

STEP 1 | 開始之前

1. 遵循以下先決條件：
   - 僅 Windows 7 Service Pack 2 及更新版本和 macOS 10.10 及更新版本的端點支援此功能。
   - 您必須確保用於將 IP 位址指定到這些端點上虛擬網路介面卡的 IP 集區不包含任何 IPv6 位址。如果 Windows 或 macOS 端點上的實體介面卡僅支援 Ipv4 位址，當您設定 GlobalProtect 閘道以將 Ipv6 位址指定到連線至閘道之端點上的虛擬網路介面卡時，端點使用者將無法存取您從 VPN 通道排除的視訊串流應用程式。
   - 如果從 VPN 通道中排除了視訊串流流量，則不要在 VPN 通道中包含 Web 瀏覽器應用程式，例如 Firefox 或 Chrome。這可確保分割通道組態中沒有衝突的邏輯，且您的使用者可以從 Web 瀏覽器串流視訊。
   - 若要從 VPN 通道中排除 Sling TV 應用程式流量，請根據應用程式設定分割通道。
2. 設定 GlobalProtect 閘道。
3. 選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> *<gateway-config>*以修改現有閘道或新增一個。

STEP 2 | 啟用分割通道。

1. 在 **GlobalProtect Gateway Configuration**（**GlobalProtect** 閘道組態對話方塊）中，選取 **Agent**（代理程式）> **Tunnel Settings**（通道設定）以啟用 **Tunnel Mode**（通道模式）。
2. 為 GlobalProtect 應用程式設定通道參數。

STEP 3 | （僅限通道模式）從 VPN 通道排除 HTTP/HTTPS 視訊串流流量。

1. 在 **GlobalProtect Gateway Configuration**（**GlobalProtect** 閘道組態對話方塊）中，選取 **Agent**（代理程式）> **Video Traffic**（視訊流量）。

2. 啟用此選項以 **Exclude video applications from the tunnel**（從通道排除視訊應用程式）。

   如果您啟用此選項，但沒有從 *VPN* 通道排除的特定視訊串流應用程式，則所有視訊串流流量都會被排除。

3. （選用）**Browse**（瀏覽）**Applications**（應用程式）清單以檢視您可從 VPN 通道排除的所有視訊串流應用程式。按一下您要排除之應用程式的新增圖示 ( )。例如，按一下 **directv** 的新增圖示以從 VPN 通道排除 DIRECTV 視訊串流流量。
4. **Add**（新增）您要從 VPN 通道排除的視訊串流應用程式，使用 **Applications**（應用程式）下拉式清單—**Applications**（應用程式）清單之縮減版。您可新增最多 200 個視訊應用程式項目至清單。例如，選取 **youtube-streaming**（**youtube** 串流）以從 VPN 通道排除所有 YouTube 視訊串流流量。

STEP 4 | 儲存閘道組態。

1. 按一下**OK**（確定）儲存閘道組態。
2. **Commit**（提交）您的變更。

GlobalProtect 入口網站

- GlobalProtect 入口網站概要
- 設定 GlobalProtect 入口網站的先決工作
- 設定 GlobalProtect 入口網站存取權
- 定義 GlobalProtect 代理程式組態
- 自訂 GlobalProtect 應用程式
- 自訂 GlobalProtect 入口網站登入、歡迎與說明頁面
- GlobalProtect 無用戶端 VPN

GlobalProtect 入口網站概要

GlobalProtect 入口網站提供 GlobalProtect 基礎結構的管理功能。參與 GlobalProtect 網路的每個端點都會收到入口網站的設定資訊，包括可用閘道的相關資訊，以及連線到閘道可能需要的任何用戶端憑證。此外，無論是 macOS 或是 Windows 端點，入口網站都能為其控制 GlobalProtect 應用程式的行為和散佈。

入口網站不會散佈用於行動端點的 *GlobalProtect* 應用程式。若要取得適用於行動端點的 *GlobalProtect* 應用程式，一般使用者必須從裝置商店下載此應用程式。*Apple App Store* 適用於 *iOS*、*Google Play* 適用於 *Android*、*Chrome Web Store* 適用於 *Chromebook*，*Microsoft Store* 適用於 *Windows 10 UWP*。然而，部署至行動應用程式使用者的代理程式組態會控制閘道，而行動端點具有閘道的存取權限。如需支援版本的詳細資訊，請參閱 GlobalProtect 支援的作業系統版本為何？

除了散佈 GlobalProtect 應用程式軟體，您可以將 GlobalProtect 入口網站設定為對一般企業 Web 應用程式（採用 HTML、HTML5 和 Javascript 技術）提供安全的遠端存取。使用者可從具有 SSL 功能的 Web 瀏覽器獲得安全存取的好處，而不必安裝 GlobalProtect 應用程式軟體。當您需要為合作夥伴或派遣員工啟用應用程式存取權時，以及要安全地啟用未受管理的資產（包括個人端點）時，此功能相當實用。請參閱 GlobalProtect 無用戶端 VPN。

設定 GlobalProtect 入口網站的先決工作

您必須先完成下列工作，才能設定 GlobalProtect 入口網站：

- 為您打算用來設定入口網站的防火牆建立介面（與區域）。請參閱為 GlobalProtect 建立介面與區域。
- 設定入口網站伺服器憑證、閘道伺服器憑證、SSL/TLS 服務設定檔，並選擇性地設定要部署至一般使用者的所有用戶端憑證，以實現與 GlobalProtect™ 服務之間的 SSL/TLS 連線。請參閱在 GlobalProtect 元件之間啟用 SSL。
- 已定義將用來驗證 GlobalProtect 使用者的選用驗證設定檔與/或憑證設定檔。請參閱驗證。
- 設定 GlobalProtect 閘道和瞭解在多重閘道設定中的閘道優先順序。

設定 GlobalProtect 入口網站存取權

在完成設定 GlobalProtect 入口網站的先決工作之後，如下所述設定 GlobalProtect 入口網站：

STEP 1 | 新增入口網站。

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後 **Add**（新增）入口網站。
2. 輸入入口網站的 **Name**（名稱）。

   閘道名稱不能包含空格，且對於每個虛擬系統來說是唯一的。
3. （選用）從 **Location**（位置）欄位中選取此入口網站所屬的虛擬系統。

STEP 2 | 指定網路設定以使 GlobalProtect 應用程式能夠與入口網站通訊。

如果您還沒有為入口網站建立網路介面，請參閱為 GlobalProtect 建立介面與區域。如果您尚未為此入口網站建立 SSL/TLS 服務設定檔，請參閱為 GlobalProtect 元件部署伺服器憑證。

在您已設定 *GlobalProtect* 入口網站或閘道的介面上，請勿附加允許 *HTTP*、*HTTPS*、*Telnet* 或 *SSH* 的介面管理設定檔，因為這會啟用從網際網路存取管理介面的存取權。請遵照保護管理存取權的最佳做法，來確保您可以保障防火牆的管理存取權，以防攻擊成功。

1. 選取 **General**（一般）。
2. 在網路設定區域，選取 **Interface**（介面）。
3. 指定用於閘道 Web 服務的 **IP Address Type**（IP 位址類型）和 **IP address**（IP 位址）。
   - IP 位址類型可以是 **IPv4 Only**（僅限 IPv4）、**IPv6 Only**（僅限 IPv6）或 **IPv4 and IPv6**（IPv4 和 IPv6）。如果您的網路支援雙堆疊組態（也就是會同時執行 IPv4 和 IPv6），請使用 **IPv4 and IPv6**（IPv4 和 IPv6）。
   - IP 位址必須與 IP 位址類型相容。例如，`172.16.1.0`（適用於 IPv4）或 `21DA:D3:0::2F3b`（適用於 IPv6）。對於雙堆疊組態，輸入 IPv4 和 IPv6 位址。
4. 選取 **SSL/TLS Service Profile**（SSL/TLS 服務設定檔）。

STEP 3 | 選取自訂登入與說明頁面或完全停用登入與說明頁面。關於建立自訂登入頁面與說明頁面的詳細資訊，請參閱自訂 GlobalProtect 入口網站登入、歡迎與說明頁面。

1. 選取 **General**（一般）。
2. 在外觀區域，設定下列任意設定：
   - 若要設定 **Portal Login Page**（入口網站登入頁面）以便使用者存取入口網站，請選取 **factory-default**（原廠預設）登入頁面，**Import**（匯入）自訂登入頁面，或 **Disable**（停用）登入頁面的存取權限。
   - 若要設定 **App Help Page**（應用程式說明頁面）以向使用者提供使用 GlobalProtect 應用程式的協助，請選取 **factory-default**（原廠預設）說明頁面，**Import**（匯入）自訂說明頁面，或選取 **None**（無）以從 GlobalProtect 狀態面板的 **Settings**（設定）功能表中移除 **Help**（說明）選項。

STEP 4 | 指定入口網站驗證使用者的方式。

1. 選取 **Authentication**（驗證）。
2. 設定下列任何入口網站驗證設定：

   如果您還沒有為此入口網站建立伺服器憑證並簽發閘道憑證，請參閱為 GlobalProtect 元件部署伺服器憑證。

   - 若要保障入口網站與 GlobalProtect 應用程式間的通訊安全，為入口網站選取 **SSL/TLS Service Profile**（SSL/TLS 服務設定檔）。

- 若要使用本機使用者資料庫或外部驗證服務（例如 LDAP、Kerberos、TACACS+、SAML 或 RADIUS（包括 OTP））驗證使用者，請定義 GlobalProtect 用戶端驗證設定。
- 若要根據用戶端憑證或智慧卡/CAC 驗證使用者，請選取對應的 **Certificate Profile**（憑證設定檔）。您必須使用簡易憑證註冊通訊協定 (SCEP) 預部署用戶端憑證或部署驗證用使用者指定用戶端憑證。
  - 如果您想要求使用者使用其使用者認證與用戶端憑證對入口網站進行驗證，則需要 **Certificate Profile**（憑證設定檔）與 驗證設定檔。
  - 如果您要允許使用者使用其使用者認證或用戶端憑證對入口網站進行驗證，且為使用者驗證選取了 驗證設定檔，則 **Certificate Profile**（憑證設定檔）為選用項目。
  - 如果您要允許使用者使用其使用者認證或用戶端憑證對入口網站進行驗證，但沒有為使用者驗證選取 驗證設定檔，則 **Certificate Profile**（憑證設定檔）為必選項目。
  - 如果您未設定任何與特定作業系統相符的 Authentication Profile（驗證設定檔），則 **Certificate Profile**（憑證設定檔）為必選項目。

  如果您允許使用者使用使用者認證或用戶端憑證對入口網站進行驗證，請選取 *Username Field*（使用者名稱欄位）設為 *Subject*（主體）或 *Subject Alt*（主體別名）的 *Certificate Profile*（憑證設定檔）。

STEP 5 | 定義使用者成功對入口網站進行驗證後，GlobalProtect 應用程式從連線端點收集的資料。

GlobalProtect 應用程式會將此資料傳送至入口網站，以與您為每個入口網站代理程式組態定義的 選取準則 進行比對。根據此準則，入口網站會將特定代理程式組態傳遞至連線的 GlobalProtect 應用程式。

1. 選取 **Portal Data Collection**（入口網站資料收集）。
2. 設定下列任何資料收集設定：
   - 如果您要 GlobalProtect 應用程式從連線端點收集機器憑證，請選取指定要收集之機器憑證的 **Certificate Profile**（憑證設定檔）。
   - 如果要 GlobalProtect 應用程式從連線端點收集自訂主機資訊，請在自訂檢查區域定義下列登錄或 plist 資料：
     - 若要從 Windows 端點收集登錄資料，請選取 **Windows** 並 **Add**（新增）**Registry Key**（登錄機碼）及對應的 **Registry Value**（登錄值）。
     - 若要從 macOS 端點收集 plist 資料，請選取 **Mac** 並 **Add**（新增）**Plist** 機碼及對應的 **Key**（機碼）值。

STEP 6 | 儲存入口網站組態。

1. 按一下 **OK**（確定）以儲存設定。
2. **Commit**（提交）變更。

定義 GlobalProtect 用戶端驗證組態

各 GlobalProtect 用戶端驗證組態指定設定，讓使用者可以透過 GlobalProtect 入口網站驗證。您可以為各作業系統自訂設定，或進行設定以套用至所有端點。例如，您可以設定 Android 使用者使用 RADIUS 驗證，和設定 Windows 使用者使用 LDAP 驗證。您也可以為從網頁瀏覽器存取入口網站的使用者自訂用戶端驗證（以下載 GlobalProtect 應用程式）或為協力廠商 IPsec VPN (X-Auth) 對 GlobalProtect 閘道的存取進行自訂。

STEP 1 | 設定 GlobalProtect 入口網站存取權。

STEP 2 | 指定入口網站驗證使用者的方式。

您可以設定 GlobalProtect 入口網站以透過本機使用者資料庫或外部驗證服務（如 LDAP、Kerberos、TACACS+、SAML 或 RADIUS（包括 OTP））來驗證使用者。如果您未設定驗證設定檔與/或憑證設定檔，請參閱驗證以瞭解相關指示。

在 GlobalProtect 入口網站組態對話方塊（**Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>*），選取 **Authentication**（驗證）以透過下列設定 **Add**（新增）新的 **Client Authentication**（用戶端驗證）組態：

- 輸入用於識別用戶端驗證組態的 **Name**（名稱）。
- 指定您要部署此組態的端點。若要將此組態套用至所有端點，須接受 **OS**（作業系統）預設值 **Any**（任何）。若要將此組態套用至執行特定作業系統的端點，請選取 **OS**（作業系統），例如 **Android**。或者，您可將此組態套用至從 Web **Browser**（瀏覽器）連線至 無用戶端 VPN 入口網站 的端點。
- 若要讓使用者能夠使用其使用者認證對入口網站或閘道進行驗證，請選取或新增 **Authentication Profile**（驗證設定檔）。
  - 如果您想要求使用者使用其使用者認證與用戶端憑證對入口網站或閘道進行驗證，則需要 **Authentication Profile**（驗證設定檔）與 Certificate Profile（憑證設定檔）。
  - 如果您要允許使用者使用其使用者認證或用戶端憑證對入口網站或閘道進行驗證，且為使用者驗證選取了 Certificate Profile（憑證設定檔），則 **Authentication Profile**（驗證設定檔）為選用項目。
  - 如果您要允許使用者使用其使用者認證或用戶端憑證對入口網站或閘道進行驗證，但沒有為使用者驗證選取 Certificate Profile（憑證設定檔）（或將 **Certificate Profile**（憑證設定檔）設為 **None**（無）），則 **Authentication Profile**（驗證設定檔）為必選項目。
- （選用）輸入要用於 GlobalProtect 入口網站登入的自訂 **Username Label**（使用者名稱標籤）（例如，電子郵件地址 **(username@domain**）。
- （選用）輸入要用於 GlobalProtect 入口網站登入的自訂 **Password Label**（密碼標籤）（例如，雙因素權杖式驗證的密碼）。
- （選用）輸入 **Authentication Message**（驗證訊息）幫助一般使用者理解登入期間使用到哪些認證。訊息長度最多為 256 個字元（預設為 `Enter login credentials`）。
- 選取下列選項之一以定義使用者是否可以使用認證與/或用戶端憑證對入口網站進行驗證：
  - 若要要求使用者同時使用認證與用戶端憑證對入口網站進行驗證，請將 **Allow Authentication with User Credentials OR Client Certificate**（允許使用使用者憑證或用戶端憑證進行驗證）選項設定為 **No (User Credentials AND Client Certificate Required)**（否（需要使用者認證與用戶端憑證））（預設）。
  - 若要允許使用者使用認證或用戶端憑證對入口網站進行驗證，請將 **Allow Authentication with User Credentials OR Client Certificate**（允許使用使用者憑證或用戶端憑證進行驗證）選項設定為 **Yes (User Credentials OR Client Certificate Required)**（是（需要使用者認證或用戶端憑證））。

    當您將此選項設為 **Yes**（是）時，GlobalProtect 入口網站首先會搜尋端點以取得用戶端憑證。如果端點沒有用戶端憑證或您沒有為用戶端驗證組態設定憑證設定檔，則一般使用者必須使用其使用者認證對入口網站進行驗證。

STEP 3 | 透過清單頂部的 OS 指定組態安排用戶端驗證，且組態套用於清單底部的 **Any**（任何）作業系統（**Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> **<portal-config>** > **Authentication**（驗證））。藉助安全性規則評估，入口網站會從清單頂端開始尋找符合項。找到符合項目時，會將對應的設定傳遞給應用程式。

- 若要在組態清單中上移用戶端驗證組態，請選取設定並按一下 **Move Up**（上移）。
- 若要在組態清單中下移用戶端組態，請選取設定並按一下 **Move Down**（下移）。

STEP 4 | （選用）若要透過驗證設定檔和憑證設定檔啟用雙因素驗證，在入口網站組態中進行二者的設定。

在使用者獲得存取權之前，入口網站必須透過兩種方法一起驗證端點。

（僅限 *Chrome*）如果您將入口網站設為使用用戶端與 *LDAP* 進行雙因素驗證，執行 *Chrome OS 47* 或更新版本的 *Chromebook* 會收到選取用戶端憑證的過多提示。若要防止收到過多提示，請設定原則以在 *Google* 管理控制台中指定用戶端憑證，然後將該原則部署至受管理的 *Chromebook*：

1. 登入至 Google 管理控制台，選取 *Device management*（裝置管理）> *Chrome management*（*Chrome* 管理）> *User settings*（使用者設定）。
2. 在 *Client Certificates*（用戶端憑證）區段中，輸入下列 *URL* 模式以 *Automatically Select Client Certificate for These Sites*（自動為這些網站選取用戶端憑證）：

   ```
   {"pattern": "https://[*.]","filter":{}}
   ```
3. 按一下 *Save*（儲存）。*Google* 管理控制台在幾分鐘內即可將原則部署至所有裝置。

在 GlobalProtect 入口網站組態對話方塊中（**Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>*），選取 **Authentication**（驗證）以選取用於根據用戶端憑證或智慧卡驗證使用者的 **Certificate Profile**（憑證設定檔）。

憑證的 *[通用名稱] (CN)* 及（如果適用）*[主旨替代名稱] (SAN)* 欄位，必須完全符合您用來設定入口網站之介面的 *IP* 位址或 *FQDN*，否則與入口網站間的 *HTTPS* 連線將會失敗。

STEP 5 | 儲存入口網站組態。

1. 按一下 **OK**（確定）儲存組態。
2. **Commit**（提交）變更。

定義 GlobalProtect 代理程式組態

在 GlobalProtect 使用者連線至 GlobalProtect 入口網站並成功向其驗證後，入口網站會根據您定義的設定將代理程式組態遞送至應用程式。如果您對需要特定組態的使用者或群組有不同的角色，您可以為每個使用者類型或使用者群組建立獨立的代理程式組態。入口網站使用端點 OS 和使用者名稱或群組名稱以確定部署的代理程式組態。藉助其他安全性規則評估，入口網站會從清單頂端開始搜尋符合項。找到符合項時，入口網站會將組態傳遞給應用程式。

設定可能包括以下內容：

- 端點可連線的閘道清單。
- 在外部閘道之間，使用者可以為工作階段手動選取的任何閘道。
- 要使應用程式能夠與 GlobalProtect 閘道之間建立 SSL 連線所必需的根 CA 憑證。
- SSL 轉送 Proxy 解密的根 CA 憑證。
- 端點在連線時應出示給閘道的用戶端憑證。僅當需要在應用程式和入口網站或閘道之間相互驗證時，需要此組態。
- 端點在連線時應出示給入口網站或閘道的端點加密 cookie。僅當您啟用入口網站以產生 Cookie 時，其才被包含在內。

- 端點用來決定連線至本機網路還是外部網路的設定。
- 應用程式行為設定，如一般使用者在顯示中看到的內容，是否儲存其 GlobalProtect 密碼，以及是否提示升級其軟體。

如果入口網站關閉或無法連線，應用程式將使用其上次成功入口網站連線中的快取版代理程式組態來取得設定，其中包括要連線的閘道、使用哪些根 *CA* 憑證與閘道間建立安全通訊，以及使用的連線方法。

使用下列程序建立代理程式組態。

STEP 1 | 將一或多個受信任的根 CA 憑證新增至入口網站代理程式設定，讓 GlobalProtect 應用程式來驗證入口網站和閘道的識別。

入口網站會在憑證檔案中部署該憑證，該憑證網站僅可供 GlobalProtect 讀取。

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）。
2. 選取您新增代理程式組態的入口網站組態，然後選取 **Agent**（代理程式）頁籤。
3. 在 **Trusted Root CA**（受信任的根 **Ca**）欄位中欄位中 **Add**（新增），然後選取用來簽發閘道和/或伺服器憑證的 CA 憑證。

   Web 介面會出示 CA 憑證的列表，系統會在作為 GlobalProtect 入口網站服務的防火牆上匯入這些憑證。Web 介面也會從您可以選取的憑證清單中，排除終端實體憑證（有時稱為分葉憑證）。您也可以 **Import**（匯入）新 CA 憑證。

   在建立和新增憑證時請使用下列最佳做法：

   - 使用相同的憑證簽發者來為所有的閘道簽發憑證。
   - 將完整的憑證鏈（受信任的根 *CA* 和中繼 *CA* 憑證）新增至入口網站代理程式設定。
4. （選用）若有 GlobalProtect 以外的用途（例如，SSL 轉送 proxy 解密），請部署其他 CA 憑證。

   此選項可讓您使用入口網站來將憑證部署至端點與代理程式，以在本機根憑證存放區中安裝它們。若您沒有其他散佈這些伺服器憑證的方法或是偏好使用入口網站來進行憑證散佈，此動作可能會很有用。

   對於 SSL 轉送 proxy 解密，您會指定防火牆用來（僅限 Windows 和 macOS 端點）終止 HTTPS 連線、檢查原則遵循流量，並重新建立 HTTPS 連線以轉送加密流量的轉送信任憑證。

   1. 如上一步所述新增該憑證。
   2. 啟用選項以 **Install in Local Root Certificate Store**（在本機根憑證存放區上安裝）。

      當使用者登入入口網站時，入口網站自動遞送憑證並在端點本機商店中安裝，從讓您無需手動安裝憑證。

STEP 2 | 新增代理程式組態。

代理程式組態可指定用來部署至連線應用程式的 GlobalProtect 設定。您必須定義至少一個代理程式設定。

1. 從入口網站組態中（**Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>*），**Add**（新增）新的代理程式組態。
2. 輸入 **Name**（名稱）來識別組態。如果您打算建立多個設定，請確定您為每個設定定義的名稱具有描述性，足以讓您識別這些設定。

STEP 3 | （選用）進行設定以指定具有此組態的使用者將如何透過入口網站進行驗證。

如果閘道透過用戶端憑證驗證端點，您必須選取散佈此憑證的源。

設定下列任何 **Authentication**（驗證）設定：

- 若要啟用使用者以透過用戶端憑證驗證入口網站，選取 **Client Certificate**（用戶端憑證）來源（**SCEP**、**Local**（本機）或 **None**（無））散佈憑證及其私密金鑰至端點。如果使用內部 CA 將憑證散佈到端點，請選取 **None**（無）（預設值）。若要確保入口網站產生並遞送及其憑證至應用程式，以在本機憑證商店中儲存和使用入口網站和閘道驗證憑證，選取 **SCEP** 和關聯的 SCEP 設定檔。這些憑證為裝置特定且僅可用於發往的端點。若要為所有端點使用相同憑證，選取一個入口網站的 **Local**（本機）憑證。選取 **None**（無），入口網站不會推送憑證至端點，但您可以使用其他方式獲得端點的憑證。
- 指定是否 **Save User Credentials**（儲存使用者認證）。選取 **Yes**（是）以儲存使用者名稱和密碼（預設），選取 **Save Username Only**（僅儲存使用者名稱）以僅儲存使用者名稱，選取 **Only with User Fingerprint**（僅透過使用者指紋）以儲存使用者的生物特徵（指紋）或臉部 ID認證（僅限 iOS X 端點），或選取 **No**（否）以不儲存認證。

  如果您設定入口網站或閘道以提示動態密碼，如一次性密碼 (OTP)，使用者必須在每次登入時輸入新密碼。在此情況下，GlobalProtect 應用程式忽略選擇，以儲存使用者名稱和密碼，如有指定，則僅儲存使用者名稱。如需更多資訊，請參閱使用一次性密碼 (OTP) 啟用雙因素驗證。

  若您選取 GlobalProtect 以 **Only with User Fingerprint**（僅透過使用者指紋）**Save User Credentials**（儲存使用者認證），在允許 GlobalProtect 驗證之前，GlobalProtect 可以利用應用程式的作業系統功能對使用者進行驗證。一般使用者必須套用與端點上信任指紋範本相符的指紋，以使用儲存的密碼進行 GlobalProtect 入口網站和閘道驗證。在 iOS X 裝置上，GlobalProtect 還支援透過 Face ID 進行的臉部識別。GlobalProtect 不會儲存用於驗證的指紋或臉部範本，但依賴作業系統掃描功能確定掃描比對的有效性。

STEP 4 | 如果 GlobalProtect 端點在內部網路上時不需要通道連線，設定內部主機偵測。

1. 選取 **Internal**（內部）。
2. 啟用 **Internal Host Detection**（內部主機偵測）（**IPv4** 或 **IPv6**）。
3. 輸入只能從內部網路到達之主機的 **IP Address**（**IP** 位址）。您指定的 IP 位址必須與 IP 位址類型相容（**IPv4** 或 **IPv6**）。例如，172.16.1.0（適用於 IPv4）或 21DA:D3:0:2F3b（適用於 IPv6）。
4. 輸入與您所輸入 IP 位址的 DNS **Hostname**（主機名稱）。嘗試連線至 GlobalProtect 的端點嘗試在指定位址上進行 DNS 反向查找。如果查找失敗，端點確定其位於外部網路上，然後啟動通道連線至外部閘道清單上的某個閘道。

STEP 5 | 設定對協力廠商行動端點管理系統的存取權。

如果使用此組態的行動端點將受協力廠商行動端點管理系統，則必須執行此步驟。所有端點最初都會連線至入口網站，且如果協力廠商行動端點管理系統已在對應的入口網站代理程式組態上設定，則會將端點向其重新導向以進行註冊。

1. 輸入與您的行動端點管理系統關聯的端點簽入介面 IP 位址或 FQDN。您在此輸入的值必須與端點簽入介面相關聯之伺服器憑證的值完全符合。您可以指定 IPv6 或 IPv4 位址。
2. 為行動端點管理系統指定將接聽註冊要求的 **Enrollment Port**（註冊連接埠）。此值必須符合在行動端點管理系統中所設定的值（預設 = 443）。

STEP 6 | 為入口網站代理程式組態指定選取準則。

入口網站會使用您指定的選取準則來決定要將哪個設定遞送至所連線的 GlobalProtect 應用程式。因此，如果您擁有多個組態，請必須確保這些設定排序正確。入口網站只要找到符合項目便會傳遞設定。因此，較具體的設定必須位於較一般性設定的前方。關於代理程式組態清單排序的說明，請參閱步驟 12。

選取 **Config Selection Criteria**（設定選取準則），然後設定下列任何選項：

- 若要指定此組態要套用的使用者、使用者群組與/或作業系統，請選取 **User/User Group**（使用者/使用者群組），然後設定下列任何選項：
  - 若要傳遞此設定至在特定作業系統上運行的應用程式，請 **Add**（新增）並選取此設定適用的 **OS**（作業系統）（**Android**、**Chrome**、**iOS**、**Linux**、**Mac**、**Windows** 或 **WindowsUWP**）。將 **OS**（作業系統）設為 **Any**（任何）以向所有作業系統部署組態。

- 若要將此組態限制在特定使用者和/或使用者群組，請 **Add**（新增）並選取您要接收此組態的 **User/User Group**（使用者/使用者群組）。針對每個要新增的使用者/群組重複此步驟。若要將組態限制為尚未登入其端點的使用者，請從 **User/User Group**（使用者/使用者群組）下拉式清單中選取 **pre-logon**（預先登入）。要套用設定至任何使用者而不考慮登入狀態（包括預登入和已登入使用者），從 **User/User Group**（使用者/使用者群組）下拉式清單中選取 **any**（任何）。

  您必須先依照啟用群組對應所述將使用者對應至群組，才能將組態限制給特定的群組。

- 若要根據特定裝置屬性傳遞此組態至應用程式，請選取 **Device Checks**（裝置檢查），然後設定下列任何選項：
  - 若要根據 Active Directory 或 Azure AD 中端點序號的存在狀況傳遞此組態，請從 **Machine account exists with device serial number**（機器帳戶存在裝置序號）下拉式清單中選取選項。如果您將此選項設為 **Yes**（是），則代理程式組態將僅套用至序號存在的端點（受管理端點）。如果您將此選項設為 **No**（否），則代理程式組態將僅套用至序號不存在的端點（不受管理端點）。如果您將此選項設為 **None**（無），則組態不會根據端點序號的存在狀況傳遞給應用程式。
  - 若要根據端點的機器憑證傳遞此組態，請選取 **Certificate Profile**（憑證設定檔）以與端點上安裝的機器憑證進行比對。
- 若要根據自訂主機資訊將此組態傳遞給應用程式，請選取 **Custom Checks**（自訂檢查）。啟用 **Custom Checks**（自訂檢查），然後定義下列任何登錄與 plist 資料：
  - 若要確認 Windows 端點是否具有特定登錄機碼，請使用下列步驟：
    1. **Add**（新增）新的登錄機碼（**Custom Checks**（自訂檢查）> **Registry Key**（登錄機碼））。
    2. 出現提示時，輸入要比對的 **Registry Key**（登錄機碼）。
    3. （選用）若只要在端點沒有指定登錄機碼或機碼值時傳遞此組態，請選取 **Key does not exist or match the specified value data**（機碼不存在或不符合指定的值資料）。
    4. （選用）若要根據特定登錄值傳遞此組態，須 **Add**（新增）**Registry Value**（登錄值）與對應 **Value Data**（值資料）。若只要在端點沒有指定 **Registry Value**（登錄值）或 **Value Data**（值資料）時傳遞此組態，請選取 **Negate**（否定）。
  - 若要確認 macOS 端點在 plist 中是否具有特定項目，請使用下列步驟：
    1. **Add**（新增）新的 plist（**Custom Checks**（自訂檢查）> **Plist**）。
    2. 出現提示時，輸入 **Plist** 名稱。
    3. （選用）若只要在端點沒有指定 plist 時傳遞此組態，請選取 **Plist does not exist**（**Plist** 不存在）。
    4. （選用）若要根據 Plist 內的特定機碼-值配對傳遞此組態，請按一下 **Add**（新增），然後輸入 **Key**（機碼）和對應 **Value**（值）。若要比對確實沒有指定機碼或值的端點，請選取 **Negate**（否定）。

STEP 7 | 指定使用此組態的使用者可以連線的外部閘道。

當您設定閘道時，考慮下列最佳作法：

- 如果您將內部與外部閘道新增至相同的組態，請務必啟用 *Internal Host Detection*（內部主機偵測）（步驟 *4*）。
- 若要瞭解更多關於 *GlobalProtect* 應用程式如何確定連線的閘道，請參閱多閘道組態中的閘道優先順序。

1. 選取 **External**（外部）。
2. **Add**（新增）使用者可以連線的 **External Gateways**（外部閘道）。
3. 輸入閘道的描述性 **Name**（名稱）。您在此輸入的名稱應該符合您在設定閘道時所定義的名稱，而且該名稱應該具有足夠的描述性，讓使用者能夠知道他們所連線的目標閘道位置。
4. 在 **Address**（位址）欄位中輸入設定閘道所在介面的 FQDN 或 IP 位址。您可以設定 IPv4 或 IPv6 位址。您指定的位址必須與閘道伺服器憑證中的通用名稱 (CN) 完全符合。

5. **Add**（新增）一或多個該閘道的 **Source Regions**（來源區域）或選取 **Any**（任何）以讓該閘道可供所有區域使用。當使用者連線時，GlobalProtect 會辨識區域，並只允許使用者連線到針對該區域所設定的閘道。在選取閘道時，會先考慮使用來源閘道，然後才是閘道優先順序。
6. 按一下欄位並選取下列值之一來設定閘道的 **Priority**（優先順序）：
   - 如果您只擁有一個外部閘道，您可以將設定值保留為 **Highest**（最高）（預設值）。
   - 如果您擁有多個外部閘道，可修改優先順序值（範圍從 **Highest**（最高）到 **Lowest**（最低）），來指定套用此組態的目標特定使用者群組的偏好設定。例如，如果您希望使用者群組連線至本機閘道，您可以將優先順序設定為高於在地理位置上更遠的閘道。之後，優先順序值會用來加權代理程式的閘道選取演算法。
   - 如果您不想讓應用程式與閘道之間自動建立連線，請選取 **Manual only**（僅限手動）。此設定在測試環境中很有用。
7. 選取 **Manual**（手動）核取方塊以讓使用者能夠手動切換至閘道。

STEP 8 | 指定使用此組態的使用者可以連線的內部閘道。

如果您的組態包含內部閘道，請勿使用視需要作為連線方法。

1. 選取 **Internal**（內部）。
2. **Add**（新增） 使用者可以連線的 **Internal Gateways**（內部閘道）。
3. 輸入閘道的描述性 **Name**（名稱）。您在此輸入的名稱應該符合您在設定閘道時所定義的名稱，而且該名稱應該具有足夠的描述性，讓使用者能夠知道他們所連線的目標閘道位置。
4. 在 **Address**（位址）欄位中輸入設定閘道所在介面的 FQDN 或 IP 位址。您可以設定 IPv4 或 IPv6 位址。您指定的位址必須與閘道伺服器憑證中的通用名稱 (CN) 完全符合。
5. （選用）將一或多個 **Source Addresses**（來源位址）**Add**（新增）至閘道設定。來源位址可以是 IP 子網路、範圍或預先定義的位址。GlobalProtect 支援 IPv6 和 IPv4 位址。使用者連線時，GlobalProtect 會辨識端點來源位址，並只允許使用者連線到針對該位址所設定的閘道。
6. 按一下 **OK**（確定）儲存您的變更。
7. （選用）將 **DHCP Option 43 Code**（**DHCP** 選項 **43** 代碼）**Add**（新增）至閘道設定。您可以包含一或多個與廠商特定資訊相關聯的子選項代碼（選項 43），系統已將 DHCP 伺服器設定為將這些資訊提供給用戶端。例如，您可能擁有與 IP 位址為 192.168.3.1 相關聯的子選項代碼 100。

   使用者連線時，GlobalProtect 入口網站會在入口網站設定中將選項代碼清單傳送給 GlobalProtect 應用程式，而應用程式會選取選項所指示的閘道。

   若來源位址和 DHCP 選項都設定好，出示給端點的可用閘道清單將會以此兩種設定的結合（聯合）為基礎。

   只有在 *Windows* 和 *macOS* 端點上才支援 *DHCP* 選項。*DHCP* 選項無法用來選取使用 *IPv6* 位址的閘道。
8. （選用）選取 **Internal Host Detection**（內部主機偵測） 可讓 GlobalProtect 應用程式判定其是否位在企業網路中。當使用者嘗試登入時，應用程式會對特定 **IP Address**（**IP** 位址）的內部 **Hostname**（主機名稱）執行反向 DNS 查詢。

   如果端點在企業網路中，主機將用作可到達的參考點。如果應用程式發現主機，端點則在網路中且應用程式連線至內部閘道；如果應用程式未能找到內部主機，則端點不在網路中且應用程式會連線至其中一個外部閘道。

   您可以設定 **Internal Host Detection**（內部主機偵測）的 **IPv4** 或 **IPv6** 位址。您指定的 IP 位址必須與 IP 位址類型相容。例如，172.16.1.0（適用於 IPv4）或 21DA:D3:0:2F3b（適用於 IPv6）。

STEP 9 | 針對使用此組態的使用者自訂 GlobalProtect 應用程式行為。

根據需要修改 **App**（應用程式） 設定。如需每個選項的詳細資訊，請參閱自訂 GlobalProtect 應用程式。

STEP 10 | （選用）定義您想讓應用程式從集合中收集與/或排除的任何自訂主機資訊設定檔 (HIP) 資料。

只有在您打算使用 *HIP* 功能且當要收集的資訊無法使用標準 *HIP* 物件來收集時，或者當您沒興趣收集的 *HIP* 資訊存在時，此步驟才適用。如需設定及使用 *HIP* 功能的詳細資訊，請參閱主機資訊。

如需收集自訂 *HIP* 資料的其他資訊，請參閱 從端點收集應用程式與處理資料。

1. 選取 **HIP Data Collection**（**HIP** 資料收集）。
2. 啟用 GlobalProtect 應用程式以 **Collect HIP Data**（收集 **HIP** 資料）。
3. 指定應用程式在提交可用資料之前應搜尋 HIP 資料的 等候時間上限（秒）（範圍是 10-60 秒；預設為 20 秒）。
4. 選取 **Certificate Profile**（憑證設定檔），以便 GlobalProtect 入口網站用於與 GlobalProtect 應用程式傳送的機器憑證進行比對。
5. 選取 **Exclude Categories**（排除類別），來排除特定類別及/或類別中的廠商、應用程式或版本。如需詳細資訊，請參閱設定以 HIP 為基礎的原則強制執行。
6. 選取 **Custom Checks**（自訂檢查），然後定義您要從執行此代理程式組態之主機收集的任何自訂資料。

STEP 11 | 儲存代理程式組態。

按一下 **OK**（確定）儲存代理程式組態。

STEP 12 | 安排代理程式組態，以將適當的組態部署至每個應用程式。

當應用程式連線時，入口網站會將封包中的來源資訊與您已定義的代理程式組態進行比較。藉助安全性規則評估，入口網站會從清單頂端開始尋找符合項。找到符合項目時，會將對應的設定傳遞給應用程式。

- 若要將組態清單中的代理程式組態向上移，請選取該組態並按一下 **Move Up**（上移）。
- 若要將組態清單中的代理程式組態向下移，請選取該組態並按一下 **Move Down**（下移）。

STEP 13 | 儲存入口網站組態。

1. 按一下確定儲存入口網站設定。
2. **Commit**（提交）變更。

自訂 GlobalProtect 應用程式

入口網站代理程式組態可讓您自訂一般使用者如何與安裝在其端點的 GlobalProtect 應用程式互動。您可以自訂應用程式的顯示與行為，並為您建立的不同 GlobalProtect 代理程式組態定義不同的應用程式設定。例如，您可以指定下列內容：

- 使用者可以存取的功能表與檢視。
- 使用者是否可以解除安裝或停用應用程式（僅適用於使用者登入連線方法）。
- 成功登入後是否顯示歡迎頁面。您也可以設定使用者是否可以關閉歡迎頁面，並可以自訂 GlobalProtect 入口網站登入、歡迎與說明頁面，來解釋如何在您的環境中使用 GlobalProtect。
- 無論 GlobalProtect 應用程式自動升級或提示使用者手動升級。
- 在多因素驗證需要存取敏感網路資源時是否提示使用者。

您還可在 Windows 登錄、Windows 安裝程式 (Msiexec) 及全域 macOS plist 中定義應用程式設定。在 Web 介面（入口網站代理程式組態）中所定義的設定，將優先於在 Windows 登錄、Msiexec 及 macOS plist 中所定義的設定。如需詳細資訊，請參閱明顯部署應用程式設定。

只能透過 Windows 登錄或 Windows 安裝程式 (Msiexec) 使用的其他設定可讓您：

- 指定應用程式是否在 Windows SSO 失敗時，提示一般使用者提供認證。
- 指定預設入口網站 IP 位址（或主機名稱）。
- 啟用 GlobalProtect 以在使用者登入端點之前啟動連線。
- 部署在 GlobalProtect 建立連線前後，或在 GlobalProtect 中斷連線之後執行的指令碼。
- 設定 GlobalProtect 應用程式，以封裝 Windows 端點上的第三方認證，以在使用第三方認證提供者時啟用 SSO。

如需詳細資訊，請參閱可自訂應用程式設定。

STEP 1 | 選取您要自訂的代理程式組態。

您還可從 *Windows* 登錄、*Windows* 安裝程式 *(Msiexec)* 及 *macOS plist* 進行大部分應用程式設定。但是，在 *Web* 介面中所定義的設定，將優先於在 *Windows* 登錄、*Msiexec* 及 *macOS plist* 中所定義的設定。如需詳細資訊，請參閱明顯部署應用程式設定。

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）。
2. 選取您要新增代理程式組態的入口網站，或 **Add**（新增）一個。
3. 在 **Agent**（代理程式）頁籤上，選取您要修改的代理程式組態或 **Add**（新增）一個新的。
4. 選取 **App**（應用程式）頁籤。

   應用程式組態區域會顯示帶有預設值的應用程式設定，您可以為各代理程式組態進行自訂。當您變更預設行為時，文字顏色從灰色變為預設顏色。

STEP 2 | 指定應用程式為其 GlobalProtect 連線使用的 **Connect Method**（連線方法）。

使用預登入（一直開啟）、預登入然後視需要，或使用者登入（一直開啟）連線方法，以內部閘道存取網路。

在應用程式組態區域，選取下列 **Connect Method**（連線方法）選項之一：

- **User-logon (Always On)**（使用者登入（一直開啟））—GlobalProtect 應用程式將會在使用者登入端點（或網域）後立即自動連線。當與 SSO（僅限 Windows 端點）搭配使用時，GlobalProtect 登入對於一般使用者而言是明顯的。

  在 *iOS* 端點上，因為 *GlobalProtect* 強制所有流量經過通道，此設定會防止一次性密碼 *(OTP)* 應用程式運作。
- **Pre-logon (Always On)**（預登入（一直開啟））—在使用者登入端點之前，GlobalProtect 應用程式會驗證使用者並建立至 GlobalProtect 閘道的 VPN 通道。此選項要求您使用外部 PKI 解決方案以預部署機器憑證至接收此組態的各端點。如需關於預登入的詳細資訊，請參閱使用預先登入的遠端存取 VPN。
- **On-demand (Manual user initiated connection)**（視需要（手動使用者起始的連線））—使用者將必須手動啟動應用程式來連線至 GlobalProtect。請僅針對外部閘道使用此連線方法。
- **Pre-logon then On-demand**（預登入然後視需要）—與 **Pre-logon (Always On)**（預登入（一直開啟））連線方法類似，此連線方法（需要內容發行版本 590-3397 或以上）讓 GlobalProtect 應用程式在使用者登入端點之前驗證使用者，並建立至 GlobalProtect 閘道的 VPN 通道。與預登入連線方法不同，在使用者登入端點後，如果連線由於任何原因終止，使用者必須手動啟動應用程式以連線至 GlobalProtect。此選項的好處是，您可以讓使用者在密碼過期或忘記密碼後，指定一個新密碼，但仍需要此使用者在登入後手動啟動連線。

STEP 3 | 指定是否為網路存取強制執行 GlobalProtect 連線。

若要為網路存取強制執行 *GlobalProtect*，我們建議您僅為在 *User-logon*（使用者登入）或 *Pre-logon*（預登入）模式下連線的使用者啟用此功能。*On-demand*（視需要）模式下連線的使用者無法在允許的寬限期內建立連線。

在應用程式組態區域，設定下列任意選項：

- 若要強制所有網路流量周遊 GlobalProtect 通道，設定 **Enforce GlobalProtect Connection for Network Access**（強制執行 **GlobalProtect** 連線以進行網路存取）為 **Yes**（是）。依預設網路存取無需 GlobalProtect，意味著 GlobalProtect 停用或中斷連線時，使用者仍可存取網際網路。若要在流量被封鎖之前為使用者提供說明，設定 GlobalProtect 以 **Displays Traffic Blocking Notification Message**（顯示流量封鎖通知訊息）並選取指定何時顯示此訊息（**Traffic Blocking Notification Delay**（流量封鎖通知延遲））。

  Enforce GlobalProtect Connection for Network Access（強制執行 *GlobalProtect* 連線以進行網路存取）啟用後，您需要考慮讓使用者能以密碼關閉 *GlobalProtect* 應用程式。*Enforce GlobalProtect Connection for Network Access*（強制執行 *GlobalProtect* 連線以進行網路存取）功能，透過網路存取時對 *GlobalProtect* 連線的需求，增強網路安全性。在少數情況下，端點可能會無法連線至 *VPN*，需要遠端管理員登入以進行疑難排解。關閉 *GlobalProtect* 應用程式（對 Windows 或 macOS）使用管理員在疑難排解工作階段提供的密碼，您可以讓管理員遠端連線至您的端點。

- 透過輸入這些 IP 位址至 **Allow traffic to specified hosts/networks when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established**（當執行 **GlobalProtect** 連線以進行網路存取已啟用但未建立 **GlobalProtect** 連線時允許流量進入特定主機/網路）欄位，設定用於網路存取的特定本機 IP 位址或網路區段的排除。當您執行 GlobalProtect 以存取網路但 GlobalProtect 無法建立連線時，指定最多 10 個您想要允許存取的 IP 位址或網路區段。

  此選項需要內容發行版本*8196-5685* 或以上。

  透過設定排除，您可以讓使用者在 GlobalProtect 中斷連線時存取本機資源，從而提高使用者體驗。例如，當 GlobalProtect 未連線時，GlobalProtect 可以允許存取連結本機位址。這讓使用者能夠存取本機網路區段或廣播網域。

- 如果使用者必須登入網頁驗証才能存取網際網路，請指定 **Captive Portal Exception Timeout (sec)**（網頁驗證例外逾時（秒））），以表示使用者登入網頁驗証所需的時間（以秒為單位，範圍是 0 至 3600 秒；預設為 0 秒）。如果使用者未在此時段內登入，網頁驗證登入頁面將逾時，且使用者將無法使用網路。

  若要讓 GlobalProtect 應用程式在偵測到網頁驗證時顯示通知訊息，請將 **Display Captive Portal Detection Message**（顯示網頁驗證偵測訊息）設為 **Yes**（是）。在 **Captive Portal Notification Delay (sec)**（網頁驗證通知延遲（秒））欄位，輸入 GlobalProtect 應用程式顯示此訊息之前等待的時間（以秒為單位，範圍是 0 至 120 秒；預設為 5 秒）。GlobalProtect 在偵測到網頁驗證之後，但在網際網路可連線之前啟動此計時器。您還可提供其他說明，方法是設定 **Captive Portal Detection Message**（網頁驗證偵測訊息）。

  若要在網頁驗證偵測時自動啟動預設 Web 瀏覽器，以便使用者可以無縫登入至被控制的入口網站，請在 **Automatically Launch Webpage in Default Browser Upon Captive Portal Detection**（網頁驗證偵測時自動在預設瀏覽器中啟動網頁）欄位，輸入您想要用於進行初次連線嘗試的網站的完全合格網域名稱 (FQDN) 或 IP 位址，以在預設 Web 瀏覽器啟動時啟動 Web 流量（最大長度為 256 個字元）。然後，網頁驗證會攔截此網站連線嘗試，並將預設 Web 瀏覽器重新導向至網頁驗證登入頁面。若此欄位為空（預設），則 GlobalProtect 不會在網頁驗證偵測時自動啟動預設 Web 瀏覽器。

  這些選項需要內容發行版本 *607-3486* 或以上。*Captive Portal Notification Delay*（網頁驗證通知延遲）需要內容發行版本 *8118-5277* 或以上。*Automatically Launch Webpage in Default Browser Upon Captive Portal Detection*（網頁驗證偵測時在預設瀏覽器中自動啟動網頁）選項需要 *2019* 年 *7* 月 *8* 日或以後發行的內容發行版本。

STEP 4 | 指定其他 GlobalProtect 連線設定。

當單一登入 *(SSO)* 啟用（預設）時，*GlobalProtect* 應用程式會使用使用者的 *Windows* 登入認證以自動驗證 *GlobalProtect* 入口網站與閘道並建立連線。這也會使 *GlobalProtect* 應用程式封裝協力廠商認證，以確保即便使用協力廠商認證提供者，*Windows* 使用者也能夠驗證並連線。

在應用程式組態區域，設定下列任意選項：

- （僅限 Windows 與 macOS；macOS 支援需要內容發行版本 8196-5685 或以上）將 使用單一登入 **(Windows)** 或使用單一登入 **(macOS)** 設為 **No**（否）以停用單一登入。

  如果您設定 *GlobalProtect* 閘道以透過 SAML 驗證 對使用者進行驗證，並 產生和接受 cookie 以進行驗證覆寫，則必須在使用者的 *Windows* 使用者名稱不同於其 *SAML* 使用者名稱（例如，*Windows* 使用者名稱為「*user*」，而 *SAML* 使用者名稱為「*"user123*」），或一個使用者名稱包含完整網域名稱（例如，*Windows* 使用者名稱為「*user*」，而 *SAML* 使用者名稱為「*user@example.com*」）時，將 *Use Single Sign-On*（使用單一登入）選項設為 *No*（否）。
- 指定 GlobalProtect 應用程式 **Automatically Use SSL When IPSec Is Unreliable**（當 **IPSec** 不可靠時自動使用 **SSL**）的時間（以小時為單位；範圍是 0-168 小時）。如果您設定此選項，則 GlobalProtect 應用程式在指定的時段內不會嘗試建立 IPSec 通道。每當 IPSec 通道因通道保持運作逾時而關閉時，此計時器會啟動。

  如果您接受預設值 0，且應用程式可以成功建立 IPSec 通道，則其不會返回建立 SSL 通道。只有無法建立 IPSec 通道時，其才會返回建立 SSL 通道。

  此選項需要 *2019* 年 *7* 月 *8* 日或以後發行的內容發行版本。
- 為 GlobalProtect 應用程式選擇 SSL 連線選項。您可根據地理位置與網路效能選擇僅執行 SSL 連線、取消允許 SSL 連線或允許使用者選擇 SSL 或 IPSec（預設），以提供最佳使用者體驗。

  在應用程式組態區域，選擇要允許的 **Connect with SSL Only**（僅使用 **SSL** 連線）選項。

  此選項需要內容發行版本 *8207-5750* 或以上。

  - **Yes**（是）—要求所有 GlobalProtect 用戶端僅使用 SSL 連線。
  - **No**（否）—使用在閘道上設定用於進行 VPN 連線的通訊協定連線。如果閘道組態啟用了 IPSec，則其會使用 IPSec 進行 VPN 連線。如果閘道設定了 SSL，則其會使用 SSL 進行 VPN 連線。
  - **User can Change**（使用者可變更）—無論使用者想要使用 SSL 還是 IPSec，都允許其在 GlobalProtect 應用程式上進行變更。

    在應用程式上，使用者可以選取 **Settings**（設定）> **General**（一般）以啟用 **Connect with SSL Only**（僅使用 **SSL** 連線），及選取 **Settings**（設定）> **Connection**（連線）以驗證 **Protocol**（通訊協定）為 **SSL**。
- 輸入 GlobalProtect 應用程式在首次嘗試失敗後可重新嘗試連線至 **Maximum Internal Gateway Connection Attempts**（內部閘道的最大次數）（範圍是 0-100；建議設為 4 或 5；預設值為 0，這表示 GlobalProtect 應用程式未重新嘗試連線）。透過增加此值，可讓應用程式在以下情況下連線至內部閘道：暫時關閉或無法到達，但在指定重新嘗試次數用盡前重新開啟。增加值還可確保內部閘道接收最新的使用者及主機資訊。
- 輸入 **GlobalProtect App Config Refresh Interval**（**GlobalProtect** 應用程式設定重新整理時間間隔）指定 GlobalProtect 入口網站重新整理用戶端組態之前的等候小時數（範圍是 1-168；預設為 24）。
- （僅適用於 Windows）根據您的安全性需求，指定是否 **Retain Connection on Smart Card Removal**（在移除智慧卡時保持連線）。依預設，此選項設定為 **Yes**（是），意味著當使用者移除帶用戶端憑證的智慧卡時 GlobalProtect 保留通道。若要終止通道，設定此選項為 **No**（否）。

此功能需要內容發行版本 *590-3397* 或以上。

- 設定 **Automatic Restoration of VPN Connection Timeout**（**VPN** 連線逾時自動還原），以指定通道斷線時 GlobalProtect 要採取的動作。設定此選項為 **Yes**（是），以允許 GlobalProtect 在通道中斷連線後嘗試重新建立連線。設定此選項為 **No**（否），以防止 GlobalProtect 在通道中斷連線後嘗試重新連線。設定 **Wait Time Between VPN Connection Restore Attempts**（**VPN** 連線還原嘗試之間的等候時間），以調整 GlobalProtect 在嘗試還原連線之間的等候時間（單位為秒；範圍為 1 至 60 秒；預設為 5）。

  透過一直開啟連線方法，如果使用者在逾時值到期之前，從外部網路切換至內部網路，*GlobalProtect* 不會執行網路重新搜索。因此，*GlobalProtect* 會將連線還原至上一個已知的外部閘道。若要觸發內部主機偵測，使用者必須從 *GlobalProtect* 狀態面板上的設定功能表選取 *Refresh Connection*（重新整理連線）。

STEP 5 | 設定擁有此代理程式組態的使用者適用的功能表和 UI 檢視。

在應用程式組態區域，設定下列任意選項：

- 如果您希望使用者看到應用程式內的基本狀態資訊，請將 **Enable Advanced View**（啟用進階檢視）設定為 **No**（否）。啟用此選項後，使用者可以透過以下標籤檢視資訊：
  - **General**（一般）—使用與 GlobalProtect 帳戶關聯的使用者名稱和入口網站。
  - **Notification**（通知）—顯示任何 GlobalProtect 通知。

  預設值為 **Yes**（是）。啟用此選項後，使用者可以檢視以下其他頁籤：
  - **Connection**（連線）—列出為 GlobalProtect 應用程式設定的閘道及關於每個閘道的資訊。
  - **Host Profile**（主機設定檔）—顯示 GlobalProtect 用來透過 HIP 監控和執行安全性原則的端點資料。
  - **Troubleshooting**（疑難排解）—顯示關於網路組態、路由設定、活動連線及日誌的資訊。您還可收集由 GlobalProtect 產生的日誌並設定記錄層級。
- 如果您想要隱藏端點上的 GlobalProtect 系統匣圖示，請將 **Display GlobalProtect Icon**（顯示 **GlobalProtect** 圖示）設定為 **No**（否）。圖示隱藏後，使用者無法執行某些工作，例如變更儲存的密碼、重新搜索網路、重新提交主機資訊、檢視疑難排解資訊，或啟動視需要連線然而，必要時，會顯示 HIP 通知訊息、登入提示及憑證對話方塊。
- 若要防止使用者執行網路搜索，請設定 **Enable Rediscover Network Option**（啟用「重新發現網路」選項）為 **No**（否）。停用此選項時，**Refresh Connection**（重新整理連線）選項會在 GlobalProtect 狀態面板的設定功能表中變成灰色。
- 若要防止使用者手動將 HIP 資料重新提交至閘道，請將 **Enable Resubmit Host Profile Option**（啟用「重新提交主機設定檔」選項）設定為 **No**（否）。此選項預設為啟用，而且在 HIP 式安全原則防止使用者存取資源時很有用，因為它可讓使用者修正電腦中的相容性問題，然後再重新提交 HIP 資料。
- （僅適用於 Windows）若要允許 GlobalProtect 顯示系統匣中的通知，設定 **Show System Tray Notifications**（顯示系統匣通知）為 **Yes**（是）。
- 當使用者密碼即將過期時，若要建立自訂訊息以向使用者顯示，請輸入 **Custom Password Expiration Message (LDAP Authentication Only)**（客戶密碼到期資訊（僅限 **LDAP** 身份驗證））。最大訊息長度為 200 個字元。
- 若要建立自訂訊息以在使用者改變其 Active Directory（AD）密碼時指定密碼原則或需求，請輸入 **Change Password Message**（變更密碼訊息）。最大訊息長度為 255 個字元。

STEP 6 | 定義使用此組態的一般使用者可以從應用程式中執行的操作。

- 設定 **Allow User to Change Portal Address**（允許使用者變更入口網站位址）為 **No**（否），以停用 GlobalProtect 應用程式狀態面板上的 **Portal**（入口網站）欄位。由於使用者將無法指定連線的入口網站，您必須在 Windows 登錄中提供預設入口網站位址（`HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup`

含機碼 `Portal`）或 macOS plist（字典 `PanSetup` 下的 `/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist` 含機碼 `Portal`）。如需詳細資訊，請參閱明顯部署應用程式設定。

- 若要防止使用者關閉歡迎頁面，設定 **Allow User to Dismiss Welcome Page**（允許使用者屏除歡迎頁面）至 **No**（否）。當此選項設定為 **Yes**（是）時，使用者可關閉歡迎頁面並防止 GlobalProtect 在後續登入後顯示該頁面。

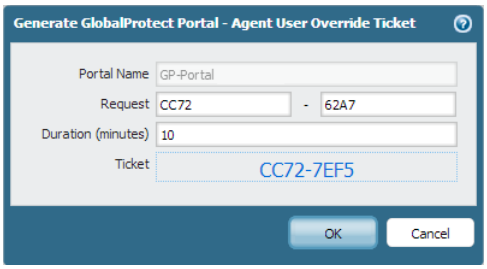
STEP 7 | 指定使用者是否可以停用 GlobalProtect 應用程式。

Allow User to Disable GlobalProtect（允許使用者停用 **GlobalProtect**）選項適用於 **Connect Method**（連線方法）為 **User-Logon (Always On)**（使用者登入（一直開啟））的代理程式組態。在使用者登入模式下，應用程式會在使用者登入端點後立即自動連線。此模式有時稱為「一直開啟」，這也就是使用者為何必須取代此行為以停用 GlobalProtect 應用程式。

依預設，此選項會設定為 **Allow**（允許），以允許使用者停用 GlobalProtect 而無需提供註解、密碼或票証號碼。

如果 *GlobalProtect* 系統匣圖示不可見，使用者將無法停用 *GlobalProtect* 應用程式。如需詳細資訊，請參閱步驟 5。

- 若要透過使用者登入連線方法防止使用者停用 GlobalProtect，請將 **Allow User to Disable GlobalProtect App**（允許使用者停用 **GlobalProtect** 應用程式）設為 **Disallow**（不允許）。
- 若要允許使用者僅在提供密碼時停用 GlobalProtect，請將 **Allow User to Disable GlobalProtect App**（允許使用者停用 **GlobalProtect** 應用程式）設為 **Allow with Passcode**（允許且須提供密碼）。然後，在停用 GlobalProtect 應用程式區域，輸入（並確認）一般使用者必須提供的 **Passcode**（密碼）。
- 若要允許使用者僅在提供票證時停用 GlobalProtect，設定 **Allow User to Disable GlobalProtect**（允許使用者停用 **GlobalProtect**）為 **Allow with Ticket**（允許且須提供票證）。使用此選項時，停用動作將觸發應用程式產生要求編號，一般使用者必須向管理者提供此編碼。接下來，管理者要按一下 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）頁面的 **Generate Ticket**（產生票證），並輸入來自使用者的要求編號來產生票證。管理者會將票證提供給一般使用者，該使用者再將其輸入到 [停用 GlobalProtect] 對話方塊中以停用應用程式。



- 若要限制使用者可以停用 GlobalProtect 應用程式的次數，請在停用 GlobalProtect 應用程式區域指定 **Max Times User Can Disable**（使用者可停用最大次數）值。數值 0（預設）表示未限制使用者停用應用程式的次數。

此設定僅適用於 *Allow*（允許）、*Allow with Comment*（允許且提供註解）和 *Allow with Passcode*（允許且提供密碼）停用選項。

如果您的使用者達到了 GlobalProtect 應用程式的最大停用次數，且之後必須繼續能夠停用此應用程式：

- 您可以在 GlobalProtect 入口網站代理程式組態中增加 **Max Times User Can Disable**（使用者可停用最大次數）值（**Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **Agent**（代理程式）> *<agent-config>* > **App**（應用程式））。使用者必須從 GlobalProtect 狀態面

板的設定功能表選取 **Refresh Connection**（重新整理連線）或建立新的 GlobalProtect 連線才能使新值生效。
  - 使用者可以透過重新安裝應用程式來重設計數器。
- 若要限制應用程式可以停用的次數，請在停用 GlobalProtect 應用程式區域輸入 **Disable Timeout (min)**（停用逾時（分鐘））值。值 0（預設值）表示對於使用者可以保持應用程式停用的時間長度沒有限制。

此設定僅適用於 *Allow*（允許）、*Allow with Comment*（允許且提供註解）和 *Allow with Passcode*（允許且提供密碼）停用選項。

STEP 8 | 指定使用者是否可以解除安裝 GlobalProtect 應用程式。

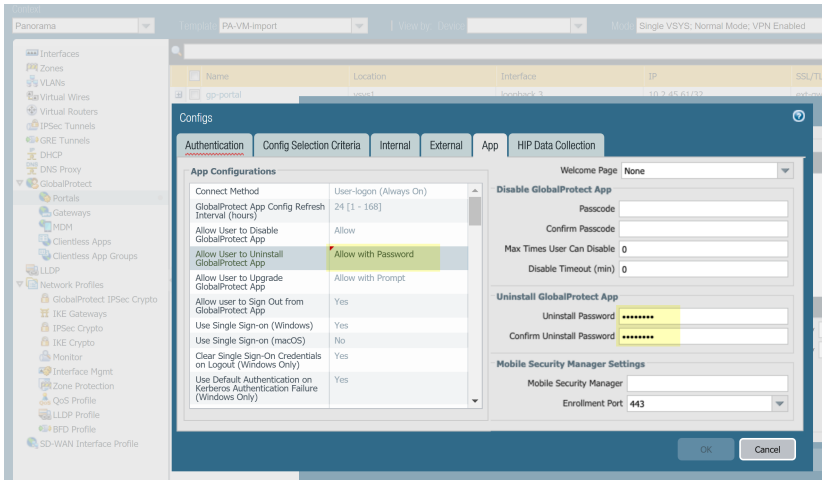
使用 **Allow User to Uninstall GlobalProtect App**（允許使用者解除安裝 **GlobalProtect** 應用程式）選項允許使用者解除安裝 GlobalProtect 應用程式、防止其解除安裝 GlobalProtect 應用程式，或允許其在指定您建立的密碼時解除安裝。

當此設定第一次連線至入口網站時，將被推送至端點裝置登錄，並儲存用於其連線的每個入口網站。

此選項需要內容發行版本 *8207-5750* 或以上。

- 若要允許使用者不受限制地解除安裝 GlobalProtect 應用程式，請選取 **Allow**（允許）。
- 若要防止使用者解除安裝 GlobalProtect 應用程式，請選取 **Disallow**（不允許）。

  在 Windows 登錄中將其設為 **Disallow**（不允許）後，該入口網站的值將在 `Computer\\HKEY_LOCAL_MACHINE\\SOFTWARE\\Palo Alto Networks\\GlobalProtect\\Settings\\ 'Uninstall = 1'` 下設為 1。
- 若要允許使用者透過密碼解除安裝 GlobalProtect 應用程式，請選取 **Allow with Password**（允許透過密碼）；然後，在解除安裝 GlobalProtect 應用程式區段，輸入解除安裝密碼並確認解除安裝密碼。



STEP 9 | 指定使用者是否可以登出 GlobalProtect 應用程式。

在應用程式組態區域，將 **Allow user to Sign Out from GlobalProtect App**（允許使用者登出 **GlobalProtect** 應用程式）設為 **No**（否），以防止使用者登出 GlobalProtect 應用程式，將 **Allow user to Sign Out from GlobalProtect App**（允許使用者登出 **GlobalProtect** 應用程式）設為 **Yes**（是）以允許使用者登出。

此選項需要內容發行版本*8196-5685* 或以上。

STEP 10 | 設定使用者接收此組態的憑證設定和行為。

在應用程式組態區域，設定下列任意選項：

- **Client Certificate Store Lookup**（用戶端憑證商店查找）—選取應用程式應從哪個商店查找用戶端憑證。**User**（使用者）憑證儲存在 Windows 的目前使用者憑證存放區以及 macOS 的個人金鑰鏈中。**Machine**（機器）憑證儲存在 Windows 的本機電腦憑證存放區以及 macOS 的系統金鑰鏈中。依預設，應用程式將在兩個位置查找 **User and machine**（使用者和機器）憑證。
- **SCEP Certificate Renewal Period (days)**（**SCEP** 憑證更新週期）—透過 SCEP，入口網站可以在憑證到期之前請求一個新的用戶端憑證。憑證到期之前的時間是可選的*SCEP* 憑證更新週期。指定憑證到期前的可設定天數內，入口網站可從企業 PKI 系統中的 SCEP 伺服器要求新憑證（範圍是 0-30；預設為 7）。值 0 表示入口網站在重新整理用戶端組態時，不會自動更新代理程式憑證。

  對於 GlobalProtect 應用程式要在更新週期獲得新憑證，使用者必須登入應用程式。例如，假設用戶端憑證的使用期限為 90 天，此憑證更新期為 7 天，且使用者在憑證的使用期限內最後 7 天登入，入口網站會擷取新憑證並將其與新的代理程式組態一起部署。如需更多資訊，請參閱部署驗證用使用者指定用戶端憑證。
- **Extended Key Usage OID for Client Certificate**（用戶端憑證擴展金鑰使用物件識別 **(OID)**）（僅限 Windows 和 macOS 終端）—僅限您啟用客戶端身份驗證時，才能使用此選項，預期終端上存在多個用戶端憑證，並已識別用於篩選用戶端證書的次要用途。此選項能讓您使用關聯物件識別 (OID) 為用戶端憑證指定次要用途。例如，若只要顯示也具有伺服器驗證用途的用戶端憑證，請輸入 OID 1.3.6.1.5.5.7.3.1。當 GlobalProtect 應用程式只找到一個與次要用途相符的用戶端憑證時，GlobalProtect 將使用該憑證自動選取並進行驗證。否則，GlobalProtect 會提示使用者從符合標準的用戶端憑證篩選清單中選取用戶端憑證。如需包含通用憑證用途 OID 的詳細資訊，請參閱 PAN-OS 7.1 新功能指南。
- 如果在入口網站憑證不可用時，您不想要應用程式建立與入口網站的連線，請設定 **Allow User to Continue with Invalid Portal Server Certificate**（允許使用者繼續使用無效入口網站伺服器憑證）為 **No**（否）。請牢記入口網站僅提供代理程式組態；其不提供網路存取。因此對入口網站的安全程度低於對閘道的安全。不過，如果您已為入口網站部署受信任伺服器憑證，停用此選項可協助防止中間人 (MITM) 攻擊。

STEP 11 | 指定多因素驗證收到存取敏感網路資源的要求時，使用者是否會收到登入提示。

對於內部閘道連線，可能需要額外驗證才能存取敏感網路資源（例如，財務應用程式或軟體開發應用程式）。您可以設定 GlobalProtect 以便進行多因素驗證通知以存取這些資源。

在應用程式組態區域，設定下列任意選項：

- 將 **Enable Inbound Authentication Prompts from MFA Gateways**（從 **MFA** 閘道啟用輸入驗證提示）設為 **Yes**（是）。若要支援多重要素驗證 (MFA)，GlobalProtect 應用程式必須收到從閘道傳來的 UDP 提示並進行確認。選取 **Yes**（是）可讓 GlobalProtect 應用程式收到提示並進行確認。依預設，此值設為 **No**（否），代表 GlobalProtect 會封鎖來自閘道的 UDP 提示。
- 指定 **Network Port for Inbound Authentication Prompts (UDP)**（輸入驗證提示的網路連接埠 **(UDP)**），以供 GlobalProtect 應用程式用於從 MFA 閘道接收輸入驗證提示。預設連接埠為 4501。若要變更連接埠，請指定 1 到 65535 的數字。
- 指定 GlobalProtect 應用程式可信任的 **Trusted MFA Gateways**（受信任 **MFA** 閘道），進行多因素驗證。當 GlobalProtect 應用程式在指定的網路連接埠上收到 UDP 訊息時，GlobalProtect 只會在 UDP 提示是來自受信任的閘道時顯示驗證訊息。
- 設定 **Inbound Authentication Message**（輸入驗證訊息）；例如，您已嘗試存取需要另外驗證的受保護資源。請繼續到以下網址進行驗證：。當使用者嘗試存取需要額外驗證的資源時，GlobalProtect 會收到並顯示輸入驗證訊息。GlobalProtect 會自動將您設定多因素驗證時指定的驗證入口網站頁面 URL，附加到傳入驗證訊息。

STEP 12 | （僅適用於 Windows）為接收此組態的 Windows 端點進行設定。

- **Resolve All FQDNs Using DNS Servers Assigned by the Tunnel (Windows Only)**（使用通道指派的 **DNS** 伺服器解析所有 **FQDN**（僅限 **Windows**））—設定 GlobalProtect 通道的 DNS 解析偏好。如果

未解析閘道上設定的 DNS 伺服器初始查詢，選取 **No**（否），以允許 Windows 端點將 DNS 查詢傳送至設定在實體介面卡上的 DNS 伺服器。此選項會保留原生 Windows 行為，以遞歸方式查詢所有介面卡上全部的 DNS 伺服器，但可能導致解析部分 DNS 查詢需要很長的等待時間。選取 **Yes**（是）（預設）以允許 Windows 端點透過您在閘道上設定的 NDS 伺服器來解析全部 DNS 查詢，而非允許 Windows 端點將部分 DNS 查詢傳送到設置在實體介面卡上的 DNS 伺服器。

此功能不支援透過 *TCP* 連線的 *DNS*。

此功能需要內容發行版本 *731* 或以上，且 *GlobalProtect* 應用程式版本為 *4.0.3* 和更新版本。

- **Send HIP Report Immediately if Windows Security Center (WSC) State Changes**（**Windows** 安全中心 **(WSC)** 狀態變更後立即發送 **HIP** 報告）—選取 **No**（否）可防止 GlobalProtect 應用程式在 Windows 安全中心 (WSC) 變更時傳送 HIP 資料。選取 **Yes**（是）（預設值）可在 WSC 狀態變更時立即傳送 HIP 資料。
- **Clear Single Sign-On Credentials on Logout**（登出時清空 **Single Sign-on**（單點登錄-**SSO**）認證）—選取 **No**（否）可在使用者登出時保留單一登入認證。選取 **Yes**（是）（預設值）可清除認證，並強制使用者在下次登入時輸入認證。
- **Use Default Authentication on Kerberos Authentication Failure**（當 **Kerberos** 驗證失敗時使用預設驗證）—選取 **No**（否）以僅適用 **Kerberos** 驗證。選取 **Yes**（是）（預設值）可在 Kerberos 驗證失敗後，使用預設驗證方法重試。

STEP 13 | （僅適用於 Window）設定適用於 Windows 端點的 GlobalProtect 應用程式以 **Detect Proxy for Each Connection**（偵測每個連線的 **Proxy**）。

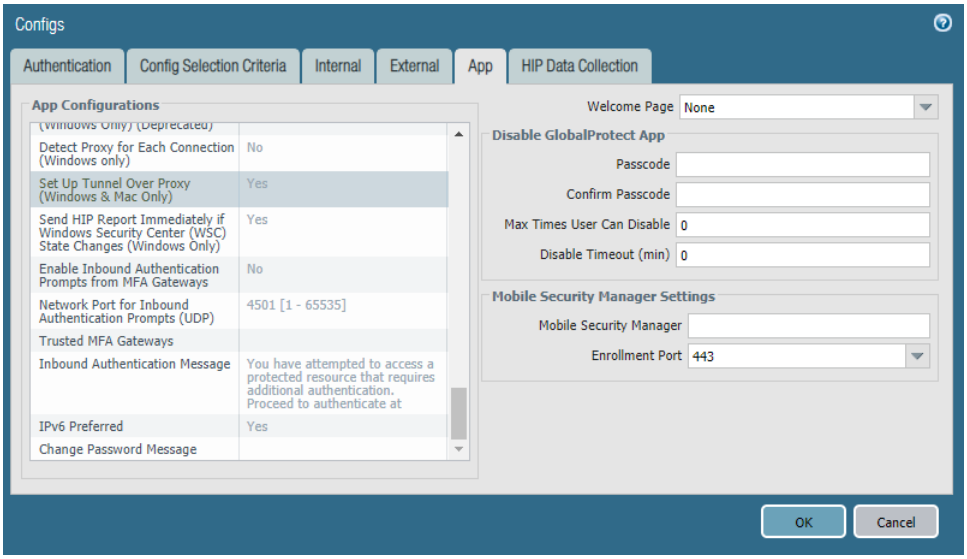
如需基於 *proxy* 使用之網路流量行為的詳細資訊，請參閱 Proxy 上的通道連線 。

- 選取 **No**（否）可自動偵測 proxy 連線入口網站，並使用該 proxy 進行後續連線。
- 選取 **Yes**（是）（預設值）可在每次連線時自動偵測 proxy。

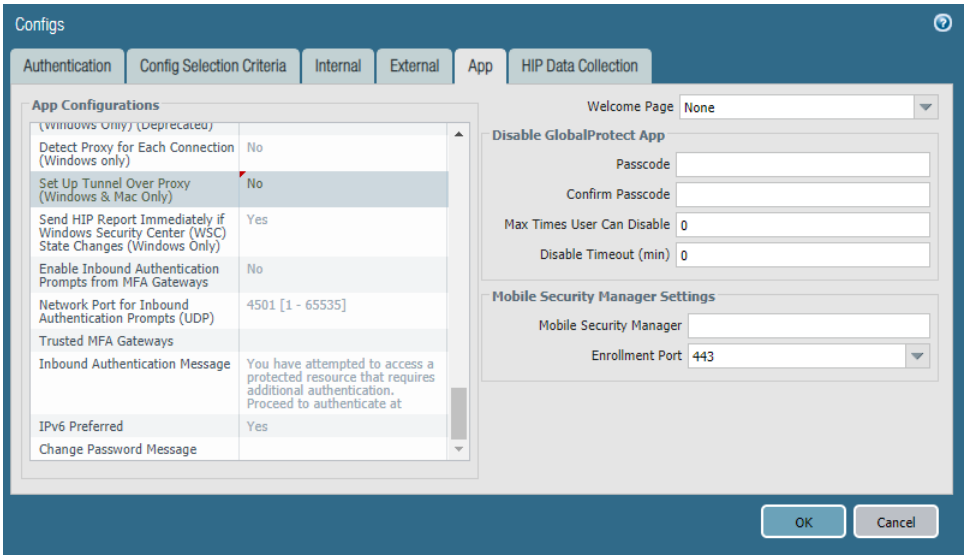
STEP 14 | （僅限 Windows 和 macOS）指定 GlobalProtect 是否必須使用或繞過代理。

透過此設定，您可基於 GlobalProtect 代理程式的使用設定網路流量行為。更多詳細資訊，請參閱 Proxy 上的通道連線 。

- 若要要求 GlobalProtect 使用 Proxy，請將 **Set Up Tunnel Over Proxy (Windows & Mac only)**（透過代理程式設定通道（僅限 **Windows** 和 **Mac**））選項設為 **Yes**（是）。



- 若要要求 GlobalProtect 繞過 Proxy，請將 **Set Up Tunnel Over Proxy (Windows & Mac only)**（透過代理程式設定通道（僅限 **Windows** 和 **Mac**））選項設為 **No**（否）。



STEP 15 | 如果連線至 GlobalProtect 入口網站或閘道時，您的端點頻繁遇到延遲或變慢，可考慮調整入口網站和 TCP 逾時值。

若要允許端點有更多時間連線至入口網站或閘道，或接收來自入口網站或閘道的資料，可根據需要增加逾時值。如果 GlobalProtect 應用程式無法建立連線，請牢記增加該值可導致更長的等待時間。相對地，當入口網站或閘道在逾時之前未回應，減少該值可以防止 GlobalProtect 應用程式建立連線。

在應用程式組態區域，設定下列任意逾時選項：

- **Portal Connection Timeout (sec)**（入口網站連線逾時（秒））—請求連線至入口網站因入口網站無任何回應而逾時前的秒數（從 1 到 600）。當您的防火牆執行的應用程式和威脅內容版本早於 777-4484 時，預值值為 30。以內容版本777-4484 開始，預設值為 5。
- **TCP Connection Timeout (sec)**（**TCP** 連線逾時（秒））—由於連線兩端均無回應使得 TCP 連線要求逾時之前的秒數（從 1 到 600）。當您的防火牆執行的應用程式和威脅內容版本早於 777-4484 時，預值值為 60。以內容版本777-4484 開始，預設值為 5。
- **TCP Receive Timeout (sec)**（**TCP** 接收逾時（秒））—由於缺少 TCP 要求的某些部分回應使得 TCP 連線要求逾時之前的秒數（範圍是 1-600；預設為 30）。

STEP 16 | 透過指定 **User Switch Tunnel Rename Timeout**（使用者切換通道重命名超時），指定是否允許在現有 VPN 通道上執行遠端桌面連線。當新使用者透過遠端桌面協議 (RDP) 連線至 Windows 機器時，閘道會重新指派 VPN 通道給新使用者。閘道可在新使用者上強制執行安全原則。

允許 VPN 通道上的遠端桌面連線，對於 IT 管理員需要透過遠端桌面通訊協議 (RDP) 存取遠端使用者系統的情況很有用。

依預設，**User Switch Tunnel Rename Timeout**（使用者切換通道重命名超時）值設定為 0 意味著 GlobalProtect 閘道在有新使用者於 VPN 通道上驗證時，終止該連線。若要修改此行為，設定 1 至 600 秒的逾時值。如果新使用者未在超時值結束之前登入閘道，GlobalProtect 閘道將終止指派到第一個使用者的 VPN 通道。

變更 *User Switch Tunnel Rename Timeout*（使用者切換通道重命名超時）值僅影響 *RDP* 通道，且在設定時不會重命名預登入通道。

STEP 17 | 若要讓 GlobalProtect 在使用者登出端點後保留現有的 VPN 通道，請指定 **Preserve Tunnel on User Logoff Timeout**（使用者登出後保留通道逾時）值（範圍為 0 至 600 秒；預設值為 0 秒）。若您接受預設值 0，則 GlobalProtect 在使用者登出後不會保留通道。

此選項需要 *2019* 年 *7* 月 *8* 日或以後發行的內容發行版本。

當您設定 GlobalProtect 以保留 VPN 通道時，考慮以下 GlobalProtect 連線行為：

- 如果同一使用者登出後在指定的逾時時間內重新登入，無論是在總是開啟還是視需模式下，GlobalProtect 都會保持連線，且無需任何使用者互動（包括入口網站與閘道驗證）。如果使用者未在指定的逾時時間內重新登入，通道將中斷連線，且使用者必須重新建立 GlobalProtect 連線。
- 如果使用者登出端點，然後另一使用者在總是開啟或視需模式下登入至同一端點，則只有當新使用者在指定的逾時時間內透過 GlobalProtect 成功進行身份驗證後，才會為新使用者重新命名現有通道。如果新使用者未在指定的逾時時間內登入且成功進行身份驗證，現有通道會中斷連線且必須建立新的 GlobalProtect 連線。如果新使用者處於總是開啟模式，GlobalProtect 會嘗試自動建立新連線。如果新使用者處於視需模式，其必須手動建立新的 GlobalProtect 連線。

STEP 18 | 指定 GlobalProtect 應用程式升級的方式。

如果您想要控制使用者在何時能升級，您可以基於組態來自訂應用程式升級。舉例來說，如果您想在將版本部署至整個使用者群之前，先以一小群使用者測試，您可以建立組態，且該組態只套用到 IT 群組，如此能讓該群組的使用者升級並測試，而所有其他使用者/群組的組態則關閉升級。在您完全測試完新版本之後，可以針對剩餘使用者修改代理程式設定以允許升級。

依預設，**Allow User to Upgrade GlobalProtect App**（允許使用者升級 **GlobalProtect** 應用程式）選項設定為 **Allow with Prompt**（允許且提供提示），這表示當防火牆上啟動了新版本的應用程式時，會提示一般使用者升級。若要修改此行為，請選取下列其中一個選項：

- **Allow Transparently**（明顯允許）—無需與使用者互動就會自動升級。在使用者遠端工作或從公司網路內連線時都可以升級。
- **Internal**（內部）—假設使用者是從公司網路內連線，則不與使用者互動就會自動升級。建議採用此設定，以避免在低頻寬情況下升級速度緩慢。使用者從公司網路外部連線時系統會延遲更新，直到使用者從公司網路內連線後才會重新啟動。您必須設定內部閘道和內部主機偵測，才能使用此選項。
- **Disallow**（不允許）—此選項防止應用程式升級。
- **Allow Manually**（手動允許）—一般使用者啟動應用程式升級。在此情況下，使用者必須從 GlobalProtect 狀態面板的設定功能表中選取 **Check Version**（檢查版本），來確定是否存在新應用程式版本，然後再根據需要升級。請注意，如果 GlobalProtect 應用程式對使用者為隱藏，此選項將無法使用。如需關於 **Display GlobalProtect Icon**（顯示 **GlobalProtect** 圖示）設定的詳細資訊，請參閱步驟 5。

對於 *Allow Transparently*（明顯允許）和 *Internal*（內部）的升級，在入口網站上的 *GlobalProtect* 軟體版本比端點上的 *GlobalProtect* 軟體版本更新時才會升級。例如，連線到 *GlobalProtect 3.1.1* 入口網站的 *GlobalProtect 3.1.3* 代理程式將不會升級。

STEP 19 | 新增 **Change Password Message**（變更密碼訊息），指定使用者在變更密碼時必須遵循的密碼原則或需求（例如，密碼必須包含至少一個數字與一個大寫字母）。

STEP 20 | 指定成功登入後是否顯示歡迎頁面。

歡迎頁面是一種實用的方式，可引導使用者前往他們只能在連線至 GlobalProtect 時存取的內部資源，例如貴企業的內部網路或其他內部伺服器。

依預設，應用程式成功連線的唯一指示是顯示在系統匣/功能表列中的球形文字說明訊息。

若要在成功登入後顯示歡迎頁面，請從 **Welcome Page**（歡迎頁面）下拉式清單中選取 **factory-default**（原廠預設值）。GlobalProtect 會在 GlobalProtect 應用程式中顯示歡迎頁面。您也可以選取一個自訂歡迎頁面來提供使用者特定資訊，或特定使用者群組的特定資訊（根據所部署的入口網站設定）。如需建立自訂頁面的詳細資訊，請參閱自訂 GlobalProtect 入口網站登入、歡迎與說明頁面。

STEP 21 | （僅限 Windows）指定是否要 GlobalProtect 應用程式 **Display Status Panel at Startup**（在啟動時顯示狀態面板）。

- 若要在使用者首次建立 GlobalProtect 連線時隱藏狀態面板，請選取 **No**（否）。
- 若要在使用者首次建立 GlobalProtect 連線時自動顯示狀態面板，請選取 **Yes**（是）。使用此選項時，使用者必須按一下狀態面板以外的部分才能手動將其關閉。

STEP 22 | 儲存代理程式組態。

1. 如果您已完成自訂代理程式組態，請按一下 **OK**（確定）以儲存代理程式組態。否則，請返回定義 GlobalProtect 代理程式組態以完成代理程式組態自訂。
2. 按一下**OK**（確定）儲存入口網站組態。
3. **Commit**（提交）變更。

自訂 GlobalProtect 入口網站登入、歡迎與說明頁面

GlobalProtect 提供預設登入、歡迎與/或說明頁面。不過，您也可以建立自己的自訂頁面，使其包含企業品牌、可接受的使用原則，以及內部資源的連結。

您也可以停用瀏覽器對入口網站登入頁面的存取權限，以防止對 *GlobalProtect* 入口網站嘗試進行未授權驗證（請從 *Network*（網路）> *GlobalProtect* > *Portals*（入口網站）> *<portal_config* > *General*（一般）設定 *Portal Login Page*（入口網站登入頁面）> *Disable*（停用）選項）。當入口網站登入頁面已停用時，您可以改用軟體散佈工具，如 *Microsoft* 的 *System Center Configuration Manager (SCCM)*，以允許您的使用者下載並安裝 *GlobalProtect* 應用程式。

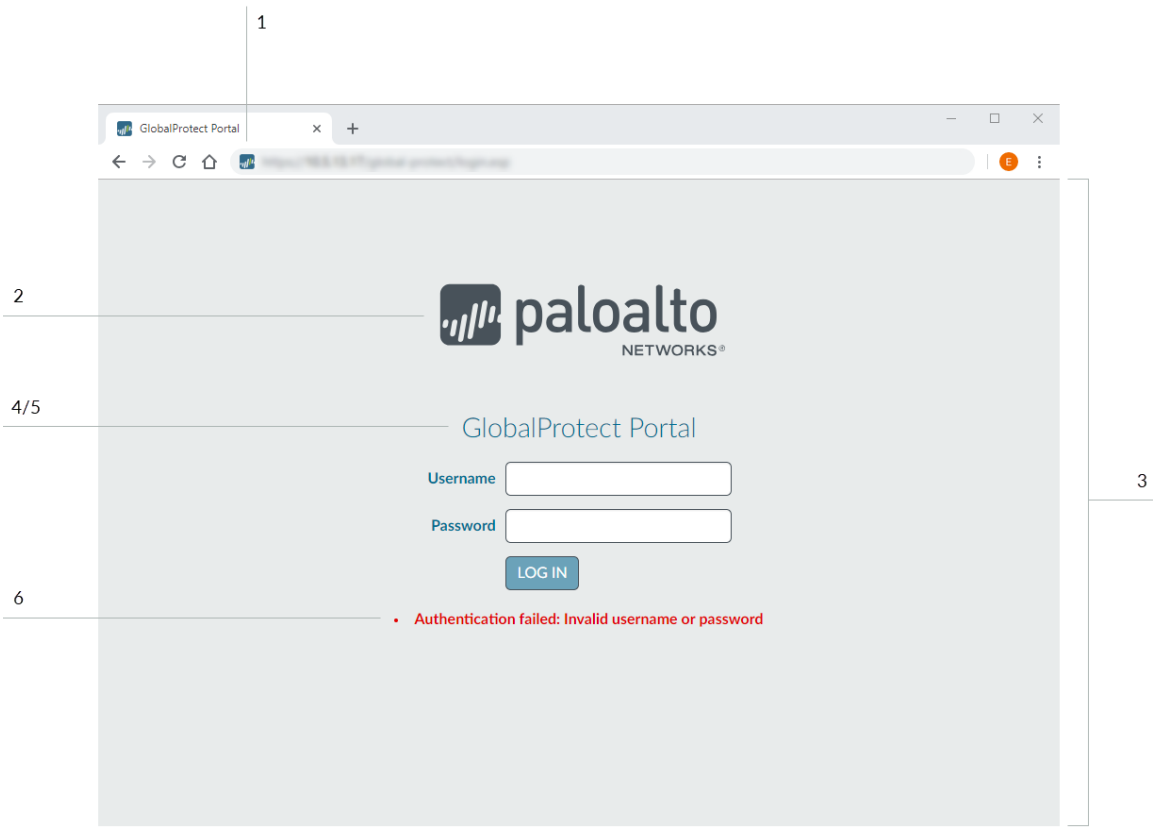
STEP 1 | 匯出預設入口網站登入、歡迎、幫助頁面或首頁。

1. 選取 **Device**（裝置）> **Response Pages**（回應頁面）。
2. 選取對應 GlobalProtect 入口網站頁面的連結，例如 **GlobalProtect Portal Login Page**（**GlobalProtect** 入口網站登入頁面）。
3. 選取 **Default**（預設）的預先定義頁面，然後按一下 **Export**（匯出）。

STEP 2 | 編輯匯出的頁面。

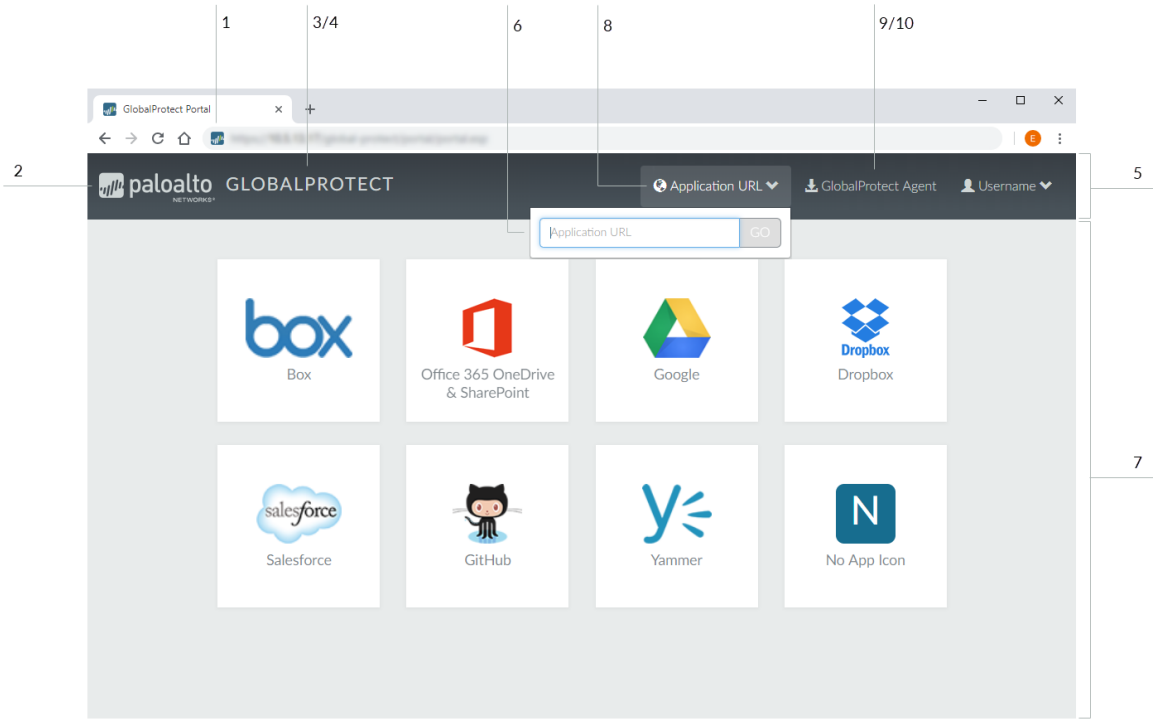
1. 使用您所選取的 HTML 文字編輯器來開啟並編輯頁面。
2. 若要編輯登入頁面或首頁，請設定下列任何變數：

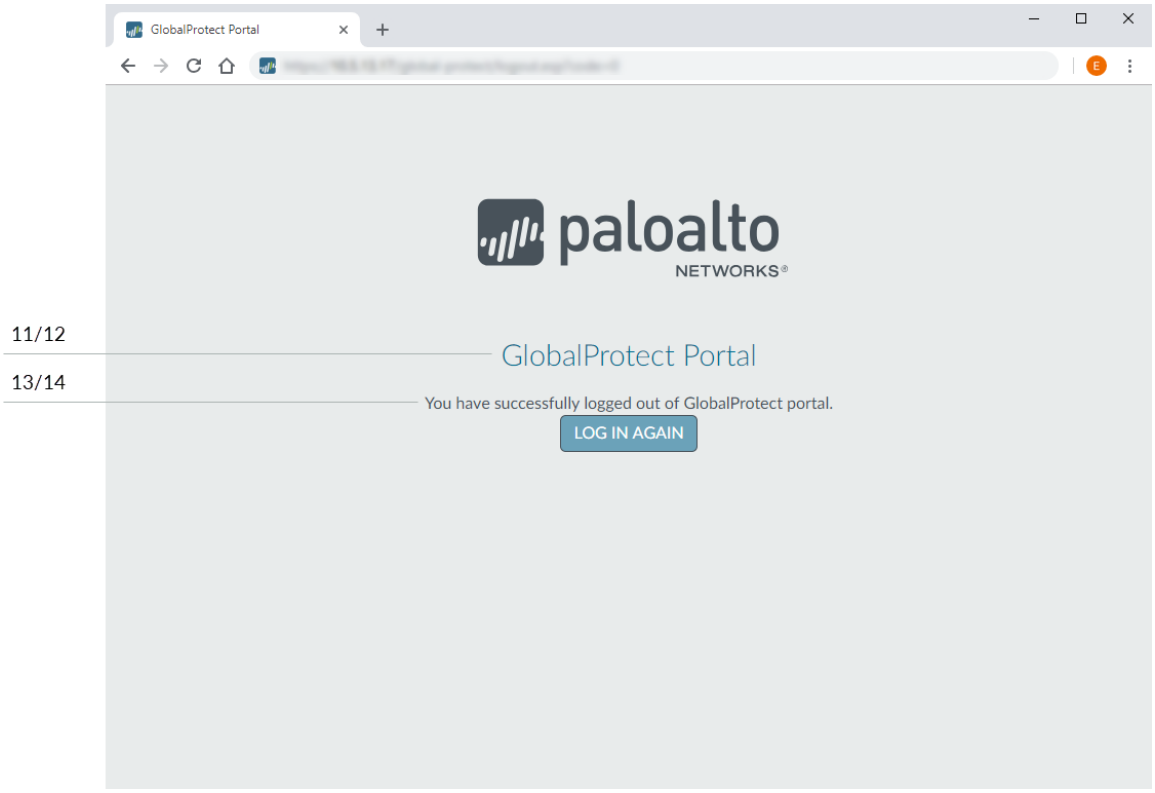
- **GlobalProtect Portal Login Page**（**GlobalProtect** 入口網站登入頁面）：



標籤編號	變數	說明	範例
1	favicon	Web 瀏覽器位址列中所顯示圖示之 URL。	`var favicon = 'http:// cdn.slidesharecdn. com/logo-24x24. jpg? 3975762018';`
2	logo	公司標誌之 URL。	`var logo = 'http:// cdn.slidesharecdn. com/logo-96x96. jpg? 1382722588';`
3	bg_color	登入頁面背景顏色。	`var bg_color = '#D3D3D3';`
4	gp_portal_name	公司標誌下方顯示的文字。	`var gp_portal_name = 'GlobalProtect 入口網站';`
5	gp_portal_name_color	公司標誌下方顯示的文字顏色。	`var gp_portal_name_ color = '#000000';`
6	error_text_color	登入失敗訊息的文字顏色。	`var error_text_ color = '#196390';`

- **GlobalProtect Portal Home Page**（**GlobalProtect** 入口網站首頁）：





標籤編號	變數	說明	範例
1	`favicon`	Web 瀏覽器位址列中所顯示圖示之 URL。	`var favicon = 'http://cdn.slidesharecdn.`

標籤編號	變數	說明	範例
			com/logo-24x24. jpg? 3975762018';
2	logo	公司標誌之 URL。	var logo = 'http:// cdn.slidesharecdn. com/logo-96x96. jpg? 1382722588';
3	navbar_text	導覽列文字。	var navbar_text = 'GlobalProtect';
4	navbar_text_color	導覽列文字顏色。	var navbar_text_ color = '#D3D3D3';
5	navbar_text_color	導覽列背景顏色。	var navbar_bg_color = '#A9A9A9';
6	dropdown_bg_color	下拉式功能表背景顏色。	var dropdown_bg_ color = '#FFFFFF';
7	bg_color	首頁背景顏色。	var bg_color = '#D3D3D3';
8	label_custom_app_url	自訂/內部應用程式 URL 標籤。	var label_custom_ app_url = '應用程式 URL';
9	display_ globalprotect_agent	顯示或隱藏 GlobalProtect 應用程式下載按鈕的選項。輸入 1 以顯示下載按鈕。輸入 0 以隱藏下載按鈕。	var display_ globalprotect_agent = 1;
10	label_globalprotect_ agent	GlobalProtect 應用程式下載按鈕標籤。	var label_ globalprotect_agent = 'GlobalProtect 代理程式';

標籤編號	變數	說明	範例
11	gp_portal_name	入口網站登出頁面上公司標誌下方顯示的文字。	var gp_portal_name = 'GlobalProtect 入口網站';
12	gp_portal_name_color	入口網站登出頁面上公司標誌下方顯示的文字顏色。	var gp_portal_name_ color = '#000000';
13	logout_text_array	使用者登出入口網站後，入口網站登出頁面上顯示的訊息。 您僅可修改現有訊息，無法新增訊息或刪除任何現有訊息。	var logout_text_ array = ["您已成功登出 GlobalProtect 入口網站", "GlobalProtect 閘道未經授權。請聯絡系統管理員。", "使用者未經過 GlobalProtect 入口網站的身份驗證。", "系統錯誤，請聯絡系統管理員。", "系統錯誤，無法刪除使用者工作階段。請聯絡系統管理員。", "無法建立使用者工作階段。已達最大容量。請聯絡系統管理員。"];
14	logout_text_color	使用者登出入口網站後，入口網站登出頁面上顯示的訊息文字顏色。	var logout_text_ color = '#000000';

3. 以新檔案名稱儲存編輯的頁面。請確保該頁面保留其 UTF-8 編碼。

STEP 3 | 匯入新的回應頁面。

1. 選取 **Device**（裝置）> **Response Pages**（回應頁面）。
2. 選取對應 GlobalProtect 入口網站頁面的連結。
3. **Import**（匯入）新入口網站頁面。在 **Import File**（匯入檔案）欄位中輸入路徑與檔案名稱，或 **Browse**（瀏覽）以尋找並選取檔案。
4. （選用）從 **Destination**（目的地）下拉式清單中選取將要使用此登入頁面的虛擬系統，或選取 **shared**（共用）（預設）以使其可用於所有虛擬系統。
5. 按一下 **OK**（確定）匯入檔案。

STEP 4 | 設定入口網站以使用新頁面。

- **Portal Login Page**（入口網站登入頁面）、**Portal Landing Page**（入口網站登陸頁面）和 **App Help Page**（應用程式說明頁面）：
  1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）。
  2. 選取您要新增登入、登陸（首頁）或應用程式說明頁面至的入口網站。
  3. 在 **General**（一般）頁籤的外觀區域，從對應下拉式清單中選取新頁面。
- **Custom Welcome Page**（自訂歡迎頁面）：
  1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）。

2. 選取您要新增歡迎頁面至的入口網站。
3. 在 **Agent**（代理程式）頁籤中，選取您要新增歡迎頁面的代理程式組態。
4. 在 **App**（應用程式）頁籤上，從 **Welcome Page**（歡迎頁面）下拉式清單選取新頁面。
5. 按一下 **OK**（確定）儲存代理程式組態。

STEP 5 | 儲存入口網站組態。

按一下**OK**（確定）儲存入口網站組態，然後**Commit**（提交）變更。

STEP 6 | 確定顯示新頁面。

- 測試登入頁面—打開 Web 瀏覽器，前往入口網站的 URL（切勿將 :4443 連接埠號碼新增至 URL 的結尾，否則會將您導向至防火牆的 Web 介面）。例如，請輸入 **`https://myportal`** 而不是 **`https://myportal:4443`**。新入口網站登入頁面將會顯示。
- 測試首頁—打開 Web 瀏覽器，前往入口網站的 URL（切勿將 :4443 連接埠號碼新增至 URL 的結尾，否則會將您導向至防火牆的 Web 介面）。例如，請輸入 **`https://myportal`** 而不是 **`https://myportal:4443`**。輸入 **Username**（用戶名稱）與 **Password**（密碼），然後 **LOG IN**（登入）至入口網站。新入口網站首頁將會顯示。
- 測試說明頁面—按一下 GlobalProtect 系統匣圖示以啟動 GlobalProtect 應用程式。當狀態面板開啟時，按一下設定圖示 () 以開啟設定功能表。選取 **Help**（說明）以檢視新的說明頁面。
- 測試歡迎頁面—按一下 GlobalProtect 系統匣圖示以啟動 GlobalProtect 應用程式。當狀態面板開啟時，按一下設定圖示 () 以開啟設定功能表。選取 **Welcome Page**（歡迎頁面）以檢視新的歡迎頁面。

GlobalProtect 應用程式

- 下載 GlobalProtect 應用程式
- 部署 GlobalProtect 應用程式軟體
- 定義 GlobalProtect 代理程式組態
- 自訂 GlobalProtect 應用程式
- 明顯部署代理程式設定

向一般使用者部署 GlobalProtect 應用程式

為了連線至 GlobalProtect™，端點必須執行 GlobalProtect 應用程式。軟體部署方法取決於端點類型，如下所述：

平台	部署架構選項
macOS 和 Windows 端點	您可以透過下列幾種方法在 macOS 和 Windows 端點上散佈並安裝軟體： • 直接從入口網站—將應用程式軟體下載至裝載入口網站的防火牆，並予以啟動，以使一般使用者在連線至入口網站時能夠安裝更新。此方法具有一定的靈活性，因為它可讓您根據您針對每個使用者、群組及/或作業系統定義的用戶端組態控制一般使用者如何以及何時接收更新。不過，如果您擁有大量需要更新的應用程式，可能會使您的入口網站超載。如需說明，請參閱在入口網站裝載應用程式更新。 • 從 **Web** 伺服器—如果您有許多端點需要同時升級應用程式，請考慮在 Web 伺服器裝載應用程式更新，以降低防火牆的負載。如需說明，請參閱在網頁伺服器裝載應用程式更新。 • 從命令行明顯部署—對於 Windows 端點，您可以使用 Windows 安裝程式 (Msiexec) 自動部署應用程式設定。不過，若要使用 Msiexec 升級至更新的應用程式版本，您必須先解除安裝現有應用程式。此外，Msiexec 還可讓您透過在 Windows 登錄中設定值來直接在端點部署應用程式設定。同樣地，您也可以透過在 macOS plist 中進行設定來部署應用程式設定至 macOS 端點。請參見明顯部署應用程式設定。 • 使用群組原則規則—在 Active Directory 環境中，也可以使用 Active Directory 群組原則將 GlobalProtect 應用程式散佈至一般使用者。AD 群組原則可讓您自動修改 Windows 端點設定及軟體。如需如何使用群組原則自動將程式散佈至端點或使用者的詳細資訊，請參閱 http://support.microsoft.com/kb/816102 的文章。 • 來自行動端點管理系統—如果您使用行動管理系統，如 MDM 或 EMM 以管理您的行動端點，您可以使用此系統部署和設定 GlobalProtect 應用程式。請參見行動端點管理。
Windows 10 手機和 Windows 10 UWP	• 來自行動端點管理系統—如果您使用行動管理系統，如 MDM 或 EMM（支援 Windows 10 端點），您可以使用此系統部署和設定 GlobalProtect 應用程式。請參見行動端點管理。 • 來自 **Microft Store**—一般使用者也可以直接從 Microsoft Store 下載並安裝 GlobalProtect 應用程式。如需怎樣下載與測試 GlobalProtect 應用程式安裝的指示，請參閱下載與安裝 GlobalProtect 行動應用程式。
iOS 和 Android 端點	• 來自行動端點管理系統—如果您使用行動管理系統，如 MDM 或 EMM，您可以使用此系統部署和設定 GlobalProtect 應用程式。請參見行動端點管理。 • 來自應用程式商店—一般使用者也可以直接從 Apple App Store（iOS 端點）或 Google Play（Android 端點）下載並安裝 GlobalProtect 應用程式。如需怎樣下載與測試 GlobalProtect 應用程式安裝的指示，請參閱下載與安裝 GlobalProtect 行動應用程式。
Chromebook	• 從 **Google** 管理控制台—Google 管理控制台讓您可以從中心的 web 式位置管理 Chromebook 設定和應用程式。若要透過 Google 管理控制台在受管理的 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式，請參閱透過 Google 管理控制台在受管理的 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式。

平台	部署架構選項
	僅 特定 Chromebook 支援適用於 *Android* 的 *GlobalProtect* 應用程式。不支援 *Android* 應用程式的 *Chromebooks* 必須繼續執行適用于 *Chrome* 的 *GlobalProtect* 應用程式，其不支援 *GlobalProtect* 應用程式 *5.0* 及更新版本。 • 從 **AirWatch**—您可在已向 AirWatch 註冊的受管理 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式。在部署應用程式後，設定並部署 VPN 設定檔以自動為一般使用者設定 GlobalProtect 應用程式。若要透過 AirWatch 在受管理的 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式，請參閱 透過 AirWatch 在受管理的 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式。
Linux	從支援網站下載適用於 Linux 的 GlobalProtect 應用程式後，您可透過下列方式散佈並安裝此應用程式： • 使用 **Linux** 應用程式散佈工具—Linux 應用程式散佈通常使用協力廠商工具（如 Chef 和 Puppet）進行管理，對於 Linux 作業系統，則使用本機儲存庫（例如，Ubuntu 儲存庫和 RHEL 儲存庫）。如需詳細資訊，請參閱 Linux 作業系統的文件。 • 手動安裝—如果您讓軟體可供一般使用者使用，其可使用 Linux 工具手動安裝軟體，例如 **apt** 或 **dpkg**。如需怎樣安裝適用於 Linux 的 GlobalProtect 應用程式的指示，請參閱 GlobalProtect 應用程式使用者指南。

部署 *GlobalProtect* 應用程式軟體的另一個方法，是可以將 *GlobalProtect* 入口網站設定為對一般企業 *Web* 應用程式（採用 *HTML*、*HTML5* 和 *Javascript* 技術）提供安全的遠端存取。使用者可從具有 *SSL* 功能的 *Web* 瀏覽器獲得安全存取的好處，而不必安裝 *GlobalProtect* 應用程式軟體。請參閱 GlobalProtect 無用戶端 VPN。

下載 GlobalProtect 應用程式

如果您是一般使用者，請聯絡 *IT* 管理員以取得支援的最新 *GlobalProtect* 軟體。

在為一般使用者部署 GlobalProtect 應用程式之前，您必須先將新應用程式安裝套件下載至裝載您入口網站的防火牆，然後再啟動軟體以下載到連線至入口網站的應用程式。此部署方法適用於所有非行動應用程式版本。若要下載行動版本的 GlobalProtect 應用程式，請查看行動裝置的應用程式商店（如需詳細資訊，請參閱 下載及安裝 GlobalProtect 行動應用程式）。

若要直接下載最新應用程式至防火牆，防火牆必須具有服務路由，以使它能夠存取 Palo Alto Networks 更新伺服器（請參閱 向一般使用者部署 GlobalProtect 應用程式）。如果防火牆無權存取網際網路，您可以使用連線至網際網路的電腦，從 Palo Alto Networks 軟體更新支援網站下載應用程式軟體套件，然後再將其手動上載至防火牆。

若要手動下載應用程式軟體套件：

STEP 1 | 登入 Palo Alto Networks 客戶支援入口網站 (https://support.paloaltonetworks.com/)。

您必須擁有有效的 *Palo Alto Networks* 帳戶以登入，並從軟體更新頁面下載軟體。如果您無法登入且需要協助，前往https://www.paloaltonetworks.com/support/tabs/overview.html。

STEP 2 | 選取 **Updates**（更新）> **Software Updates**（軟體更新）。

STEP 3 | 選取不同作業系統的 GlobalProtect 應用程式版本。

STEP 4 | 檢閱應用程式版本的版本資訊，然後選取下載連結以繼續下載。

STEP 5 | 向一般使用者部署 GlobalProtect 應用程式.

請參閱 Palo Alto Networks 相容性矩陣，了解您可安裝各 GlobalProtect 應用程式版本的作業系統。

在入口網站代管應用程式更新

部署 GlobalProtect 應用程式軟體最簡單的方法是將新應用程式安裝套件下載至裝載您入口網站的防火牆，然後再啟動軟體以下載到連線至入口網站的應用程式。若要自動執行此操作，防火牆必須具有服務路由，以使它能夠存取 Palo Alto Networks 更新伺服器。如果防火牆無權存取網際網路，您可以使用連線至網際網路的電腦，從 Palo Alto Networks 軟體更新支援網站 下載 GlobalProtect 應用程式 軟體套件，然後再將其手動上載至防火牆。

您可以定義應用程式軟體更新在入口網站代理程式組態中的部署方式—在應用程式連線至入口網站時自動進行更新、在系統提示使用者升級應用程式，還是一般使用者可以手動檢查並下載新應用程式版本。如需建立代理程式組態的詳細資訊，請參閱 定義 GlobalProtect 代理程式組態。

STEP 1 | 在裝載 GlobalProtect 入口網站的防火牆上，檢查新的應用程式軟體映像。

選取 **Device**（裝置）> **GlobalProtect Client**（**GlobalProtect** 用戶端）以檢視可用的應用程式軟體映像清單。

- 如果防火牆有權存取更新伺服器，請按一下 **Check Now**（立即檢查）來檢查最新更新。如果在 **Action**（動作）欄中的值為 **Download**（下載），則表示有新版本的此應用程式可用。
- 如果防火牆無權存取更新伺服器，您必須從 Palo Alto Networks 軟體更新支援網站手動下載軟體映像，如步驟 2 所述。

STEP 2 | 下載應用程式軟體影像檔。

- 如果防火牆有權存取更新伺服器，請找到您需要的應用程式版本，然後按一下 **Download**（下載）。完成下載後，**Action**（動作）欄中的值會變更為 **Activate**（啟動）。
- 如果防火牆無權存取更新伺服器，下載 GlobalProtect 應用程式。下載此軟體映像後，返回防火牆的 **Device**（裝置）> **GlobalProtect Client**（**GlobalProtect** 用戶端）頁面以 **Upload**（上載）。

STEP 3 | 啟動應用程式軟體影像檔，以使一般使用者能夠從入口網站下載。

一次只能啟動應用程式軟體影像檔的一個版本。如果您啟動新版本，但卻有一些應用程式需要之前啟動的版本，您必須再次啟動所需版本才能使其可供下載。

- 如果您已從更新伺服器自動下載映像，請按一下 **Activate**（啟動）。
- 如果您已手動將軟體映像上傳到防火牆，請按一下 **Activate From File**（從檔案啟動），然後從下拉式清單中選取您上傳的 **GlobalProtect Client File**（**GlobalProtect** 用戶端檔案）。按一下 **OK**（確定）來啟動所選映像。您可能需要先重新整理頁面，然後版本才會顯示為 **Currently Activated**（目前已啟動）。

在 Web 伺服器代管應用程式更新

如果您有大量必須安裝及/或更新 GlobalProtect 應用程式軟體的端點，請考慮在外部 Web 伺服器裝載 GlobalProtect 應用程式軟體映像。這樣有助於在使用者連線並下載應用程式時降低防火牆的負載。

STEP 1 | 將您要在 Web 伺服器裝載的 GlobalProtect 應用程式版本下載至防火牆，並予以啟動。

請依照在入口網站裝載應用程式更新所述，遵循從防火牆下載並啟動應用程式軟體的步驟而執行。

STEP 2 | 下載您要在 Web 伺服器裝載的 GlobalProtect 應用程式軟體映像。

下載在入口網站啟動的相同映像。

從 Web 瀏覽器，下載 GlobalProtect 應用程式。

STEP 3 | 將軟體映像檔案發佈至您的 Web 伺服器。

STEP 4 | 將一般使用者重新導向至 Web 伺服器。

在裝載入口網站的防火牆上，在操作模式中輸入下列 CLI 命令：

```
> set global-protect redirect on > set global-protect redirect
 location <path>
```

其中 *<path>* 是裝載映像的資料夾 URL 路徑（例如 **`https://acme/GP`**）。

STEP 5 | 測試重新導向。

1. 從 Web 瀏覽器中，前往下列 URL：

   ```
   https://<portal address or name>
   ```

   例如 **`https://gp.acme.com`**。
2. 在入口網站登入頁面，輸入您的使用者 **Name**（名稱）與 **Password**（密碼），然後按一下 **LOGIN**（登入）。成功登入後，入口網站應該會將您重新導向至下載。

測試應用程式安裝

使用下列程序測試 GlobalProtect 應用程式安裝。

STEP 1 | 建立用來測試應用程式安裝的代理程式組態。

首次在端點安裝 *GlobalProtect* 應用程式軟體時，一般使用者必須使用具有管理權限的帳戶才能登入系統。後續的應用程式軟體更新則不需要管理權限。

最佳做法是，建立一個代理程式組態並將其限制為小型使用者群組，例如負責管理防火牆的 *IT* 部門管理員：

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）。
2. 選取您要修改的現有入口網站組態或 **Add**（新增）新的入口網站組態
3. 在 **Agent**（代理程式）頁籤上，選取現有組態或按一下 **Add**（新增）來新增一個用來部署至測試使用者/群組的組態。
4. 在 **User/User Group**（使用者/使用者群組）頁籤上，**Add**（新增）將測試應用程式的 **User/User Group**（使用者/使用者群組）。
5. 在 **App**（應用程式）頁籤上，將 **Allow User to Upgrade GlobalProtect App**（允許使用者升級 **GlobalProtect** 應用程式）設定為 **Allow with Prompt**（透過提示允許）。按一下 **OK**（確定）來儲存組態。
6. （選用）在 **Agent**（代理程式）頁籤上，選取您剛剛建立或修改的代理程式組態，然後按一下 **Move Up**（上移），使其在清單上位於您已建立之較一般的組態之上。

當 GlobalProtect 應用程式連線時，入口網站會將封包中的來源資訊與您已定義的代理程式組態進行比較。藉助安全性規則評估，入口網站會從清單頂端開始尋找符合項。找到符合項目時，會將對應的設定傳遞給應用程式。

7. **Commit**（提交）變更。

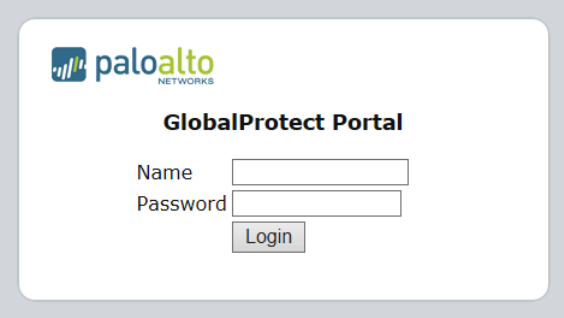
STEP 2 | 登入 GlobalProtect 入口網站。

1. 啟動 Web 瀏覽器並前往下列 URL：

```
https://<portal address or name>
```

例如 `https://gp.acme.com`。

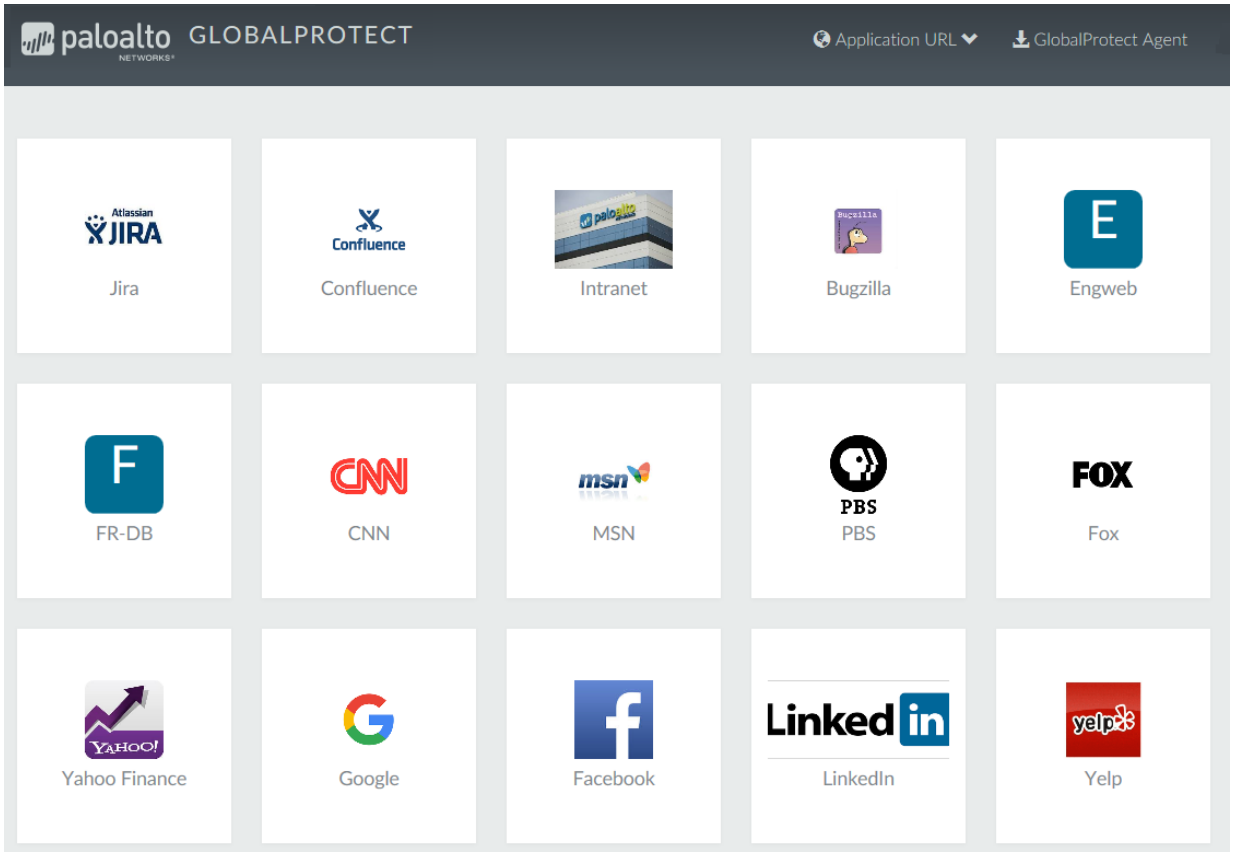
2. 在入口網站登入頁面，輸入您的使用者 **Name**（名稱）與 **Password**（密碼），然後按一下 **LOG IN**（登入）。



STEP 3 | 導覽至應用程式下載頁面。

在大多數情況下，應用程式下載頁面會在您登入至入口網站後立即出現。使用此頁面來下載最新應用程式軟體封包。

如果您已啟用 GlobalProtect 無用戶端 VPN 存取，當您登入至入口網站時，應用程式頁面會在您登入至入口網站後開啟（而不是代理程式下載頁面）。選取 **GlobalProtect Agent**（**GlobalProtect** 代理程式）來開啟下載頁面。



STEP 4 | 下載應用程式。

1. 若要開始下載，請按一下電腦上執行的作業系統所對應的連結。

2. 開啟軟體安裝檔案。
3. 當系統提示您執行或儲存軟體時，按一下 **Run**（執行）。
4. 若系統提示，請按一下 **Run**（執行）啟動「GlobalProtect 安裝精靈」。

首次在端點安裝 *GlobalProtect* 應用程式軟體時，一般使用者必須使用具有管理權限的帳戶才能登入系統。後續的應用程式軟體更新則不需要管理權限。

STEP 5 | 完成 GlobalProtect 應用程式安裝。

1. 從「GlobalProtect 安裝精靈」中按一下 **Next**（下一步）。
2. 按一下 **Next**（下一個）接受預設安裝資料夾 (`C:\Program Files\Palo Alto Networks\GlobalProtect`) 或按一下 **Browse**（瀏覽）以選取新位置，然後按兩次 **Next**（下一個）。
3. 安裝完成後，**Close**（關閉）精靈。

STEP 6 | 登入 GlobalProtect。

1. 按一下系統匣圖示，啟動 GlobalProtect 應用程式。狀態面板將開啟。
2. 輸入入口網站的 FQDN 或 IP 位址，然後按一下 **Connect**（連線）。
3. （選用）依預設，根據管理員定義的設定和可用閘道的回應時間，您將自動連線至 **Best Available**（現有最佳）閘道。若要連線至不同閘道，可從 **Gateway**（閘道）下拉式清單中選取閘道（僅限外部閘道）。

此選項僅適用於您啟用手動閘道選取的情況。

4. （選用）根據連線模式，按一下 **Connect**（連線）以啟動連線。
5. （選用）若出現提示，請輸入 **Username**（使用者名稱）和 **Password**（密碼），然後按一下 **Sign In**（登入）。

如果驗證成功，您將連線至公司網路，且狀態面板將顯示 **Connected**（已連線）或 **Connected - Internal**（已連線—內部）狀態。如果設定了 GlobalProtect 歡迎頁面，其將在您成功登入後顯示。

下載及安裝 GlobalProtect 行動應用程式

GlobalProtect 應用程式提供一種簡單的方式來將企業安全原則向外延伸到行動端點。對於執行 GlobalProtect 應用程式的其他遠端端點而言，行動應用程式會提供在 IPsec 或 SSL VPN 通道上對於您企業網路的安全存取。應用程式將會自動連線至距離一般使用者目前位置最近的閘道。此外，與端點之間的來往流量也會自動受限於與您公司網路上其他主機相同的安全原則強制執行。行動應用程式還會收集有關主機設定的資訊，並可以將此資訊用於強化的 HIP 式安全原則強制執行。

有兩種主要方法可安裝 GlobalProtect 應用程式：您可以從協力廠商 MDM 部署該應用程式，並明顯將其推送至您受管理的端點，或者從端點的官方商店安裝。

- iOS 端點—App Store
- Android 端點與 Chromebooks—Google Play

  從 GlobalProtect 應用程式 5.0 開始，適用于 Chrome OS 的 GlobalProtect 應用程式將不受支援；請改為使用適用于 Android 的 GlobalProtect 應用程式。
- Windows 10 手機和 Windows 10 UWP 端點—Microsoft Store

此工作流程說明了如何在行動端點上直接安裝 GlobalProtect 應用程式。如需怎樣從 AirWatch 部署 GlobalProtect 應用程式的指示，請參閱使用 AirWatch 部署 GlobalProtect 行動應用程式。

STEP 1 | 建立用來測試應用程式安裝的代理程式組態。

最佳做法是，建立一個代理程式組態並將其限制為小型使用者群組，例如負責管理防火牆的 IT 部門管理員：

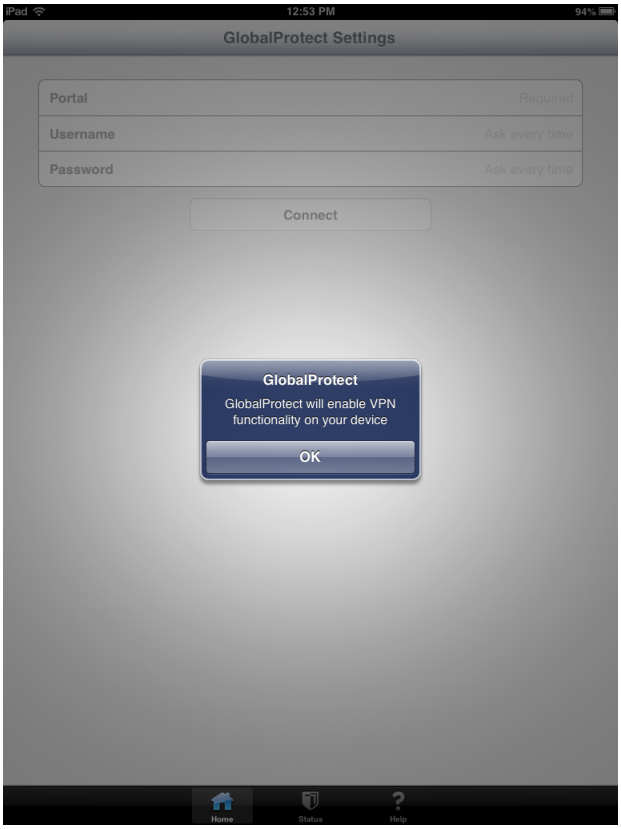
1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）。
2. 選取現有入口網站組態以修改或 **Add**（新增）一個。
3. 在 **Agent**（代理程式）頁籤上，選取現有組態或按一下 **Add**（新增）來新增一個用來部署至測試使用者/群組的組態。
4. 在 **User/User Group**（使用者/使用者群組）頁籤上，**Add**（新增）將測試應用程式的 **User/User Group**（使用者/使用者群組）。
5. 選取您要測試的應用程式的 **OS**（作業系統）（**iOS**、**Android** 或 **WindowsUWP**）。
6. （選用）選取您剛剛建立/修改的代理程式組態，然後按一下 **Move Up**（上移），使其位於清單上您已建立之較一般的組態之上。
7. **Commit**（提交）變更。

STEP 2 | 從端點中，依照提示下載及安裝應用程式。

- 對於 Android 端點，請在 Google Play 中搜尋應用程式。
- 對於 iOS 端點，請在 App Store 中搜尋應用程式。
- 對於 Windows 10 UWP 端點，請在 Microsoft Store 中搜尋應用程式。

STEP 3 | 啟動應用程式。

成功安裝之後，GlobalProtect 應用程式圖示會顯示在端點的主畫面中。若要啟動應用程式，點選此圖示。當提示啟用 GlobalProtect VPN 功能時，點選 **OK**（確定）。



STEP 4 | 連線至入口網站。

1. 系統提示時，輸入 **Portal**（入口網站）名稱或位址、使用者 **Name**（名稱）與 **Password**（密碼）。入口網站名稱必須是 FQDN，而且開頭不應有 https://。

2. 點選 **Connect**（連線），並確認應用程式是否已成功與 GlobalProtect 之間建立連線。

   如果已設定協力廠商行動端點管理系統，應用程式將會提示您進行註冊。

明顯部署應用程式設定

從入口網站設定部署應用程式設定還有一種可行的方法，即直接透過 Windows 登錄、全域 macOS plist，或者（僅限於 Windows 端點）從 Windows 安裝程式 (Msiexec) 進行定義。這種方法的好處是，可以在 GlobalProtect 應用程式設定初次連線至 GlobalProtect 入口網站之前將其部署至端點。

在入口網站設定中定義的設定會一直取代在 Windows 登錄或 macOS plist 中定義的設定。如果您已在登錄或 plist 中定義設定，但入口網站組態卻指定了不同的設定，那麼應用程式從入口網站接收的設定就會取代在端點定義的設定。此取代也套用於登入相關設定，例如是否視需要連線、是否使用單一登入 (SSO)，以及在入口網站憑證無效時應用程式是否可以連線。因此，您應避免衝突的設定。此外，入口網站設定會在端點進行快取，如果重新啟動 GlobalProtect 應用程式或端點，將會使用此快取的設定。

以下幾節說明可自訂的應用程式設定，以及如何透明地將這些設定部署到 Windows 與 macOS 端點：

- 可自訂的應用程式設定
- 部署應用程式設定至 Windows 端點
- 部署應用程式設定至 macOS 端點

除了使用 *Windows* 登錄與 *macOS Plist* 部署 *GlobalProtect* 應用程式設定外，您可以讓 *GlobalProtect* 應用程式從端點收集特定的 *Windows* 登錄或 *macOS Plist* 資訊，包括安裝在端點上應用程式的資料、在端點上執行的處理程序，以及這些應用程式與處理程序的屬性或特性。接著您可以監控資料，並將它新增至安全性規則中用作比對條件。您可根據安全性規則，強制執行符合某些所定義登錄設定的端點流量。此外，您可以設定自訂檢查來從端點收集應用程式與處理資料。

可自訂的應用程式設定

除了預先部署入口網站位址外，您也可以定義應用程式設定。若要部署應用程式設定至 Windows 端點，您需要在 Windows 登錄中定義金鑰 (`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`)。若要部署應用程式設定至 Mac 端點，您需要在 macOS plist 的 `PanSetup` 字典中定義項目 (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`)。在 Windows 端點上，您也可以使用 Windows Installer 來部署來自 Msiexec 的應用程式設定。

下列主題說明每個自訂應用程式設定。在 GlobalProtect 入口網站代理程式組態中所定義的設定，將優先於在 Windows 登錄或 macOS plist 中所定義的設定。

部分設定在 *Web* 介面上並沒有對應的入口網站組態設定，且必須使用 *Windows* 登錄或 *Msiexec* 加以設定。這些額外設定包括：*`can-prompt-user-credential`*、*`wrap-cp-guid`* 及 *`filter-non-gpcp`*。

- 應用程式顯示選項
- 使用者行為選項
- 應用程式行為選項
- 指令碼部署選項

應用程式顯示選項

下表列出了可在 Windows 登錄和 macOS Plist 中設定，以自訂 GlobalProtect 應用程式顯示的選項。

表 3: 表格：可自訂的應用程式設定

入口網站代理程式組態	Windows 登錄/ macOS Plist	Msiexec 參數	預設值
啟用進階視圖	`enable-advanced-view yes | no`	`ENABLEADVANCEDVIEW=”yes | no”`	`yes`
顯示 GlobalProtect 圖示	`show-agent-icon yes | no`	`SHOWAGENTICON=”yes | no”`	`yes`
啟用重新發現網路選項	`rediscover-network yes | no`	`REDISCOVERNETWORK=”yes | no”`	`yes`
啟用 Resubmit Host Profile（重新提交主機設定檔）選項	`resubmit-host-info yes | no`	`RESUBMITHOSTINFO=”yes | no”`	`yes`
顯示系統託盤通知	`show-system-tray-notifications yes | no`	`SHOWSYSTEMTRAYNOTIFICATIONS=”yes | no”`	`yes`

使用者行為選項

下表列出了可在 Windows 登錄和 macOS Plist 中設定，以自訂使用者與 GlobalProtect 應用程式互動的選項。

表 4: 表格：可自訂的使用者行為選項

入口網站代理程式組態	Windows 登錄/ macOS Plist	Msiexec 參數	預設值
允許使用者更改入口網站位址	`can-change-portal yes | no`	`CANCHANGEPORTAL=”yes | no”`	`yes`
允許使用者屏除歡迎頁	`enable-hide-welcome-page yes | no`	`ENABLEHIDEWELCOMEPAGE=”yes | no”`	`yes`
允許使用者繼續使用無效入口網站伺服器憑證	`can-continue-if-portal-cert-invalid yes | no`	`CANCONTINUEIFPORTALCERTINVALID= ”yes | no”`	`yes`
允許使用者禁用 GlobalProtect 應用程式	`disable-allowed yes | no`	`DISABLEALLOWED="yes | no"`	`no`
儲存使用者認證 指定 0 以防止 GlobalProtect 儲存認證，1 表示儲存使用者名稱和密碼，2 表示僅儲存使用者名稱。	`save-user-credentials 0 | 1 | 2`	`SAVEUSERCREDENTIALS 0 | 1 | 2`	不適用

入口網站代理程式組態	Windows 登錄/ macOS Plist	Msiexec 參數	預設值
不在入口網站中 **Allow user to save password**（允許使用者儲存密碼）在 PAN-OS 7.1 和更新版本的網路介面中被棄用，但可透過 Windows 登錄和 macOS plist 設定。**Save User Credentials**（儲存使用者認證）欄位中指定的任何值會覆寫此處指定的值。	`can-save-password yes | no`	`CANSAVEPASSWORD="yes | no"`	`yes`
僅限 **Windows**/不在入口網站 此設定讓 GlobalProtect 認證提供者能夠顯示 **Start GlobalProtect Connection**（啟動 **GlobalProtect** 連線）按鍵，以便使用者可以手動啟動 GlobalProtect 預先登入連線。	`ShowPrelogonButton yes | no`	不適用	`no`

應用程式行為選項

下表列出了可在 Windows 登錄和 macOS Plist 中設定，以自訂 GlobalProtect 應用程式行為的選項。

表 5: 表格：可自訂的應用程式行為選項

入口網站代理程式組態	Windows 登錄/macOS Plist	Msiexec 參數	預設值
連接方法	`connect-method on-demand | pre-logon | user-logon`	`CONNECTMETHOD="on-demand | pre-logon | user-logon"`	`user-logon`
GlobalProtect 應用程式配置刷新時間間隔（小時）	`refresh-config-interval <hours>`	`REFRESHCONFIGINTERVAL= "<hours>"`	`24`
連接時更新 **DNS** 設置（僅 **Windows**）	`flushdns yes | no`	`FLUSHDNS="yes | no"`	`no`

入口網站代理程式組態	Windows 登錄/macOS Plist	Msiexec 參數	預設值
Windows 安全中心 (WSC) 狀態變更後立即發送 HIP 報告（僅 Windows）	`wscautodetect yes | no`	`WSCAUTODETECT="yes | no"`	`no`
檢測每個連接的代理（僅 Windows）	`ProxyMultipleAuto Detection yes | no`	`ProxyMultipleAuto Detection="yes | no"`	`no`
登出時清空 Single Sign-on（單點登錄-SSO）認證（僅 Windows）	`LogoutRemoveSSO yes | no`	`LogoutRemoveSSO="yes | no"`	`yes`
Kerberos 身份驗證失敗時使用默認身份驗證（僅 Windows）	`krb-auth-fail-fallback yes | no`	`KRBAUTHFAILFALLBACK= "yes | no"`	`no`
客戶密碼到期資訊（僅 LDAP 身份驗證）	`PasswordExpiryMessage <message>`	`PasswordExpiryMessage "<message>"`	
入口網站連接逾時（秒）	`PortalTimeout <portaltimeout>`	`PORTALTIMEOUT= "<portaltimeout>"`	`5`
TCP 連接逾時（秒）	`ConnectTimeout <connecttimeout>`	`CONNECTTIMEOUT= "<connecttimeout>"`	`5`
TCP 接收逾時（秒）	`ReceiveTimeout <receivetimeout>`	`RECEIVETIMEOUT= "<receivetimeout>"`	`30`
用戶端憑證商店查找	`certificate-store-lookup user | machine | user and machine | invalid`	`CERTIFICATESTORELOOKUP= "user | machine | user and machine | invalid"`	`user and machine`
SCEP 憑證更新週期（天數）	`scep-certificate-renewal-period <renewalPeriod>`	不適用	`7`
最大內部閘道連接嘗試次數	`max-internal-gateway-connection-attempts <maxValue>`	`MIGCA="<maxValue>"`	`0`
用戶端憑證擴充金鑰使用物件識別碼 (OID)	`ext-key-usage-oid-for-client-cert <oidValue>`	`EXTCERTOID="<oidValue>"`	不適用
使用者切換通道重命名逾時（秒）	`user-switch-tunnel-rename-timeout <renameTimeout>`	不適用	`0`

入口網站代理程式組態	Windows 登錄/macOS Plist	Msiexec 參數	預設值
使用單一登入 （僅限 Windows）	`use-sso yes | no`	`USESSO="yes | no"`	`yes`
不在入口網站中 此設定指定預設入口網站 IP 位址（或主機名稱）。	`portal <IPaddress>`	`PORTAL="<IPaddress>"`	不適用
不在入口網站中 此設定會啟用 GlobalProtect 以在使用者登入裝置和連線至 GlobalProtect 入口網站之前，先啟動 VPN 通道。	`prelogon 1`	`PRELOGON="1"`	`1`
僅限 Windows/不在入口網站 此設定可與單一登入 (SSO) 搭配使用，可指示在 SSO 失敗時是否提示使用者提供憑證。	`can-prompt-user-credential yes | no`	`CANPROMPTUSERCREDENTIAL=”yes | no”`	`yes`
僅限 Windows/不在入口網站 此設定會將第三方認證提供者的圖標從 Windows 登入頁面中過濾掉，因此只會顯示原生的 Windows 圖標。*	`wrap-cp-guid {third party credential provider guid}`	`WRAPCPGUID=”{guid_value]” FILTERNONGPCP=”yes | no”`	`no`
僅限 Windows/不在入口網站 此設定是設定 wrap-cp-guid 的額外選項，允許除了原生的 Windows 登入圖標外，第三方認證提供者的圖標也會顯示在 Windows 登入頁面上。*	`filter-non-gpcp no`	不適用	不適用
僅限 Windows/不在入口網站	`reserved-ipv4 <reserved-ipv4>`	`RESERVEDIPV4=”<reserved-ipv4>”`	不適用

入口網站代理程式組態	Windows 登錄/macOS Plist	Msiexec 參數	預設值
此設定可讓您向 Windows 端點指派靜態 IP 位址。	**reserved-ipv6 <reserved-ipv6>**	**RESERVEDIPV6="<reserved-ipv6>"**	

如需使用 *Windows* 登錄或 *Windows Installer (Msiexec)* 啟用這些設定的詳細步驟，請參閱 Windows 端點上協力廠商認證提供者的 SSO 封裝。

指令碼部署選項

下表顯示啟用 GlobalProtect，在建立連線前後和中斷連線之前起始指令碼的選項。由於這些選項在入口網站中不可用，您必須定義相關金鑰的值—pre-vpn-connect、post-vpn-connect 或 pre-vpn-disconnect—來自 Windows 登錄或 macOS plist。如需建立部署原則的詳細步驟，請參閱透過 Windows 登錄部署指令碼、透過 Msiexec 部署指令碼或透過 macOS Plist 部署指令碼。

表格：可自訂的指令碼部署選項

入口網站代理程式組態	Windows 登錄/macOS Plist	Msiexec 參數	預設值
執行命令設定中指定的指令碼（包括傳遞至指令碼的任何參數）。 支援環境變數。 在命令中指定完整路徑。	命令 **<parameter1> <parameter2> [...]** Windows 範例： **command %userprofile%\vpn_script.bat c: test_user** macOS 範例： **command $HOME/vpn_script.sh /Users/test_user test_user**	**PREVPNCONNECTCOMMAND= "<parameter1> <parameter2> [...]"** **POSTVPNCONNECTCOMMAND= "<parameter1> <parameter2> [...]"** **PREVPNDISCONNECTCOMMAND= "<parameter1> <parameter2> [...]"**	不適用
（選用）指定命令執行的權限（預設為使用者：如果您不指定內容，命令將按照目前作用中的使用者運行）。	內容管理員 | 使用者	**PREVPNCONNECTCONTEXT= "admin | user"** **POSTVPNCONNECTCONTEXT= "admin | user"** **PREVPNDISCONNECTCONTEXT= "admin | user"**	使用者
（選用）指定 GlobalProtect 應用程式等候命令執行的時間，以秒為單位（範圍 0-120）。如果命令在逾時之前未完成，應用程式會繼續建立連線或中斷連線。0（預設值）值意味著應用程式不會等候執行命令。	**timeout <value>** 範例： **timeout 60**	**PREVPNCONNECTTIMEOUT= "<value>"** **POSTVPNCONNECTTIMEOUT= "<value>"** **PREVPNDISCONNECTTIMEOUT= "<value>"**	0

入口網站代理程式組態	Windows 登錄/macOS Plist	Msiexec 參數	預設值
不支援 *post-vpn-connect*。			
（選用）指定命令中所使用的檔案的完整路徑。GlobalProtect 應用程式將透過對比總和檢查碼金鑰內指定的數值進行檢查，確認檔案的完整性。 支援環境變數。	**file <path_file>**	**PREVPNCONNECTFILE=”<path_file>”** **POSTVPNCONNECTFILE=”<path_file>”** **PREVPNDISCONNECTFILE=”<path_file>”**	不適用
（選用）指定檔案金鑰中參考的檔案 sha256 總和檢查碼。如已指定，則當 GlobalProtect 應用程式產生的總和檢查碼與此處指定的總和檢查碼相符時，GlobalProtect 應用程式將僅執行命令。	**checksum <value>**	**PREVPNCONNECTCHECKSUM=”<value>”** **POSTVPNCONNECTCHECKSUM=”<value>”** **PREVPNDISCONNECTCHECKSUM=”<value>”**	不適用
（選用）當命令無法執行或退出時帶有非零的返回碼時，指定向使用者顯示的錯誤訊息。 此訊息必須為 *1,024* 個或更少的 *ANSI* 字元。	**error-msg <message>** 範例： **error-msg Failed executing pre-vpn-connect action!**	**PREVPNCONNECTERRORMSG=”<message>”** **POSTVPNCONNECTERRORMSG=”<message>”** **PREVPNDISCONNECTERRORMSG=”<message>”**	不適用

部署應用程式設定至 Windows 端點

使用 Windows 登錄或 Windows 安裝程式 (Msiexec) 可將 GlobalProtect 應用程式與設定透明地部署至 Windows 端點。

- 在 Windows 登錄中部署代理程式設定
- 從 Msiexec 部署代理程式設定
- 透過 Windows 登錄部署指令碼
- 透過 Msiexec 部署指令碼
- Windows 端點上協力廠商認證提供者的 SSO 封裝
- 透過 Windows 登錄啟用協力廠商認證的 SSO 封裝。
- 透過 Windows 安裝程式啟用協力廠商認證的 SSO 封裝

在 *Windows* 登錄中部署應用程式設定

您可以在 GlobalProtect 應用程式第一次連線到 GlobalProtect 入口網站前，使用 Windows 登錄將該應用程式的設定部署至 Windows 端點。使用下表所述的選項使用 Windows 登錄為 Windows 端點自訂應用程式設定。

除了使用 *Windows* 登錄來部署 *GlobalProtect* 應用程式設定外，您還可以允許 *GlobalProtect* 應用程式從 *Windows* 端點收集特定的 *Windows* 登錄資訊。接著您可以監控資料，並將它新增至安全性規則中用作比對條件。您可根據安全性規則，強制執行符合某些所定義登錄設定的端點流量。此外，您可以設定自訂檢查來從端點收集應用程式與處理資料。

STEP 1 | 在 Windows 登錄中找到 GlobalProtect 應用程式自訂設定。

開啟 Windows 登錄（在命令提示字元中輸入 **regedit**），然後移至：

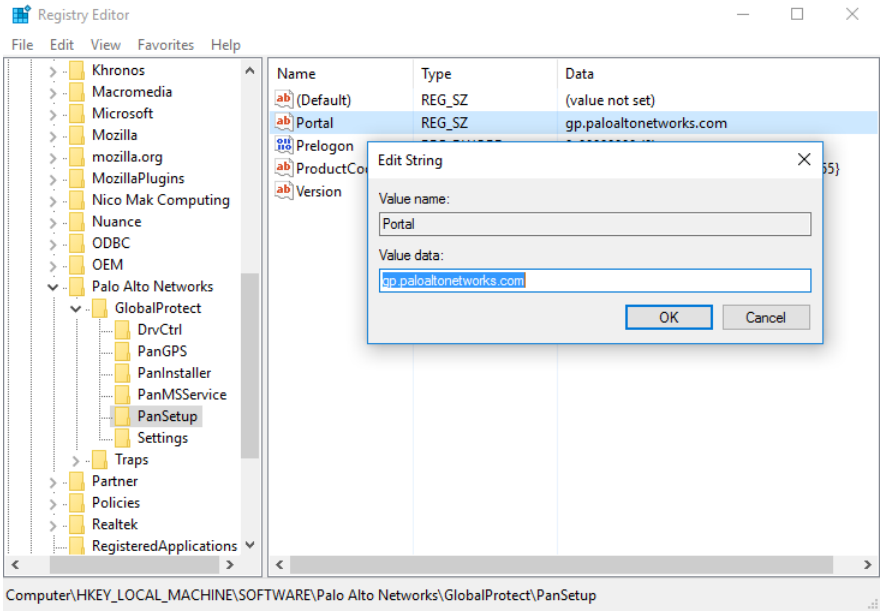
```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\
```

STEP 2 | 設定入口網站名稱。

如果不想讓一般使用者手動輸入入口網站位址（即使是初次連線），您可以透過 Windows 登錄預先部署入口網站位址。

1. 在 Window 登錄中，前往：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup
   ```
2. 右鍵按一下 **Portal**（入口網站）並選取 **Modify**（修改）。
3. 在 **Value data**（值資料）欄位輸入入口網站名稱，然後按一下 **OK**（確定）。



STEP 3 | 將各種設定部署至 Windows 端點，包括 GlobalProtect 應用程式的連線方法和單一登入 (SSO)。

檢視可自訂應用程式設定以取得您可以使用 Windows 登錄設定的完整命令與值清單。

STEP 4 | 允許 GlobalProtect 應用程式封裝 Windows 端點上的第三方認證，如此一來即使正在使用第三方認證提供者仍允許 SSO。

透過 Windows 登錄啟用協力廠商認證的 SSO 封裝。

從 *Msiexec* 部署應用程式設定

在 Windows 端點，您可以選取從 Windows 安裝程式 (Msiexec) 使用下列語法自動部署 GlobalProtect 應用程式與應用程式設定：

```
msiexec.exe /i GlobalProtect.msi <SETTING>="<value>"
```

Msiexec 是一個可執行程式，可從命令行安裝或設定產品。在端點上執行 *Microsoft Windows XP* 或更新的作業系統，您在命令提示上可使用的字串最大長度為 *8,191* 個字元。

Msiexec 範例	說明
`msiexec.exe /i GlobalProtect.msi /quiet PORTAL="portal.acme.com"`	在安靜模式下安裝 GlobalProtect（無使用者介面）並設定入口網站位址。
`msiexec.exe /i GlobalProtect.msi CANCONTINUEIFPORTALCERTINVALID="no"`	安裝 GlobalProtect 並選取當憑證無效時，防止使用者連線至入口網站。

如需設定與對應預設值的完整清單，請參閱自訂應用程式設定。

您也可以透過 Windows 安裝程式啟用協力廠商認證的 SSO 封裝。

透過 *Windows* 登錄部署指令碼

您可以透過 Windows 登錄啟用自訂指令碼對 Windows 端點的部署。

您可以設定 GlobalProtect 應用程式，為以下事件起始和執行指令碼：建立通道前後，中斷通道連線前。若要在特定事件上執行指令碼，參考該事件命令登錄項目的批次指令碼。

視乎組態設定，GlobalProtect 應用程式可在應用程式建立到閘道的連線前後，以及在應用程式中斷連線前執行指令碼。使用下列工作流程透過 Windows 登錄為 Windows 端點自訂應用程式設定。

端點支援讓您可以部署指令碼的登錄設定，該端點執行 *GlobalProtect* 應用程式 *2.3* 和更新的版本。

STEP 1 | 打開 Windows 登錄，找到 GlobalProtect 應用程式自訂設定。

視乎您希望執行指令碼的時間，開啟 Windows 登錄（在命令提示中輸入 **regedit**）並前往下列金鑰位置之一（連線前後或中斷連線前）：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\pre-vpn-connect
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\post-vpn-connect
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\pre-vpn-disconnect
```

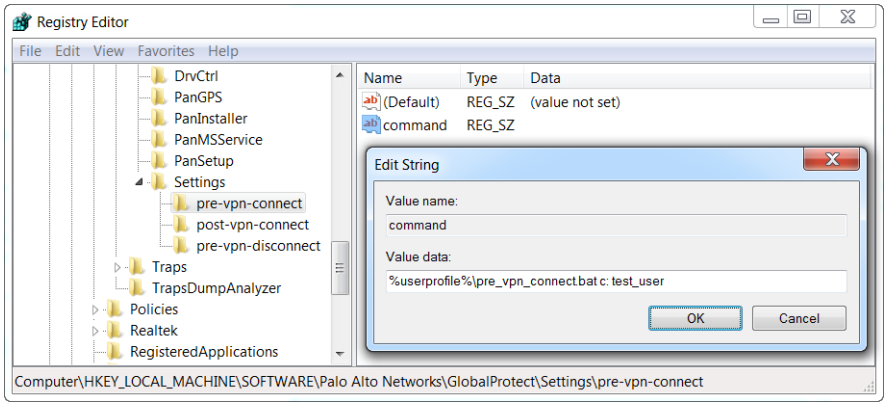
如果金鑰未位於 *Settings*（設定）金鑰內，則透過右鍵按一下 *Settings*（設定）並選取 *New*（新）> *Key*（金鑰）來建立金鑰。

STEP 2 | 透過建立名稱為 **command** 的新字串值，啟用 GlobalProtect 應用程式以執行指令碼。

此處指定的批次檔案應包含您想要在裝置上執行的特定指令碼（包括傳遞至指令碼的任意參數）。

1. 如果 `command` 字串不存在，則應建立（右鍵按一下 `pre-vpn-connect`、`post-vpn-connect`、或 `pre-vpn-disconnect` 金鑰，選取 **New**（新增）> **String Value**（字串值），然後將其命名為 **command**）。
2. 右鍵按一下 `command` 並選取 **Modify**（修改）。
3. 輸入 GlobalProtect 應用程式運行的命令或指令碼。例如：

```
%userprofile%\pre_vpn_connect.bat c: test_user
```



STEP 3 | （選用）根據需要為各命令新增登錄項目。

建立或修改登錄字串及其對應值，包括 `context`、`timeout`、`file`、`checksum` 或 `error-msg`。如需其他資訊，請參閱可自訂應用程式設定。

透過 *Msiexec* 部署指令碼

在 Windows 端點上，您可以使用 Windows 安裝程式 (Msiexec) 部署應用程式自動運行的 GlobalProtect 應用程式、應用程式設定和指令碼（請參閱可自訂應用程式設定）。若要執行此操作，請使用下列語法：

```
msiexec.exe /i GlobalProtect.msi <SETTING>="<value>"
```

Msiexec 是一個可執行程式，可從命令行安裝或設定產品。在系統上執行 *Microsoft Windows XP* 或更新版本，您在命令提示上可使用的字串最大長度為 *8,191* 個字元。

此限制套用於其他程序繼承的命令行、個別環境變數（如使用者設定檔變數），以及所有環境變數擴充。如果您從命令行執行批次檔案，此限制也將套用至批次檔案程序。

例如，若要部署執行特定連線或中斷連線事件的指令碼，您可以使用與下列範例類似的語法：

範例：使用 **Msiexec** 部署在連線事件之前執行的指令碼

對於可以複製並貼上的指令碼，請見此處。

```
msiexec.exe /i GlobalProtect.msi PREVPNCONNECTCOMMAND="%userprofile
%\pre_vpn_connect.bat c: test_user" PREVPNCONNECTCONTEXT="user"
 PREVPNCONNECTTIMEOUT="60" PREVPNCONNECTFILE="C:\Users\test_user
\pre_vpn_connect.bat"
 PREVPNCONNECTCHECKSUM="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
 8647ccf599" PREVPNCONNECTERRORMSG="Failed executing pre-vpn-connect action."
```

如需設定與對應預設值的完整清單，請參閱自訂應用程式設定。

範例：使用 **Msiexec** 部署在連線事件前後及中斷連線之前執行的指令碼

對於可以複製並貼上的指令碼，請見此處。

```
msiexec.exe /i GlobalProtect.msi PREVPNCONNECTCOMMAND="%userprofile
%\pre_vpn_connect.bat c: test_user" PREVPNCONNECTCONTEXT="user"
 PREVPNCONNECTTIMEOUT="60" PREVPNCONNECTFILE="C:\Users\test_user
\pre_vpn_connect.bat"
 PREVPNCONNECTCHECKSUM="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
 8647ccf599" PREVPNCONNECTERRORMSG="Failed executing pre-vpn-
connect action." POSTVPNCONNECTCOMMAND="c:\users\test_user
\post_vpn_connect.bat c: test_user" POSTVPNCONNECTCONTEXT="admin"
 POSTVPNCONNECTFILE="%userprofile%\post_vpn_connect.bat"
 POSTVPNCONNECTCHECKSUM="b48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
 8647ccf598" POSTVPNCONNECTERRORMSG="Failed executing post-vpn-connect
 action." PREVPNDISCONNECTCOMMAND="%userprofile%\pre_vpn_disconnect.bat
 c: test_user" PREVPNDISCONNECTCONTEXT="admin" PREVPNDISCONNECTTIMEOUT="0"
 PREVPNDISCONNECTFILE="C:\Users\test_user\pre_vpn_disconnect.bat"
 PREVPNDISCONNECTCHECKSUM="c48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b0
 118647ccf597" PREVPNDISCONNECTERRORMSG="Failed executing pre-vpn-disconnect
 action."
```

如需設定與對應預設值的完整清單，請參閱自訂應用程式設定。

Windows 端點上協力廠商認證提供者的 *SSO* 封裝

在 Windows 7 端點上，GlobalProtect 應用程式使用 Microsoft 認證提供者架構以支援單一登入 (SSO)。透過 SSO，GlobalProtect 認證提供者封裝 Windows 原生認證提供者，讓 GlobalProtect 使用 Windows 登入認證，自動驗證和連線至 GlobalProtect 入口網站和閘道。此外，下一次登入時，如果 Windows 10 使用者的密碼過期或管理員要求變更密碼，SSO 封裝可讓其使用 GlobalProtect 認證提供者更新 Active Directory (AD) 密碼。

當端點上還存在其他協力廠商認證提供者時，GlobalProtect 認證提供者將無法收集使用者的 Windows 登入認證。因此，GlobalProtect 將無法自動連線至 GlobalProtect 入口網站與閘道。如果 SSO 失敗，您可以識別協力廠商認證提供者，並設定 GlobalProtect 應用程式以封裝這些協力廠商認證，讓使用者僅使用 Windows 登入認證成功驗證至 Windows、GlobalProtect 和協力廠商認證提供者。

或者，您可以設定 Windows 顯示分割登入圖標：一個用於各協力廠商認證提供者，另一個用於原生 Windows 登入。這在協力廠商認證提供者新增不適用於 GlobalProtect 的其他功能時，非常有用。

如果您要將 *GlobalProtect* 認證提供者從 *Windows* 端點移除，可在命令提示中執行 ***GlobalProtectPanGPS.exe -u*** 命令。

使用 Windows 登錄或 Windows Installer (`msiexec`) 允許 GlobalProtect 封裝協力廠商認證：

- 透過 Windows 登錄啟用協力廠商認證的 SSO 封裝。

- 透過 Windows 安裝程式啟用協力廠商認證的 SSO 封裝

> 協力廠商認證提供者 *(CP)* 的 *GlobalProtect SSO* 封裝取決於協力廠商 *CP* 設定。在某些情況下，如果協力廠商 *CP* 實作不允許 *GlobalProtect* 成功封裝其 *CP*，*GlobalProtect SSO* 封裝可能無法正常使用。

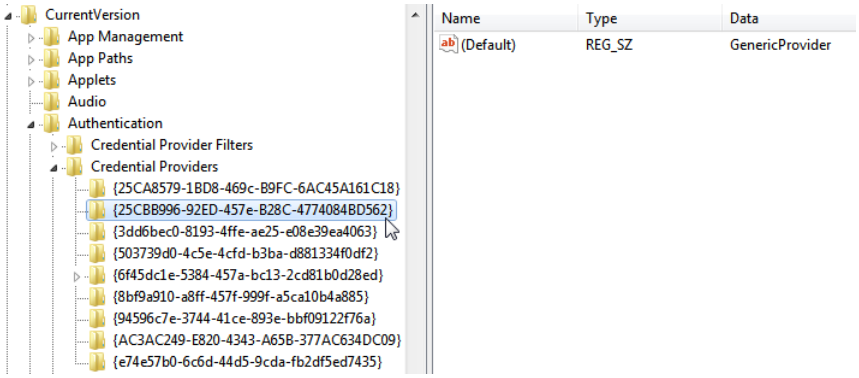
透過 *Windows* 登錄啟用協力廠商認證的 *SSO* 封裝。

在 Windows 登錄中使用下列步驟可允許 SSO 在 Windows 7 端點上封裝協力廠商認證。

STEP 1 | 開啟 Windows 登錄，然後找到您要封裝的協力廠商認證提供者其全域唯一識別碼 (GUID)。

1. 從命令提示中，輸入 **`regedit`** 命令以開啟 Windows 登錄編輯器。
2. 前往下列 Windows 登錄位置以檢視目前安裝的認證提供者清單：

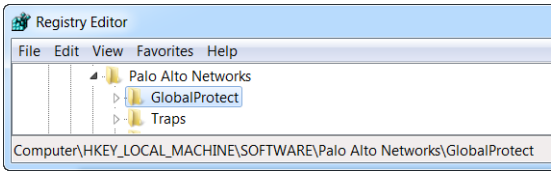
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion \Authentication\Credential Providers`。
3. 複製所要封裝認證提供者的 GUID 金鑰（GUID 的兩側要包括大括弧 — { 與 } ）：



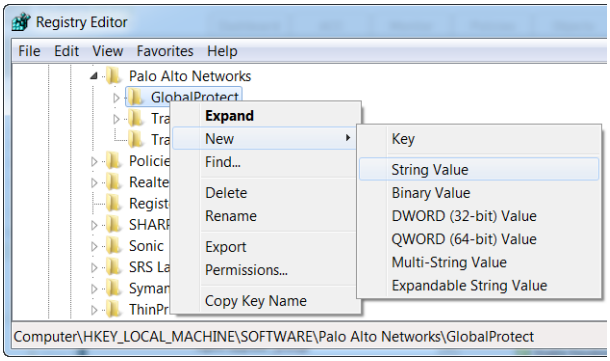
STEP 2 | 透過將 **`wrap-cp-guid`** 設定新增至 GlobalProtect 登錄，來啟用第三方廠商認證提供者的 SSO 封裝。

1. 前往下列 Windows 登錄位置：

   `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\ GlobalProtect`：



2. 右鍵按一下 **GlobalProtect** 資料夾，然後選取 **New**（新）> **String Value**（字串值）以新增新的字串值。



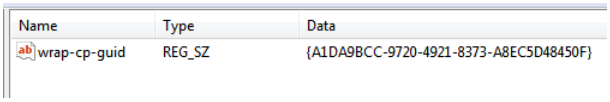
3. 設定下列 **String Value**（字串值）欄位：
   - 名稱：**wrap-cp-guid**
   - 值資料：{<**third-party credential provider GUID**>}

   對於 *Value data*（值資料）欄位，您輸入的 *GUID* 值必須用大括弧括住：*{ and }*。

   以下為 **Value data**（值資料）欄位中的協力廠商認證提供者 GUID 範例：

   ```
   {A1DA9BCC-9720-4921-8373-A8EC5D48450F}
   ```

   對於新的 **String Value**（字串值），`wrap-cp-guid` 會顯示為字串值的 **Name**（名稱），GUID 會顯示為 **Value Data**（值資料）。

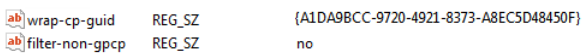


STEP 3 | 接下來的步驟：

- 透過此設定，可在登入畫面上對使用者顯示原生的 Windows 登入圖標。當使用者按一下圖標，並透過其 Windows 認證登入系統時，該單一登入將使用者向 Windows、GlobalProtect 和協力廠商認證提供者進行驗證。
- （選用）如果您想要在登入畫面上顯示多個圖標（例如，原生 Windows 圖標與協力廠商認證提供者的圖標），請繼續進行步驟 4。
- （選用）如果您想要為使用者指定預設認證提供者，請繼續進行步驟 5。
- （選用）如果您想要從登入畫面隱藏協力廠商認證提供者圖標，請繼續進行步驟 6。

STEP 4 | （選用）允許使用者登入時對使用者顯示協力廠商認證提供者圖標。

新增第二個 **String Value**（字串值），其 **Name**（名稱）為 **filter-non-gpcp**，然後為字串的 **Value data**（值資料）輸入 **no**：



將此字串值新增至 GlobalProtect 設定後，會在 Windows 登入畫面對使用者呈現兩個登入選項：原生的 Windows 圖標與協力廠商認證提供者的圖標。

STEP 5 | 為使用者登入指定預設認證提供者。

1. 開啟 Windows 登錄，以找到您要指定為預設認證提供者的協力廠商認證提供者其全域唯一識別碼 (GUID)。
   1. 從命令提示中，輸入 `regedit` 命令以開啟 Windows 登錄編輯器。

2. 前往下列 Windows 登錄位置以檢視目前安裝的認證提供者清單：

   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion \Authentication\Credential Providers`。
3. 複製認證提供者的完整 GUID 金鑰（GUID 的兩側要包括大括弧 — { 與 } ）：

2. 開啟本機群組原則編輯器以啟用並指定預設認證提供者。
   1. 從命令提示中，輸入 `gpedit.msc` 命令以開啟本機群組原則編輯器。
   2. 選取 **Computer Configuration**（電腦組態）> **Administrative Templates**（管理範本）> **System**（系統）> **Logon**（登入）。
   3. 在 **Setting**（設定）下，按兩下 **Assign a default credential provider**（指定預設認證提供者）以開啟指定預設認證提供者視窗。
   4. 將原則設定為 **Enabled**（已啟用）。
   5. 在 **Assign the following credential provider as the default credential provider**（指定下列認證提供者作為預設認證提供者）下，輸入認證提供者的 GUID（已從 Windows 登錄複製）。
   6. 按一下 **Apply**（套用），然後按一下 **OK**（確定）以儲存變更。

STEP 6 | （選用）從 Windows 登入畫面隱藏協力廠商認證提供者圖標。

1. 開啟 Windows 登錄，以找到您要隱藏的協力廠商認證提供者其全域唯一識別碼 (GUID)。
   1. 從命令提示中，輸入 `regedit` 命令以開啟 Windows 登錄編輯器。
   2. 前往下列 Windows 登錄位置以檢視目前安裝的認證提供者清單：

      `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion \Authentication\Credential Providers`。
   3. 複製所要隱藏認證提供者的完整 GUID 金鑰（GUID 的兩側要包括大括弧 — { 與 } ）。
2. 開啟本機群組原則編輯器以隱藏協力廠商認證提供者。
   1. 從命令提示中，輸入 `gpedit.msc` 命令以開啟本機群組原則編輯器。
   2. 選取 **Computer Configuration**（電腦組態）> **Administrative Templates**（管理範本）> **System**（系統）> **Logon**（登入）。
   3. 在 **Setting**（設定）下，按兩下 **Exclude credential providers**（排除認證提供者）以開啟排除認證提供者視窗。
   4. 將原則設定為 **Enabled**（已啟用）。
   5. 在 **Exclude the following credential providers**（排除下列認證提供者）下，輸入所要隱藏認證提供者的 GUID（已從 Windows 登錄複製）。

      若要隱藏多個認證提供者，請以逗號分隔各個 *GUID*。
   6. 按一下 **Apply**（套用），然後按一下 **OK**（確定）以儲存變更。

STEP 7 | 完成您的變更。

一旦變更完成，請重新啟動您的系統以使變更生效。

透過 *Windows* 安裝程式啟用協力廠商認證的 *SSO* 封裝

在 Windows 安裝程式 (Msiexec) 中使用下列選項可允許 SSO 在 Windows 7 端點上封裝協力廠商認證提供者。

- 封裝協力廠商認證，並在使用者登入時對使用者顯示原生圖標。使用者可按一下圖標，然後使用其原生 Windows 認證登入端點。透過單一登入，使用者可以對 Windows、GlobalProtect 及協力廠商認證提供者進行驗證。

  從 Windows 安裝程式 (Msiexec) 使用下列語法：

```
msiexec.exe /i GlobalProtect.msi WRAPCPGUID="{guid_value}" FILTERNONGPCP="yes"
```

在上述語法中，**FILTERNONGPCP** 參數會使用協力廠商認證篩選出登入系統的選項，藉此為使用者簡化驗證。

- 如果您想要讓使用者能夠選取使用協力廠商認證登入，請從 Windows 安裝程式 (Msiexec) 使用下列語法：

```
msiexec.exe /i GlobalProtect.msi WRAPCPGUID="{guid_value}" FILTERNONGPCP="no"
```

在上述語法中，**FILTERNONGPCP** 參數會篩選出協力廠商認證提供者的登入圖標，藉此僅顯示原生圖標，此參數設為 "**no**"。在此狀況中，當使用者登入 Windows 端點時，會對使用者顯示原生 Windows 圖標與協力廠商認證提供者圖標。

部署應用程式設定至 macOS 端點

使用 macOS 全域 Plist（屬性清單）檔案進行 GlobalProtect 應用程式自訂設定或部署指令碼至 macOS 端點。

- 在 macOS Plist 中部署應用程式設定
- 透過 macOS Plist 部署指令碼

在 *macOS Plist* 中部署應用程式設定

您可以在 macOS 全域 Plist（屬性清單）檔案中設定 GlobalProtect 應用程式自訂設定。這可讓您在 GlobalProtect 應用程式設定初次連線至 GlobalProtect 入口網站之前將其部署至 macOS 端點。

在 macOS 端點上，Plist 檔案位於 `/Library/Preferences` 或 `~/Library/Preferences` 中。波狀符號 (~) 表示位置位於目前使用者的主資料夾內。macOS 端點上的 GlobalProtect 應用程式會檢查是否有 GlobalProtect Plist 設定。如果該位置沒有 Plist，GlobalProtect 應用程式會在 `~/Library/Preferences` 中搜尋 Plist 設定。

除了使用 *macOS Plist* 來部署 *GlobalProtect* 應用程式設定外，您還可以允許 *GlobalProtect* 應用程式從端點收集特定的 *macOS Plist* 資訊。接著您可以監控資料，並將它新增至安全性規則中用作比對條件。您可根據安全性規則，強制執行符合某些所定義登錄設定的端點流量。此外，您可以設定自訂檢查來從端點收集應用程式與處理資料。

STEP 1 | 打開 GlobalProtect Plist 檔案，找到 GlobalProtect 應用程式自訂設定。

使用 Xcode 或替代 plist 編輯器來打開 plist 檔案：

`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`

然後前往：

`/Palo Alto Networks/GlobalProtect/Settings`

如果 `Settings` 字典不存在，則建立一個。將每個機碼新增至 `Settings`（設定）字典作為字串。

STEP 2 | 設定入口網站名稱。

如果不想讓一般使用者手動輸入入口網站位址（即使是初次連線），您可以透過 Plist 預先部署入口網站位址。在 `PanSetup` 字典中，設定 `Portal` 的項目。

STEP 3 | 將各種設定部署至 macOS 端點，包括 GlobalProtect 應用程式的連線方法。

檢視可自訂應用程式設定，查看您可使用 macOS plist 設定的完整機碼與值清單。

透過 *macOS Plist* 部署指令碼

當使用者首次連線至 GlobalProtect 閘道時，GlobalProtect 應用程式會下載設定檔並在 GlobalProtect macOS 屬性檔案內 (plist) 儲存應用程式設定。除了變更應用程式設定外，您可以在下列情況下使用 Plist 來部署指令碼：建立通道前後，或中斷通道連線之前。使用下列工作流程透過 Plist 部署指令碼至 macOS 端點。

端點支援讓您可以部署指令碼的 *macOS plist* 設定，該端點執行 *GlobalProtect* 應用程式 *2.3* 和更新的版本。

STEP 1 | （執行 Mac OS X 10.9 或更新 OS 的端點）排清設定快取。這可以防止 OS 在變更 plist 後使用快取偏好設定。

若要清除預設偏好設定快取，請從 macOS 終端執行 **killall cfprefsd** 命令。

STEP 2 | 打開 GlobalProtect plist 檔案，然後找到或建立與連線或中斷連線事件關聯的 GlobalProtect 字典。您可以新增設定的字典將決定 GlobalProtect 應用程式執行指令碼的時間。

使用 Xcode 或替代 plist 編輯器來打開 plist 檔案 (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`) 然後前往下列字典位置之一：

- `/PaloAlto Networks/GlobalProtect/Settings/pre-vpn-connect`
- `/Palo Alto Networks/GlobalProtect/Settings/post-vpn-connect`
- `/Palo Alto Networks/GlobalProtect/Settings/pre-vpn-disconnect`

如果 *`Settings`* 字典不存在，則建立一個。然後，在 *`Settings`* 中，為您想要執行指令碼的事件建立一個字典。

STEP 3 | 透過建立名稱為 **command** 的新字串，讓 GlobalProtect 應用程式能執行指令碼。

此處指定的值應參考您想要在端點上執行的命令介面指令碼（包括傳遞至指令碼的參數）。

如果 `command` 字串不存在，新增至字典並指定 **Value**（值）欄位內的指令碼和參數。例如：

```
$HOME\pre_vpn_connect.sh /Users/username username
```

支援環境變數。

最佳作法是，在命令中指定完整路徑。

STEP 4 | （選用）新增與命令相關的其他設定，包括管理員權限、指令碼逾時值、批次檔案的總和檢查碼值，以及命令無法成功執行時顯示的錯誤訊息。

建立或修改 plist 內的其他字串（`context`、`timeout`、`file`、`checksum` 和/或 `error-msg`）並輸入其對應值。如需其他資訊，請參閱可自訂應用程式設定。

STEP 5 | 儲存變更內容至 plist 檔案。

儲存 plist。

GlobalProtect 無用戶端 VPN

GlobalProtect 無用戶端 VPN 會向常見企業 Web 應用程式提供安全的遠端存取。使用者可從具有 SSL 功能的 Web 瀏覽器獲得安全存取的好處，而不必安裝 GlobalProtect 軟體。當您需要為合作夥伴或派遣員工啟用應用程式存取權時，以及要安全地啟用未受管理的資產（包括個人端點）時，此功能相當實用。您可以設定 GlobalProtect 入口網站登陸頁面來提供對以使用者與使用者群組為基礎的 Web 應用程式的存取，並允許 SAML 啟用之應用程式的單一登入。下列主題提供的資訊是說明如何對無用戶端 VPN 進行設定與疑難排解。

- 無用戶端 VPN 概要
- 支援的技術
- 設定無用戶端 VPN
- 對無用戶端 VPN 進行疑難排解

無用戶端 VPN 概要

當您設定 GlobalProtect 無用戶端 VPN，遠端使用者即可使用 Web 瀏覽器登入至 GlobalProtect portal 入口網站，並能啟用您為使用者發行的 Web 應用程式。根據使用者或使用者群組，您可以讓使用者存取供其使用的應用程式集，或讓使用者透過輸入自訂的應用程式 URL，來存取額外的公司應用程式。

使用者登入至入口網站後，可以查看已發行的應用程式頁面，有清單列出他們能使用的應用程式。您可以使用 GlobalProtect 入口網站上預設的應用程式登陸頁面，或為您的企業建立自訂登陸頁面。

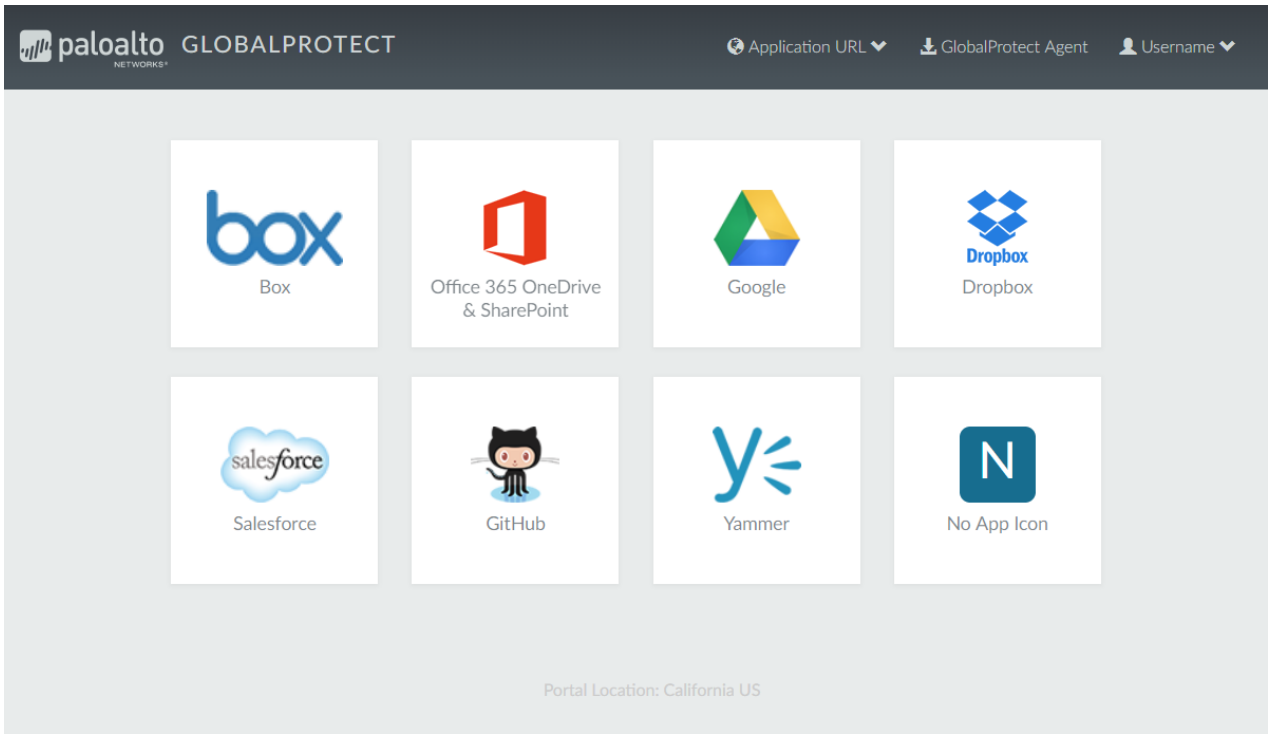


圖 3: 無用戶端 VPN 的應用程式登陸頁面

因為此頁面取代了預設的入口網站登陸頁面，此頁面會包含 GlobalProtect 應用程式下載頁面的連結。設定後，使用者可以選取 **Application URL**（應用程式 **URL**），並輸入 URL 來啟動額外、未發行的公司 Web 應用程式。

當您只設定一個 Web 應用程式（並關閉對未發行應用程式的存取權），而不是將使用者帶到已發行的應用程式頁面，則在使用者登入時，該應用程式就會自動啟動。如果您未設定 GlobalProtect 無用戶端 VPN，使用者登入至入口網站時，將會看見應用程式軟體下載頁面。

您在設定 GlobalProtect 無用戶端 VPN 時，需要安全性原則允許從 GlobalProtect 端點至安全性區域（與裝載應用程式登陸頁面的 GlobalProtect 入口網站關聯）的流量，並允許從 GlobalProtect 入口網站區域至安全性區域（其中裝載應用程式伺服器）以使用者為基礎的流量。您所定義的安全性原則，會控制哪些使用者具有權限能使用已發行的應用程式。

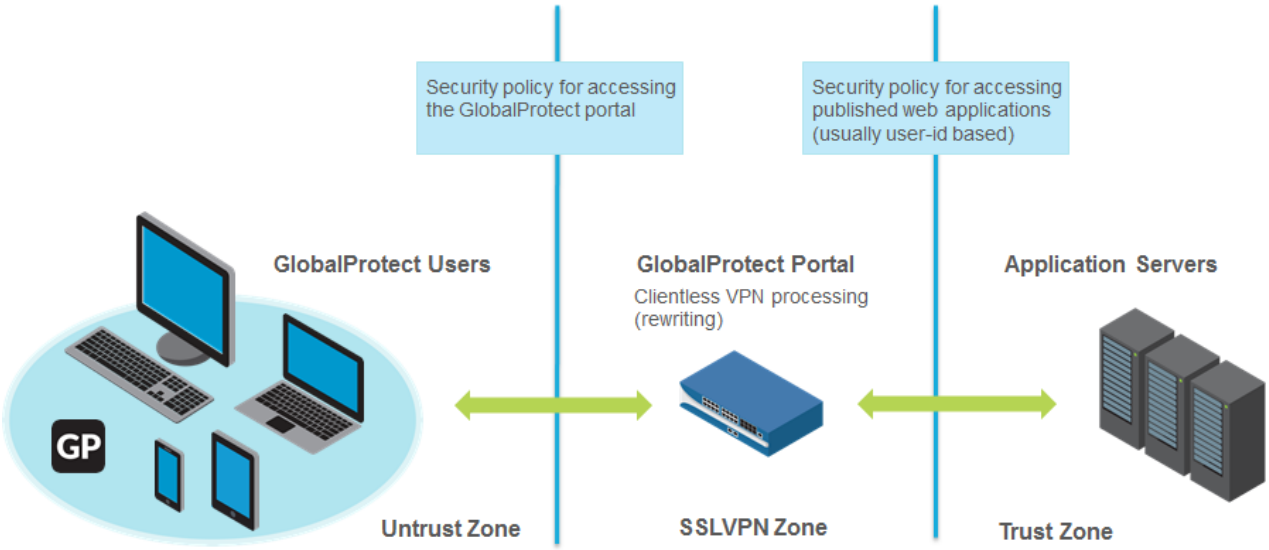


圖 4: 無用戶端 **VPN** 的區域和安全性原則

支援的技術

您現在可以將 GlobalProtect 入口網站設定為對一般企業 Web 應用程式提供安全的遠端存取。如需最佳結果，請確保您在控制的環境中徹底測試無用戶端 VPN 應用程式，再部署它們或讓其可供大量使用者使用。

技術	支援版本

Web 應用程式技術	• HTML
	• HTML5
	• HTML5-Web-Sockets
	• Javascript
	• 遠端桌面協議 (RDP)、VNC 或 SSH
	  • 虛擬桌面架構 (VDI) 和虛擬機 (VM) 環境，例如 Citrix XenApp 和 XenDesktop 或 VMWare Horizon 和 Vcenter，支援透過 HTML5 進行本機存取。您可透過無用戶端 VPN 將RDP、VNC 或 SSH 套用至這些機器，無需額外的協力廠商中介軟體。
	  • 在不包含對 HTML5 或無用戶端 VPN 支援的其他 Web 應用程式技術的本機支援的環境中，您可透過無用戶端 VPN 使用 HOBLink 或 Thinfinity 等協力廠商進行 RDP。
	• Adobe Flash—使用無用戶端 VPN，瀏覽器可提供使用 Adobe Flash、Microsoft Word 文件或 Adobe PDF 的內容。但是，無用戶端 VPN 無法重寫 Adobe Flash、Microsoft Word 文件或 Adobe PDF 中的 HTML URL 或連結，從而無法正確呈現內容。
	其他技術（例如 Microsoft Sliverlight 或 XML/XSLT）則不受支援。

作業系統	• Windows • macOS • iOS • Android • Chrome • Linux
支援的瀏覽器	• Chrome • Edge • Internet Explorer • Safari • Firefox

設定無用戶端 VPN

若要設定 GlobalProtect 無用戶端 VPN：

STEP 1 | 開始之前

- 從 GlobalProtect 入口網站在裝載無用戶端 VPN 的防火牆上安裝 GlobalProtect 訂閱。請參閱 啟動授權和訂閱。
- 安裝最新的 GlobalProtect 無用戶端 VPN 動態更新（參閱安裝內容與軟體更新）並為安裝新動態內容更新設定排程。建議的最佳做法是，始終為 GlobalProtect 無用戶端 VPN 安裝最新內容更新。

GlobalProtect Clientless VPN	Last checked: 2016/11/09 17:03:03 PST		Schedule: Every hour (Download and Install)			
58-11	panup-all-gp-58-11.candidate	GlobalProtectCli...	Full	75 KB	2016/11/07 18:57:21 PST	✔
58-10	panup-all-gp-58-10.candidate	GlobalProtectCli...	Full	74 KB	2016/10/25 17:51:17 PDT	✔ previously

- 最佳做法是，為裝載無用戶端 VPN 的 GlobalProtect 入口網站設定另外一個 FQDN。請勿使用與 PAN-OS Web 介面相同的 FQDN。
- 在標準 SSL 連接埠（TCP 連接埠 443）上裝載 GlobalProtect 入口網站。不支援非標準的連接埠。

STEP 2 | 設定使用 GlobalProtect 無用戶端 VPN 時可用的應用程式。在使用者登入（應用程式登陸頁面）時，GlobalProtect 入口網站會在使用者能看見的登陸頁面上顯示這些應用程式。

1. 選取 **Network**（網路）> **GlobalProtect** > **Clientless Apps**（無用戶端應用程式）並 **Add**（新增）一或多個應用程式。對於每個應用程式，指定下列設定：
   - **Name**（名稱）—應用程式的描述性名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
   - **Location**（位置）（針對多重虛擬系統模式下的防火牆）—可以在其中使用無用戶端 VPN 應用程式的虛擬系統 (vsys)。針對並未處於多重虛擬系統模式下的防火牆，**Location**（位置）欄位不會顯示。
   - **Application Home URL**（應用程式首頁 **URL**）—應用程式所在的 URL（最多 4095 個字元）。
   - **Application Description**（應用程式說明）（選用）—應用程式的說明（最多 255 個字元）。
   - **Application Icon**（應用程式圖示）（選用）—該圖示用於發行的應用程式頁面上以識別應用程式。您可以進行瀏覽以上載圖示。
2. 按一下 **OK**（確定）。

STEP 3 | （選用）建立群組來管理 Web 應用程式集。

如果您想管理多個應用程式集合，或根據使用者群組提供存取權，無用戶端應用程式群組相當實用。例如，G&A 團隊的財務應用程式或工程團隊的開發者應用程式。

1. 選取 **Network**（網路）> **GlobalProtect** > **Clientless App Groups**（無用戶端應用程式群組）。**Add**（新增）新的無用戶端 VPN 應用程式群組，並指定下列設定：
   - **Name**（名稱）—應用程式群組的描述性名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
   - **Location**（位置）（針對多重虛擬系統模式下的防火牆）—可以在其中使用無用戶端 VPN 應用程式的虛擬系統 (vsys)。針對並未處於多重虛擬系統模式下的防火牆，**Location**（位置）欄位不會顯示。

2. 在 **Applications**（應用程式）區段中，將應用程式 **Add**（新增）至群組。您可以從現存的無用戶端 VPN 應用程式清單中選取，或定義 **New Clientless App**（新的無用戶端應用程式）。
3. 按一下 **OK**（確定）。

STEP 4 | 設定 GlobalProtect 入口網站以提供無客戶端 VPN 服務。

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後選取現有的入口網站組態或 **Add**（新增）新的入口網站。請參閱 設定 GlobalProtect 入口網站存取權 。
2. 在 **Authentication**（驗證）頁籤中，您可以：
   - （選用）為無用戶端 VPN 建立指定的用戶端驗證。在此情況下，選取 **Browser**（瀏覽器）做為 **Client Authentication**（用戶端驗證）的 **OS**（作業系統）。
   - 使用現有的用戶端驗證。
3. 在 **Clientless**（無用戶端）> **General**（一般）下，選取 **Clientless VPN**（無用戶端 **VPN**）來啟用入口網站服務，並進行下列設定：
   - 針對裝載應用程式登陸頁面的 GlobalProtect 入口網站，指定 **Hostname**（主機名稱）（IP 位址或 FQDN）。此主機名稱用於重新編寫應用程式 URL。如需重新編寫 URL 的詳細資訊，請參閱步驟 8。

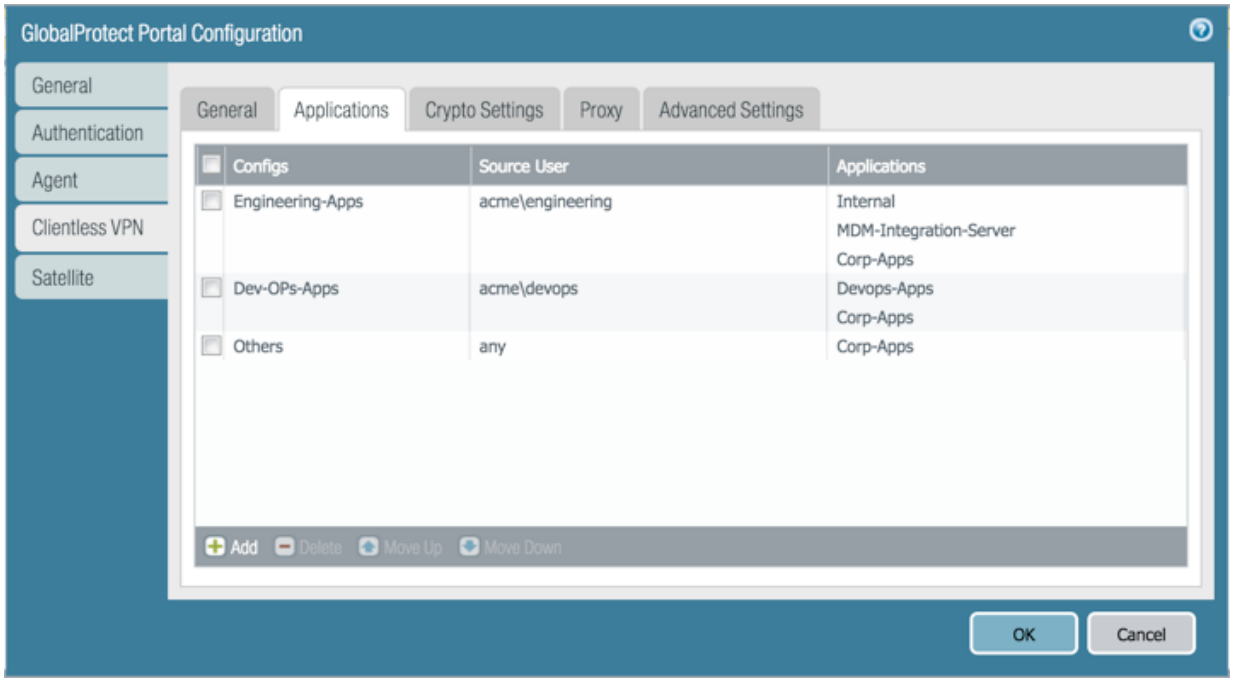
     如果您使用網路位址轉譯 *(NAT)* 來提供 *GlobalProtect* 入口網站的存取權，則您輸入的 *IP* 位址或 *FQDN* 必須符合（或解析為）*GlobalProtect* 入口網站的 *NAT IP* 位址（公用 *IP* 位址）。因為使用者無法在自訂的連接埠上存取 *GlobalProtect* 入口網站，所以在 *NAT* 之前的連接埠必須是 *TCP* 連接埠 *443*。

   - 指定 **Security Zone**（安全性區域）。此區域作為防火牆和應用程式之間的流量來源區域。針對此區域到應用程式區域所定義的安全性規則，可決定使用者能存取的應用程式。
   - 選取 **DNS Proxy** 伺服器或設定 **New DNS Proxy**（新的 **DNS Proxy**）。GlobalProtect 會使用此 Proxy 來解析應用程式名稱。請參閱 DNS Proxy 物件。
   - **Login Lifetime**（登入存留時間）—指定無用戶端 VPN 工作階段有效的時間長度上限（小時或分鐘）。工作階段的時間一般為 3 小時。小時數範圍為 1 至 24；分鐘數範圍為 60 至 1,440。工作階段的過期後，使用者就必須重新驗證並啟動新的無用戶端 VPN 工作階段。
   - **Inactivity Timeout**（無活動逾時）—指定無用戶端 VPN 工作階段可以閒置的時間長度（小時或分鐘）。無活動逾時一般為 30 分鐘。小時數範圍為 1-24；分鐘數範圍為 5 -1440。如果在指定的時間長度內使用者未曾活動過，使用者就必須重新驗證並啟動新的無用戶端 VPN 工作階段。
   - **Max User**（最大使用者數）—指定可同時登入至入口網站的最多使用者人數。如果未指定數值，則會假設為端點容量。如果端點容量未知，則會假設容量為 50 名使用者。在達到使用者數目上限時，其他無用戶端 VPN 使用者就無法登入到入口網站。

STEP 5 | 將使用者與使用者群組對應至應用程式。

此對應可控制使用者或使用者群組，能從 GlobalProtect 無用戶端 VPN 工作階段啟動哪些應用程式。

GlobalProtect 入口網站會使用您指定的使用者/使用者群組設定，來決定要將哪個設定傳遞給所連線的 GlobalProtect 無用戶端 VPN 使用者。因為入口網站會從清單頂端開始尋找符合項，如果您擁有多個設定，請必須確保這些設定排序正確，並對應至所需的應用程式。入口網站只要找到符合項目，便會將相關設定傳遞給 GlobalProtect 無用戶端 VPN 使用者。



將應用程式發行至使用者/使用者群組，或允許使用者/使用者群組啟動未發行的應用程式，不代表可以存取那些應用程式。您使用安全性原則控制對應用程式（不論是否已發行）的存取。

您必須先設定群組對應（*Device*（裝置）> *User Identification*（使用者識別）> *Group Mapping Settings*（群組對應設定）），才能選取群組。

1. 在 **Applications**（應用程式）頁籤上，**Add**（新增）**Applications to User Mapping**（應用程式至使用者對應）以便讓使用者與所發行的應用程式相符。
   - **Name**（名稱）—輸入對應的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
   - **Display application URL address bar**（顯示應用程式 **URL** 位址列）—選取此選項來顯示應用程式 URL 位址列，使用者可由此啟動未發行至應用程式登陸頁面上的應用程式。啟用後，使用者可選取 **Application URL**（應用程式 **URL**）
2. 指定 **Source Users**（來源使用者）。您可 **Add**（新增）目前應用程式組態所套用的個別使用者或使用者群組。這些使用者有權使用 GlobalProtect 無用戶端 VPN 來啟動所設定的應用程式。除了使用者與群組，您還可指定何時要將這些設定套用於使用者或群組：
   - **any**（任何）—套用於所有使用者的應用程式組態（無需 **Add**（新增）使用者或使用者群組）。
   - **select**（選取）—僅套用於您 **Add**（新增）至此清單的使用者與使用者群組的應用程式組態。
3. 將個別的應用程式或應用程式群組 **Add**（新增）至對應。您納入設定中的 **Source Users**（來源使用者）可以使用 GlobalProtect 無用戶端 VPN 來連結至您所新增的應用程式。

STEP 6 | 指定無用戶端 VPN 工作階段的安全性設定。

1. 在 **Crypto Settings**（加密設定）頁籤上，請針對防火牆與已發行之應用程式之間的 SSL 工作階段，指定驗證和加密演算法。
   - **Protocol Versions**（通訊協定版本）—選取所需的最低和最高 TLS/SSL 版本。TLS 版本越高，連線就越安全。選項包括 **SSLv3**、**TLSv1.0**、**TLSv1.1** 或 **TLSv1.2**。

- **Key Exchange Algorithms**（金鑰交換演算法）—選取金鑰交換所支援的演算法類型。選項包括：**RSA**、Diffie-Hellman (**DHE**) 或 Elliptic Curve Ephemeral Diffie-Hellman (**ECDHE**)。
- **Encryption Algorithms**（加密演算法）—選取所支援的加密演算法。我們建議使用 **AES128** 或更高版本。
- **Authentication Algorithms**（驗證演算法）—選取所支援的驗證演算法。選項包括：**MD5**、**SHA1**、**SHA256** 或 **SHA384**。建議使用 **SHA256** 或更高級的演算法。

2. 在應用程式出示伺服器憑證發生下列問題時，請選取要採取的動作：

- **Block sessions with expired certificate**（封鎖憑證過期的工作階段）—如果伺服器憑證已到期，則封鎖應用程式的存取。
- **Block sessions with expired certificate**（封鎖簽發者不受信任的工作階段）—如果伺服器憑證是由不受信任的憑證授權單位所簽發，則封鎖應用程式的存取。
- **Block sessions with unknown certificate status**（封鎖包含未知憑證狀態的工作階段）—如果 OCSP 或 CRL 服務所傳回的憑證撤銷狀態未知，則封鎖應用程式的存取。
- **Block sessions on certificate status check timeout**（在憑證狀態檢查逾時後封鎖工作階段）—如果在憑證狀態檢查逾時後才收到憑證狀態服務所傳來的回應，則封鎖應用程式的存取。

STEP 7 | （選用）指定一或多個 Proxy 伺服器設定以存取應用程式。

僅支援對 *Proxy* 基本驗證（使用者名稱和密碼）。

如果使用者需要透過 Proxy 伺服器連線到應用程式，請指定 **Proxy Server**（**Proxy** 伺服器）。您可以新增多個 Proxy 伺服器設定，每個網域集一個。

- **Name**（名稱）—用來識別 Proxy 伺服器的標籤（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
- **Domains**（網域）—新增由 Proxy 伺服器所提供的網域。您可以在網域名稱的開頭使用萬用字元 (*) 來指出多個網域。
- **Use Proxy**（使用 **Proxy**）—選取以指派要提供網域存取權的 Proxy 伺服器。
- **Server**（伺服器）—指定 Proxy 伺服器的 IP 位址或主機名稱。
- **Port**（連接埠）—指定與 Proxy 伺服器通訊的連接埠。
- **User**（使用者）、**Password**（密碼）—指定要登入 Proxy 伺服器所需提供的 **User**（使用者）和 **Password**（密碼）憑證。再次指定密碼以進行驗證。

STEP 8 | （選用）指定對應用程式網域的任何特殊處理。

無用戶端 VPN 會作為反向 Proxy 並且會修改已發行之 Web 應用程式所傳回的 Web 頁面。它會重新編寫所有 URL 並對遠端使用者出示重新編寫的頁面，如此在遠端使用者存取其中任何一個 URL 時，要求會經過 GlobalProtect 入口網站。

在某些情況下，應用程式可能會有不需透過入口網站存取的頁面（例如，應用程式可能包含來自 yahoo.finance.com 的金融指數顯示板）。您可以排除這些頁面。

在 **Advanced Settings**（進階設定）頁籤上，**Add**（新增）網域名稱、主機名稱或 IP 位址到 **Rewrite Exclude Domain List**（重新編寫排除網域清單）。這些網域已排除在重新編寫規則之外，且不能重新編寫。

主機名稱和網域名稱不支援路徑。主機名稱和網域名稱的萬用字元 (*) 只能出現在名稱開頭處（例如，*.etrade.com）。

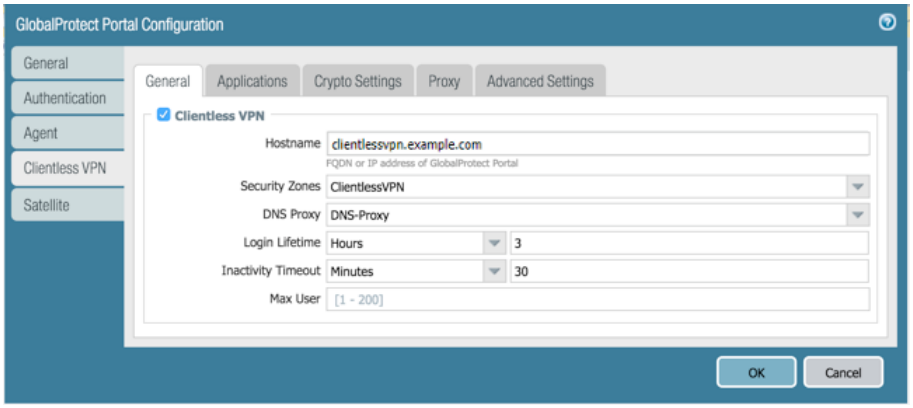
STEP 9 | 儲存入口網站組態。

1. 按兩下 **OK**（確定）。
2. **Commit**（提交）您的變更。

STEP 10 | 設定安全性原則規則讓使用者能存取已發行的應用程式。

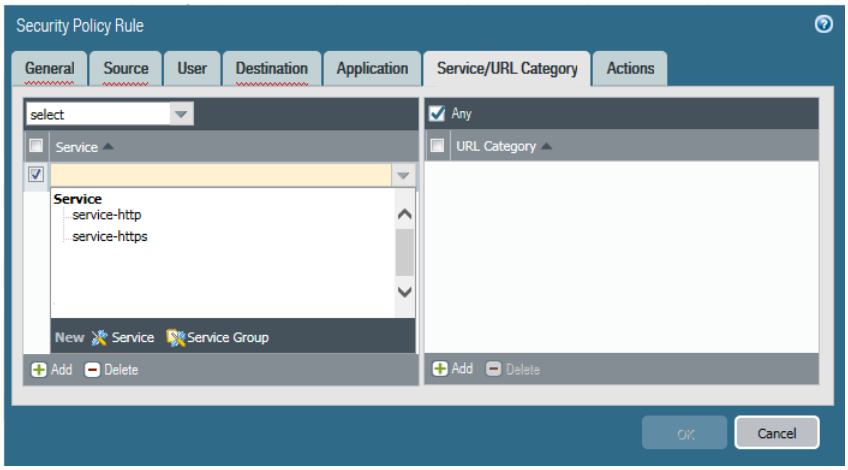
針對下列情況您會需要安全性原則：

- 讓使用者可從網際網路連線至裝載無用戶端 VPN 的 GlobalProtect 入口網站。這是從非信任或網際網路區域到裝載無用戶端 VPN 入口網站區域的流量。
- 讓無用戶端 VPN 使用者可連線到網際網路。這是從無用戶端 VPN 區域到非信任或網際網路區域的流量。



- 讓無用戶端 VPN 使用者可連線到公司資源。這是從無用戶端 VPN 區域到信任或公司區域的流量。您所定義的安全性原則，會控制哪些使用者具有權限能使用已發行的應用程式。請確保為裝載已發行應用程式伺服器的安全性區域，設定 **Enable User Identification**（啟用使用者識別）。

  依預設，**Security Policy Rule**（安全性原則規則）中的 **Service/URL**（服務/**URL**）設為 **application-default**（應用程式預設）。在此預設的設定下，無用戶端 VPN 不會對 HTTPS 網站起作用。變更 **Service/URL**（服務/**URL**）來包含 **service-http**（服務 **http**）與 **service-https**（服務 **https**）。



- 當您設定 Proxy 伺服器以存取無用戶端 VPN 時，請確保將 Proxy IP 位址和連接埠包含在安全性原則的定義中。透過 Proxy 伺服器存取應用程式時，只會套用為 Proxy IP 位址和連接埠定義的安全性原則。

STEP 11 | （選用）若要設定無用戶端 VPN 入口網站登陸頁面，以顯示無用戶端 VPN 使用者連線之入口網站的位置，請指定設定入口網站之防火牆的實體位置。

當無用戶端 VPN 用者遇到異常行為時（例如網路效能低），可向支援或服務台專業人員提供此位置資訊，以取得疑難排解協助。其還可使用此位置資訊來確定自己與入口網站的距離。根據此距離，其可評估是否需要切換至較近的入口網站。

如果您未指定入口網站位置，無用戶端 *VPN* 入口網站登陸頁面將顯示空白位置欄位。

- 在 **CLI** 中—使用下列 CLI 命令指定設定入口網站之防火牆的實體位置：

```
<username@hostname> set deviceconfig setting global-protect
 location <location>
```

- 在 **XML API** 中—使用下列 XML API 指定設定入口網站之防火牆的實體位置：
  - 裝置 —設定入口網站之防火牆的名稱
  - 位置 —設定入口網站之防火牆的位置

```
curl -k -F file=@filename.txt -g 'https://<firewall>/api/?
key=<apikey>&type=config&action=set&xpath=/config/devices/
entry[@name='<device-name>']/deviceconfig/setting/global-
protect&element=<location>location-string</location>'
```

無用戶端 *VPN* 流量的來源 *IP* 位址（如應用程式所示）為進入介面（入口網站可透過此介面連線到應用程式）的 *IP* 位址或當來源 *NAT* 正在使用時轉譯的 *IP* 位址。

對無用戶端 VPN 進行疑難排解

因為此功能包含動態重寫 HTML 應用程式，某些應用程式的 HTML 內容可能無法正確重寫而且會損壞應用程式。如果問題發生，請使用下表的命令來協助您辨識可能的原因：

表 6: 表格：重寫引擎統計資料

動作	命令
CLI 命令	
列出正在使用的無用戶端 VPN 動態內容的版本 您也可以從 **Device**（裝置）> **Dynamic Updates**（動態更新）> **GlobalProtect Clientless VPN**（**GlobalProtect** 無用戶端 **VPN**）檢視動態更新版本。	**show system setting ssl-decrypt memory** proxy uses shared allocator SSL certificate cache:目前項目：1 Allocated 1, Freed 0 Current CRE (61-62) :3456 KB (Actual 3343 KB) Last CRE (60-47) :3328 KB (Actual 3283 KB) 在此範例中，目前動態更新為版本 61-62，而最新的安裝動態更新為版本 60-47。
列出無用戶端 VPN 作用中（目前）使用者	**show global-protect-portal current-user portal GPClientlessPortal filter-user all-users** GlobalProtect Portal :GPClientlessPortal Vsys-Id :1 User : paloaltonetworks.com\johndoe Session-id :1SU2vrPIDfdopGf-7gahMTCiX8PuL0S0 Client-IP :5.5.5.5 Inactivity Timeout :1800 Seconds before inactivity timeout :1750 Login Lifetime :10800 Seconds before login lifetime :10748 Total number of user sessions:1
顯示 DNS 解析結果 對於判斷是否有 DNS 問題時此方法可能很有用。如果有 DNS 問題，您會注意到對在 CLI 輸出中無法解析的 FQDN 的查詢。	**show system setting ssl-decrypt dns-cache** Total DNS cache entries:89 Site IP Expire(secs) Interface bugzilla.panw.local 10.0.2.15 querying 0 www.google.com 216.58.216.4 Expired 0 stats.g.doubleclick.net 74.125.199.154 Expired 0
顯示儲存的所有無用戶端 VPN 使用者工作階段與 cookie	**show system setting ssl-decrypt gp-cookie-cache** User: johndoe, Session-id:1SU2vrPIDfdopGf-7gahMTCiX8PuL0S0, Client-ip:199.167.55.50
顯示重寫統計資料 對於辨識無用戶端 VPN 重寫引擎的健康狀態很有用。 請參閱 表格：重寫引擎統計資料 會說明重寫統	**show system setting ssl-decrypt rewrite-stats** Rewrite Statistics initiate_connection :11938 setup_connection :11909 session_notify_mismatch :1 reuse_connection :37 file_end :4719 packet :174257 packet_mismatch_session :1 peer_queue_update_rcvd :167305 peer_queue_update_sent :167305

動作	命令
計資料與其意義或目的之資訊。	peer_queue_update_rcvd_failure:66 setup_connection_r :11910 packet_mismatch_session_r :22 pkt_no_dest :23 cookie_suspend :2826 cookie_resume :2826 decompress :26 decompress_freed :26 dns_resolve_timeout :27 stop_openend_response :43 received_fin_for_pending_req :26 Destination Statistics To mp :4015 To site :12018 To dp :17276 Return Codes Statistics ABORT :18 RESET :30 PROTOCOL_UNSUPPORTED :7 DEST_UNKNOWN :10 CODE_DONE :52656 DATA_GONE :120359 SWITCH_PARSER :48 INSERT_PARSER :591 SUSPEND :2826 Total Rewrite Bytes :611111955 Total Rewrite Useconds :6902825 Total Rewrite Calls :176545
偵錯命令	
對在無用戶端 VPN 入口網站執行的防火牆上的日誌啟用偵錯	**debug dataplane packet-diag set log feature ssl all** **debug dataplane packet-diag set log feature misc all** **debug dataplane packet-diag set log feature proxy all** **debug dataplane packet-diag set log feature flow basic** **debug dataplane packet-diag set log on**
在無用戶端 VPN 入口網站執行的防火牆上啟用封包擷取	**debug dataplane packet-diag set capture username *<portal-username>*** **debug dataplane packet-diag set capture stage clientless-vpn-client file *<clientless-vpn-client-file>*** **debug dataplane packet-diag set capture stage clientless-vpn-server file *<clientless-vpn-server-file>*** **debug dataplane packet-diag set capture stage firewall file *<firewall-file>*** **debug dataplane packet-diag set capture stage receive file *<receive-file>*** **debug dataplane packet-diag set capture stage transmit file *<transmit-file>*** **debug dataplane packet-diag set capture on** 當您執行封包擷取命令時，一般使用者登入至無用戶端 *VPN* 入口網站後會出現同意頁面，告訴他們使用者工作階段期間擷取的封包將包含未加密（明文）資料。如果使用者同意此封包擷取工作階段，則可移至應用程式登陸頁面，開始擷取封包。如果使用者不同意此封包擷取工作階段，其將登出無用戶端 *VPN* 入口網站，且必須聯絡管理員以繼續進行常規使用者工作階段（不擷取封包）。 如果您對進行中的使用者工作階段執行封包擷取命令，這些使用者將自動登出無用戶端 *VPN* 入口網站，且必須重新登入才能接受或拒絕封包擷取工作階段。
顯示封包擷取檔案	**debug dataplane packet-diag show setting** --- Packet diagnosis setting: --- Packet filter Enabled: no Match pre-parsed packet: no ---

動作	命令
	Logging Enabled: no Log-throttle: no Sync-log-by-ticks: yes Features:Counters: --- Packet capture Enabled: yes Snaplen:0 Username: test1 Stage clientless-vpn-client: file client.pcap Captured: packets - 3558 bytes - 11366322 Maximum: packets - 0 bytes - 0 Stage clientless-vpn-server: file server.pcap Captured: packets - 1779 bytes - 5651923 Maximum: packets - 0 bytes - 0 ---
匯出封包擷取檔案至安全複製 (SCP) 伺服器	**scp export filter-pcap** + remote-port SSH port number on remote host + source-ip Set source address to specified interface address * from from * to Destination (username@host:path) **scp export filter-pcap from *<source-file>* to *<scp-server>* Destination (username@host:path)**

表 **7:** 表格：重寫引擎統計資料

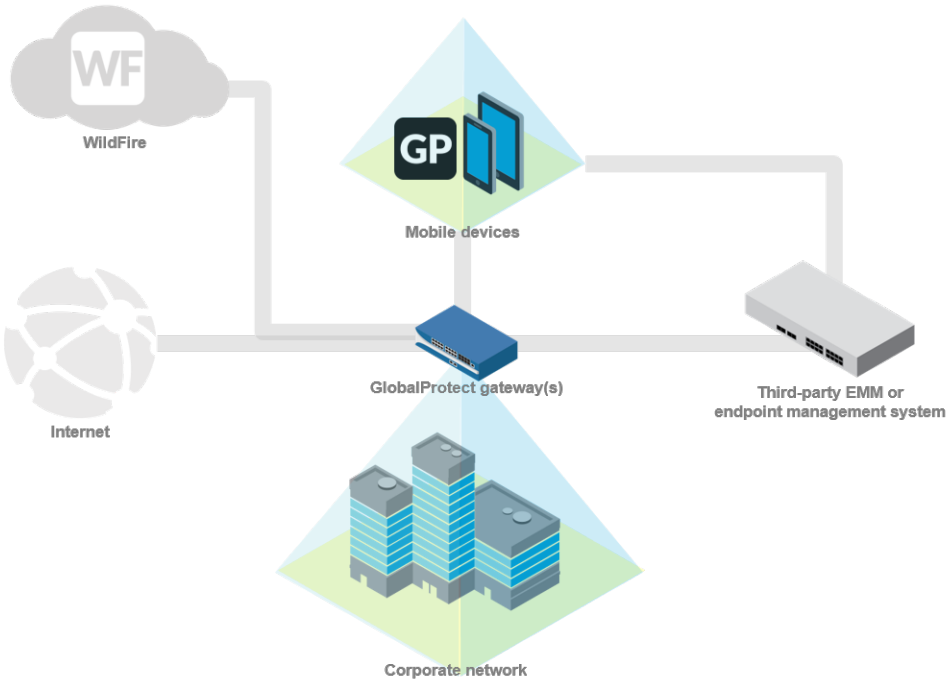
統計資料	說明
initiate_connection_failure	連線起始無法連至後端主機
setup_connection_failure	連線設定失敗
setup_connection_duplicate	複製對等工作階段存在
session_notify_mismatch	最有效的工作階段
packet_mismatch_session	無法尋找送入封包的工作階段
peer_queue_update_rcvd_failure	當封包更新由對等所接收時工作階段是無效的
peer_queue_update_sent_failure	無法將封包更新傳送至對等或無法將封包佇列長度更新傳送至對等
exceed_pkt_queue_limit	太多封包在佇列中
proxy_connection_failure	Proxy 連線失敗
setup_connection_r	將對等工作階段安裝至應用程式伺服器。此值應與 **initiate_connection** 和 **setup_connection** 的值相符。
setup_connection_duplicate_r	Duplicate sessions already in proxy
setup_connection_failure_r	無法設定對等工作階段
session_notify_mismatch_r	找不到對等工作階段
packet_mismatch_session_r	嘗試取得封包時找不到對等工作階段

統計資料	說明
exceed_pkt_queue_limit_r	保留太多封包
unknown_dest	無法找到目的地主機
pkt_no_dest	沒有此封包中目的地
cookie_suspend	暫止工作階段以擷取 cookie
cookie_resume	自具更新的 cookie 的 MP 中接收回應。此值一般會與 cookie_suspend 值相符。
decompress_failure	無法解壓縮
memory_alloc_failure	無法配置記憶體
wait_for_dns_resolve	暫止工作階段以解析 DNS 要求
dns_resolve_reschedule	因無回應（逾時前重試）而重新排定 DNS
dns_resolve_timeout	NDS 要求逾時
setup_site_conn_failure	無法將連線設定至網站 (Proxy、DNS)
site_dns_invalid	DNS 解析失敗
multiple_multipart	已處理多部位的內容類型
site_from_referer	自轉介中接收後端主機此會指示從快閃或無用戶端 VPN 沒有重寫的其他內容中失敗的重寫連結。
received_fin_for_pending_req	自伺服器接受 FIN 以擱置來自用戶端的要求
unmatched_http_state	未預期的 HTTP 內容此可指示剖析 http 標頭或內文的問題。

行動裝置管理

行動裝置管理概要

隨著行動端點的功能變得更加強大，一般使用者越來越依賴於使用這些裝置執行業務工作。但是，這些端點在存取貴公司網路的同時，也會連線至網際網路，使裝置暴露於威脅與漏洞風險之下。



行動裝置管理 (MDM) 系統或企業行動管理 (EMM) 系統透過讓您自動部署企業帳戶組態和 VPN 設定至相符的端點，簡化行動端點的管理。您也可以透過與已被危害的端點互動的方式，使用您的行動裝置管理系統修復安全性漏洞。這不僅能夠保護企業資料，還能夠保護一般使用者的資料。例如，如果一般使用者丟失端點，您可以從行動裝置管理系統遠端鎖定端點，甚至（徹底或選擇性地）抹除端點。

除了行動裝置管理系統可提供的帳戶和遠端裝置管理功能外，當與您的現有 GlobalProtect™ VPN 架構整合後，您可以使用端點報告的主機資訊，對透過 GlobalProtect 閘道存取應用程式的行為採取安全原則。您也可以監控 Palo Alto 新世代防火牆內建的工具，監控行動端點流量。

GlobalProtect 與 MDM 或 EMM 系統整合

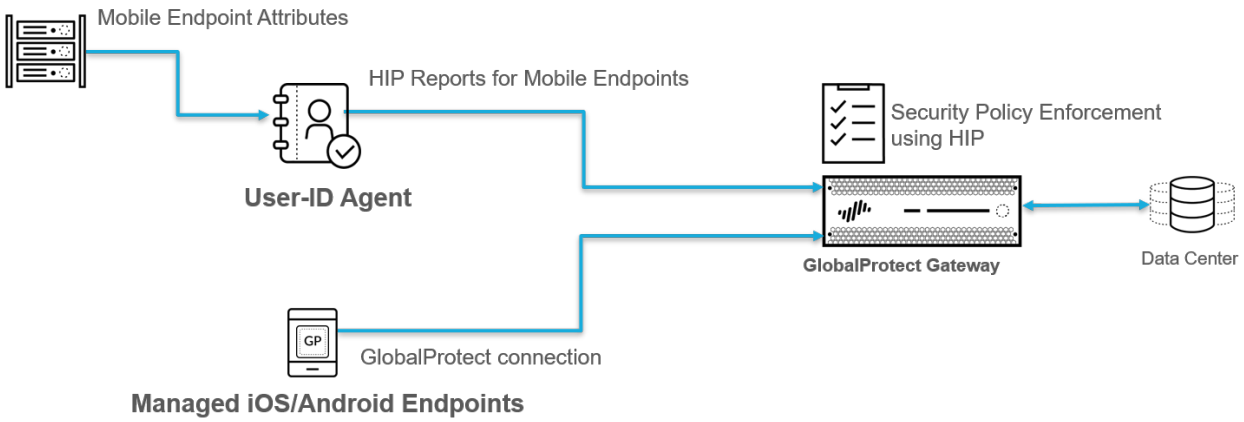
您可透過下列方法之一將 GlobalProtect 部署與 MDM 或 EMM 系統整合：

防火牆與 MDM 或 EMM 系統整合（僅適用於 AirWatch）

您可設定 Windows User-ID 代理程式以與 AirWatch MDM 伺服器通訊，以便從連線端點收集主機資訊。User-ID 代理程式將此主機資訊作為 HIP 報告的一部分傳送至 GlobalProtect 閘道，用於執行以 HIP 為基礎的原則。

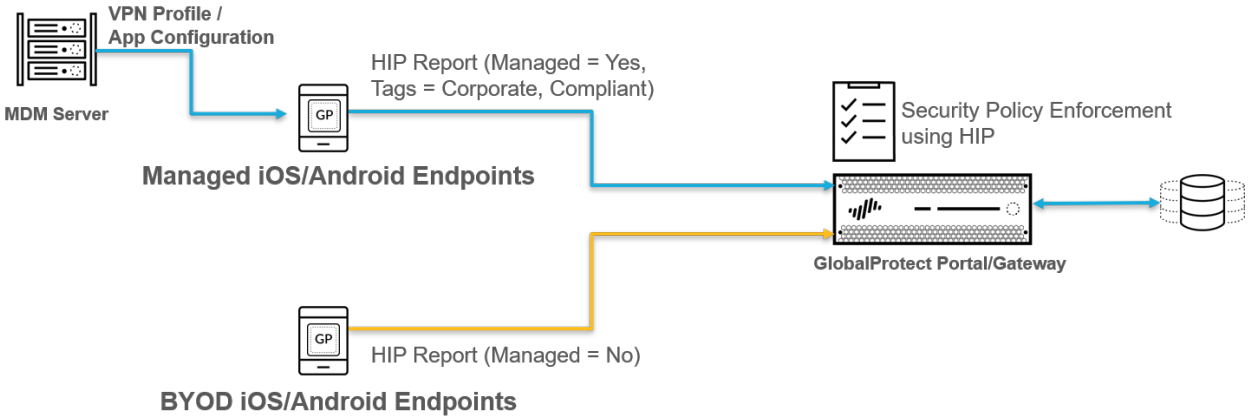
PAN-OS 8.0 及更新版本支援防火牆整合。

僅 *VMware AirWatch* 支援防火牆整合。



GlobalProtect 應用程式與 MDM 或 EMM 系統整合

從版本 5.0 開始，適用於 iOS 和 Android 端點的 GlobalProtect 應用程式可以從 MDM 系統取得廠商資料屬性和標籤。對於 iOS 端點，MDM 系統會將這些屬性作為 VPN 設定檔的一部分傳送至 GlobalProtect 應用程式。對於 Android 端點，MDM 系統將作為應用程式限制組態的一部分傳送這些屬性。然後，GlobalProtect 應用程式可以將這些屬性與標籤作為 HIP 報告的一部分傳送至 GlobalProtect 閘道，用於執行以 HIP 為基礎的原則。



GlobalProtect 應用程式整合適用於 *VMware AirWatch*、*MobileIron* 及 *Microsoft Intune*。但是，任何支援 *VPN* 設定檔中廠商資料屬性的 *MDM* 或 *EMM* 系統也支援此整合方法。

下表說明了支援的廠商資料屬性：

MDM 屬性	HIP 報告屬性	HIP 報告類別	說明
mobile_id	**主機 ID**	**總言**	端點的唯一裝置識別碼 (UDID)。
受管理	受管理	總言	此值表示端點是否受管理。如果此值為 **Yes**（是），表示端點受管理。如果此值為 **No**（否），表示端點不受管理。
合規	頁籤	行動裝置	合規狀態表示端點是否符合您定義的 MDM 合規原則（例如，**Compliant**（合規））。此值附加至 HIP 報告中的 **Tag**（標籤）屬性。
擁有權	頁籤	行動裝置	端點的擁有權類別（例如，**Employee Owned**（員工擁有））。此值附加至 HIP 報告中的 **Tag**（標籤）屬性。
頁籤	頁籤	行動裝置	與其他以 MDM 為基礎的屬性進行比對之標籤。

設定 MDM 與 GlobalProtect 整合

若要設定 MDM 與 GlobalProtect 整合，請使用下列工作流程：

STEP 1 | 設定 GlobalProtect 架構

1. 為 GlobalProtect 建立介面與區域.
2. 在 GlobalProtect 元件之間啟用 SSL.
3. 設定 GlobalProtect 使用者驗證請參閱 關於 GlobalProtect 使用者驗證。
4. 啟用群組對應.
5. 設定 GlobalProtect 閘道.
6. 為各運行閘道的防火牆啟動授權，其閘道支援行動端點上的 GlobalProtect。
7. 設定 GlobalProtect 入口網站存取權.

STEP 2 | 設定行動裝置管理系統，並確定是否僅支援公司發出的端點或支援公司和個人端點。

查看您的行動裝置管理 (MDM) 系統或企業行動管理 (EMM) 系統說明。

STEP 3 | 獲得行動端點的 GlobalProtect 應用程式。

- 應用程式商店—下載及安裝 GlobalProtect 行動應用程式
- 支援的行動裝置管理系統—部署 GlobalProtect 行動應用程式
- 其他協力廠商行動裝置管理系統—請參閱來自您廠商的部署應用程式至管理端點的說明。

STEP 4 | 設定 MDM 整合。

使用下列其中一個方法設定 MDM 整合：

- 防火牆與 MDM 或 EMM 系統整合：
  - 設定 Windows 的 User-ID 代理程式以收集主機資訊
- GlobalProtect 應用程式與 MDM 或 EMM 系統整合：
  - 透過符合資格的協力廠商 MDM 管理 GlobalProtect 應用程式
  - 透過其他協力廠商 MDM 管理 GlobalProtect 應用程式

STEP 5 | 透過主機資訊，設定目標行動端點的原則。

設定以 HIP 為基礎的原則強制執行 對於受管理的端點。

透過符合資格的協力廠商 MDM 管理 GlobalProtect 應用程式

有關如何使用符合資格的協力廠商 MDM 系統部署、設定和管理 GlobalProtect 應用程式的資訊，請參閱以下幾節：

- 符合資格的 MDM 廠商
- 部署 GlobalProtect 行動應用程式
- 一直開啟 VPN 設定
- 使用者啟動遠端存取 VPN 組態
- Per-App VPN 組態
- 啟用應用程式掃描與 WildFire 的整合
- 在適用于 macOS 端點的 GlobalProtect 應用程式上抑制通知

若您未使用 符合資格的協力廠商 MDM 系統，您可 透過其他協力廠商 MDM 管理 GlobalProtect 應用程式。

符合資格的 *MDM* 廠商

下表列出了符合資格的 MDM 廠商，以便您用於根據作業系統設定、部署和管理 GlobalProtect 應用程式。A – 表示此作業系統不被支援。

如果您要使用不符合資格的 MDM 廠商，透過其他協力廠商 MDM 管理 GlobalProtect 應用程式

支援的 MDM 廠商	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
AirWatch	✓（僅限 Per-App VPN）	✓	—	—	✓	—	—
Microsoft Intune	✓（一直開啟、無端存取與 僅限 Per-App VPN）	✓	—	—	✓（僅限一直開啟與 Per-App VPN）	—	—
MobileIron	✓（僅限一直開啟 VPN）	✓	—	—	—	—	—
Google 管理控制台	✓（適用於 Chromebook 支援的 Android 應用程式部署）；僅限應用程式部署）	—	✓（僅限應用程式部署）	—	—	—	—

> 您僅可使用 *Google* 管理控制台部署 *GlobalProtect* 應用程式；您無法使用此控制台設定 *VPN* 組態。您必須先透過 GlobalProtect 入口網站設定 *VPN* 組態，然後才能使用 *Google* 管理控制台部署應用程式。

部署 *GlobalProtect* 行動應用程式

GlobalProtect 應用程式提供一種簡單的方式來將企業安全原則向外延伸到行動端點。對於執行 GlobalProtect 應用程式的其他遠端端點而言，行動應用程式會提供在 IPsec 或 SSL VPN 通道上對於您企業網路的安全存取。應用程式將會連線至距離一般使用者目前位置最近的閘道。此外，與行動端點之間的來往

流量也會自動受限於與您公司網路上其他端點相同的安全原則強制執行。應用程式還會收集有關主機設定的資訊，並可以將此資訊用於強化的 HIP 式安全原則強制執行。

有兩種主要方法可安裝 GlobalProtect 應用程式：直接從您端點的應用程式商店安裝應用程式（請參見下載與安裝 GlobalProtect 行動應用程式）；或從行動裝置管理系統（如 AirWatch）部署並以透明方式推送應用程式至您的被管理端點。

- 透過 AirWatch 部署 GlobalProtect 行動應用程式。
- 透過 AirWatch 在受管理的 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式
- 透過 Microsoft Intune 部署 GlobalProtect 行動應用程式
- 透過 MobileIron 部署 GlobalProtect 行動應用程式
- 透過 Google 管理控制台在受管理的 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式

透過 AirWatch 部署 GlobalProtect 行動應用程式。

您可以部署 GlobalProtect 應用程式至被管理的端點，該端點已向 AirWatch 註冊。執行 iOS 或 Android 的端點必須下載 AirWatch 代理程式以向 AirWatch MDM 註冊。Windows 10 端點無需 AirWatch 代理程式，但需要您設定端點上的註冊。在部署應用程式後，設定並部署 VPN 設定檔以自動為一般使用者設定 GlobalProtect 應用程式。

如果要在受管理的 *Chromebook* 上執行適用於 *Android* 的 *GlobalProtect* 應用程式，可以 透過 AirWatch 在受管理的 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式。

STEP 1 | 在您開始前，確保您要部署 GlobalProtect 應用程式的端點已向 AirWatch 註冊：

- **Android 和 iOS**—下載 AirWatch 代理程式並遵照提示以註冊。
- **Windows Phone 和 Windows 10 UWP**—設定 Windows 10 UWP 端點以向 AirWatch 註冊（來自端點，選取 **Settings**（設定）> **Accounts**（帳戶）> **Work access**（工作存取）> **Connect**（連線））。

STEP 2 | 從 AirWatch，選取 **APPS & BOOKS**（應用程式和書本）> **Public**（公用）> **Add Application**（新增應用程式）。

STEP 3 | 選取管理此應用程式的組織群組。

STEP 4 | 選取 **Platform**（平台）（**Apple iOS**、**Android** 或 **Windows Phone**）。

STEP 5 | 在端點應用程式商店中搜尋 GlobalProtect 應用程式，或輸入 GlobalProtect 應用程式頁面的下列 URL 之一：

- **Apple iOS**—https://itunes.apple.com/us/app/globalprotect/id592489989?mt=8&uo=4
- **Android**—https://play.google.com/store/apps/details?id=com.paloaltonetworks.globalprotect
- **Windows Phone**—https://www.microsoft.com/en-us/p/globalprotect/9nblggh6bzl3

STEP 6 | 按一下 **Next**（下一步）。如果您在端點應用程式商店中搜尋應用程式，您還必須從搜尋結果清單中 **Select**（選取）應用程式。

如果您搜尋 *Android* 的 *GlobalProtect* 應用程式，但未在清單中看到該應用程式，請聯絡您的 *Android for Work* 管理員，以新增 *GlobalProtect* 至核准的公司應用程式清單或在 *Google Play Store* 中使用應用程式 *URL*。

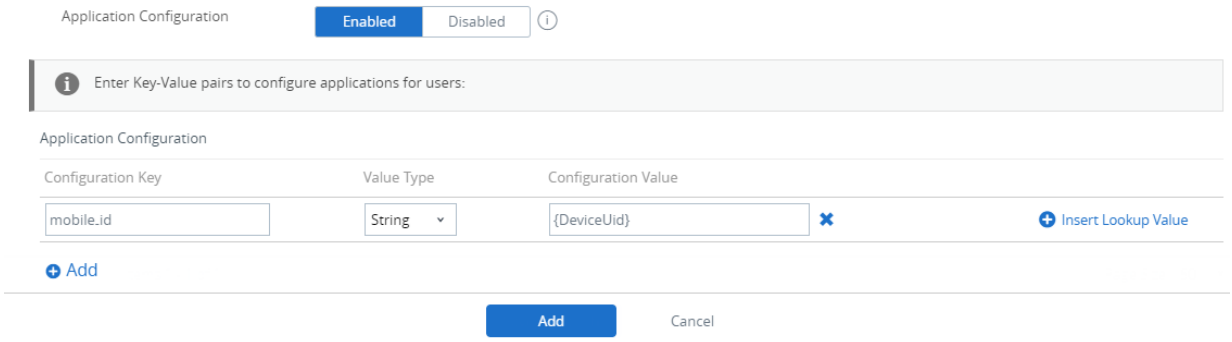
STEP 7 | 在 **Assignment**（指派）頁籤上，選取可存取此應用程式的 **Assigned Smart Groups**（指派的智慧群組）。

STEP 8 | 選取 **App Delivery Method**（應用程式傳遞方法），可以是 **Auto**（自動）以將應用程式自動推送至裝置，或 **On Demand**（視需要）。

STEP 9 | （僅限適用於 Android 的 GlobalProtect 應用程式）**Enable**（啟用）應用程式組態以使用 UDID 識別端點。

新增下列金鑰值配對：

- 組態金鑰—**`mobile_id`**
- 值類型—**`String`**
- 組態值—**`{DeviceUid}`**



STEP 10 | 選取 **Save & Publish**（儲存和發佈）將應用程式目錄推送至 **Assignment**（指派）區段內指派的智慧群組中的端點。

透過 **AirWatch** 在受管理的 **Chromebook** 上部署適用於 **Android** 的 **GlobalProtect** 應用程式

在 GlobalProtect 應用程式 5.0 及更新版本中，您可在已向 AirWatch 註冊的受管理 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式。在部署應用程式後，設定並部署 VPN 設定檔以自動為一般使用者設定 GlobalProtect 應用程式。

僅 特定 Chromebook 支援適用於 *Android* 的 *GlobalProtect* 應用程式。不支援 *Android* 應用程式的 *Chromebooks* 必須繼續執行適用于 *Chrome* 的 *GlobalProtect* 應用程式，其不支援 *GlobalProtect* 應用程式 *5.0* 及更新版本。

請勿在同一 *Chromebook* 上同時部署適用於 *Android* 的 *GlobalProtect* 應用程式與適用於 *Chrome* 的 *GlobalProtect* 應用程式。

按照下列步驟透過 AirWatch 在受管理的 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式：

STEP 1 | 設定 Google 管理控制台。

Google 管理控制台讓您能夠管理為組織中使用者提供的 Google 服務。AirWatch 使用 Google 管理控制台與 Chromebook 進行整合。

1. 以管理員身份登入 Google 管理控制台 。
2. 從控制台中，選取 **Security**（安全性）> **Advanced Settings**（進階設定）> **Manage API client access**（管理 **API** 用戶端存取）。

3. 在 **Client Name**（用戶端名稱）欄位中，輸入 AirWatch 為您提供的用戶端 ID。
4. 在 **One or More API Scopes**（一個或多個 **API** 範圍）欄位中，輸入要控制其應用程式存取權限的 Google API 範圍：

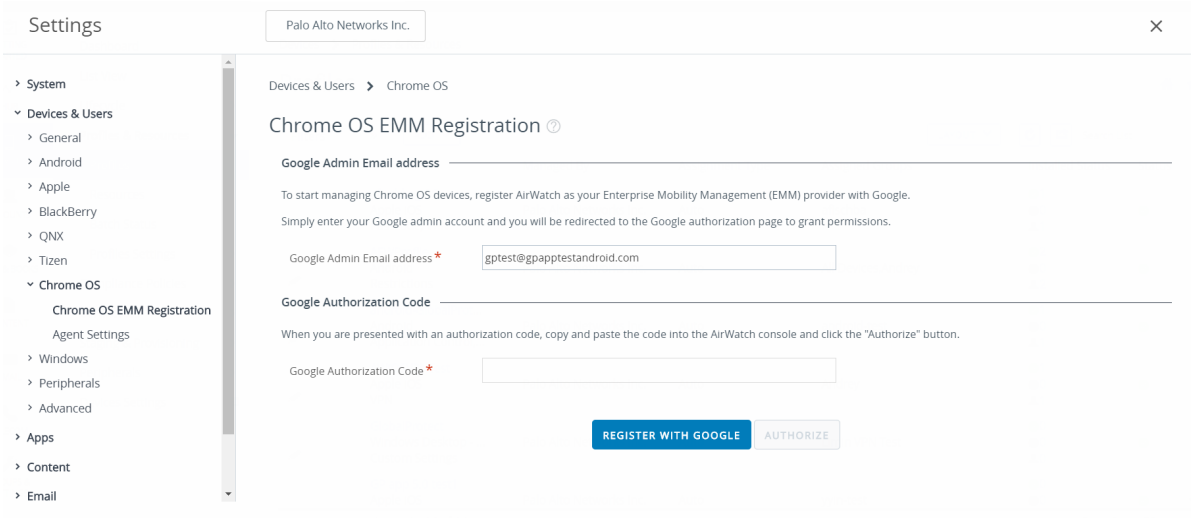
   每個 *API* 範圍都必須以逗號分隔。

   - https://www.googleapis.com/auth/chromedevicemanagementapi
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/admin.directory.device.chromeos
5. 按一下 **Authorize**（授權）。
6. 在裝置原則（**Device Management**（裝置管理）> **Device Settings**（裝置設定）> **Chrome Management**（**Chrome** 管理）> **Device Settings**（裝置設定））與使用者原則（**Device Management**（裝置管理）> **Device Settings**（裝置設定）> **Chrome Management**（**Chrome** 管理）> **User Settings**（使用者設定））中啟用 **Chrome Management - Partner Access**（**Chrome** 管理 - 合作夥伴存取）。

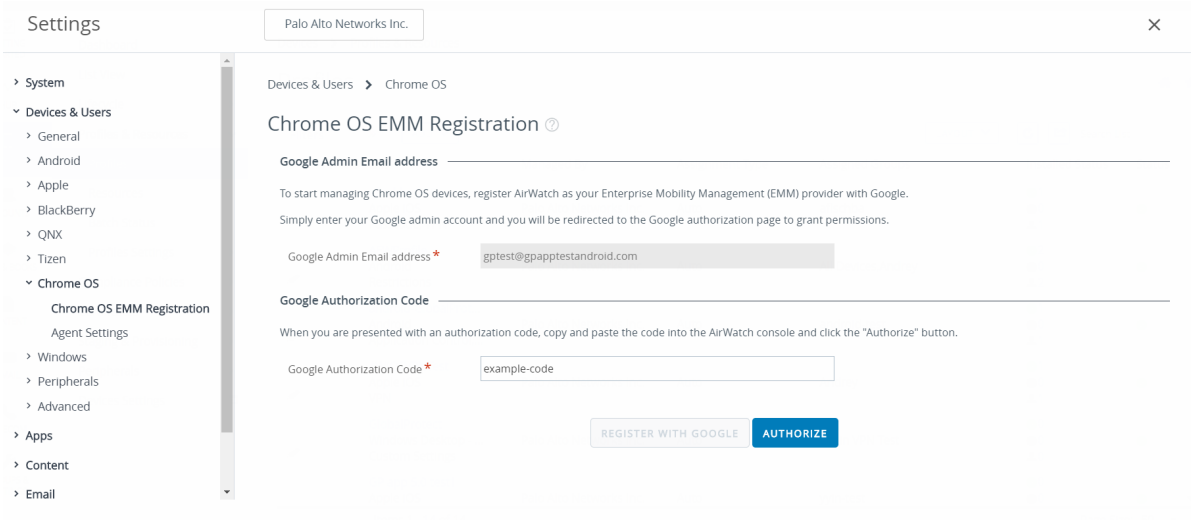
STEP 2 | 註冊 AirWatch 作為 Google 的企業行動管理 (EMM) 供應商。

若要使用 AirWatch 管理 Chromebook，您必須在 Google 管理控制台上註冊 AirWatch。

1. 登入 AirWatch 控制台。
2. 選取 **Devices**（裝置）> **Devices Settings**（裝置設定）> **Devices & Users**（裝置與使用者）> **Chrome OS** > **Chrome OS EMM Registration**（**Chrome OS EMM** 註冊）。
3. 輸入您用於存取 Google 管理控制台的 **Google Admin Email address**（**Google** 管理電子郵件地址）。
4. 按一下 **REGISTER WITH GOOGLE**（在 **GOOGLE** 中註冊）。您將被重新導向至 Google 授權頁面，以取得 Google 授權碼。



5. 輸入從 Google 授權頁面取得的 **Google Authorization Code**（**Google** 授權碼）。
6. 按一下 **AUTHORIZE**（授權）以完成註冊。



STEP 3 | 向 AirWatch 註冊 Chromebook。

您必須向 AirWatch 註冊 Chromebook 並與之同步，然後才能開始使用 AirWatch 管理 Chromebook。

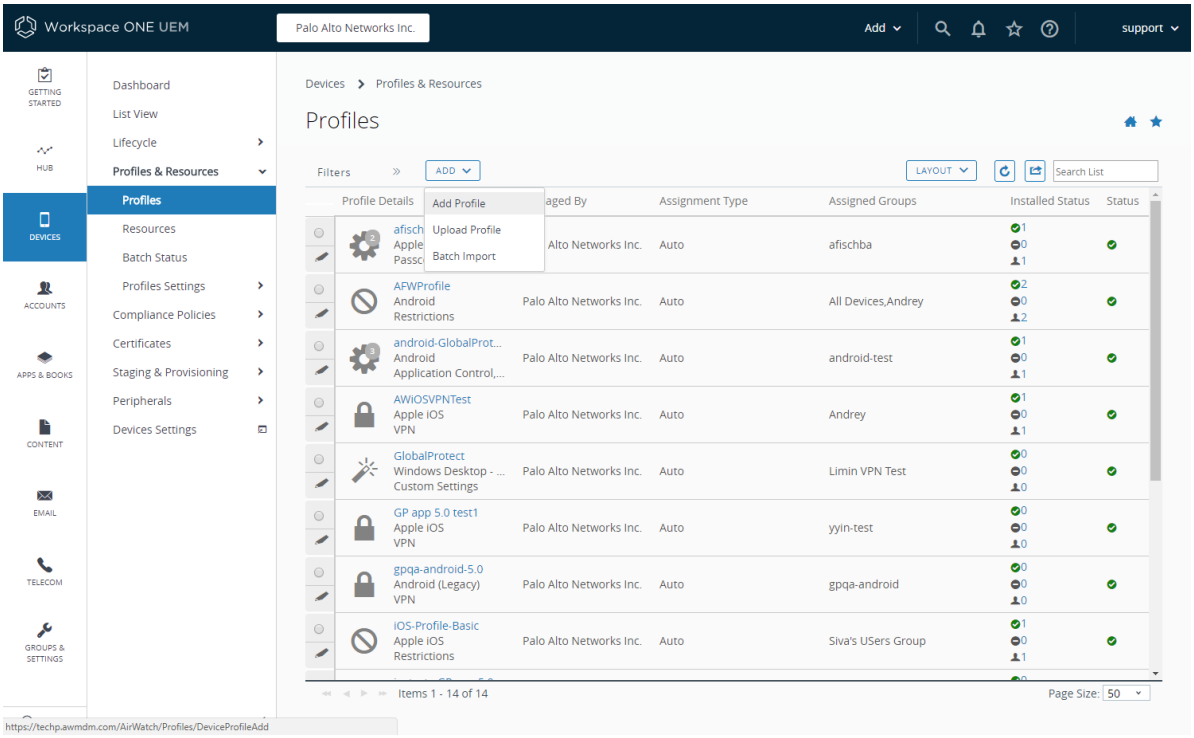
1. 從 Chromebook，按下 **CTRL+ALT+E** 以開啟企業註冊畫面。

2. 從 Google 管理歡迎頁面輸入使用者名稱與密碼或輸入您的現有 G Suite 使用者認證。
3. 按一下 **Enroll Device**（註冊裝置）。當 Chromebook 成功註冊時，您將收到確認訊息。
4. 登入 AirWatch 控制台。
5. 選取 **Devices**（裝置）> **Devices Settings & Users**（裝置設定與使用者）> **Chrome OS** > 。
6. 按一下 **Device Sync**（裝置同步）以將所有已註冊的 Chromebook 與 AirWatch 同步。

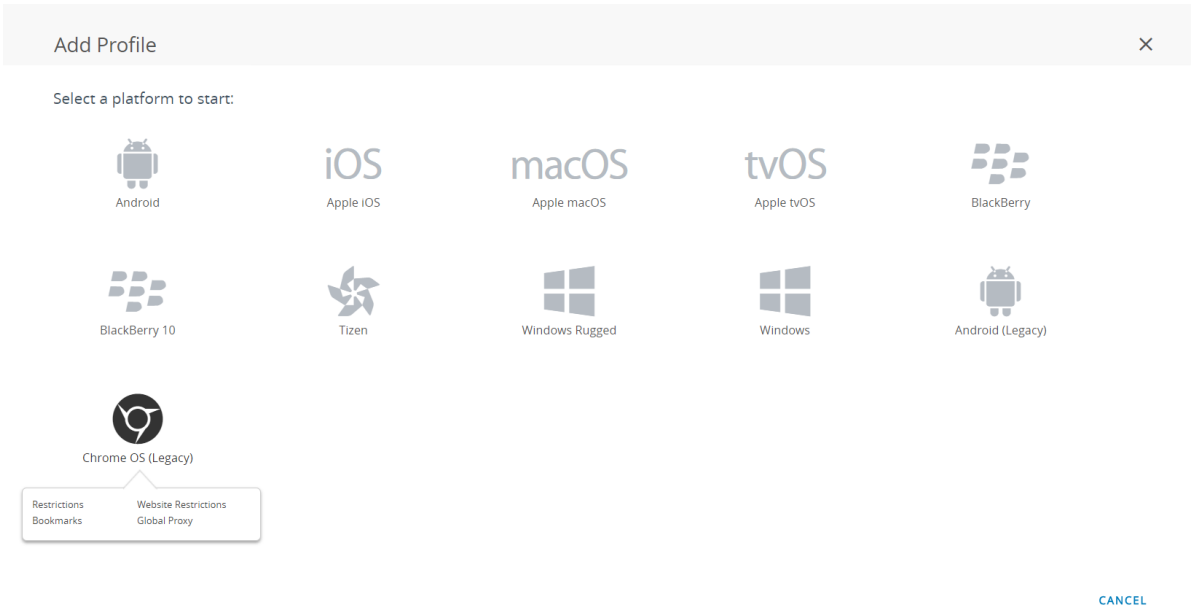
STEP 4 | 將適用於 Android 的 GlobalProtect 應用程式新增至 AirWatch 上的 Chrome OS 設定檔。

Application Control（應用程式控制）設定檔讓您能夠從 Google Play 與 Chrome Web Store 新增應用程式。

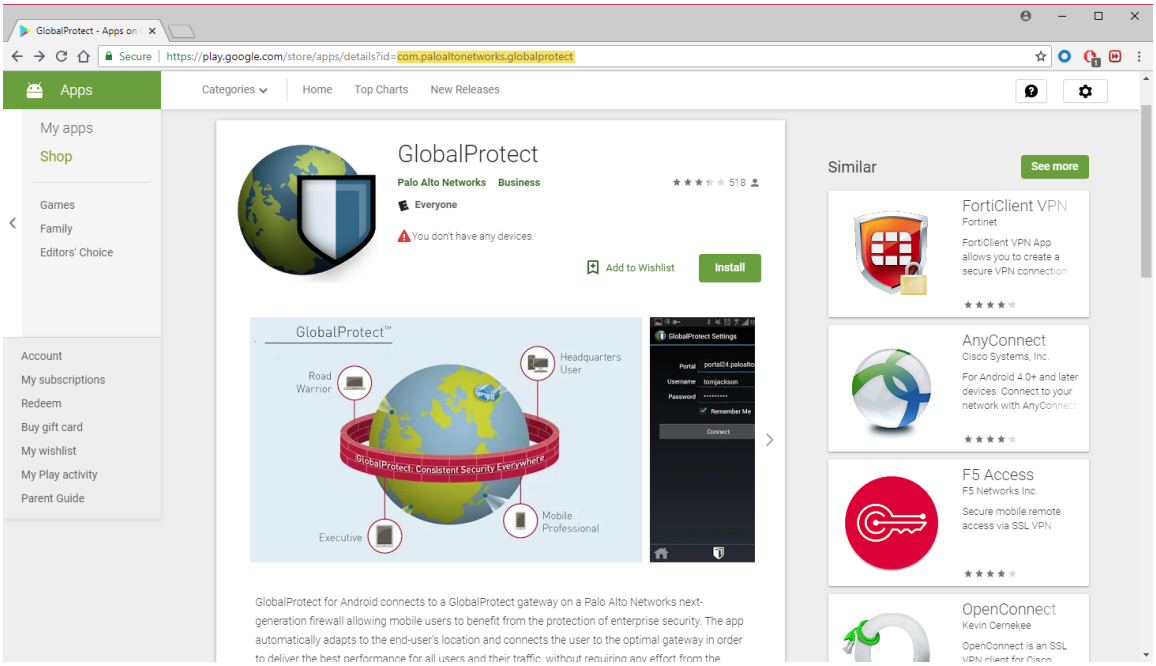
1. 登入 AirWatch 控制台。
2. 選取 **Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles**（設定檔）以 **Add**（新增）新的 Chrome OS 設定檔。



3. 從平台清單選取 **Chrome OS (Legacy)**（**Chrome OS**（舊版））。



4. 設定 **General**（一般）設定：
5. 設定 **Application Control**（應用程式控制）設定。
    1. 輸入 Google Play URL (com.paloaltonetworks.globalprotect) 中顯示的 GlobalProtect **App ID**。



2. 輸入應用程式 **Name**（名稱）。

3. 指定是否要 **Pin App to Shelf**（將應用程式釘選至貨架）。輸入 **Y** 以將應用程式釘選至 Chromebook 應用程式貨架。
4. **SAVE & PUBLISH**（儲存和發佈）您的變更。

透過 **Microsoft Intune** 部署 **GlobalProtect** 行動應用程式

您可部署 GlobalProtect 應用程式至已向 Microsoft Intune 註冊的受管理端點或端點未向 Microsoft Intune（僅限 iOS）註冊的使用者。在部署應用程式後，設定並部署 VPN 設定檔至受管理端點以自動為一般使用者設定 GlobalProtect 應用程式。

STEP 1 | 向 Microsoft Intune 註冊端點。

若要部署 GlobalProtect 應用程式至您的端點，請確保端點已向 Microsoft Intune 註冊。

STEP 2 | 新增 GlobalProtect 應用程式至 Microsoft Intune。

您必須先新增應用程式至 Microsoft Intune，才能指派 GlobalProtect 應用程式至任何使用者或端點。

STEP 3 | 設定 GlobalProtect 應用程式的應用程式指派類型。

您可透過指派應用程式至使用者或端點來確定可以存取 GlobalProtect 應用程式的對像。您必須先設定應用程式的指派類型才能指派應用程式。指派類型使應用程式可用、被需要，或解除安裝應用程式。

STEP 4 | 指派 GlobalProtect 應用程式至特定使用者或端點。

設定 GlobalProtect 應用程式的指派類型後，您便可指派應用程式至特定使用者或端點。

（僅限 *iOS*）您可指派 *GlobalProtect* 應用程式至端點未向 *Microsoft Intune* 註冊的使用者。

透過 **MobileIron** 部署 **GlobalProtect** 行動應用程式

您可以部署 GlobalProtect 應用程式至被管理的端點，該端點已向 MobileIron 註冊。在部署應用程式後，設定並部署 VPN 設定檔以自動為一般使用者設定 GlobalProtect 應用程式。

STEP 1 | 新增使用者至 MobileIron。

您必須先為每位使用者建立使用者項目，使用者才可將其端點註冊至 MobileIron。

STEP 2 | （選用）指派使用者至使用者群組。

為了根據群組成員資格而非個別使用者部署 GlobalProtect 應用程式，您可指派使用者至不同的使用者群組。

STEP 3 | 邀請使用者向 MobileIron 註冊其端點。

當您新增使用者至 MobileIron 後，可邀請他們註冊端點。

STEP 4 | 新增 GlobalProtect 應用程式至 MobileIron 應用程式目錄。

應用程式目錄列出了使用者可用的行動應用程式。您可以從公用商店（例如 Apple App Store）搜尋並新增 GlobalProtect 應用程式或將應用程式作為內部應用程式直接上載至 MobileIron。然後您必須進行應用程式散佈設定以指定 GlobalProtect 應用程式在已註冊端點上的安裝和設定方式。

透過 **Google** 管理控制台在受管理的 **Chromebook** 上部署適用於 **Android** 的 **GlobalProtect** 應用程式

Google 管理控制台讓您可以從中心的 web 式位置管理 Chromebook 設定和應用程式。您可透過控制台在受管理的 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式並設定相關 VPN 設定。

若要自動為使用者設定此應用程式，您可以選擇性地使用 Google Chromebook 管理主控台設定和部署受管理 Chrome 作業系統裝置的設定。您可使用 Google 管理主控台管理 Chromebook 設定與應用程式。

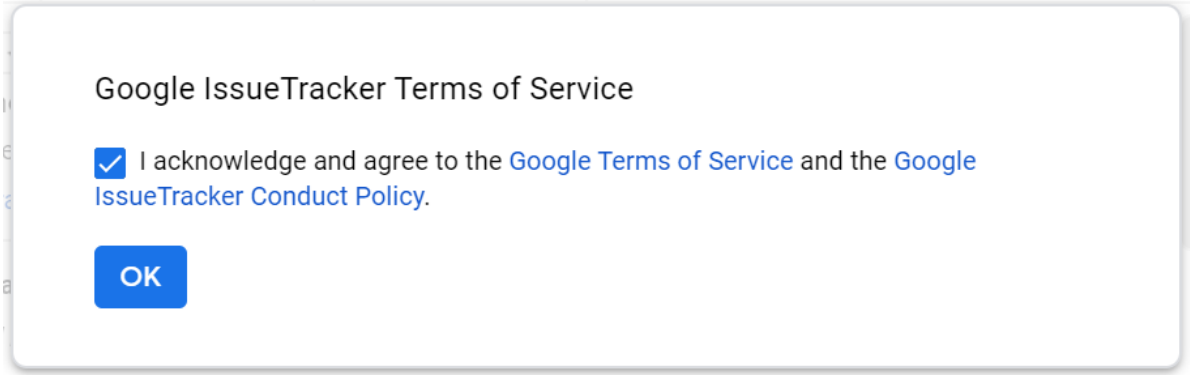
按照下列建議在受管理的 *Chromebook* 上部署適用於 *Android* 的 *GlobalProtect* 應用程式：

- 您無法使用 *Google* 管理主控台將用於進行驗證的唯一憑證推送給裝置。
- 在 *Chromebook* 上，按下 *CTRL+ALT+T* 以開啟終端命令行。使用 `route` 命令顯示裝置上安裝的路由。您可確定是否包含用於分割通道的存取路由。
- 由於應用程式經常使用不同的檔案格式，您可使用 *OpenSSL* 將憑證由 *PKCS #12* 格式轉換為 *Base64* 格式。使用 `openssl base64 -A -in` *<certificate-in-p12-format>* `-out` *<cert.txt>* 命令。

按照下列步驟透過 Google 管理控制台在受管理的 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式：

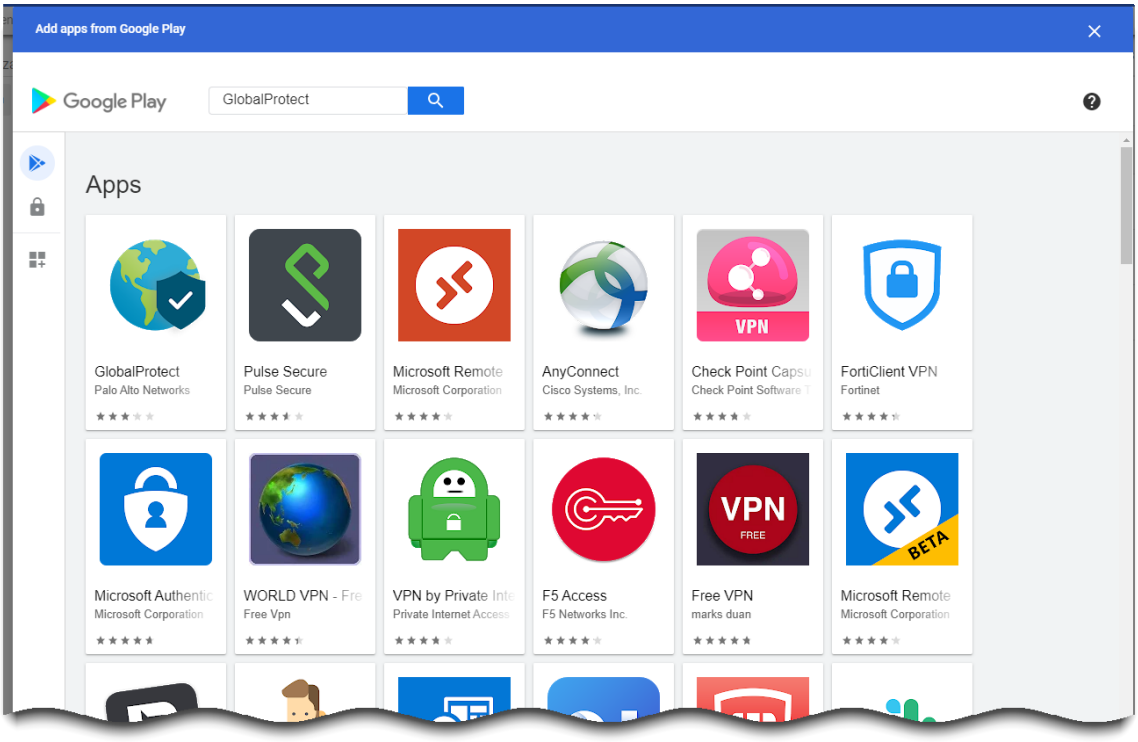
STEP 1 | 開始之前

- 在受管理的 Chromebooks 上設定 GlobalProtect 閘道以支援適用于 Android 的 GlobalProtect 應用程式。請參閱 設定 GlobalProtect 閘道。
- 在受管理的 Chromebooks 上設定入口網站並自訂適用于 Android 的 GlobalProtect 應用程式。您必須設定一個或多個 GlobalProtect 應用程式可以連線的閘道。請參閱 設定 GlobalProtect 入口網站存取權。請參閱《Palo Alto Networks 相容性矩陣》，取得 Chrome OS 上支援的 Android 功能清單。
- （推薦）在 Chromebooks 上為適用于 Android 的 GlobalProtect 應用程式啟用 SAML SSO 以進行無縫驗證。我們建議您設定 SAML SSO 以允許使用者在登入至 Chromebook 後自動連線，無需在 GlobalProtect 應用程式上重新輸入其認證。這可確保使用者能夠存取始終開啟安全性。請參閱 設定 SAML 驗證。
- 當使用者第一次在受管理的 Chromebooks 上連線至適用于 Android 的 GlobalProtect 時，在設定通道之前必須確認以下抑制 VPN 通知訊息：



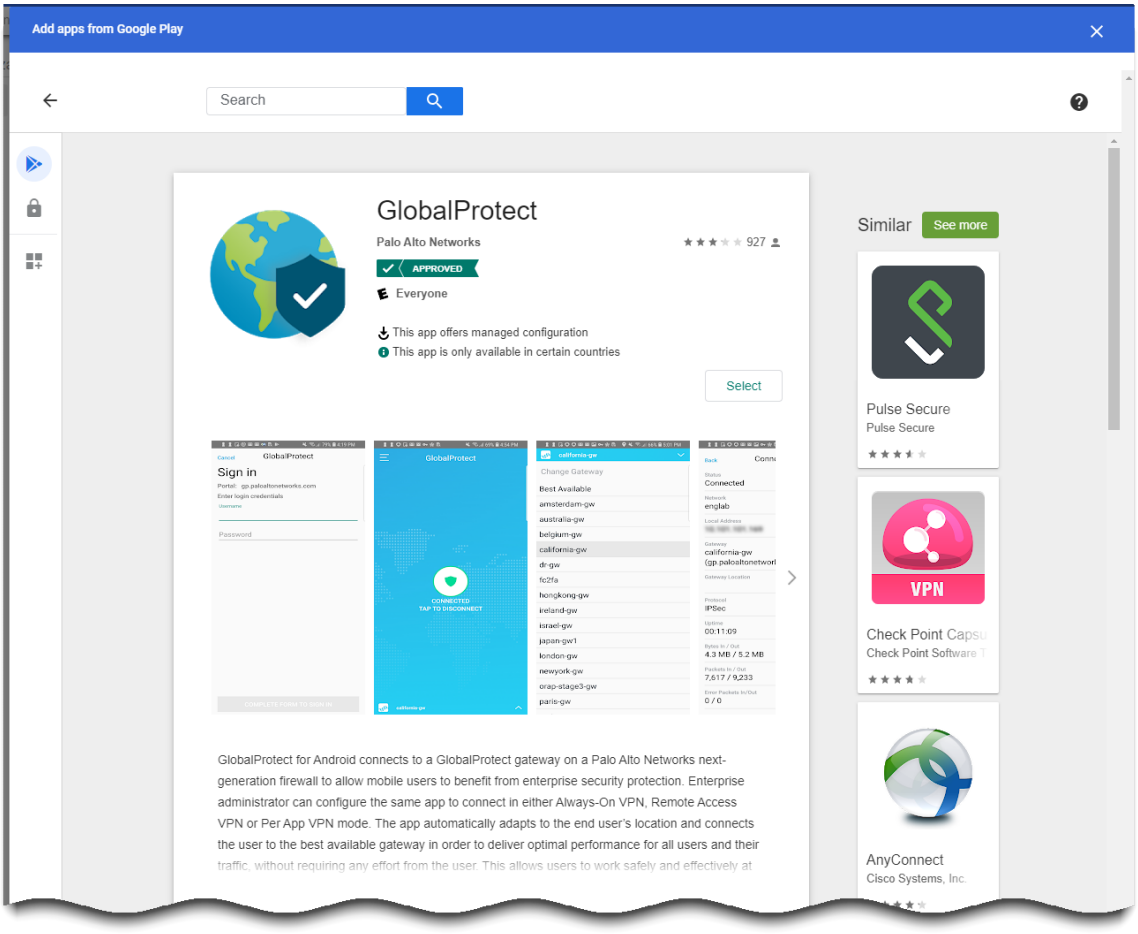
STEP 2 | 為 Chromebook 使用者核准 GlobalProtect 應用程式。

1. 以管理員身份登入 Google 管理控制台 。
2. 從管理主控台中，選取 **Device**（裝置）> **Chrome management**（**Chrome** 管理）以檢視並修改 Chrome 管理設定。
3. 選取 **Apps & extensions**（應用程式與延伸）。
4. 在應用程式與延伸區域，按一下應用程式設定頁面 連結。
5. 按一下新增 (+) 按鈕以將 GlobalProtect 新增至 Google Playstore 中經核准的 Android 應用程式清單。
6. 當 Google Play 商店啟動時，搜尋 **`GlobalProtect`** ，然後按一下 GlobalProtect 應用程式圖示。



7. 按一下 **Select**（選取）以新增 GlobalProtect 應用程式。

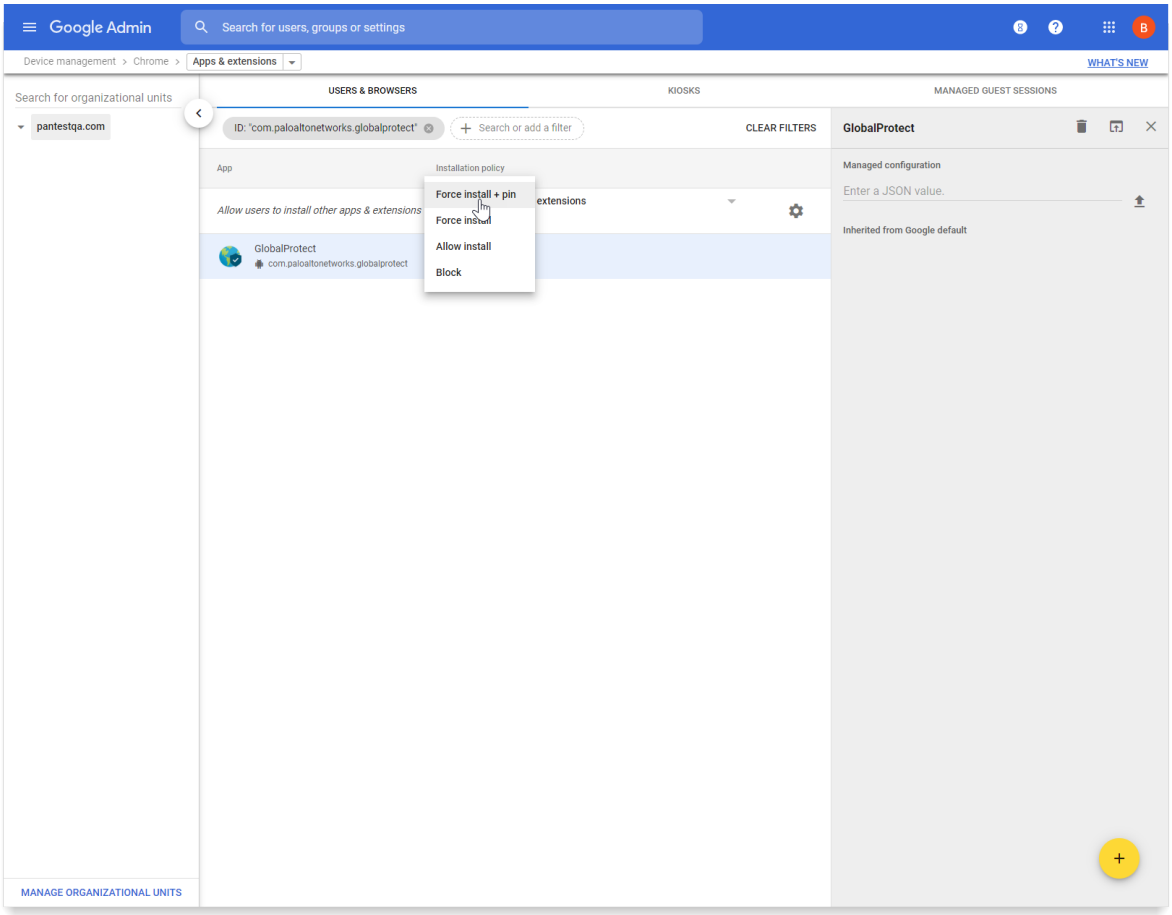
   如果 GlobalProtect 應用程式成功新增為結果，就會顯示一則訊息。



STEP 3 | 確定在 Chromebook 上安裝 GlobalProtect 應用程式的方式。

核准 GlobalProtect 應用程式後，您必須指定在 Chromebook 上安裝此應用程式的方式。為防止使用者透過解除安裝 GlobalProtect 應用程式將其繞過，須強制所有 Chromebook 在使用者登入其 Chromebook 時自動安裝 GlobalProtect 應用程式。

1. 從應用程式延伸管理設定中（**Device Management**（裝置管理）> **Chrome** > **Apps & extensions**（應用程式管理與延伸）），選取應用程式清單中的 **GlobalProtect**。
2. 從頁面左側邊緣的清單中選取您的組織單位。
3. 選取下列任意選項：
   - （推薦）強制安裝 + 釘選—啟用並釘選強制安裝的 GlobalProtect 應用程式至工作列。如果您已選取此選項，使用者將無法選擇「登出應用程式」。
   - **Force install**（強制安裝）—如果您想要確保在使用者登入至其 Chromebooks 時，GlobalProtect 應用程式自動安裝在每個 Chromebook 上，則使用此選項。若要防止使用者解除安裝 GlobalProtect 應用程式並繞過安全性與合規要求，則您需要執行 **Force install**（強制安裝）選項。如果您已選取此選項，使用者將無法選擇「登出應用程式」。
   - **Allow install**（允許安裝）—從 Google Playstore 手動安裝此應用程式。此選項也允許使用者從其 Chromebooks 解除安裝 GlobalProtect 應用程式。
   - **Block**（封鎖）—封鎖使用者安裝此應用程式。



4. **Save**（儲存）變更。

STEP 4 | 將受管理的組態套用至 GlobalProtect 應用程式。

若您已允許強制安裝 GlobalProtect 應用程式，則可將受管理的組態檔案套用至此應用程式。受管理的組態檔案包含可設定的應用程式設定值。

1. 從應用程式管理設定中（**Device Management**（裝置管理）> **Chrome management**（Chrome 管理）> **Apps & Extensions**（應用程式與延伸）），選取應用程式清單中的 **GlobalProtect**。
2. 從頁面左側邊緣的清單中選取您的組織單位。
3. 按一下頁面右側邊緣的 **Upload from file**（從檔案中上載）圖示，以選取和上載受管理的設定檔案。或者，以 JSON 格式輸入金鑰值的名稱，如下列範例組態所示。

```
{ "portal": "acme.portal.com", "username": "user123" }
```

下表顯示了受管理設定檔案中設定的範例。有關與您公司相關的設定，請聯絡您的 IT 管理員。

setting	說明	值類型	範例
入口網站	入口網站的 IP 位址或完全合格的網域名稱 (FQDN)。	字串	`acme.portal.com`
使用者名稱	用於入口網站驗證的使用者名稱。	字串	`user123`

setting	說明	值類型	範例
密碼	用於入口網站驗證的密碼。	字串	**password123**
client_certificate	用於入口網站驗證的用戶端憑證。	字串 (in Base64)	**DAFDSaweEWQ23wDSAFD**...
client_certificate _passphrase	用於入口網站驗證的用戶端憑證複雜密碼。	字串	**PA$$W0RD$123**
app_list	封鎖清單或允許清單讓您可在 per-app VPN 組態中控制哪些應用程式流量能夠通過 VPN 通道。	字串	允許清單 | 封鎖清單：**com.google.calendar; com.android.email; com.android.chrome**
connect_method	VPN 連線方法。	字串	使用者登入 | 視需要
mobile_id	用於識別行動端點的唯一識別碼，如在協力廠商 MDM 系統中設定的唯一識別碼。	字串	**5188a8193be43f42d332 dde5cb2c941e**
remove_vpn_config _via_restriction	表示移除 VPN 組態的旗標。	布林值	真 | 假
allow_vpn_bypass	允許應用程式流量繞過 VPN 通道的旗標。	布林值	真 | 假
cert_alias	用於在入口網站或閘道驗證時標識用戶端憑證的唯一名稱。	字串	公司使用者用戶端
受管理	表示裝置是否已在 MDM 伺服器上註冊的旗標。	布林值	真 | 假
擁有權	裝置的擁有權類別（例如，**Employee Owned**（員工擁有））。	字串	**byod**
合規	合規狀態，表示裝置是否符合您定義的合規原則（例如，Compliant（合規））。	字串	**yes**
頁籤	用於識別裝置的頁籤。每個頁籤都必須以逗號分隔。	字串	**GuestAccount**，**SatelliteOffice**

4. **Save**（儲存）變更。

STEP 5 | 在受管理的 Chromebook 上執行針對適用于 Android 的 GlobalProtect 應用程式的原則。

- 在受管理的 Chromebook 上使用特定于 Android 的 **Host Info**（主機資訊）Create HIP objects（建立 HIP 物件）。然後用其在任何主機資訊設定檔 (HIP) 設定檔中作為比對條件。

- 使用 HIP 設定檔作為原則規則中的比對條件，以執行相應的安全性原則。依預設，應用程式會收集資訊的資料類別，以協助識別主機的安全性狀態。

一直開啟 *VPN* 設定

在一直開啟 VPN 設定中，安全 GlobalProtect 連線一直開啟。GlobalProtect 應用程式會連線至 GlobalProtect 入口網站（在使用者登入時），以提交使用者與主機資訊，並擷取代理程式組態。當應用程式從入口網站收到代理程式組態後，其會自動連線並建立至代理程式組態中指定 GlobalProtect 閘道的 VPN 通道。

有關如何使用支援的行動裝置管理系統設定一直開啟 VPN 設定的資訊，請參閱以下幾節：

- 透過 AirWatch 進行一直開啟 VPN 設定
- 透過 Microsoft Intune 進行一直開啟 VPN 設定
- 透過 MobileIron 進行一直開啟 VPN 設定
- 使用 Google 管理控制台進行一直開啟 VPN 設定

透過 **AirWatch** 進行一直開啟 **VPN** 設定

AirWatch 是讓您可以從中央控制台管理行動端點的企業行動管理平台。GlobalProtect 應用程式提供 AirWatch 在裝置或應用程式等級管理的防火牆和行動端點之間的安全連線。使用 Android 的 GlobalProtect 作為安全連線，可進行對流量的一致檢查和對網路安全政策的強化，以預防行動端點上的威脅。

有關如何使用 AirWatch 進行一直開啟 VPN 設定的資訊，請參閱以下幾節：

- 透過 AirWatch 對 iOS 端點進行一直開啟 VPN 設定
- 透過 AirWatch 對 Windows 10 UWP 端點進行一直開啟 VPN 設定

透過 *AirWatch* 對 *iOS* 端點進行一直開啟 *VPN* 設定

在一直開啟 VPN 設定中，安全 GlobalProtect 連線一直開啟。符合 GlobalProtect 閘道上所設定特定篩選條件（如連接埠和 IP 位址）的流量一直透過 VPN 通道進行路由傳送。

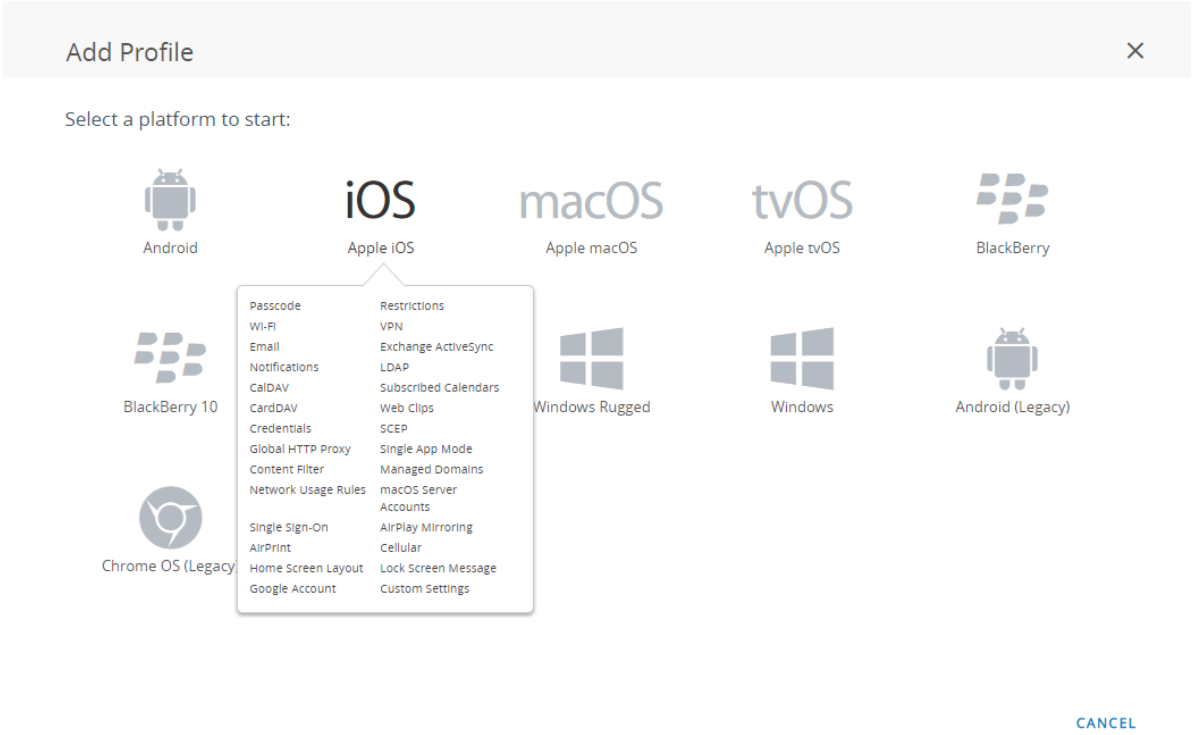
按照下列步驟使用 AirWatch 對 iOS 端點進行一直開啟 VPN 設定：

STEP 1 | 為 iOS 下載 GlobalProtect 應用程式。

- 透過 AirWatch 部署 GlobalProtect 行動應用程式。
- 從 App Store 直接下載 GlobalProtect 應用程式。

STEP 2 | 從 AirWatch 主控台修改現有 Apple iOS 設定檔或新增一個。

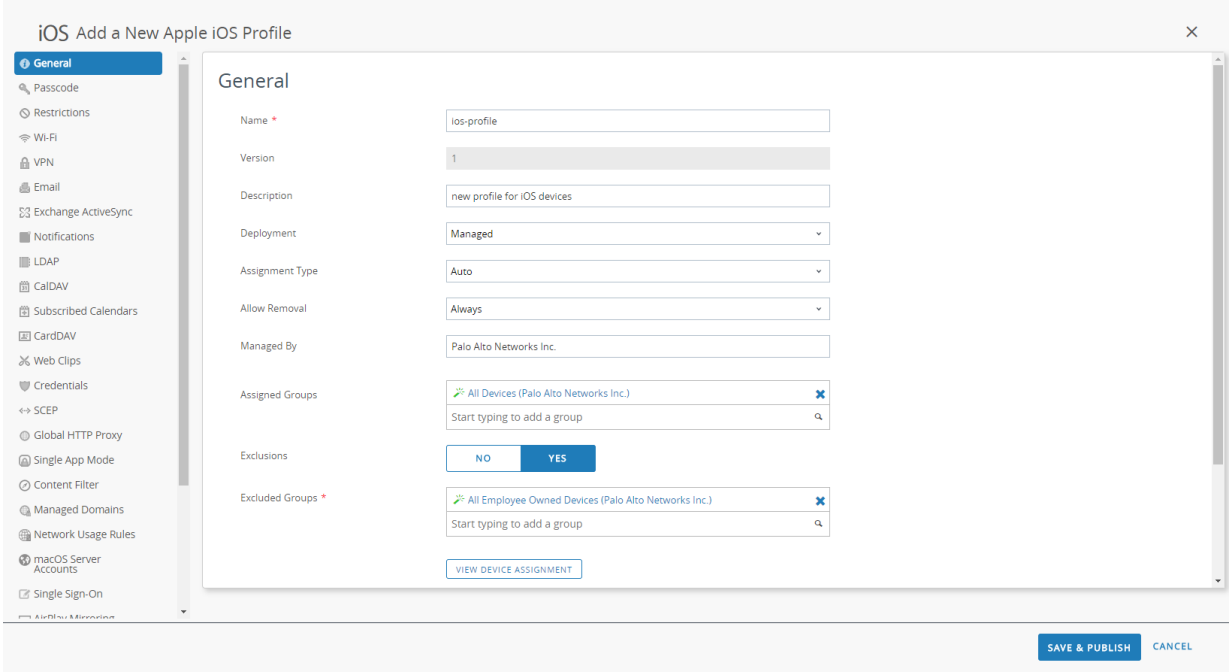
1. 選取 **Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles**（設定檔），然後 **ADD**（新增）新的設定檔。
2. 從平台清單選取 **iOS**。



STEP 3 | 設定**General**（一般）設定：

1. 輸入設定檔的 **Name**（名稱）。
2. （選用）輸入說明設定檔用途的簡短**Description**（描述）。
3. （選用）選取 **Deployment**（部署）方法，它決定設定檔是否會在取消註冊時自動移除—無論是 **Managed**（受管理）（設定檔被移除）或 **Manual**（手動）（設定檔保持安裝直到被一般使用者移除）。
4. （選用）選取 **Assignment Type**（指派類型）以決定設定檔如何部署至端點。選取 **Auto**（自動）將設定檔自動部署至所有端點，選取 **Optional**（選用）讓一般使用者能從自助式入口網站 (SSP) 安裝設定檔，或手動部署設定檔至個別端點，或選取 **Compliance**（合規性）在一般使用者違反套用於端點的合規性原則時部署設定檔。

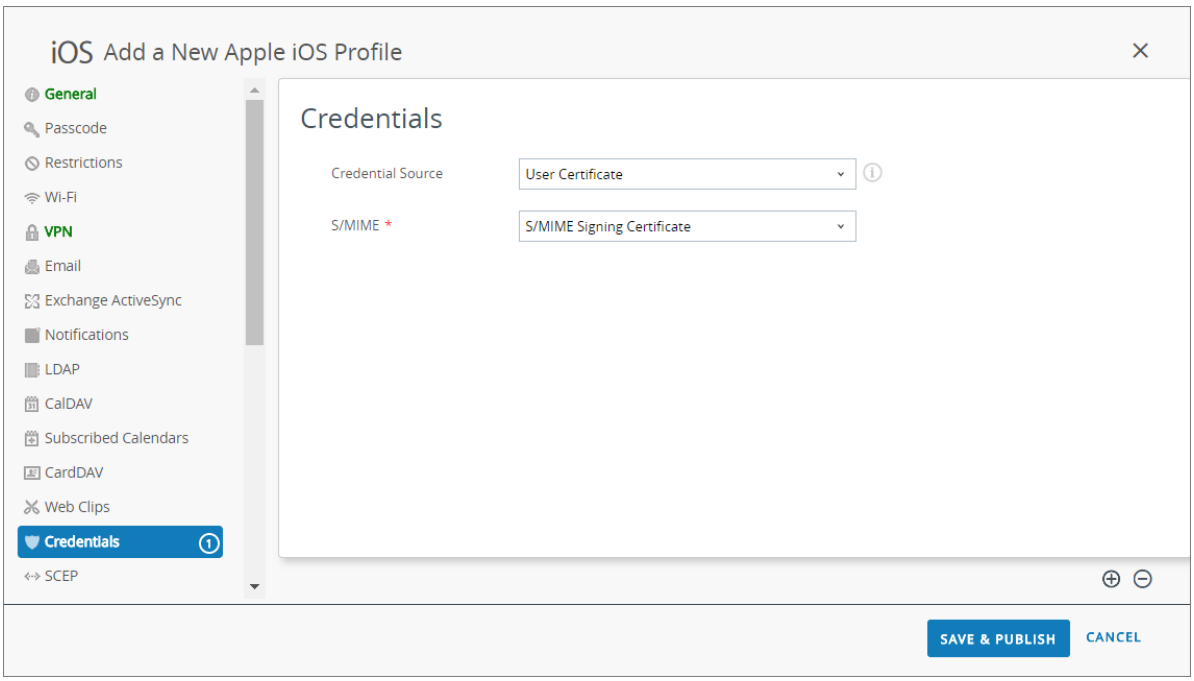
5. （選用）選取 **Allow Removal**（允許移除）以決定一般使用者能否移除設定檔。選取 **Always**（一律）讓一般使用者能在任何時候手動移除設定檔，選取 **Never**（絕不）防止一般使用者移除設定檔，或選取 **With Authorization**（透過授權）讓經過管理員授權的一般使用者能移除設定檔。選取 **With Authorization**（透過授權）會新增必要的密碼。
6. （選用）在 **Managed By**（被管理）欄位，輸入帶有設定檔管理存取的組織群組。
7. （選用）在 **Assigned Groups**（指派的群組）欄位，新增您希望新增設定檔的智慧群組。此欄位包含選項以建立新智慧群組，該智慧群組可透過規格設定用於最小 OS、設備型號、擁有權類別、組織群組等。
8. （選用）表示您是否希望包含任何 **Exclusions**（排除）至此設定檔的指派。如果選取 **Yes**（是），會顯示 **Excluded Groups**（排除群組）欄位，讓您可以選取希望從此設定檔指派中排除的智慧群組。
9. （選用）如果您啟用選項以 **Install only on devices inside selected areas**（僅在選定區域內的裝置上安裝），則設定檔僅可安裝在指定地理圍欄或 iBeacon 區域的端點上。出現提示時，請在 **Assigned Geofence Areas**（指定地理圍欄區域）欄位新增地理圍欄或 iBeacon 區域。
10. （選用）如果 **Enable Scheduling and install only during selected time periods**（僅在選定的時間段內啟用排程與安裝），您可套用時間排程（**Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles Settings**（設定檔設定）> **Time Schedules**（時間排程））至設定檔安裝，限制在端點上安裝設定檔的時間。出現提示時，請在 **Assigned Schedules**（指派排程）欄位輸入排程名稱。
11. （選用）選取您希望設定檔從所有端點移除的 **Removal Date**（移除日期）。



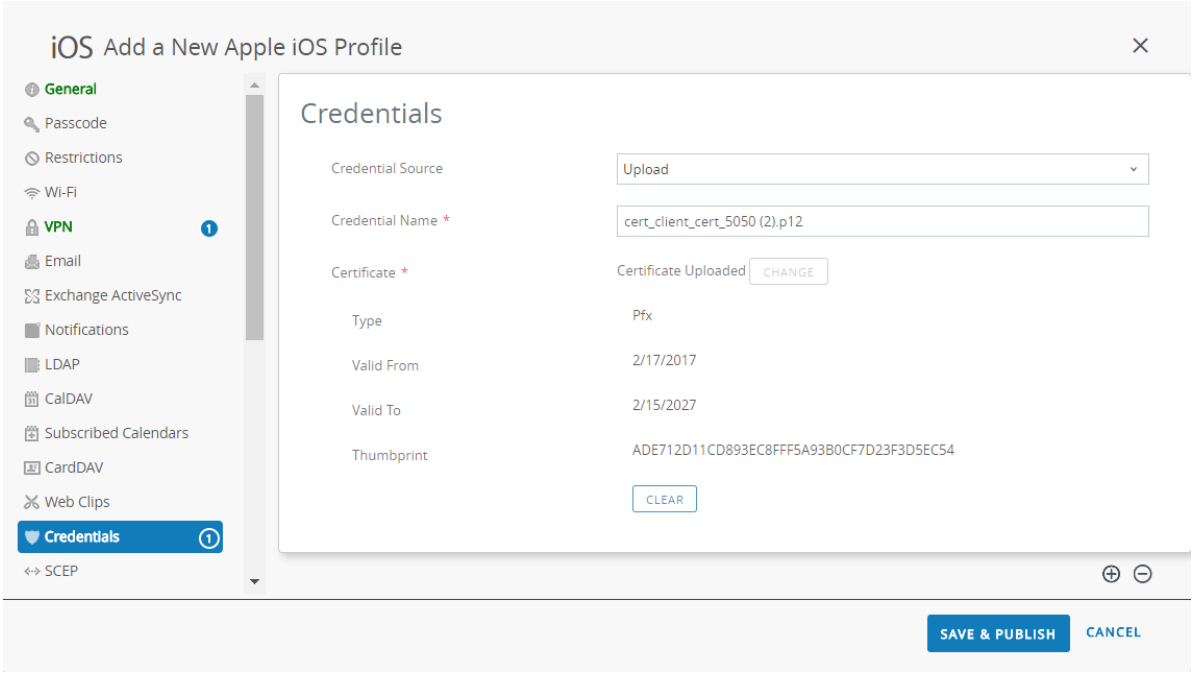
STEP 4 | （選用）如果您的 GlobalProtect 部署需要用戶端憑證驗證，請進行 **Credentials**（認證）設定：

要求的最低版本為 *iOS 12*，如果您想要透過用戶端憑證進行 *GlobalProtect* 用戶端驗證，您必須將用戶端憑證部署為從 *MDM* 伺服器推送的 *VPN* 設定檔的一部分。如果您使用任何其他方法部署來自 *MDM* 伺服器的用戶端憑證，則 *GlobalProtect* 應用程式將無法使用憑證。

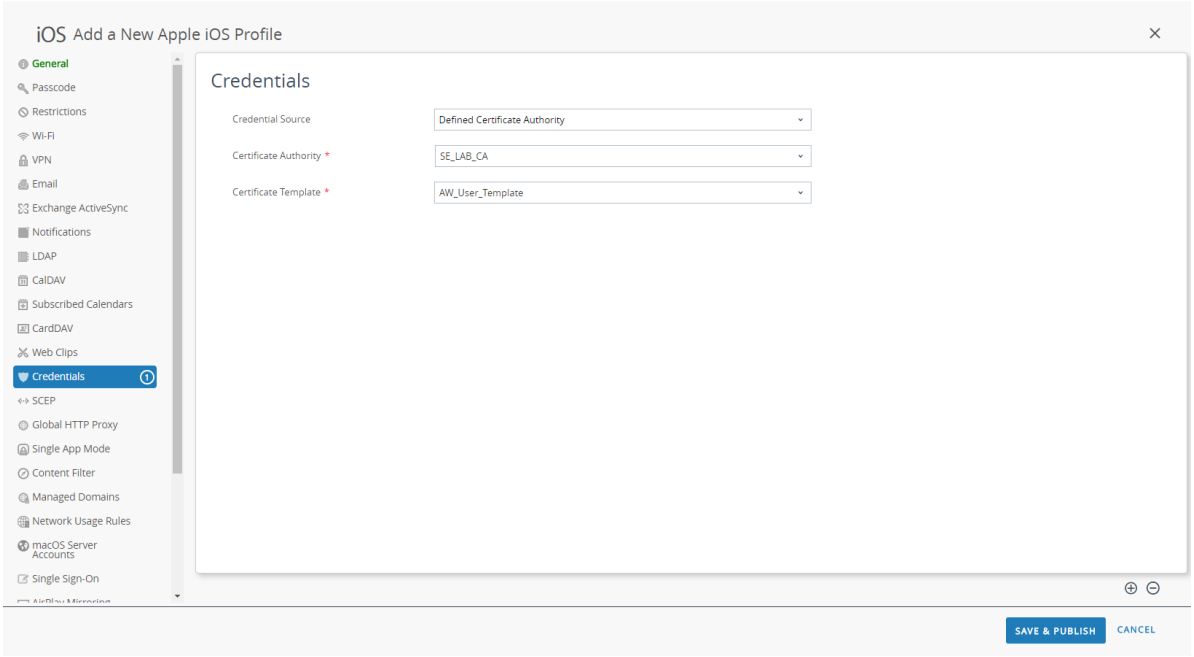
- 若要從 AirWatch 使用者提取用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **User Certificate**（使用者憑證）。
  2. 選取 **S/MIME Signing Certificate**（**S/MIME** 簽署憑證）（預設）。



- 若要手動上載用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **Upload**（上載）。
  2. 輸入 **Credential Name**（認證名稱）。
  3. 按一下 **UPLOAD**（上載）以找到並選取您要上載的憑證。
  4. 選取憑證後，按一下 **SAVE**（儲存）。

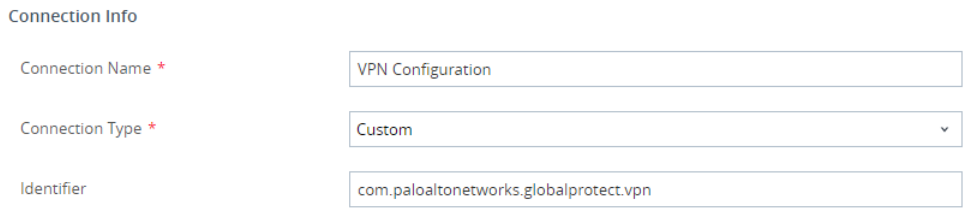


- 若要使用預先定義的憑證授權單位和範本：
  1. 將 **Credential Source**（認證來源）設定為 **Defined Certificate Authority**（定義的憑證授權單位）。
  2. 選取您想要取得憑證的 **Certificate Authority**（憑證授權單位）。
  3. 選取憑證授權單位的 **Certificate Template**（憑證範本）。



STEP 5 | 設定 **VPN** 設定：

1. 輸入要端點顯示的 **Connection Name**（連線名稱）。
2. 選取網路 **Connection Type**（連線類型）：
   - 對於 GlobalProtect 應用程式 4.1.x 及更早版本，請選取 **Palo Alto Networks GlobalProtect**。
   - 對於 GlobalProtect 應用程式 5.0 及更新版本，請選取 **Custom**（自訂）。
3. （選用）如果您將 **Connection Type**（連線類型）設定為 **Custom**（自訂），請在 **Identifier**（識別碼）欄位輸入下列捆綁 ID 以識別 GlobalProtect 應用程式：**`com.paloaltonetworks.globalprotect.vpn`**。

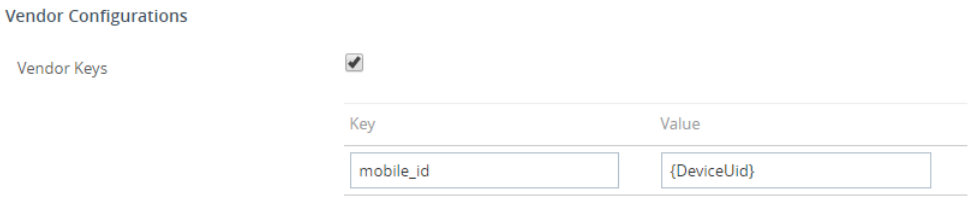


4. 在 **Server**（伺服器）欄位，輸入使用者連線的 GlobalProtect 入口網站主機或 IP 位址。
5. （選用）輸入 VPN **Account**（帳戶）用戶名或按一下新增 (+) 按鈕以檢視您可以插入的支援查閱值。
6. （選用）在 **Disconnect on idle**（閒置時中斷連線）欄位，指定應用程式停止透過 VPN 通道路由流量後端點登出 GlobalProtect 應用程式的時間（秒）。
7. 在驗證區域，選取使用者 **Authentication**（驗證）方法：**Password**（密碼）、**Certificate**（憑證）、**Password + Certificate**（密碼 + 憑證）。
8. 出現提示時，請輸入 **Password**（密碼）和/或選取 GlobalProtect 將用於驗證使用者的 **Identity Certificate**（識別身分憑證）。**Identity Certificate**（識別身分憑證）與您在 **Credentials**（認證）設定中設定的憑證相同。
9. 啟用 **VPN On Demand** 並使用新的隨需金鑰。
10. 透過動作：連線設定隨需規則。
11. （選用）選取 **Proxy** 類型並進行相關設定。

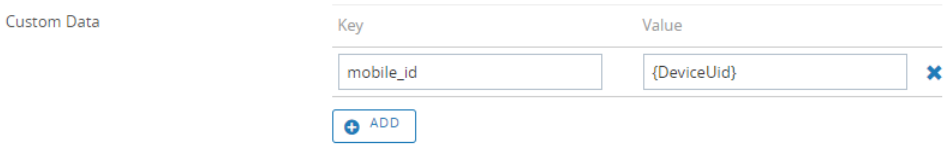
STEP 6 | （選用）（最低版本要求為 GlobalProtect 應用程式 5.0）如果您的 GlobalProtect 部署要求 HIP 與 MDM 整合，請指定唯一裝置識別碼 (UDID) 屬性。

GlobalProtect 支援與 MDM 整合以從 MDM 伺服器取得行動裝置屬性，用於以 HIP 為基礎的原則強制執行。若要使 MDM 整合能夠正常執行，GlobalProtect 應用程式必須向 GlobalProtect 閘道呈現端點的 UDID。UDID 屬性讓 GlobalProtect 應用程式能夠在以 MDM 為基礎的部署中擷取並使用 UDID 資訊。如果您從設定檔中移除 UDID 屬性，將無法再使用 MDM 整合。GlobalProtect 應用程式將產生新的 UDID，但其無法用於整合。

- 如果您使用的是 **Palo Alto Networks GlobalProtect** 網路 **Connection Type**（連線類型），請前往 **VPN** 設定並在廠商組態區域啟用 **Vendor Keys**（廠商金鑰）。將 **Key**（索引鍵）設定為 **`mobile_id`** 並將 **Value**（值）設定為 **`{DeviceUid}`**。



- 如果您使用的是 **Custom**（自訂）網路 **Connection Type**（連線類型），請前往 **VPN** 設定並在連線資訊區域 **ADD**（新增）**Custom Data**（自訂資料）。將 **Key**（索引鍵）設定為 **`mobile_id`** 並將 **Value**（值）設定為 **`{DeviceUid}`**。



STEP 7 | **SAVE & PUBLISH**（儲存和發佈）您的變更。

透過 *AirWatch* 對 *Windows 10 UWP* 端點進行一直開啟 *VPN* 設定

在一直開啟 VPN 設定中，安全 GlobalProtect 連線一直開啟。符合 GlobalProtect 閘道上所設定特定篩選條件（如連接埠和 IP 位址）的流量一直透過 VPN 通道進行路由傳送。針對更嚴格的安全要求，您可以啟用 VPN 鎖定，強制安全連線一直開啟和連線，並當應用程式未連線時停用網路存取。此組態與您通常會在 GlobalProtect 入口網站組態中設定的 **Enforce GlobalProtect for Network Access**（強制執行 **GlobalProtect** 連線以進行網路存取）選項類似。

由於 *AirWatch* 尚未將 *GlobalProtect* 作為 *Windows* 端點的正式連線供應商，您必須選取替代的 *VPN* 供應商，編輯 *GlobalProtect* 應用程式設定，並根據下列工作流程所述將組態匯入 *VPN* 設定檔。

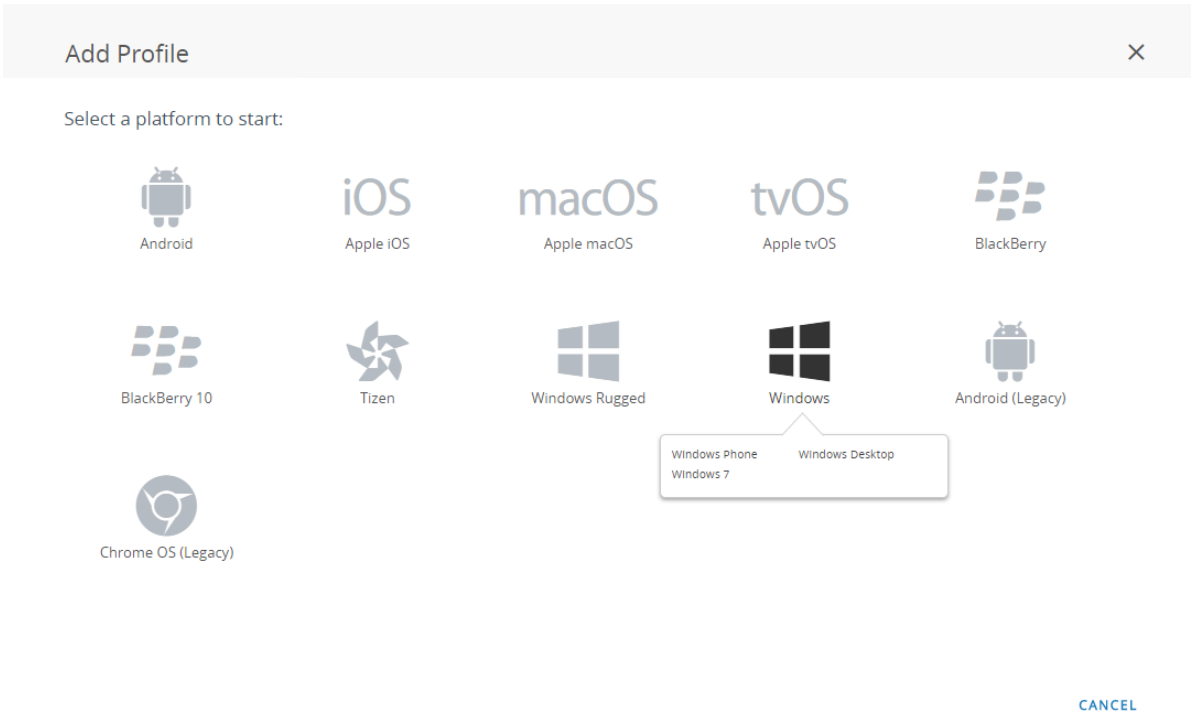
按照下列步驟使用 AirWatch 對 Windows 10 UWP 端點進行一直開啟 VPN 設定：

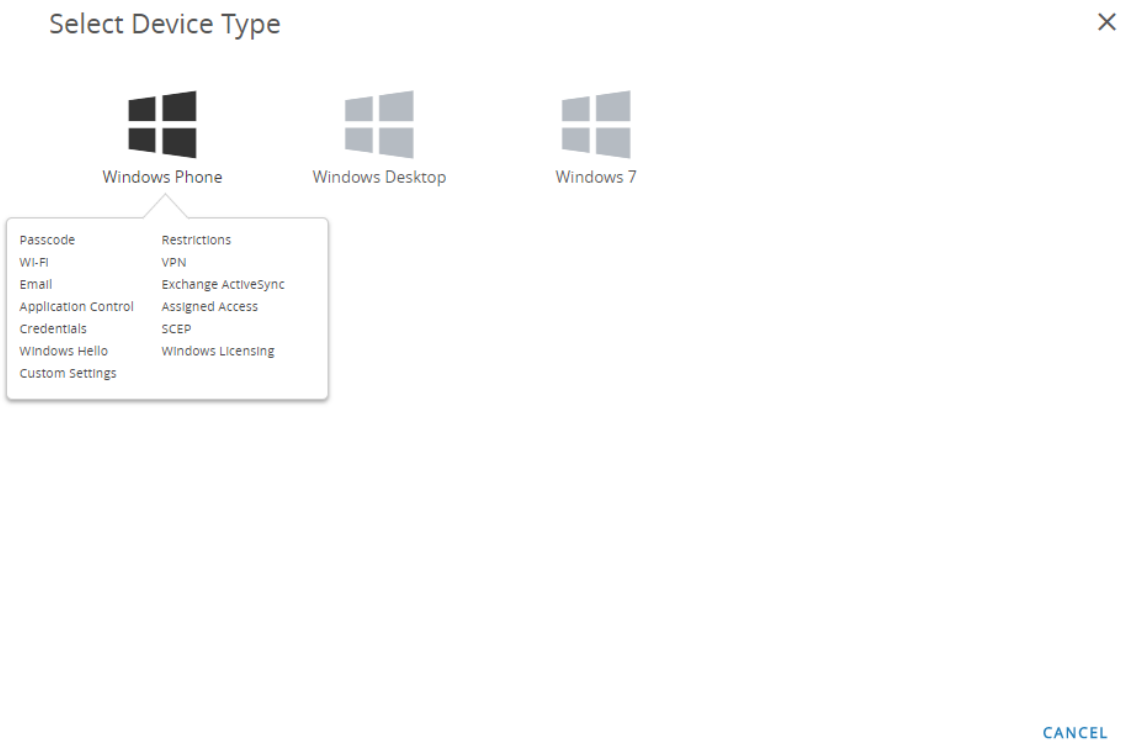
STEP 1 | 為 Windows 10 UWP 下載 GlobalProtect 應用程式：

- 透過 AirWatch 部署 GlobalProtect 行動應用程式。
- 從 Microsoft Store 直接下載 GlobalProtect 應用程式。

STEP 2 | 從 AirWatch 主控台修改現有 Windows 10 UWP 設定檔或新增一個。

1. 選取 **Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles**（設定檔），然後 **ADD**（新增）新的設定檔。
2. 選取 **Windows** 作為平台並選取 **Windows Phone** 作為裝置類型。

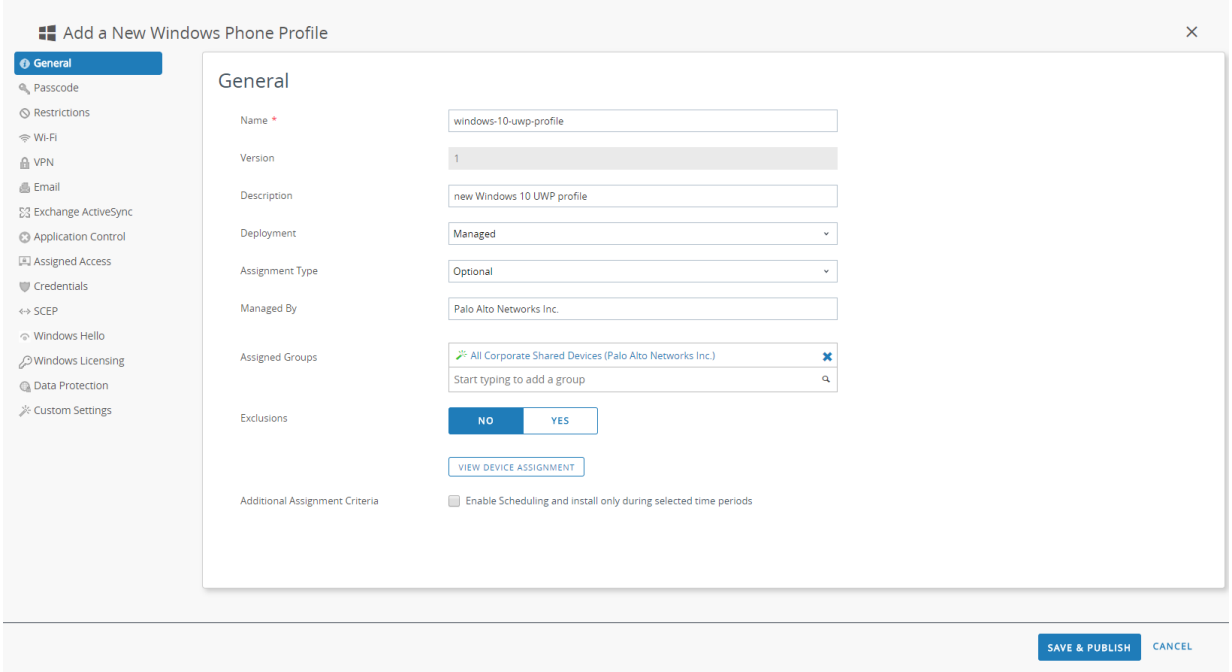




STEP 3 | 設定**General**（一般）設定：

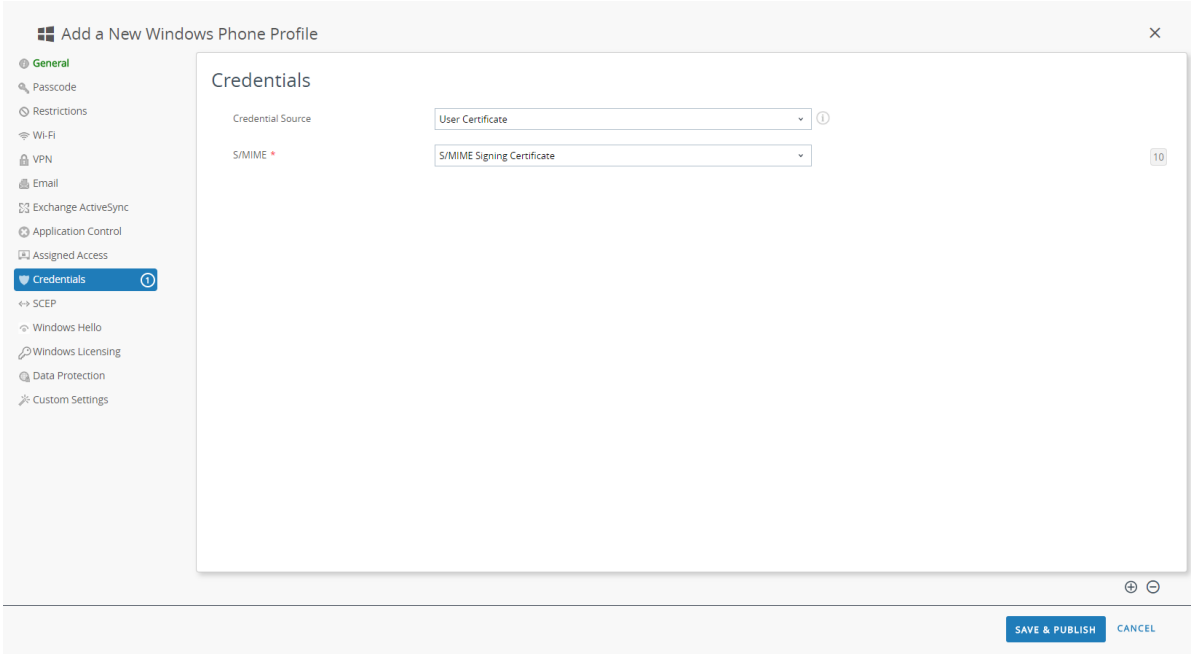
1. 輸入設定檔的 **Name**（名稱）。
2. （選用）輸入說明設定檔用途的簡短**Description**（描述）。
3. （選用）將 **Deployment**（部署）方法設定為 **Managed**（受管理）以使設定檔在取消註冊時自動移除
4. （選用）選取 **Assignment Type**（指派類型）以決定設定檔如何部署至端點。選取 **Auto**（自動）將設定檔自動部署至所有端點，選取 **Optional**（選用）讓一般使用者能從自助式入口網站 (SSP) 安裝設定檔，或手動部署設定檔至個別端點，或選取 **Compliance**（合規性）在一般使用者違反套用於端點的合規性原則時部署設定檔。
5. （選用）在 **Managed By**（被管理）欄位，輸入帶有設定檔管理存取的組織群組。

6. （選用）在 **Assigned Groups**（指派的群組）欄位，新增您希望新增設定檔的智慧群組。此欄位包含選項以建立新智慧群組，該智慧群組可透過規格設定用於最小 OS、設備型號、擁有權類別、組織群組等。
7. （選用）表示您是否希望包含任何 **Exclusions**（排除）至此設定檔的指派。如果選取 **Yes**（是），會顯示 **Excluded Groups**（排除群組）欄位，讓您可以選取希望從此設定檔指派中排除的智慧群組。
8. （選用）如果 **Enable Scheduling and install only during selected time periods**（僅在選定的時間段內啟用排程與安裝），您可套用時間排程（**Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles Settings**（設定檔設定）> **Time Schedules**（時間排程））至設定檔安裝，限制在端點上安裝設定檔的時間。出現提示時，請在 **Assigned Schedules**（指派排程）欄位輸入排程名稱。

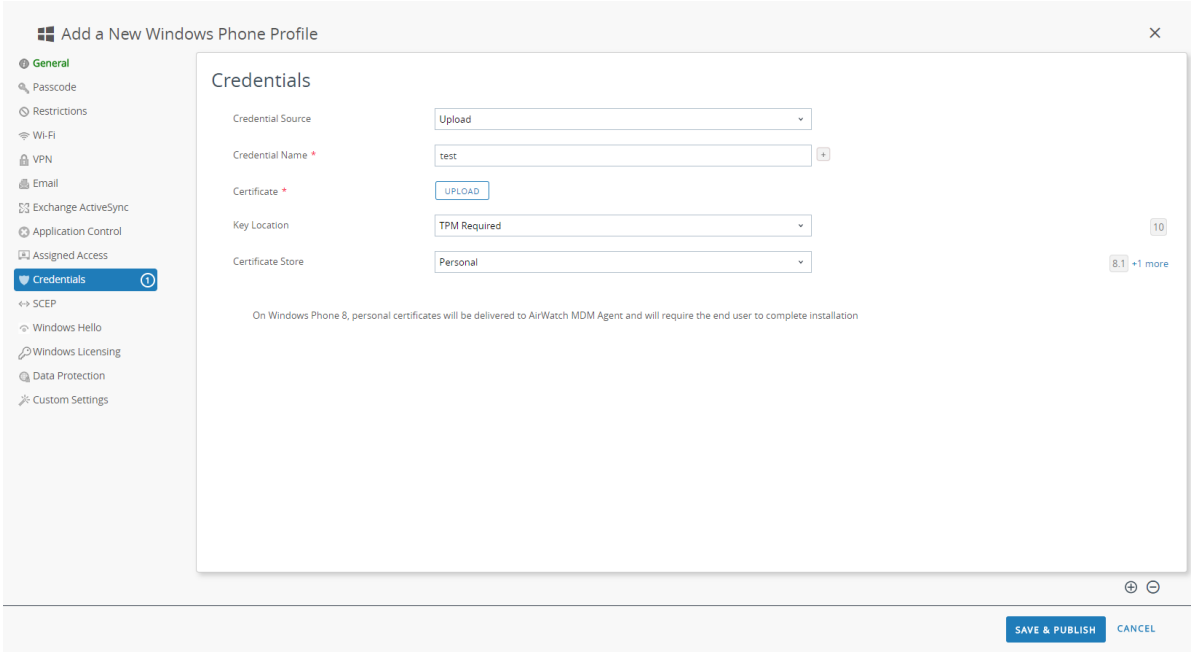


STEP 4 | （選用）如果您的 GlobalProtect 部署需要用戶端憑證驗證，請進行 **Credentials**（認證）設定：

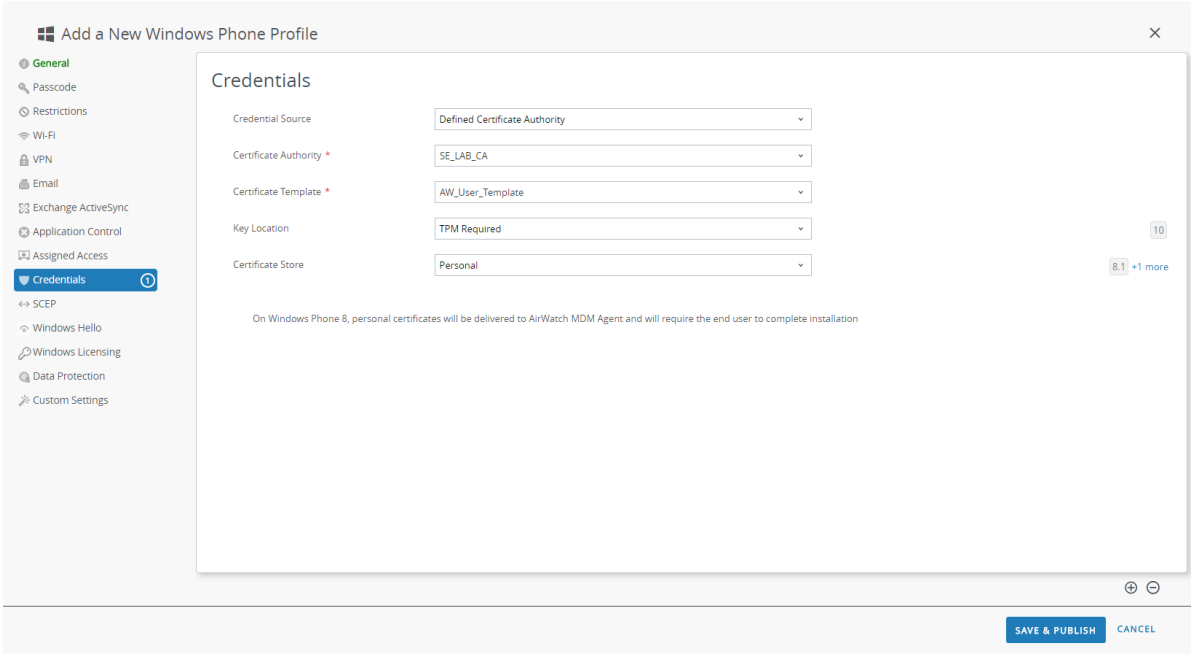
- 若要從 AirWatch 使用者提取用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **User Certificate**（使用者憑證）。
  2. 選取 **S/MIME Signing Certificate**（**S/MIME** 簽署憑證）（預設）。



- 若要手動上載用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **Upload**（上載）。
  2. 輸入 **Credential Name**（認證名稱）。
  3. 按一下 **UPLOAD**（上載）以找到並選取您要上載的憑證。
  4. 選取憑證後，按一下 **SAVE**（儲存）。
  5. 選取您想要儲存憑證私密金鑰的 **Key Location**（金鑰位置）：
     - **TPM Required**（TPM 要求）—在信任的平台模組上儲存私密金鑰。如果信任的平台模組在端點上不可用，則無法安裝私密金鑰。
     - **TPM If Present**（如果存在 **TPM**）—如果在端點上可用，在信任的平台模組上儲存私密金鑰。如果信任的平台模組在端點上不可用，私密金鑰將儲存在端點軟體中。
     - **Software**（軟體）—在端點軟體中儲存私密金鑰。
     - **Passport**（通行證）—儲存私密金鑰至 Microsoft Passport。若要使用此選項，必須在端點上安裝 AirWatch Protection Agent。
  6. 將 **Certificate store**（憑證存放區）設定為 **Personal**（個人）。



- 若要使用預先定義的憑證授權單位和範本：
  1. 將 **Credential Source**（認證來源）設定為 **Defined Certificate Authority**（定義的憑證授權單位）。
  2. 選取您想要取得憑證的 **Certificate Authority**（憑證授權單位）。
  3. 選取憑證授權單位的 **Certificate Template**（憑證範本）。
  4. 選取您想要儲存憑證私密金鑰的 **Key Location**（金鑰位置）：
     - **TPM Required**（**TPM** 要求）—在信任的平台模組上儲存私密金鑰。如果信任的平台模組在端點上不可用，則無法安裝私密金鑰。
     - **TPM If Present**（如果存在 **TPM**）—如果在端點上可用，在信任的平台模組上儲存私密金鑰。如果信任的平台模組在端點上不可用，私密金鑰將儲存在端點軟體中。
     - **Software**（軟體）—在端點軟體中儲存私密金鑰。
     - **Passport**（通行證）—儲存私密金鑰至 Microsoft Passport。若要使用此選項，必須在端點上安裝 AirWatch Protection Agent。
  5. 將 **Certificate store**（憑證存放區）設定為 **Personal**（個人）。

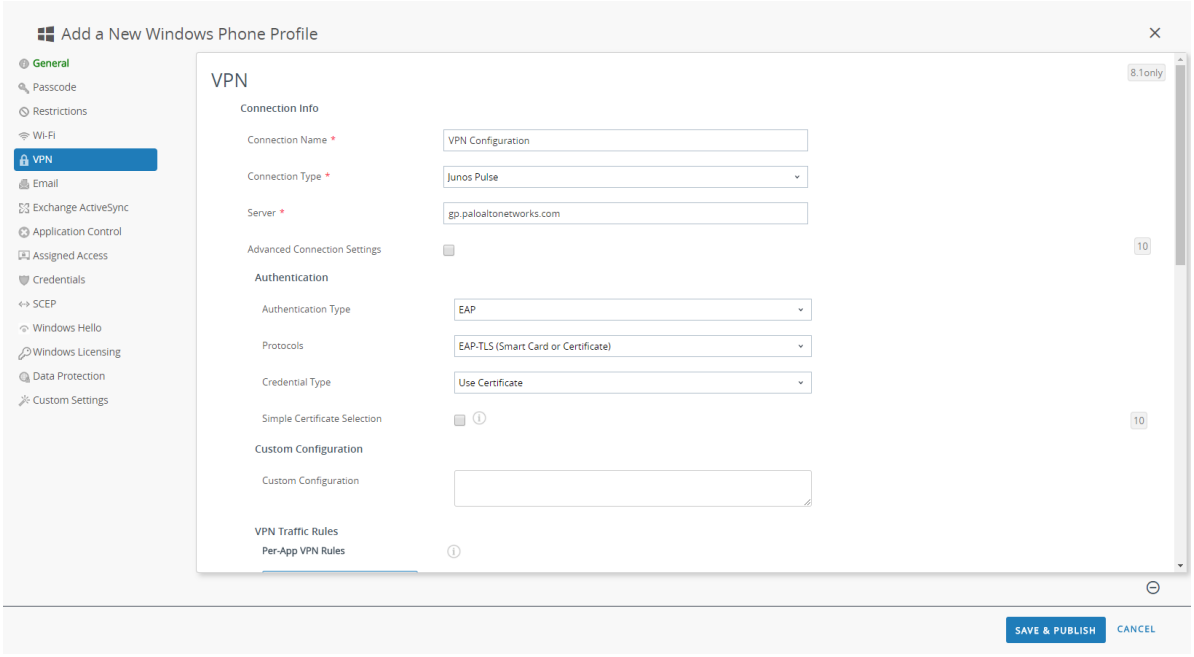


STEP 5 | 設定 **VPN** 設定：

1. 輸入要端點顯示的 **Connection Name**（連線名稱）。
2. 選取替代 **Connection Type**（連線類型）供應商（不選取 **IKEv2**、**L2TP**、**PPTP** 或 **Automatic**（自動），因為其沒有 GlobalProtect VPN 設定檔所需的相關廠商設定）。

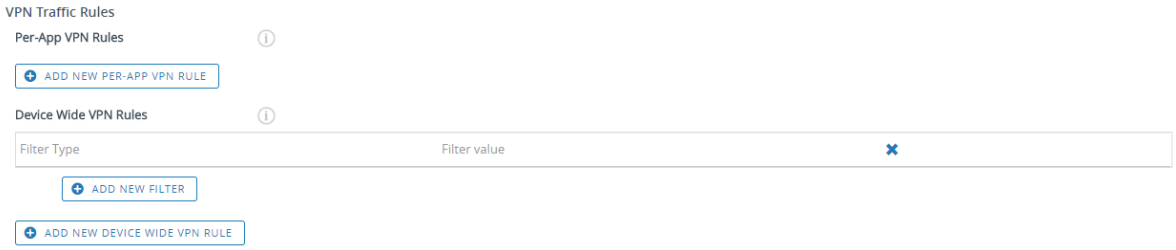
   

   您必須選取替代廠商，因為 *AirWatch* 尚未將 *GlobalProtect* 列為 *Windows* 端點的正式連線供應商。
3. 在 **Server**（伺服器）欄位，輸入使用者連線的 GlobalProtect 入口網站主機或 IP 位址。
4. 在驗證區域，選取 **Authentication Type**（驗證類型）以指定驗證一般使用者的方法。

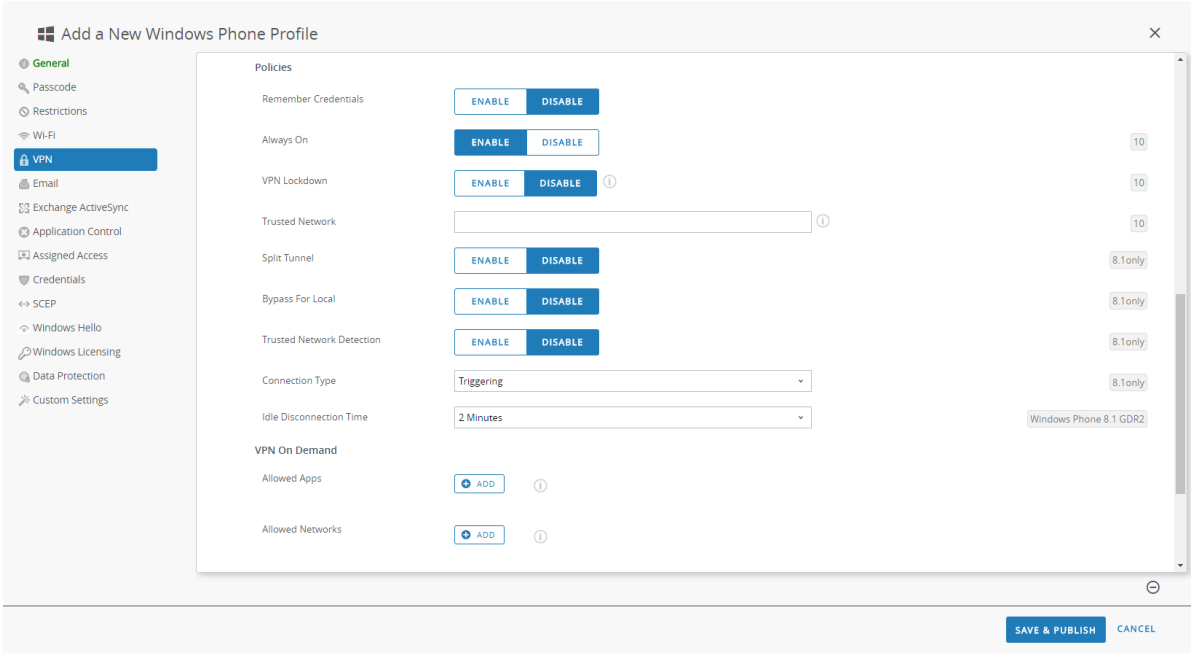


5. （選用）若要允許 GlobalProtect 儲存使用者認證，請 **ENABLE**（啟用）此選項以在原則區域內 **Remember Credentials**（記住認證）。
6. （選用）在 VPN 流量規則區域內，**ADD NEW DEVICE WIDE VPN RULE**（新增裝置範圍內的 **VPN** 規則）以透過 VPN 通道傳送符合特定路由的流量。這些規則不受應用程式約束，但在端點上評估。如果流量符合指定的相符條件，其透過 VPN 通道路由。

   透過按一下 **ADD NEW FILTER**（新增篩選條件），然後輸入 **Filter Type**（篩選類型）及對應的 **Filter Value**（篩選值）來新增比對準則。



7. 若要一直保持 GlobalProtect 連線，請在原則區域內設定下列選項之一：
   - **ENABLE**（啟用）**Always On**（一直開啟）以強制安全連線一直開啟。
   - **ENABLE**（啟用）**VPN Lockdown**（**VPN** 鎖定）以強制安全連線一直開啟和保持連線，並在應用程式未連線時停用網路存取。AirWatch 內的 **VPN Lockdown**（**VPN** 鎖定）與您在 GlobalProtect 入口網站組態中設定的 **Enforce GlobalProtect for Network Access**（強制執行 **GlobalProtect** 連線以進行網路存取）選項類似。



8. （選用）指定您想要在檢測到信任的網路連線時，GlobalProtect 僅連線至的 **Trusted Network**（信任的網路）位址。

STEP 6 | **SAVE & PUBLISH**（儲存和發佈）您的變更。

STEP 7 | 若要將連線類型供應商設定為 GlobalProtect，請編輯 XML 內的 VPN 設定檔。

若要最小化原 *XML* 內的其他編輯，在您匯出組態前，檢閱您的 *VPN* 設定檔內的設定。如果您需要在匯出 *VPN* 設定檔後變更設定，您可以在原 *XML* 中進行變更，或在 *VPN* 設定檔中更新設定並再次執行此步驟。

1. 在 **Devices**（裝置）> **Profiles**（設定檔）> **List View**（清單檢視），選取您在之前步驟中新增的設定檔旁的無線電按鈕，然後選取表格頂部的 **</>XML**。AirWatch 會打開設定檔的 XML 檢視。
2. **Export**（匯出）設定檔，然後在您選取的文字編輯器中打開。
3. 為 GlobalProtect 編輯下列設定：

- 在指定 `PluginPackageFamilyName` 的 `LoclURI` 元件中變更元件為：

  `<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>`
- 在後續的 `Data` 元件中，變更數值為：

  `<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>`

1. 將您的變更儲存至匯出的設定檔。
2. 返回 AirWatch 並選取 **Devices**（裝置）> **Profiles**（設定檔）> **List View**（清單檢視）。
3. 建立並命名一個新的設定檔（選取 **ADD**（新增）> **Add Profile**（新增設定檔）> **Windows** > **Windows Phone**（**Windows** 手機））。
4. 選取 **Custom Settings**（自訂設定）> **Configure**（設定），然後複製並粘上編輯的組態。
5. **SAVE & PUBLISH**（儲存和發佈）您的變更。

STEP 8 | 透過從 **Devices**（裝置）> **Profiles**（設定檔）> **List View**（清單檢視）選取原始設定檔，然後選取 **More Actions**（其他動作）> **Deactivate**（停用），來清除原始設定檔。AirWatch 會將設定檔移動至非使用中清單。

STEP 9 | 測試組態。

透過 **Microsoft Intune** 進行一直開啟 **VPN** 設定

Microsoft Intune 是讓您可以從中央位置管理行動端點的雲端企業行動管理平台。GlobalProtect 應用程式提供 Microsoft Intune 在裝置或應用程式等級管理的防火牆和行動端點之間的安全連線。使用 Android 的 GlobalProtect 作為安全連線，可進行對流量的一致檢查和對網路安全政策的強化，以預防行動端點上的威脅。

有關如何使用 Microsoft Intune 進行一直開啟 VPN 設定的資訊，請參閱以下幾節：

- 透過 Microsoft Intune 對 iOS 端點進行一直開啟 VPN 設定
- 透過 Microsoft Intune 對 Windows 10 UWP 端點進行一直開啟 VPN 設定

透過 *Microsoft Intune* 對 *iOS* 端點進行一直開啟 *VPN* 設定

在一直開啟 VPN 設定中，安全 GlobalProtect 連線一直開啟。符合 GlobalProtect 閘道上所設定特定篩選條件（如連接埠和 IP 位址）的流量一直透過 VPN 通道進行路由傳送。

按照下列步驟使用 Microsoft Intune 對 iOS 端點進行一直開啟 VPN 設定：

STEP 1 | 為 iOS 下載 GlobalProtect 應用程式。

- 透過 Microsoft Intune 部署 GlobalProtect 行動應用程式.

- 從 App Store 直接下載 GlobalProtect 應用程式。

STEP 2 | （選用）如果您的部署需要用基於憑證的驗證，請設定憑證設定檔。

STEP 3 | 建立新 iOS VPN 設定檔。

- 將 **Platform**（平台）設定為 **iOS**。

STEP 4 | 為 iOS 端點設定一直開啟 VPN 設定。

- 將 **Connection type**（連線類型）設定為 **Palo Alto Networks GlobalProtect**。

透過 *Microsoft Intune* 對 *Windows 10 UWP* 端點進行一直開啟 *VPN* 設定

在一直開啟 VPN 設定中，安全 GlobalProtect 連線一直開啟。符合 GlobalProtect 閘道上所設定特定篩選條件（如連接埠和 IP 位址）的流量一直透過 VPN 通道進行路由傳送。

按照下列步驟使用 Microsoft Intune 對 Windows 10 UWP 端點進行一直開啟 VPN 設定：

STEP 1 | 為 Windows 10 UWP 下載 GlobalProtect 應用程式：

- 透過 Microsoft Intune 部署 GlobalProtect 行動應用程式.
- 從 Microsoft Store 直接下載 GlobalProtect 應用程式。

STEP 2 | （選用）如果您的部署需要用基於憑證的驗證，請設定憑證設定檔。

STEP 3 | 建立新 Windows 10 UWP VPN 設定檔。

- 將 **Platform**（平台）設定為 **Windows 10** 及更新版本。

STEP 4 | 為 Windows 10 UWP 端點設定一直開啟 VPN 設定。

- 將 **Connection type**（連線類型）設定為 **Palo Alto Networks GlobalProtect**。
- 啟用 **Always On**（一直開啟）VPN。

透過 **MobileIron** 進行一直開啟 **VPN** 設定

MobileIron 是讓您可以從中央控制台管理行動端點的企業行動管理平台。GlobalProtect 應用程式提供 MobileIron 在裝置或應用程式等級管理的防火牆和行動端點之間的安全連線。使用 Android 的 GlobalProtect 作為安全連線，可進行對流量的一致檢查和對網路安全政策的強化，以預防行動端點上的威脅。

有關如何使用 MobileIron 進行一直開啟 VPN 設定的資訊，請參閱以下幾節：

- 透過 MobileIron 對 iOS 端點進行一直開啟 VPN 設定
- 透過 MobileIron 對 Android 端點進行一直開啟 VPN 設定

透過 *MobileIron* 對 *iOS* 端點進行一直開啟 *VPN* 設定

在一直開啟 VPN 設定中，安全 GlobalProtect 連線一直開啟。符合 GlobalProtect 閘道上所設定特定篩選條件（如連接埠和 IP 位址）的流量一直透過 VPN 通道進行路由傳送。

按照下列步驟使用 MobileIron 對 iOS 端點進行一直開啟 VPN 設定：

STEP 1 | 為 iOS 下載 GlobalProtect 應用程式。

- 透過 MobileIron 部署 GlobalProtect 行動應用程式.
- 從 App Store 直接下載 GlobalProtect 應用程式。

STEP 2 | （選用）如果您的部署需要用基於憑證的驗證，請新增憑證設定，然後設定憑證設定。

STEP 3 | 新增一直開啟 VPN 設定。

- 將設定類型設定為 **Always On VPN**（一直開啟 **VPN**）。

STEP 4 | 為 iOS 設定一直開啟 VPN 設定。

透過 *MobileIron* 對 *Android* 端點進行一直開啟 *VPN* 設定

在一直開啟 VPN 設定中，安全 GlobalProtect 連線一直開啟。符合 GlobalProtect 閘道上所設定特定篩選條件（如連接埠和 IP 位址）的流量一直透過 VPN 通道進行路由傳送。

按照下列步驟使用 MobileIron 對 Android 端點進行一直開啟 VPN 設定：

STEP 1 | 為 Android 下載 GlobalProtect 應用程式。

- 透過 MobileIron 部署 GlobalProtect 行動應用程式.
- 從 Google Play 直接下載 GlobalProtect 應用程式。

STEP 2 | （選用）如果您的部署需要用基於憑證的驗證，請新增憑證設定，然後設定憑證設定。

STEP 3 | 新增一直開啟 VPN 設定。

- 將設定類型設定為 **Always On VPN**（一直開啟 **VPN**）。

STEP 4 | 為 Android 設定一直開啟 VPN 設定。

使用 **Google** 管理控制台進行一直開啟 **VPN** 設定

Google 管理控制台是讓您可以從中央控制台管理 Chromebooks 的雲端企業行動管理平台。GlobalProtect 應用程式提供 Google 管理控制台在裝置或應用程式等級管理的防火牆和 Chromebooks 之間的安全連線。使用 Android 的 GlobalProtect 作為安全連線，可進行對流量的一致檢查和對網路安全政策的強化，以預防行動端點上的威脅。

使用 *Google* 管理控制台對 *Chromebooks* 進行一直開啟 *VPN* 設定

Chromebook 透過延伸支援適用於 Android 的 GlobalProtect 應用程式，對一直開啟 VPN 提供支援。在一直開啟 VPN 設定中，安全 GlobalProtect 連線一直開啟。符合 GlobalProtect 閘道上所設定特定篩選條件（如連接埠和 IP 位址）的流量一直透過 VPN 通道進行路由傳送。透過允許您的一般使用者在 Chromebook 上執行適用於 Android 的 GlobalProtect 應用程式，您可確保其始終與 GlobalProtect 連線並可存取一直開啟安全性。

- 僅 特定 Chromebook 支援適用於 *Android* 的 *GlobalProtect* 應用程式。
- 不支援 *Android* 應用程式的 *Chromebook* 必須繼續使用適用於 *Chrome* 的 *GlobalProtect* 應用程式。但是，這些 *Chromebook* 將不支援一直開啟 *VPN*。
- 如果 *Chromebook* 上安裝了適用於 *Android* 的 *GlobalProtect* 應用程式以支援一直開啟 *VPN* 功能，則不應在同一 *Chromebook* 上安裝適用於 *Chrome* 的 *GlobalProtect* 應用程式。

按照下列步驟使用 Google 管理控制台對 Chromebooks 進行一直開啟 VPN 設定。

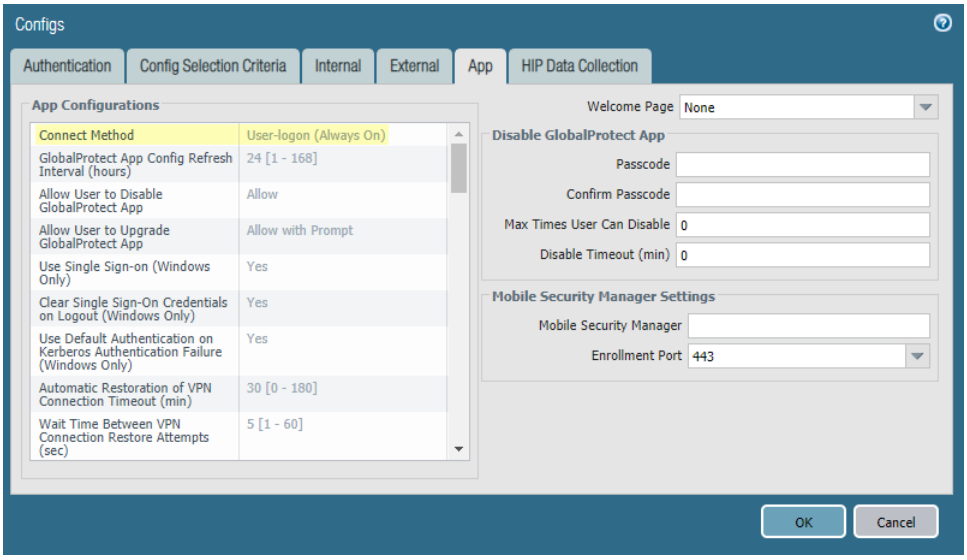
下列步驟僅適用于透過 Google 管理控制台在受管理的 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式。AirWatch 目前不支援在受管理的 Chromebook 上對適用於 Android 的 GlobalProtect 應用程式設定一直開啟 VPN 組態。

STEP 1 | 從 Palo Alto Networks 防火牆中，設定 GlobalProtect 入口網站存取權。

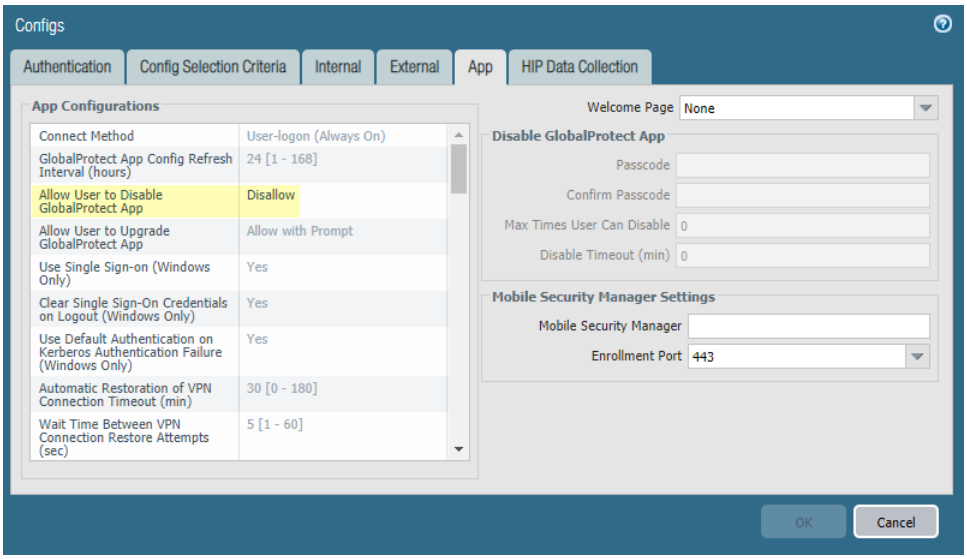
STEP 2 | 定義 GlobalProtect 代理程式組態.

STEP 3 | 自訂 GlobalProtect 應用程式.

- 若要將 GlobalProtect 連線設為一直開啟，請將 **Connect Method**（連線方法）設為 **User-logon (Always On)**（使用者登入（一直開啟））。



- 若要防止使用者停用 GlobalProtect 應用程式，請將 **Allow User to Disable GlobalProtect App**（允許使用者停用 **GlobalProtect** 應用程式）選項設為 **Disallow**（不允許）。

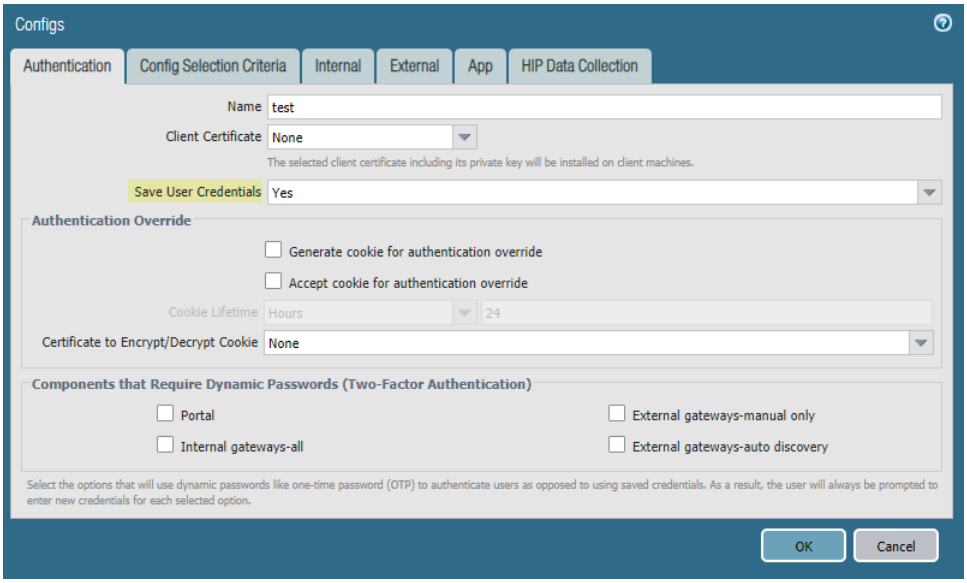


STEP 4 | 允許對 GlobalProtect 進行透明驗證。

若要防止使用者略過 GlobalProtect 驗證提示，從而在與 GlobalProtect 中斷連線時繞過 GlobalProtect，請設定下列選項之一以進行透明驗證：

- 允許使用者使用 用戶端憑證驗證 對 GlobalProtect 進行透明驗證。
- 允許 GlobalProtect 應用程式儲存使用者名稱和密碼以透明登入。

1. 從您的入口網站代理程式組態中（**Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **Agent**（代理程式）> *<agent-config>*），選取 **Authentication**（驗證）。
2. 將 **Save User Credentials**（儲存使用者認證）選項設為 **Yes**（是）。

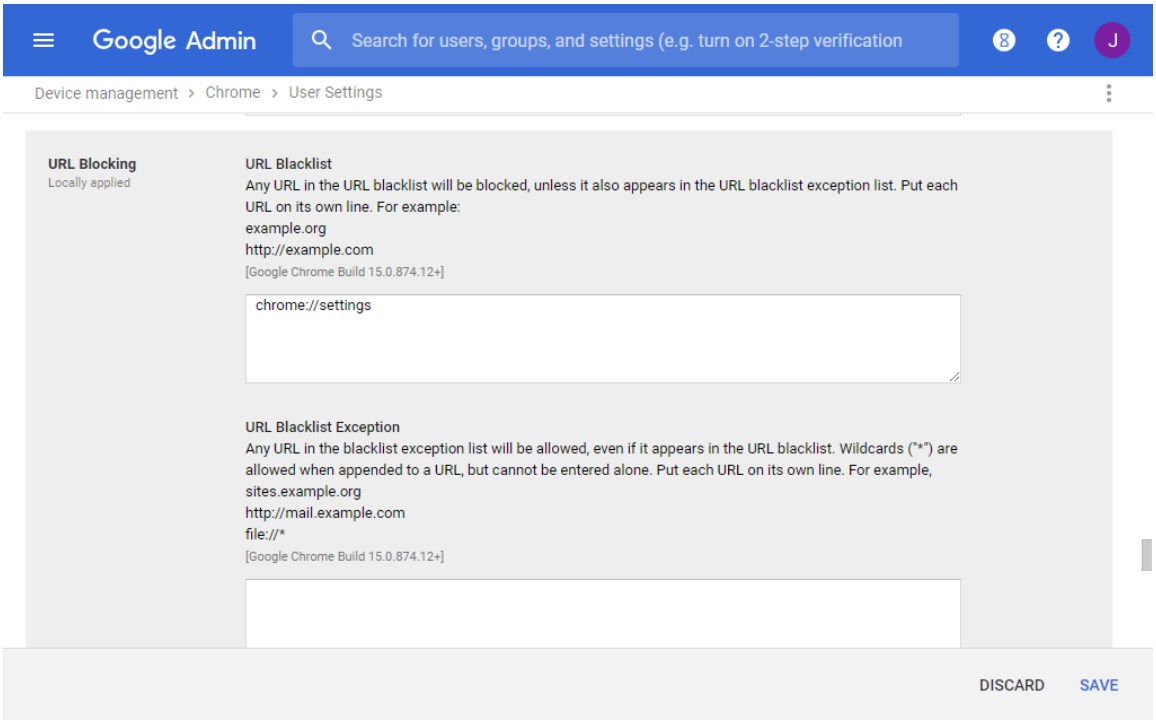


3. 按兩下 **OK**（確定）以儲存入口網站代理程式組態。

STEP 5 | 在防火牆中 **Commit**（提交）您的變更。

STEP 6 | 防止 Chromebook 使用者使用 Chrome OS VPN 設定繞過 GlobalProtect。

1. 以管理員身份登入 Google 管理控制台 。
2. 透過 Google 管理控制台在受管理的 Chromebook 上部署適用於 Android 的 GlobalProtect 應用程式 在所有受管理的 Chromebooks 上。
3. 將 Chrome 設定列入黑名單 (`chrome://settings`) 以防止使用者修改任何 VPN 設定：
   1. 選取 **Device Management**（裝置管理）> **Chrome management**（**Chrome** 管理）> **User Settings**（使用者設定）。
   2. 在 Content > URL Blocking（內容 > URL 封鎖）區域，在 **URL Blacklist**（**URL** 黑名單）文字方塊中輸入 `chrome://settings`。



4. **Save**（儲存）變更。

使用者啟動遠端存取 *VPN* 組態

在遠端存取（視需要）VPN 組態中，使用者必須手動啟動 GlobalProtect 應用程式才能建立安全 GlobalProtect 連線。GlobalProtect 應用程式會連線至 GlobalProtect 入口網站（在使用者登入時），以提交使用者與主機資訊，並擷取代理程式組態。當應用程式從入口網站收到代理程式組態後，其會連線並建立至代理程式組態中指定 GlobalProtect 閘道的 VPN 通道。

有關如何使用支援的行動裝置管理系統設定使用者啟動遠端存取 VPN 組態的資訊，請參閱以下幾節：

- 透過 AirWatch 設定使用者啟動遠端存取 VPN 組態
- 透過 Microsoft Intune 設定使用者啟動遠端存取 VPN 組態
- 透過 MobileIron 設定使用者啟動遠端存取 VPN 組態

透過 AirWatch 設定使用者啟動遠端存取 VPN 組態

AirWatch 是讓您可以從中央控制台管理行動端點的企業行動管理平台。GlobalProtect 應用程式提供 AirWatch 管理行動裝置之間的安全連線，且防火牆位於端點或應用程式等級。使用 Android 的 GlobalProtect 作為安全連線，可進行對流量的一致檢查和對網路安全政策的強化，以預防行動端點上的威脅。

有關如何使用 AirWatch 設定使用者啟動遠端存取 VPN 組態的資訊，請參閱以下幾節：

- 透過 AirWatch 為 iOS 端點設定使用者啟動遠端存取 VPN 組態
- 透過 AirWatch 為 Windows 10 UWP 端點設定使用者啟動遠端存取 VPN 組態

透過 *AirWatch* 為 *iOS* 端點設定使用者啟動遠端存取 *VPN* 組態

在遠端存取（視需要）VPN 組態中，使用者必須手動啟動應用程式才能建立安全 GlobalProtect 連線。只有在使用者啟動並建立連線後，符合 GlobalProtect 閘道上所設定特定篩選條件（如連接埠和 IP 位址）的流量才會透過 VPN 通道進行路由傳送。

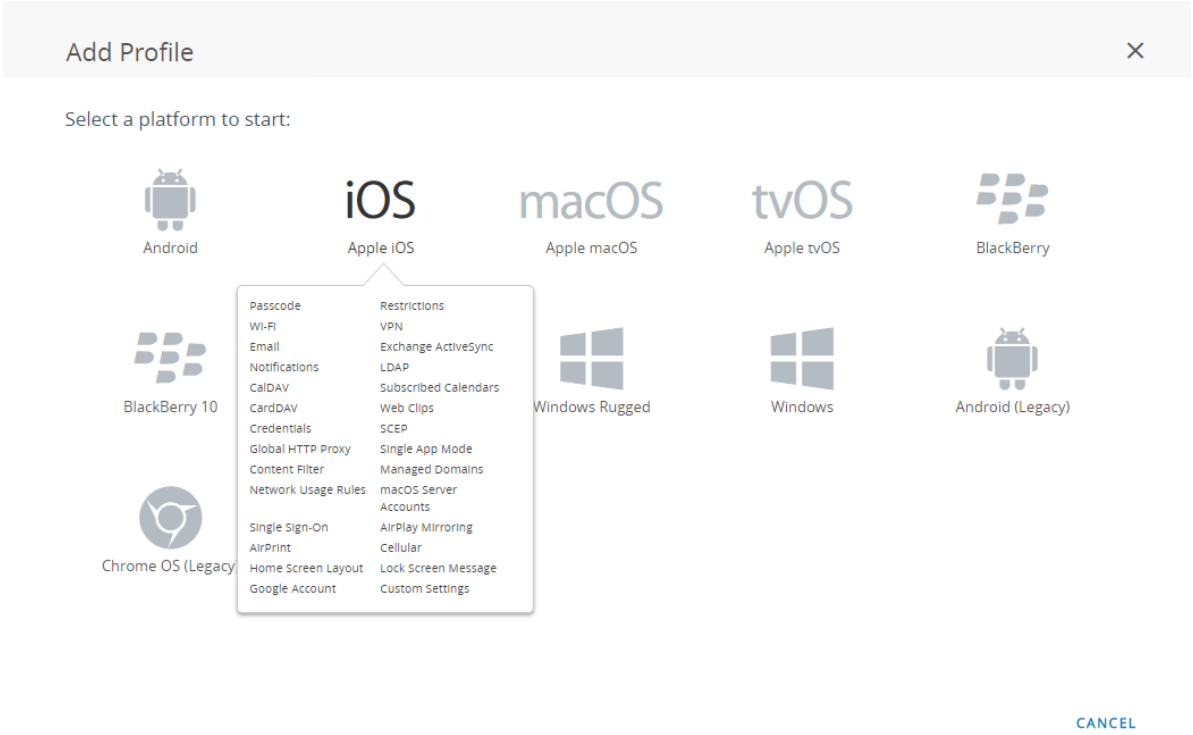
按照下列步驟使用 AirWatch 對 iOS 端點設定使用者啟動遠端存取 VPN 組態：

STEP 1 | 為 iOS 下載 GlobalProtect 應用程式。

- 透過 AirWatch 部署 GlobalProtect 行動應用程式。
- 從 App Store 直接下載 GlobalProtect 應用程式。

STEP 2 | 從 AirWatch 主控台修改現有 Apple iOS 設定檔或新增一個。

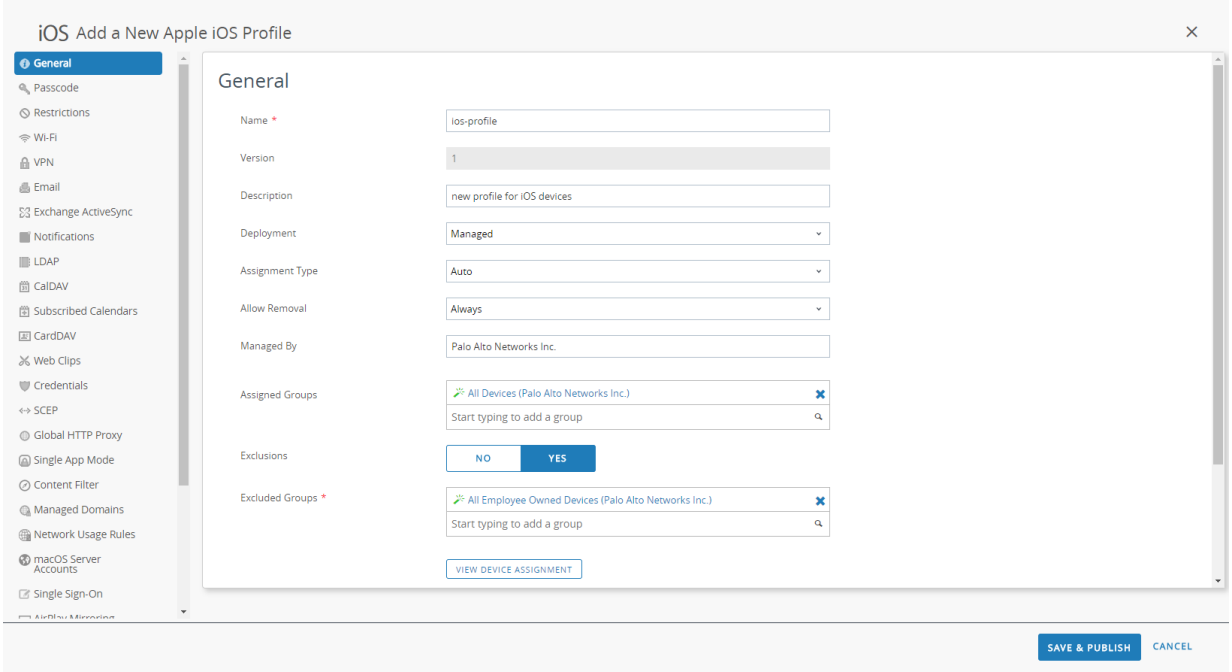
1. 選取 **Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles**（設定檔），然後 **ADD**（新增）新的設定檔。
2. 從平台清單選取 **iOS**。



STEP 3 | 設定**General**（一般）設定：

1. 輸入設定檔的 **Name**（名稱）。
2. （選用）輸入說明設定檔用途的簡短**Description**（描述）。
3. （選用）選取 **Deployment**（部署）方法，它決定設定檔是否會在取消註冊時自動移除—無論是 **Managed**（受管理）（設定檔被移除）或 **Manual**（手動）（設定檔保持安裝直到被一般使用者移除）。
4. （選用）選取 **Assignment Type**（指派類型）以決定設定檔如何部署至端點。選取 **Auto**（自動）將設定檔自動部署至所有端點，選取 **Optional**（選用）讓一般使用者能從自助式入口網站 (SSP) 安裝設定檔，或手動部署設定檔至個別端點，或選取 **Compliance**（合規性）在一般使用者違反套用於端點的合規性原則時部署設定檔。

5. （選用）選取 **Allow Removal**（允許移除）以決定一般使用者能否移除設定檔。選取 **Always**（一律）讓一般使用者能在任何時候手動移除設定檔，選取 **Never**（絕不）防止一般使用者移除設定檔，或選取 **With Authorization**（透過授權）讓經過管理員授權的一般使用者能移除設定檔。選取 **With Authorization**（透過授權）會新增必要的密碼。
6. （選用）在 **Managed By**（被管理）欄位，輸入帶有設定檔管理存取的組織群組。
7. （選用）在 **Assigned Groups**（指派的群組）欄位，新增您希望新增設定檔的智慧群組。此欄位包含選項以建立新智慧群組，該智慧群組可透過規格設定用於最小 OS、設備型號、擁有權類別、組織群組等。
8. （選用）表示您是否希望包含任何 **Exclusions**（排除）至此設定檔的指派。如果選取 **Yes**（是），會顯示 **Excluded Groups**（排除群組）欄位，讓您可以選取希望從此設定檔指派中排除的智慧群組。
9. （選用）如果您啟用選項以 **Install only on devices inside selected areas**（僅在選定區域內的裝置上安裝），則設定檔僅可安裝在指定地理圍欄或 iBeacon 區域的端點上。出現提示時，請在 **Assigned Geofence Areas**（指定地理圍欄區域）欄位新增地理圍欄或 iBeacon 區域。
10. （選用）如果 **Enable Scheduling and install only during selected time periods**（僅在選定的時間段內啟用排程與安裝），您可套用時間排程（**Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles Settings**（設定檔設定）> **Time Schedules**（時間排程））至設定檔安裝，限制在端點上安裝設定檔的時間。出現提示時，請在 **Assigned Schedules**（指派排程）欄位輸入排程名稱。
11. （選用）選取您希望設定檔從所有端點移除的 **Removal Date**（移除日期）。

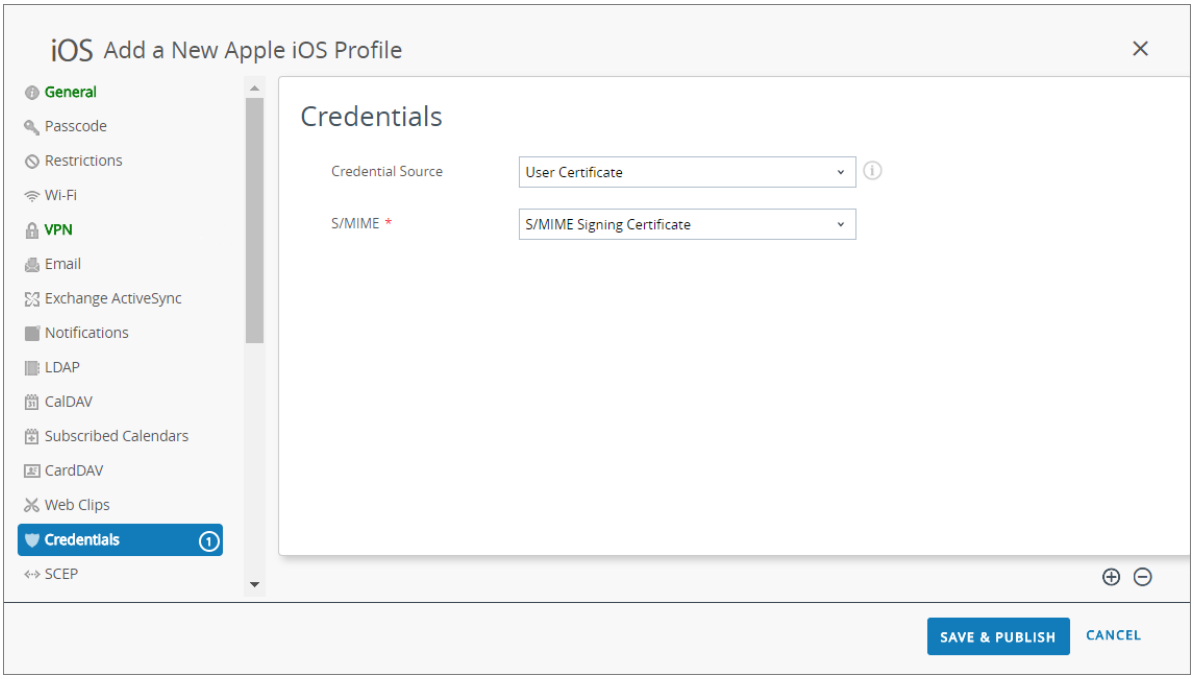


STEP 4 | 設定 **Credentials**（認證） 設定：

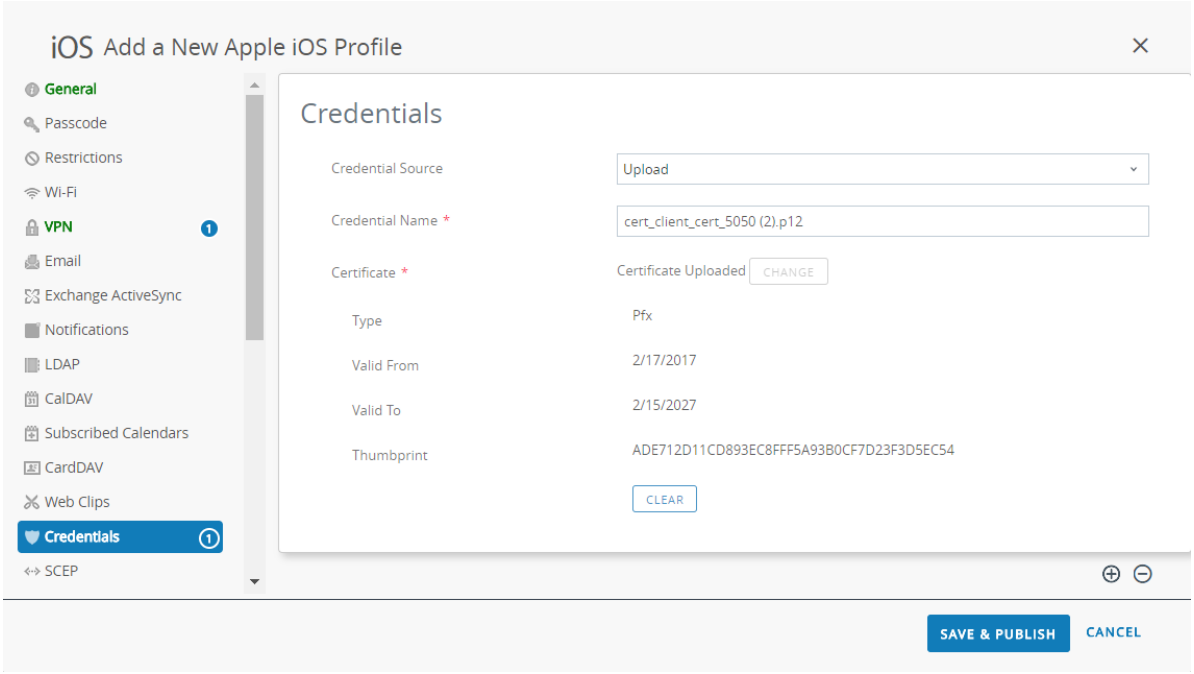
iOS 端點的所有遠端存取 *VPN* 組態都需要基於憑證的驗證。

要求的最低版本為 *iOS 12*，如果您想要透過用戶端憑證進行 *GlobalProtect* 用戶端驗證，您必須將用戶端憑證部署為從 *MDM* 伺服器推送的 *VPN* 設定檔的一部分。如果您使用任何其他方法部署來自 *MDM* 伺服器的用戶端憑證，則 *GlobalProtect* 應用程式將無法使用憑證。

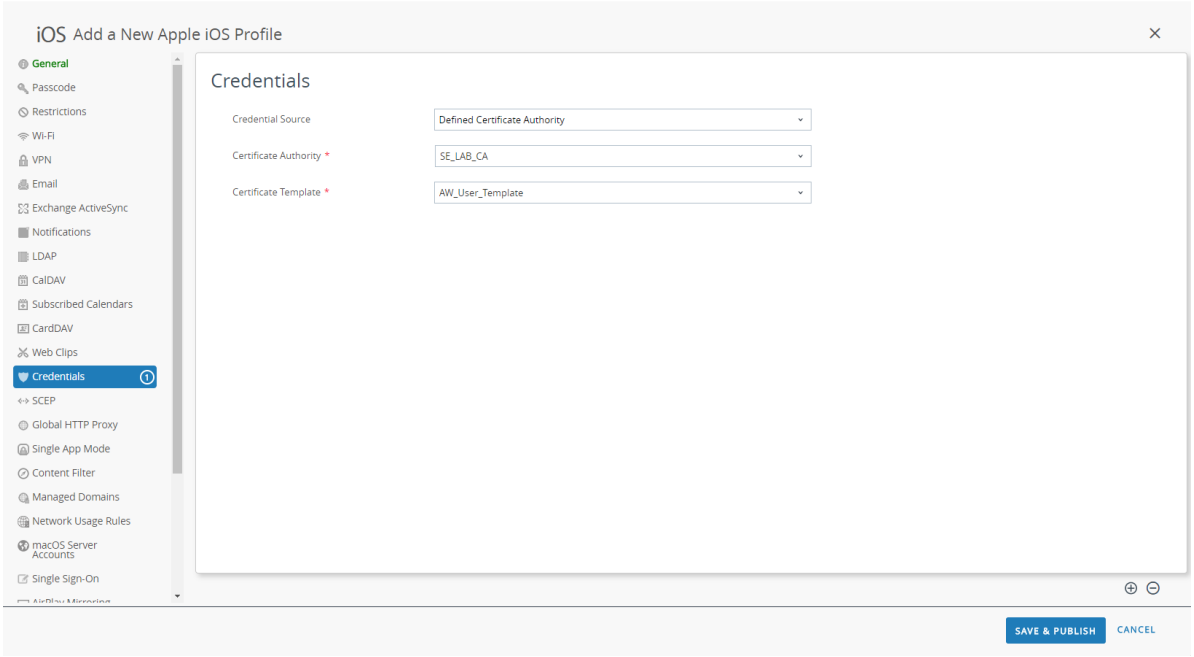
- 若要從 AirWatch 使用者提取用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **User Certificate**（使用者憑證）。
  2. 選取 **S/MIME Signing Certificate**（**S/MIME** 簽署憑證）（預設）。



- 若要手動上載用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **Upload**（上載）。
  2. 輸入 **Credential Name**（認證名稱）。
  3. 按一下 **UPLOAD**（上載）以找到並選取您要上載的憑證。
  4. 選取憑證後，按一下 **SAVE**（儲存）。



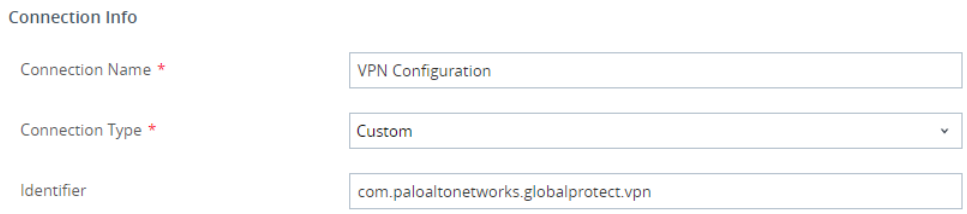
- 若要使用預先定義的憑證授權單位和範本：
  1. 將 **Credential Source**（認證來源）設定為 **Defined Certificate Authority**（定義的憑證授權單位）。
  2. 選取您想要取得憑證的 **Certificate Authority**（憑證授權單位）。
  3. 選取憑證授權單位的 **Certificate Template**（憑證範本）。



STEP 5 | 設定 **VPN** 設定：

1. 輸入要端點顯示的 **Connection Name**（連線名稱）。
2. 選取網路 **Connection Type**（連線類型）：
   - 對於 GlobalProtect 應用程式 4.1.x 及更早版本，請選取 **Palo Alto Networks GlobalProtect**。
   - 對於 GlobalProtect 應用程式 5.0 及更新版本，請選取 **Custom**（自訂）。
3. （選用）如果您將 **Connection Type**（連線類型）設定為 **Custom**（自訂），請在 **Identifier**（識別碼）欄位輸入下列捆綁 ID 以識別 GlobalProtect 應用程式：

   com.paloaltonetworks.globalprotect.vpn

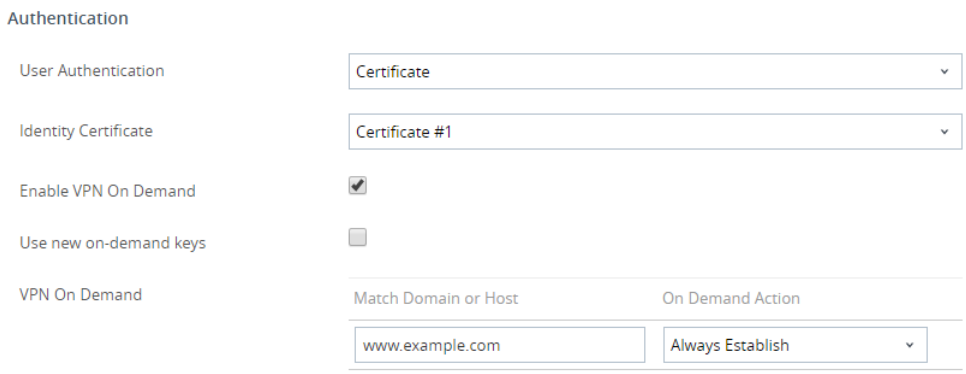


4. 在 **Server**（伺服器）欄位，輸入使用者連線的 GlobalProtect 入口網站主機或 IP 位址。
5. （選用）輸入 VPN **Account**（帳戶）用戶名或按一下新增 (+) 按鈕以檢視您可以插入的支援查閱值。
6. （選用）在 **Disconnect on idle**（閒置時中斷連線）欄位，指定應用程式停止透過 VPN 通道路由流量後端點登出 GlobalProtect 應用程式的時間（秒）。
7. 在驗證區域，將使用者 **Authentication**（驗證）方法設定為 **Certificate**（憑證）。

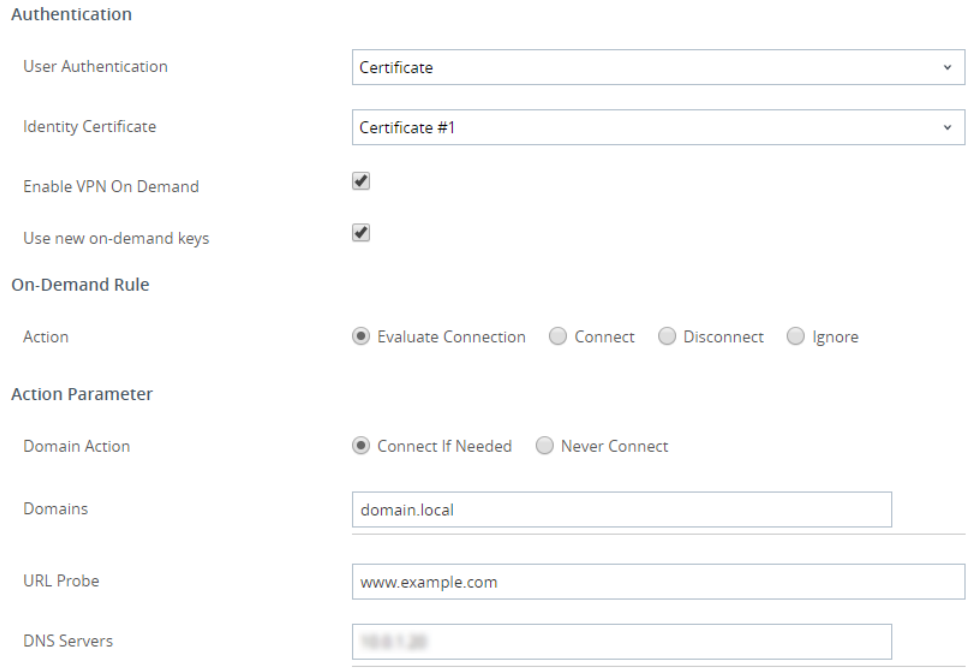
   iOS 端點的所有遠端存取 *VPN* 組態都需要基於憑證的驗證。

8. 出現提示時，請選取 GlobalProtect 將用於驗證使用者的 **Identity Certificate**（識別身分憑證）。**Identity Certificate**（識別身分憑證）與您在 **Credentials**（認證）設定中設定的憑證相同。
9. 請確保 **Enable VPN On Demand**（視需要啟用 **VPN**）選項已啟用（預設設定）。

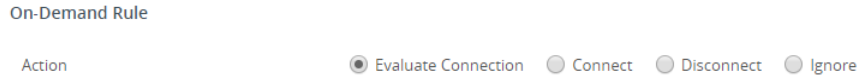
10. （選用）設定舊版 **VPN On-Demand**（視需要 **VPN**）連線規則：
    - **Match Domain or Host**（比對網域或主機）—輸入當使用者存取網域或主機名稱時觸發建立 GlobalProtect 連線的網域或主機名稱。
    - **On Demand Action**（視需要操作）—將 **On Demand Action**（視需要操作）設定為 **Establish if Needed**（根據需要建立）或 **Always Establish**（始終建立）以僅在使用者無法直接存取指定的網域或主機名稱時建立 GlobalProtect 連線。將 **On Demand Action**（視需要操作）設定為 **Never Establish**（從不建立）以防止在使用者存取指定的網域或主機名稱時建立 GlobalProtect 連線。如果連線已建立，可繼續使用。



11. （選用）透過讓 GlobalProtect 應用程式 **Use new on-demand keys**（使用新的視需要金鑰）設定更精細的視需要連線規則。您可透過按一下 **ADD RULE**（新增規則）新增多條規則。

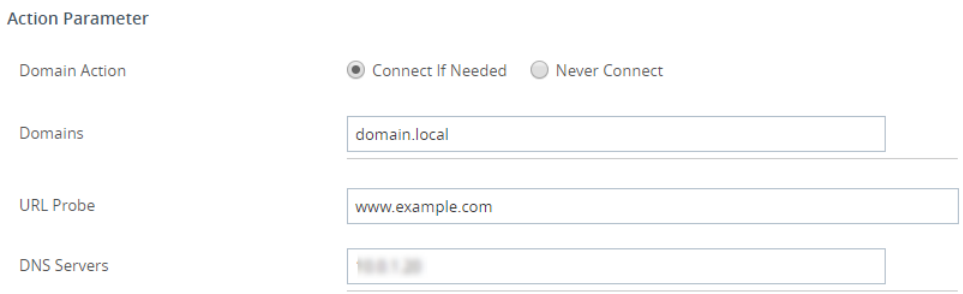


- 在視需要規則區域，選取 **Action**（操作）以根據您定義的條件來套用至 GlobalProtect 連線。
  - **Evaluate Connection**（評估連線）—根據網路和連線設定自動建立 GlobalProtect 連線。每次使用者嘗試連線至網域時，都會進行此項評估。
  - **Connect**（連線）—自動建立 GlobalProtect 連線。
  - **Disconnect**（中斷連線）—自動停用 GlobalProtect 並防止 GlobalProtect 重新連線。
  - **Ignore**（忽略）—保持現有的 GlobalProtect 連線並在 GlobalProtect 中斷連線時防止其重新連線。

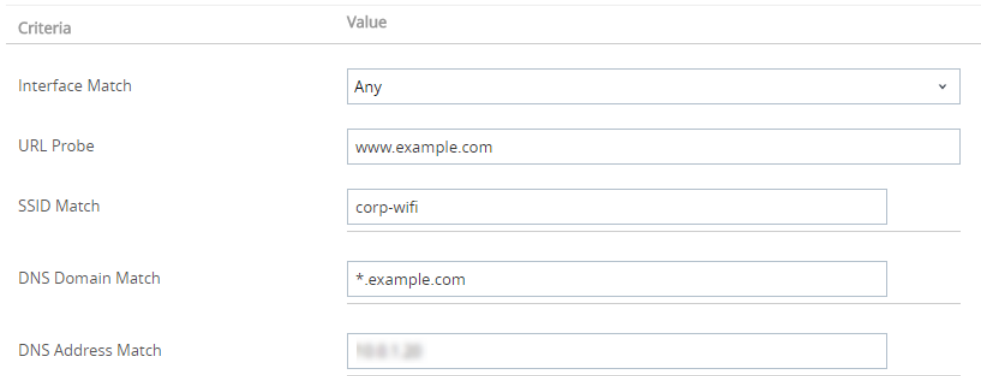


- （選用）如果您將視需要連線規則的 **Action**（操作）設定為 **Evaluate Connection**（評估連線），則您還必須設定操作參數以指定 GlobalProtect 在連線評估期間網域名稱解析失敗時是否可以嘗試重新連線（例如，當 DNS 伺服器因逾時而無法回應時）。您可透過按一下 **ADD ACTION PARAMETERS**（新增操作參數）新增多個參數。

- 將 **Domain Action**（網域操作）設定為 **Connect if Needed**（根據需要連線）以使 GlobalProtect 重新連線或 **Never Connect**（從不連線）以防止 GlobalProtect 重新連線。
- 輸入此 **Action Parameter**（操作參數）套用的 **Domains**（網域）。
- （選用）如果您將 **Domain Action**（網域操作）設定為 **Connect if Needed**（根據需要連線），則輸入您想要在 **URL Probe**（**URL** 探查）欄位中探查的 HTTP 或 HTTPS URL。如果無法解析 URL 的主機名稱，則伺服器將無法連線，或伺服器不會以 200 HTTP 狀態碼回應，GlobalProtect 連線將建立。
- （選用）如果您將 **Domain Action**（網域操作）設定為 **Connect if Needed**（根據需要連線），則輸入用於解析指定 **Domains**（網域）的 **DNS Servers**（**DNS** 伺服器）（內部或信任的外部）的 IP 位址。如果 DNS 伺服器無法連線，GlobalProtect 連線將建立。



- 設定以下條件以與您的視需要連線規則進行比對。如果端點與指定的所有條件相符，則視需要連線規則將套用至該端點。
  - **Interface Match**（介面比對）—指定連線類型以對端點的網路介面卡進行比對：**Any**（任何）、**Ethernet**、**Wi-Fi**、**Cellular**（行動網路）。
  - **URL Probe**（**URL** 探查）—輸入要與之比對的 HTTP 或 HTTPS URL。如果比對成功，將返回 200 HTTP 狀態碼。
  - **SSID Match**（**SSID** 比對）—輸入要與之比對的網路 SSID。您可透過按一下新增 (+) 按鈕新增多個網絡 SSID。對於成功的比對，端點必須至少與一個指定的網路 SSID 相符。
  - **DNS Domain Match**（**DNS** 網域比對）—輸入要與之比對的 DNS 搜尋網域。您還可以與萬用字元記錄（例如 `*.example.com`）進行比對以包含所有子網域。
  - **DNS Address Match**（**DNS** 位址比對）—輸入要與之比對的 DNS 伺服器 IP 位址。您可透過按一下新增 (+) 按鈕新增多個 DNS 伺服器 IP 位址。您還可以與包含所有未帶 IP 位址的 DNS 伺服器的單個萬用字元記錄（例如 `17.*`）進行比對。對於成功的比對，端點上列出的所有 DNS 伺服器 IP 位址都必須與指定的 DNS 伺服器 IP 位址相符。

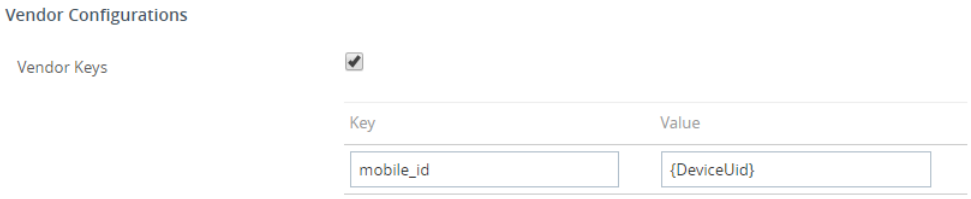


12. （選用）選取 **Proxy** 類型並進行相關設定。

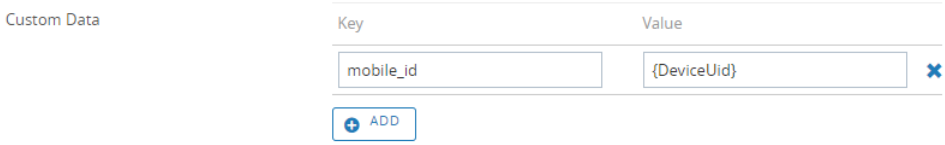
STEP 6 | （選用）（最低版本要求為 GlobalProtect 應用程式 5.0）如果您的 GlobalProtect 部署要求 HIP 與 MDM 整合，請指定唯一裝置識別碼 (UDID) 屬性。

GlobalProtect 支援與 MDM 整合以從 MDM 伺服器取得行動裝置屬性，用於以 HIP 為基礎的原則強制執行。若要使 MDM 整合能夠正常執行，GlobalProtect 應用程式必須向 GlobalProtect 閘道呈現端點的 UDID。UDID 屬性讓 GlobalProtect 應用程式能夠在以 MDM 為基礎的部署中擷取並使用 UDID 資訊。如果您從設定檔中移除 UDID 屬性，將無法再使用 MDM 整合。GlobalProtect 應用程式將產生新的 UDID，但其無法用於整合。

- 如果您使用的是 **Palo Alto Networks GlobalProtect** 網路 **Connection Type**（連線類型），請前往 **VPN** 設定並在廠商組態區域啟用 **Vendor Keys**（廠商金鑰）。將 **Key**（索引鍵）設定為 **`mobile_id`** 並將 **Value**（值）設定為 **`{DeviceUid}`**。



- 如果您使用的是 **Custom**（自訂）網路 **Connection Type**（連線類型），請前往 **VPN** 設定並在連線資訊區域 **ADD**（新增）**Custom Data**（自訂資料）。將 **Key**（索引鍵）設定為 **`mobile_id`** 並將 **Value**（值）設定為 **`{DeviceUid}`**。



STEP 7 | **SAVE & PUBLISH**（儲存和發佈）您的變更。

透過 *AirWatch* 為 *Windows 10 UWP* 端點設定使用者啟動遠端存取 *VPN* 組態

在遠端存取（視需要）VPN 組態中，使用者必須手動啟動應用程式才能建立安全 GlobalProtect 連線。只有在使用者啟動並建立連線後，符合 GlobalProtect 閘道上所設定特定篩選條件（如連接埠和 IP 位址）的流量才會透過 VPN 通道進行路由傳送。

由於 *AirWatch* 尚未將 *GlobalProtect* 作為 *Windows* 端點的正式連線供應商，您必須選取替代的 *VPN* 供應商，編輯 *GlobalProtect* 應用程式設定，並根據下列工作流程所述將組態匯入 *VPN* 設定檔。

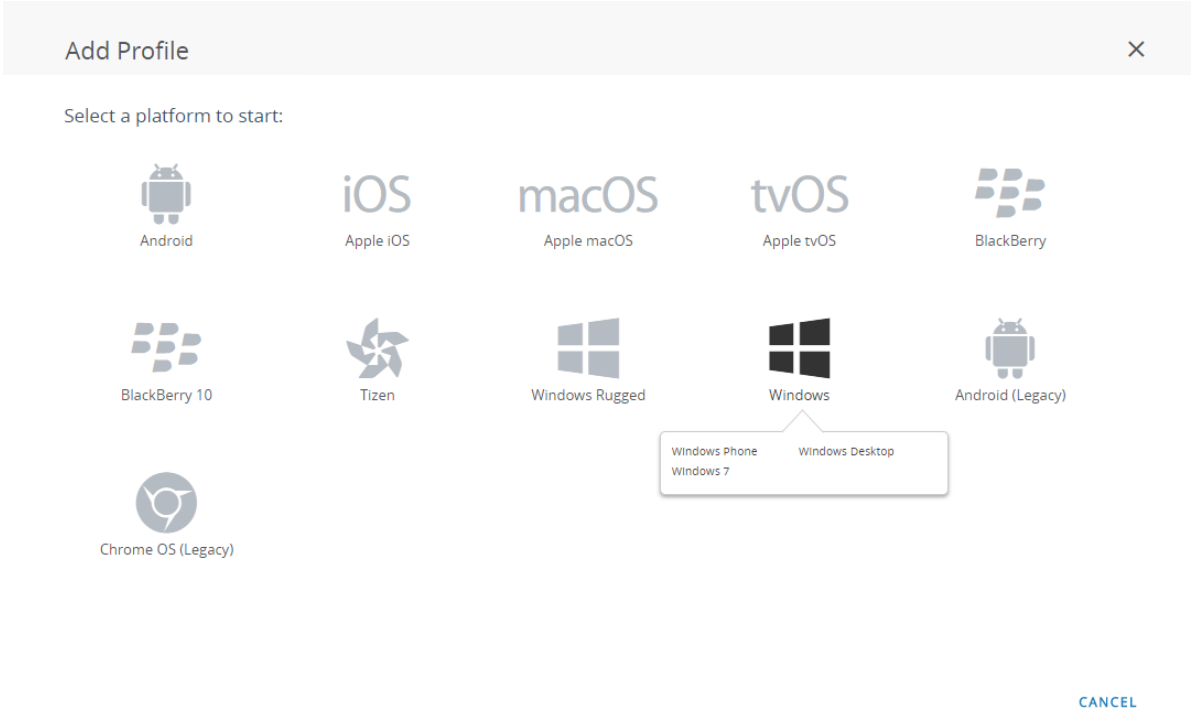
按照下列步驟使用 AirWatch 對 Windows 10 UWP 端點設定使用者啟動遠端存取 VPN 組態：

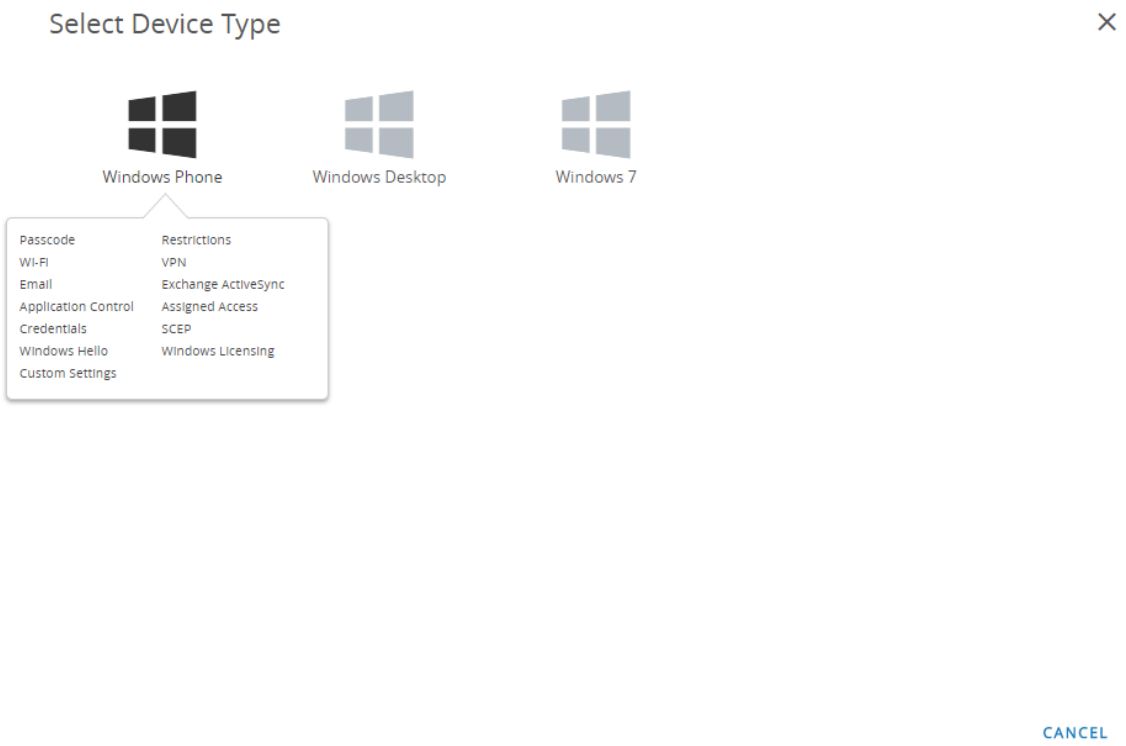
STEP 1 | 為 Windows 10 UWP 下載 GlobalProtect 應用程式：

- 透過 AirWatch 部署 GlobalProtect 行動應用程式。
- 從 Microsoft Store 直接下載 GlobalProtect 應用程式。

STEP 2 | 從 AirWatch 主控台修改現有 Windows 10 UWP 設定檔或新增一個。

1. 選取 **Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles**（設定檔），然後 **ADD**（新增）新的設定檔。
2. 選取 **Windows** 作為平台並選取 **Windows Phone** 作為裝置類型。

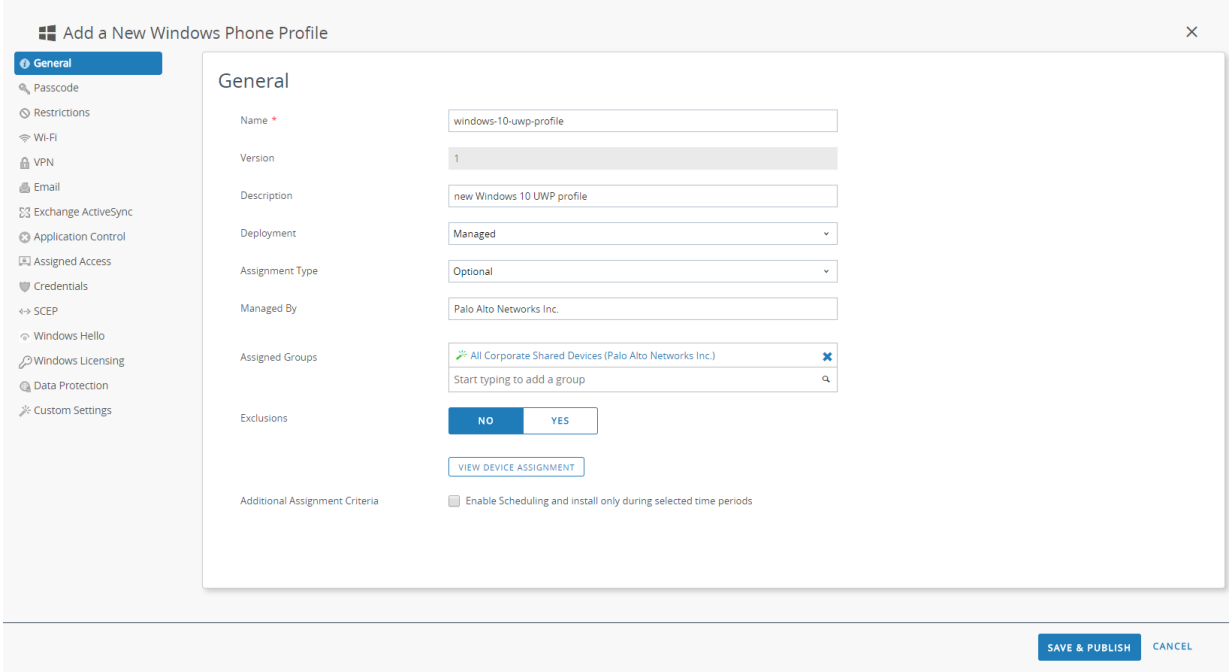




STEP 3 | 設定**General**（一般）設定：

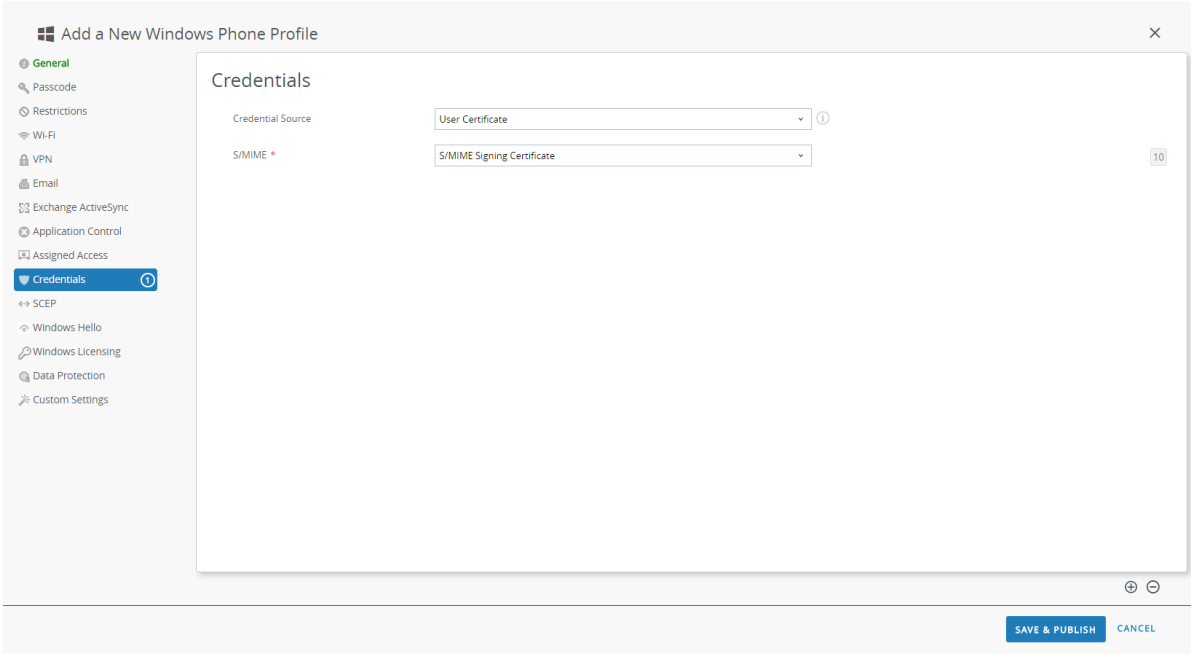
1. 輸入設定檔的 **Name**（名稱）。
2. （選用）輸入說明設定檔用途的簡短**Description**（描述）。
3. （選用）將 **Deployment**（部署）方法設定為 **Managed**（受管理）以使設定檔在取消註冊時自動移除
4. （選用）選取 **Assignment Type**（指派類型）以決定設定檔如何部署至端點。選取 **Auto**（自動）將設定檔自動部署至所有端點，選取 **Optional**（選用）讓一般使用者能從自助式入口網站 (SSP) 安裝設定檔，或手動部署設定檔至個別端點，或選取 **Compliance**（合規性）在一般使用者違反套用於端點的合規性原則時部署設定檔。
5. （選用）在 **Managed By**（被管理）欄位，輸入帶有設定檔管理存取的組織群組。

6. （選用）在 **Assigned Groups**（指派的群組）欄位，新增您希望新增設定檔的智慧群組。此欄位包含選項以建立新智慧群組，該智慧群組可透過規格設定用於最小 OS、設備型號、擁有權類別、組織群組等。
7. （選用）表示您是否希望包含任何 **Exclusions**（排除）至此設定檔的指派。如果選取 **Yes**（是），會顯示 **Excluded Groups**（排除群組）欄位，讓您可以選取希望從此設定檔指派中排除的智慧群組。
8. （選用）如果 **Enable Scheduling and install only during selected time periods**（僅在選定的時間段內啟用排程與安裝），您可套用時間排程（**Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles Settings**（設定檔設定）> **Time Schedules**（時間排程））至設定檔安裝，限制在端點上安裝設定檔的時間。出現提示時，請在 **Assigned Schedules**（指派排程）欄位輸入排程名稱。

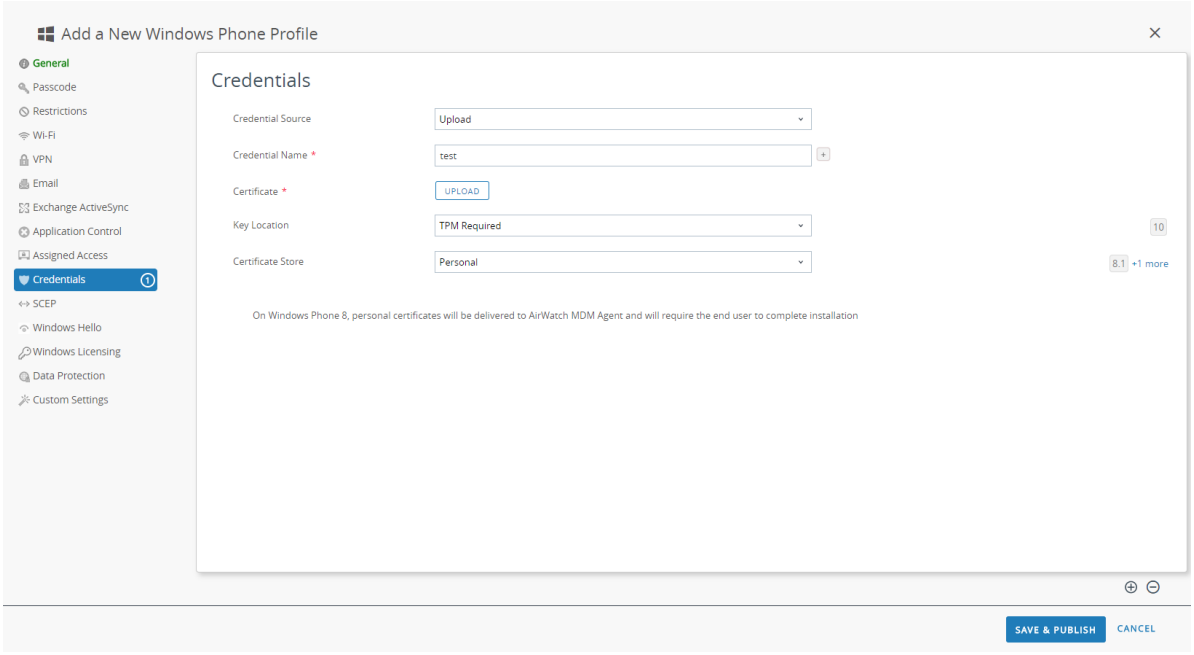


STEP 4 | （選用）如果您的 GlobalProtect 部署需要用戶端憑證驗證，請進行 **Credentials**（認證）設定：

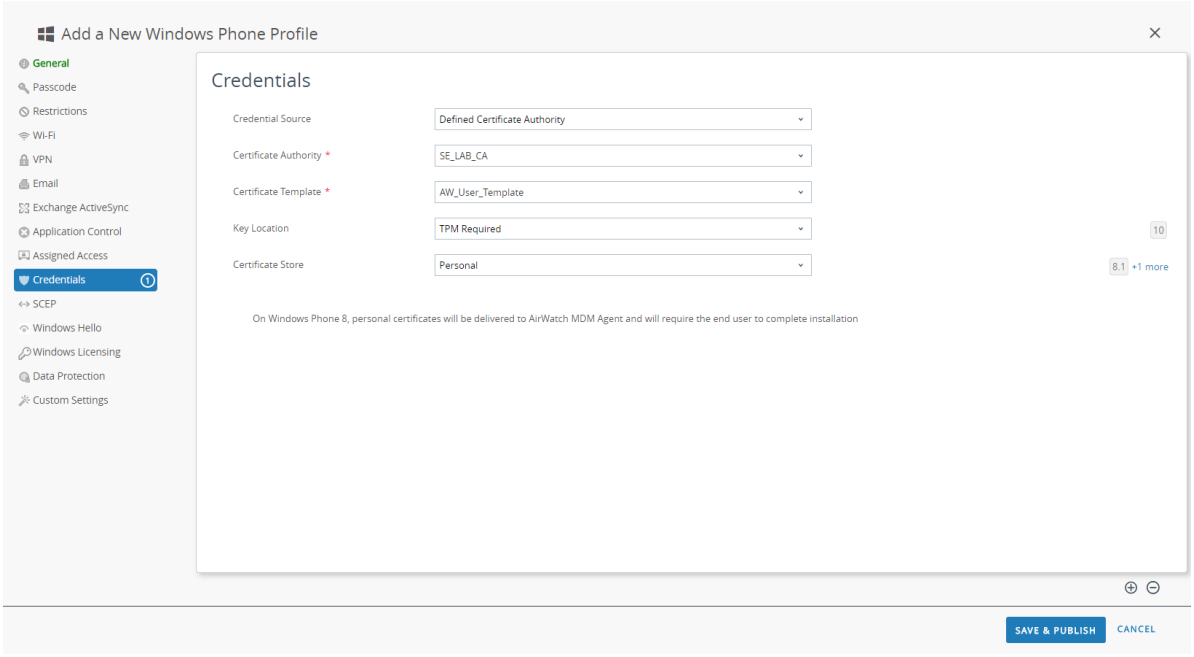
- 若要從 AirWatch 使用者提取用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **User Certificate**（使用者憑證）。
  2. 選取 **S/MIME Signing Certificate**（**S/MIME** 簽署憑證）（預設）。



- 若要手動上載用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **Upload**（上載）。
  2. 輸入 **Credential Name**（認證名稱）。
  3. 按一下 **UPLOAD**（上載）以找到並選取您要上載的憑證。
  4. 選取憑證後，按一下 **SAVE**（儲存）。
  5. 選取您想要儲存憑證私密金鑰的 **Key Location**（金鑰位置）：
     - **TPM Required**（TPM 要求）—在信任的平台模組上儲存私密金鑰。如果信任的平台模組在端點上不可用，則無法安裝私密金鑰。
     - **TPM If Present**（如果存在 **TPM**）—如果在端點上可用，在信任的平台模組上儲存私密金鑰。如果信任的平台模組在端點上不可用，私密金鑰將儲存在端點軟體中。
     - **Software**（軟體）—在端點軟體中儲存私密金鑰。
     - **Passport**（通行證）—儲存私密金鑰至 Microsoft Passport。若要使用此選項，必須在端點上安裝 AirWatch Protection Agent。
  6. 將 **Certificate store**（憑證存放區）設定為 **Personal**（個人）。



- 若要使用預先定義的憑證授權單位和範本：
  1. 將 **Credential Source**（認證來源）設定為 **Defined Certificate Authority**（定義的憑證授權單位）。
  2. 選取您想要取得憑證的 **Certificate Authority**（憑證授權單位）。
  3. 選取憑證授權單位的 **Certificate Template**（憑證範本）。
  4. 選取您想要儲存憑證私密金鑰的 **Key Location**（金鑰位置）：
     - **TPM Required**（**TPM** 要求）—在信任的平台模組上儲存私密金鑰。如果信任的平台模組在端點上不可用，則無法安裝私密金鑰。
     - **TPM If Present**（如果存在 **TPM**）—如果在端點上可用，在信任的平台模組上儲存私密金鑰。如果信任的平台模組在端點上不可用，私密金鑰將儲存在端點軟體中。
     - **Software**（軟體）—在端點軟體中儲存私密金鑰。
     - **Passport**（通行證）—儲存私密金鑰至 Microsoft Passport。若要使用此選項，必須在端點上安裝 AirWatch Protection Agent。
  5. 將 **Certificate store**（憑證存放區）設定為 **Personal**（個人）。

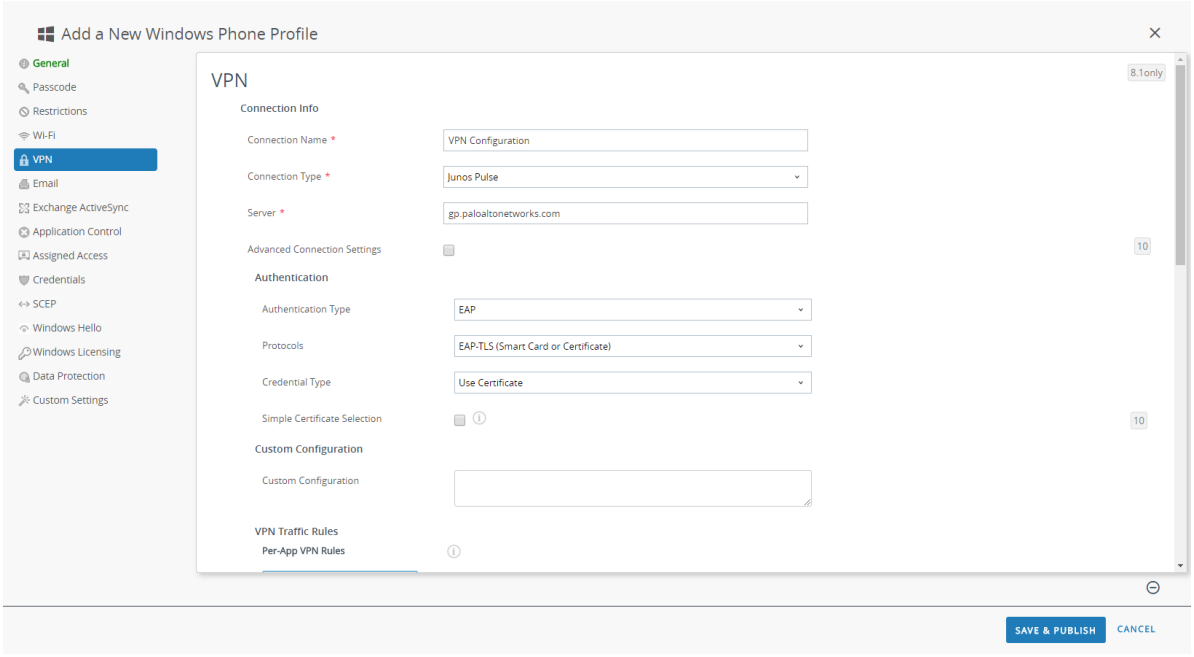


STEP 5 | 設定 **VPN** 設定：

1. 輸入要端點顯示的 **Connection Name**（連線名稱）。
2. 選取替代 **Connection Type**（連線類型）供應商（不選取 **IKEv2**、**L2TP**、**PPTP** 或 **Automatic**（自動），因為其沒有 GlobalProtect VPN 設定檔所需的相關廠商設定）。

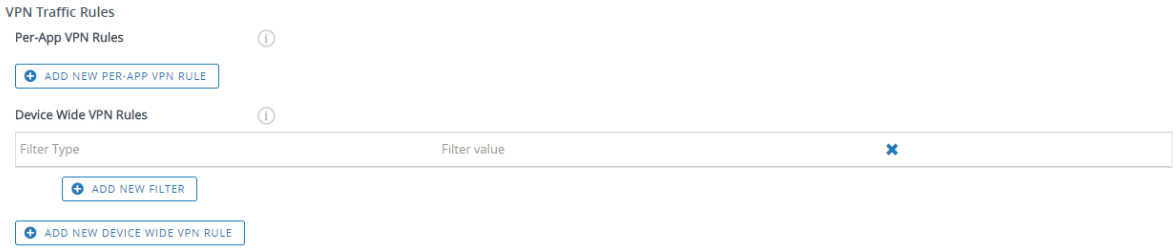
   

   您必須選取替代廠商，因為 *AirWatch* 尚未將 *GlobalProtect* 列為 *Windows* 端點的正式連線供應商。
3. 在 **Server**（伺服器）欄位，輸入使用者連線的 GlobalProtect 入口網站主機或 IP 位址。
4. 在驗證區域，選取 **Authentication Type**（驗證類型）以指定驗證一般使用者的方法。

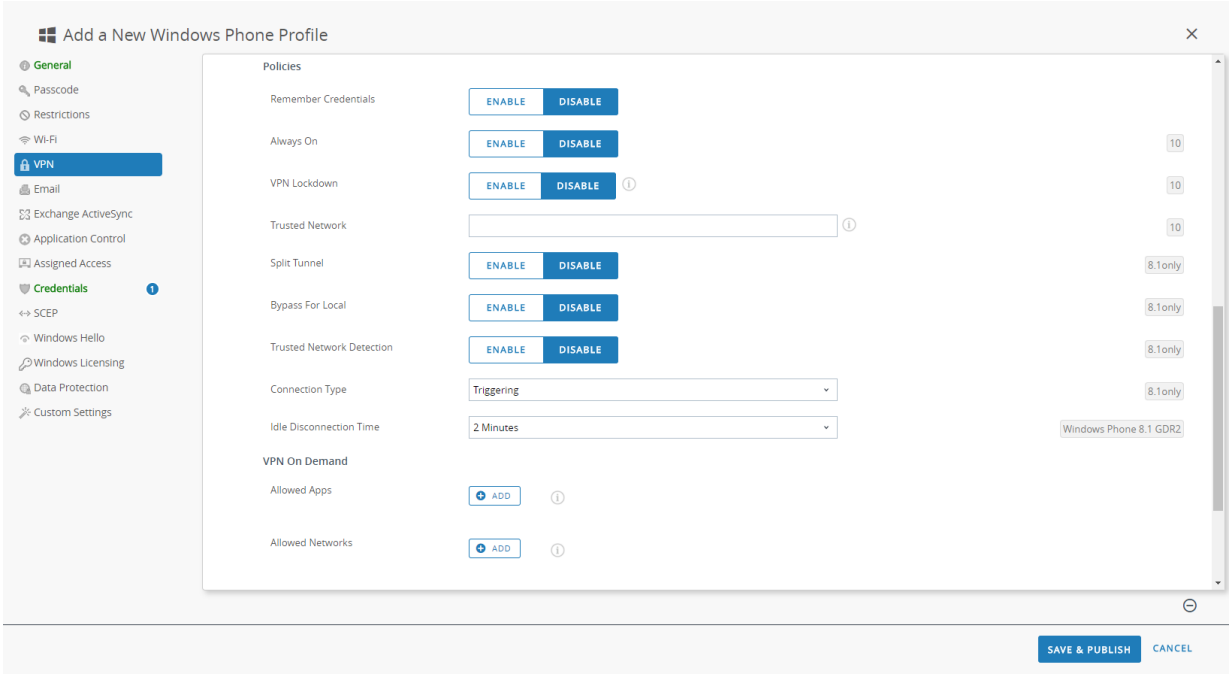


5. （選用）若要允許 GlobalProtect 儲存使用者認證，請 **ENABLE**（啟用）此選項以在原則區域內 **Remember Credentials**（記住認證）。
6. （選用）在 VPN 流量規則區域內，**ADD NEW DEVICE WIDE VPN RULE**（新增裝置範圍內的 **VPN** 規則）以透過 VPN 通道傳送符合特定路由的流量。這些規則不受應用程式約束，但在端點上評估。如果流量符合指定的相符條件，其透過 VPN 通道路由。

   透過按一下 **ADD NEW FILTER**（新增篩選條件）來新增比對準則。出現提示時，請輸入 **Filter Type**（篩選類型）和對應的 **Filter Value**（篩選值）。



7. 若要確保此設定檔使用視需要連線方法，請在原則區域內進行下列設定：
   - **DISABLE**（停用）**Always On**（一直開啟）。如果此欄位 **ENABLED**（已啟用），安全連線將一直開啟。
   - **DISABLE**（停用）**VPN Lockdown**（**VPN** 鎖定）。如果此欄位 **ENABLED**（已啟用），安全連線將一直開啟和保持連線，並在應用程式未連線時停用網路存取。AirWatch 內的 **VPN Lockdown**（**VPN** 鎖定）與您在 GlobalProtect 入口網站組態中設定的 **Enforce GlobalProtect for Network Access**（強制執行 **GlobalProtect** 連線以進行網路存取）選項類似。



STEP 6 | **SAVE & PUBLISH**（儲存和發佈）您的變更。

STEP 7 | 若要將連線類型供應商設定為 GlobalProtect，請編輯 XML 內的 VPN 設定檔。

若要最小化原 *XML* 內的其他編輯，在您匯出組態前，檢閱您的 *VPN* 設定檔內的設定。如果您需要在匯出 *VPN* 設定檔後變更設定，您可以在原 *XML* 中進行變更，或在 *VPN* 設定檔中更新設定並再次執行此步驟。

1. 在 **Devices**（裝置）> **Profiles**（設定檔）> **List View**（清單檢視），選取您在之前步驟中新增的設定檔旁的無線電按鈕，然後選取表格頂部的 **</>XML**。AirWatch 會打開設定檔的 XML 檢視。
2. **Export**（匯出）設定檔，然後在您選取的文字編輯器中打開。
3. 為 GlobalProtect 編輯下列設定：

- 在指定 `PluginPackageFamilyName` 的 `LoclURI` 元件中變更元件為：

  `<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>`
- 在後續的 `Data` 元件中，變更數值為：

  `<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>`

1. 將您的變更儲存至匯出的設定檔。
2. 返回 AirWatch 並選取 **Devices**（裝置）> **Profiles**（設定檔）> **List View**（清單檢視）。
3. 建立（選取 **Add**（新增）> **Add Profile**（新增設定檔）> **Windows** > **Windows Phone**（**Windows** 手機））並命名一個新的設定檔。
4. 選取 **Custom Settings**（自訂設定）> **Configure**（設定），然後複製並粘上編輯的組態。
5. **Save & Publish**（儲存和發佈）您的變更。

STEP 8 | 透過從 **Devices**（裝置）> **Profiles**（設定檔）> **List View**（清單檢視）選取原始設定檔，然後選取 **More Actions**（其他動作）> **Deactivate**（停用），來清除原始設定檔。AirWatch 會將設定檔移動至非使用中清單。

STEP 9 | 測試組態。

透過 **Microsoft Intune** 設定使用者啟動遠端存取 **VPN** 組態

Microsoft Intune 是讓您可以從中央位置管理行動端點的雲端企業行動管理平台。GlobalProtect 應用程式提供 Microsoft Intune 在裝置或應用程式等級管理的防火牆和行動端點之間的安全連線。使用 Android 的 GlobalProtect 作為安全連線，可進行對流量的一致檢查和對網路安全政策的強化，以預防行動端點上的威脅。

有關如何使用 Microsoft Intune 設定使用者啟動遠端存取 VPN 組態的資訊，請參閱以下章節：

- 透過 Microsoft Intune 為 iOS 端點設定使用者啟動遠端存取 VPN 組態

透過 *Microsoft Intune* 為 *iOS* 端點設定使用者啟動遠端存取 *VPN* 組態

在遠端存取（視需要）VPN 組態中，使用者必須手動啟動應用程式才能建立安全 GlobalProtect 連線。只有在使用者啟動並建立連線後，符合 GlobalProtect 閘道上所設定特定篩選條件（如連接埠和 IP 位址）的流量才會透過 VPN 通道進行路由傳送。

按照下列步驟使用 Microsoft Intune 對 iOS 端點設定使用者啟動遠端存取 VPN 組態：

STEP 1 | 為 iOS 下載 GlobalProtect 應用程式。

- 透過 Microsoft Intune 部署 GlobalProtect 行動應用程式.
- 從 App Store 直接下載 GlobalProtect 應用程式。

STEP 2 | （選用）如果您的部署需要用基於憑證的驗證，請設定憑證設定檔。

STEP 3 | 建立新 iOS VPN 設定檔。

- 將 **Platform**（平台）設定為 **iOS**。

STEP 4 | 為 iOS 端點設定視需要（遠端存取）VPN 設定。

- 將 **Connection type**（連線類型）設定為 **Palo Alto Networks GlobalProtect**。
- 在自動 VPN 設定區域，啟用 **On-demand VPN**（視需要 **VPN**）以設定當 VPN 連線啟動時進行控制的條件規則。

透過 **MobileIron** 設定使用者啟動遠端存取 **VPN** 組態

MobileIron 是讓您可以從中央控制台管理行動端點的企業行動管理平台。GlobalProtect 應用程式提供 MobileIron 在裝置或應用程式等級管理的防火牆和行動端點之間的安全連線。使用 Android 的 GlobalProtect 作為安全連線，可進行對流量的一致檢查和對網路安全政策的強化，以預防行動端點上的威脅。

有關如何使用 MobileIron 設定使用者啟動遠端存取 VPN 組態的資訊，請參閱以下章節：

- 透過 MobileIron 為 iOS 端點設定使用者啟動遠端存取 VPN 組態

透過 *MobileIron* 為 *iOS* 端點設定使用者啟動遠端存取 *VPN* 組態

在遠端存取（視需要）VPN 組態中，使用者必須手動啟動應用程式才能建立安全 GlobalProtect 連線。只有在使用者啟動並建立連線後，符合 GlobalProtect 閘道上所設定特定篩選條件（如連接埠和 IP 位址）的流量才會透過 VPN 通道進行路由傳送。

按照下列步驟使用 MobileIron 對 iOS 端點設定使用者啟動遠端存取 VPN 組態：

STEP 1 | 為 iOS 下載 GlobalProtect 應用程式。

- 透過 MobileIron 部署 GlobalProtect 行動應用程式.
- 從 App Store 直接下載 GlobalProtect 應用程式。

STEP 2 | 新增憑證設定，然後設定憑證設定。

所有視需要 *VPN* 組態都需要基於憑證的驗證。

STEP 3 | 新增視需要（遠端存取）VPN 組態。

- 將設定類型設定為 **VPN On Demand**（視需要 **VPN**）。

STEP 4 | 為 iOS 設定視需要 VPN 設定。

- 將 **Connection Type**（連線類型）設定為 **Palo Alto Networks GlobalProtect**，然後進行相關設定。

Per-App VPN 組態

在 per-app VPN 組態中，您可以指定哪個管理應用程式可透過 GlobalProtect VPN 通道傳送流量。未管理的應用程式將繼續直接連線網際網路，而非透過 GlobalProtect VPN 通道。

有關如何使用支援的行動裝置管理系統設定 per-app VPN 組態的資訊，請參閱以下幾節：

- 透過 AirWatch 設定 Per-App VPN 組態
- 透過 Microsoft Intune 設定 Per-App VPN 組態
- 透過 MobileIron 設定 Per-App VPN 組態

透過 **AirWatch** 設定 **Per-App VPN** 組態

AirWatch 是讓您可以從中央控制台管理行動端點的企業行動管理平台。GlobalProtect 應用程式提供 AirWatch 管理行動裝置之間的安全連線，且防火牆位於端點或應用程式等級。使用 Android 的

GlobalProtect 作為安全連線，可進行對流量的一致檢查和對網路安全政策的強化，以預防行動端點上的威脅。

有關如何使用 AirWatch 設定 Per-App VPN 組態的資訊，請參閱以下幾節：

- 透過 AirWatch 為 iOS 端點設定 Per-App VPN 組態
- 透過 AirWatch 為 Android 端點設定 Per-App VPN 組態
- 透過 AirWatch 對 Windows 10 UWP 端點設定 Per-App VPN 組態

透過 *AirWatch* 為 *iOS* 端點設定 *Per-App VPN* 組態

您可以透過使用 AirWatch 設定 GlobalProtect VPN 存取，從您的管理行動端點啟用內部資源存取。在 per-app VPN 組態中，您可以指定哪個管理應用程式可透過 VPN 通道路由傳送流量。未管理的應用程式將繼續直接連線網際網路，而非透過 VPN 通道。

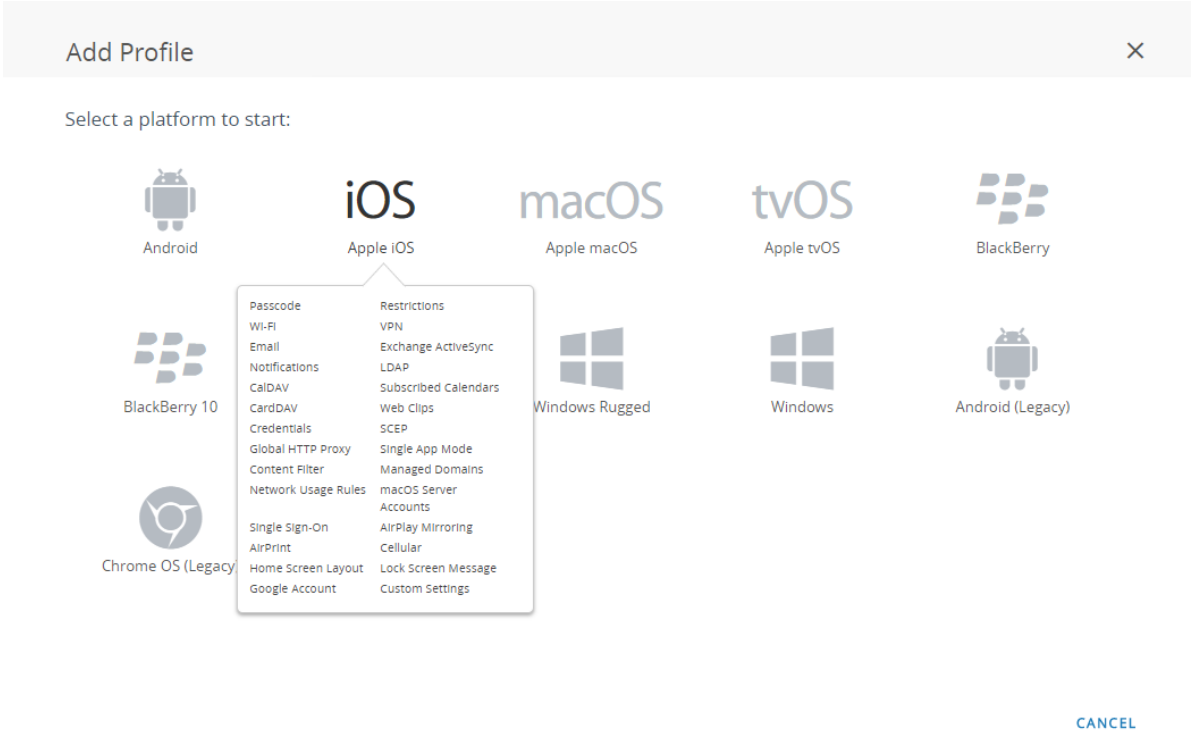
按照下列步驟使用 AirWatch 對 iOS 端點設定 Per-App VPN 組態：

STEP 1 | 為 iOS 下載 GlobalProtect 應用程式：

- 透過 AirWatch 部署 GlobalProtect 行動應用程式。
- 從 App Store 直接下載 GlobalProtect 應用程式。

STEP 2 | 從 AirWatch 主控台修改現有 Apple iOS 設定檔或新增一個。

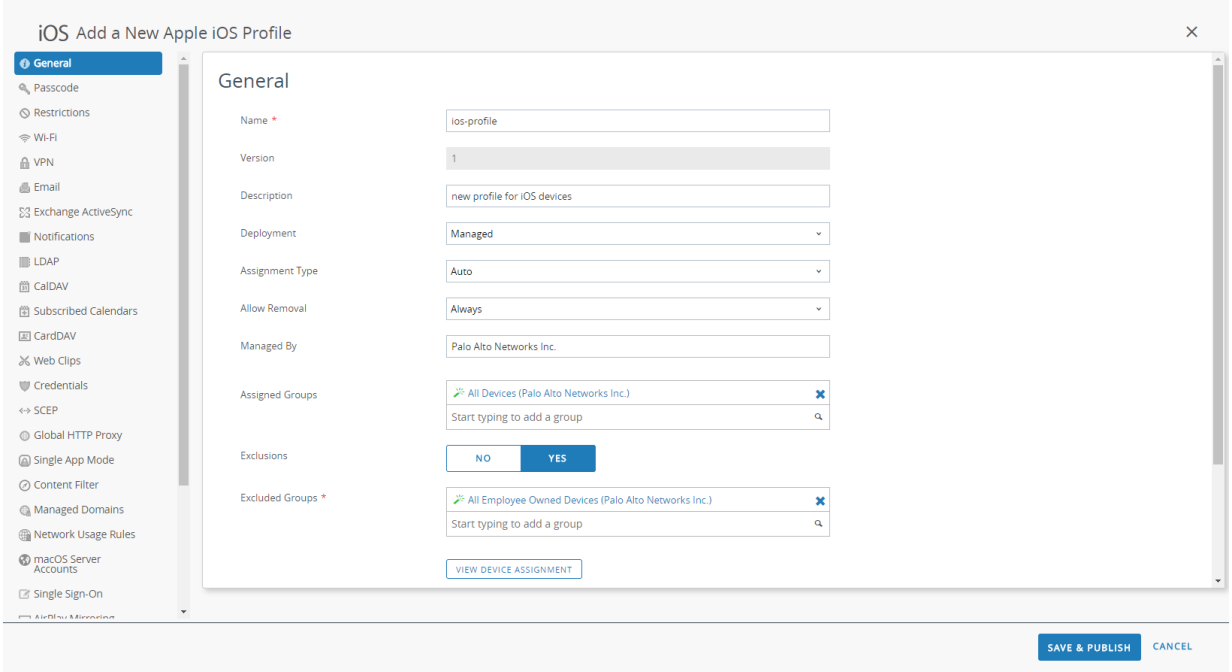
1. 選取 **Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles**（設定檔），然後 **ADD**（新增）新的設定檔。
2. 從平台清單選取 **iOS**。



STEP 3 | 設定**General**（一般）設定：

1. 輸入設定檔的 **Name**（名稱）。
2. （選用）輸入說明設定檔用途的簡短**Description**（描述）。
3. （選用）選取 **Deployment**（部署）方法，它決定設定檔是否會在取消註冊時自動移除—無論是 **Managed**（受管理）（設定檔被移除）或 **Manual**（手動）（設定檔保持安裝直到被一般使用者移除）。
4. （選用）選取 **Assignment Type**（指派類型）以決定設定檔如何部署至端點。選取 **Auto**（自動）將設定檔自動部署至所有端點，選取 **Optional**（選用）讓一般使用者能從自助式入口網站 (SSP) 安裝設定檔，或手動部署設定檔至個別端點，或選取 **Compliance**（合規性）在一般使用者違反套用於端點的合規性原則時部署設定檔。

5. （選用）選取 **Allow Removal**（允許移除）以決定一般使用者能否移除設定檔。選取 **Always**（一律）讓一般使用者能在任何時候手動移除設定檔，選取 **Never**（絕不）防止一般使用者移除設定檔，或選取 **With Authorization**（透過授權）讓經過管理員授權的一般使用者能移除設定檔。選取 **With Authorization**（透過授權）會新增必要的密碼。
6. （選用）在 **Managed By**（被管理）欄位，輸入帶有設定檔管理存取的組織群組。
7. （選用）在 **Assigned Groups**（指派的群組）欄位，新增您希望新增設定檔的智慧群組。此欄位包含選項以建立新智慧群組，該智慧群組可透過規格設定用於最小 OS、設備型號、擁有權類別、組織群組等。
8. （選用）表示您是否希望包含任何 **Exclusions**（排除）至此設定檔的指派。如果選取 **Yes**（是），會顯示 **Excluded Groups**（排除群組）欄位，讓您可以選取希望從此設定檔指派中排除的智慧群組。

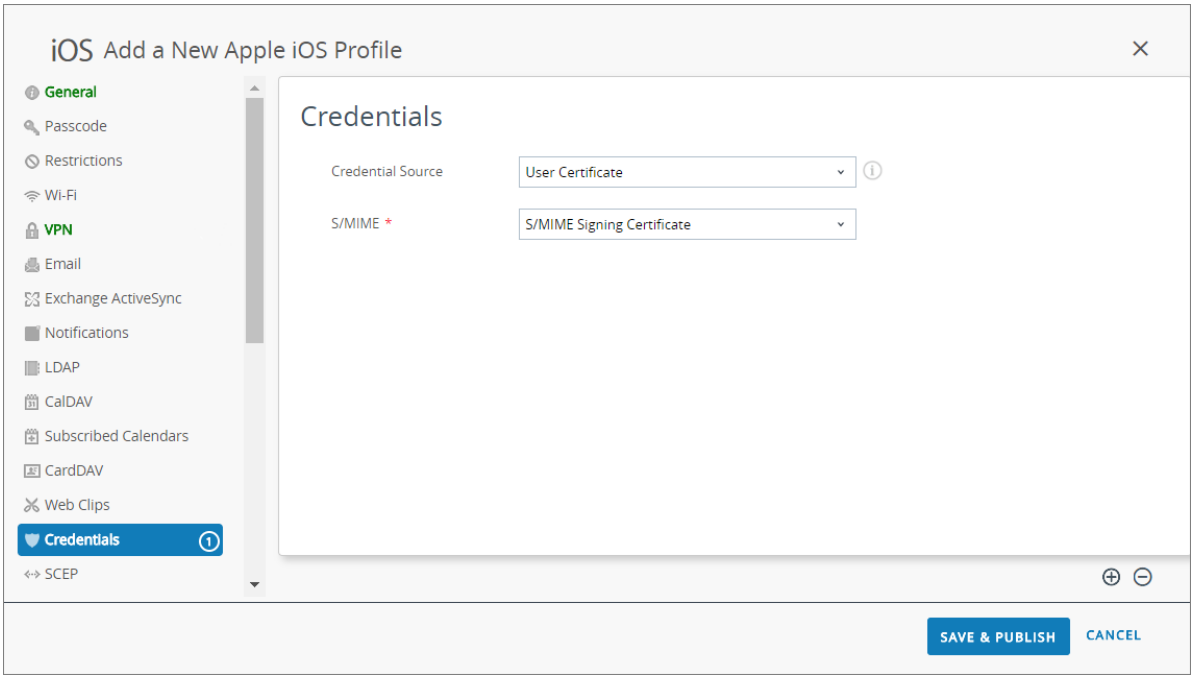


STEP 4 | 設定 **Credentials**（認證） 設定：

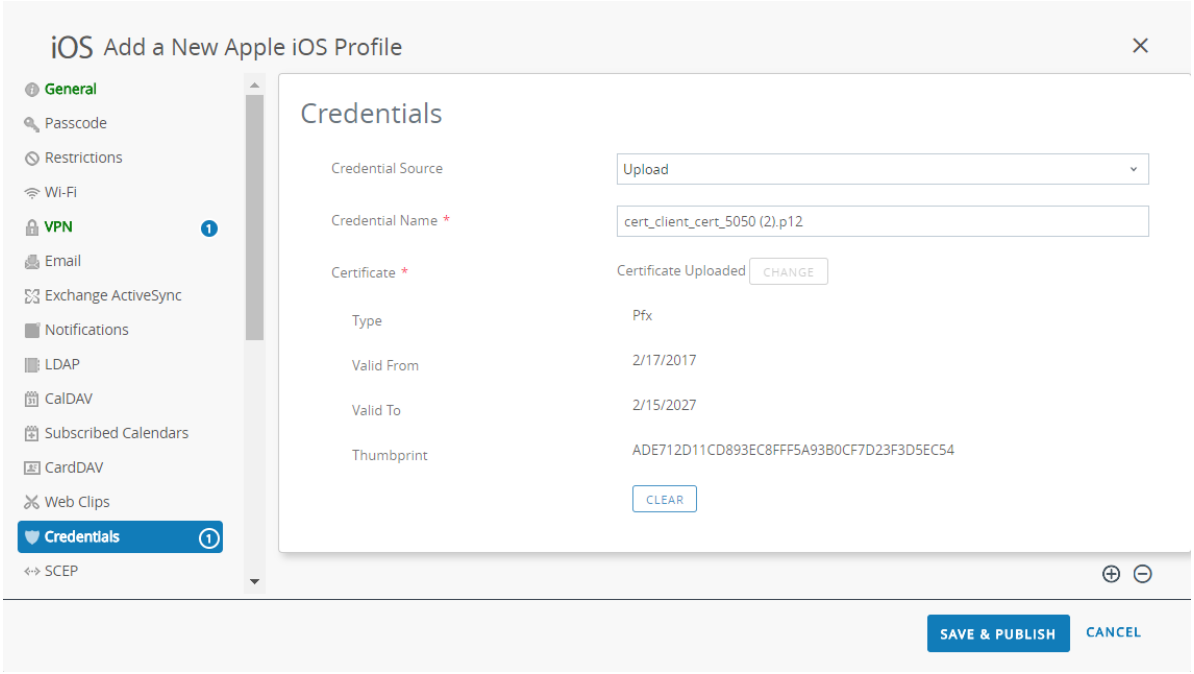
所有 *per-app VPN* 組態都需要基於憑證的驗證。

要求的最低版本為 *iOS 12*，如果您想要透過用戶端憑證進行 *GlobalProtect* 用戶端驗證，您必須將用戶端憑證部署為從 *MDM* 伺服器推送的 *VPN* 設定檔的一部分。如果您使用任何其他方法部署來自 *MDM* 伺服器的用戶端憑證，則 *GlobalProtect* 應用程式將無法使用憑證。

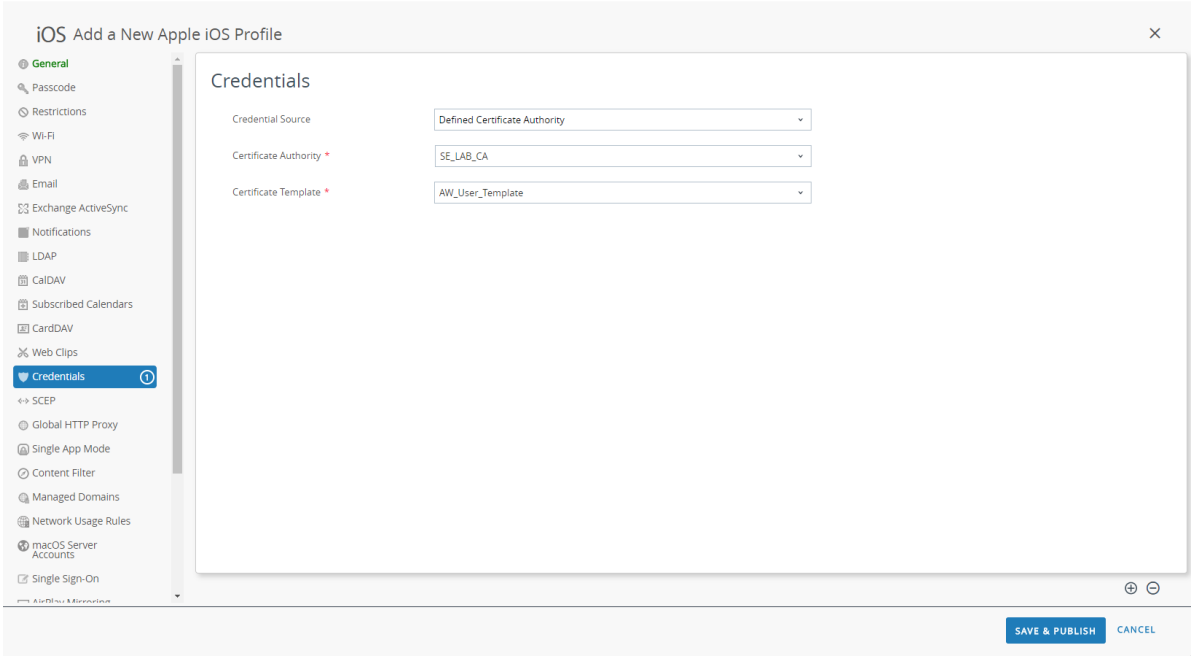
- 若要從 AirWatch 使用者提取用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **User Certificate**（使用者憑證）。
  2. 選取 **S/MIME Signing Certificate**（**S/MIME** 簽署憑證）（預設）。



- 若要手動上載用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **Upload**（上載）。
  2. 輸入 **Credential Name**（認證名稱）。
  3. 按一下 **UPLOAD**（上載）以找到並選取您要上載的憑證。
  4. 選取憑證後，按一下 **SAVE**（儲存）。



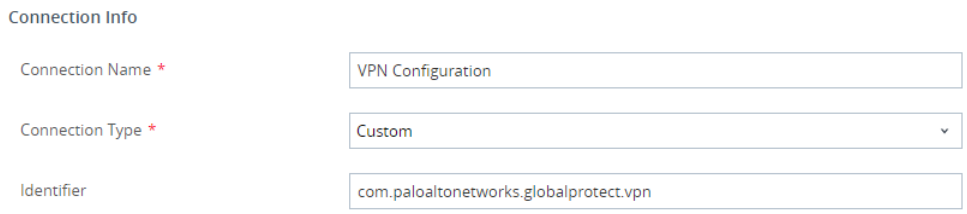
- 若要使用預先定義的憑證授權單位和範本：
  1. 將 **Credential Source**（認證來源）設定為 **Defined Certificate Authority**（定義的憑證授權單位）。
  2. 選取您想要取得憑證的 **Certificate Authority**（憑證授權單位）。
  3. 選取憑證授權單位的 **Certificate Template**（憑證範本）。



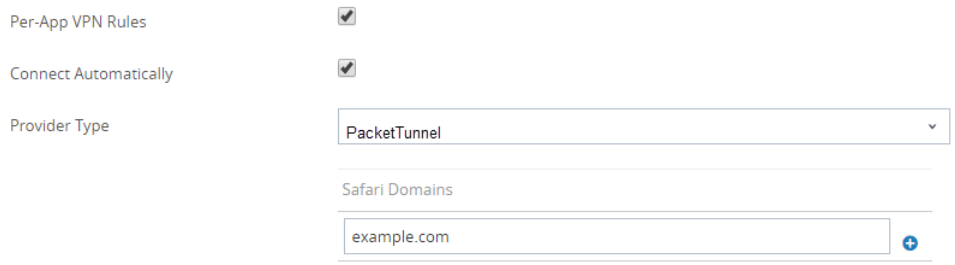
STEP 5 | 設定 **VPN** 設定：

1. 輸入要端點顯示的 **Connection Name**（連線名稱）。
2. 選取網路 **Connection Type**（連線類型）：
   - 對於 GlobalProtect 應用程式 4.1.x 及更早版本，請選取 **Palo Alto Networks GlobalProtect**。
   - 對於 GlobalProtect 應用程式 5.0 及更新版本，請選取 **Custom**（自訂）。
3. （選用）如果您將 **Connection Type**（連線類型）設定為 **Custom**（自訂），請在 **Identifier**（識別碼）欄位輸入下列捆綁 ID 以識別 GlobalProtect 應用程式：

   com.paloaltonetworks.globalprotect.vpn



4. 在 **Server**（伺服器）欄位，輸入使用者連線的 GlobalProtect 入口網站主機或 IP 位址。
5. （選用）輸入 VPN **Account**（帳戶）用戶名或按一下新增 (+) 按鈕以檢視您可以插入的支援查閱值。
6. （選用）在 **Disconnect on idle**（閒置時中斷連線）欄位，指定應用程式停止透過 VPN 通道路由流量後端點登出 GlobalProtect 應用程式的時間（秒）。
7. 啟用 **Per App VPN Rules**（**Per App VPN** 規則）以通過 GlobalProtect VPN 通道路由傳送受管理應用程式的所有流量。
   - 使 GlobalProtect **Connect Automatically**（自動連線）至指定的 **Safari Domains**（**Safari** 網域）。您可透過按一下新增 (+) 按鈕新增多個 **Safari Domains**（**Safari** 網域）。
   - 選取 **Provider Type**（供應商類型）以指定流量在通道中的傳送方式—在應用層或 IP 層。



8. 在驗證區域，將使用者 **Authentication**（驗證）方法設定為 **Certificate**（憑證）。

   所有 *per-app VPN* 組態都需要基於憑證的驗證。

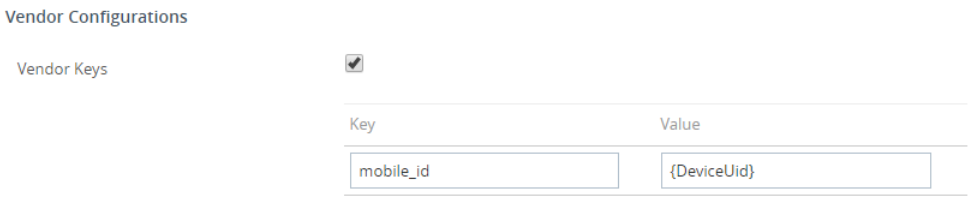
9. 出現提示時，請選取 GlobalProtect 將用於驗證使用者的 **Identity Certificate**（識別身分憑證）。**Identity Certificate**（識別身分憑證）與您在 **Credentials**（認證）設定中設定的憑證相同。

10. （選用）選取 **Proxy** 類型並進行相關設定。

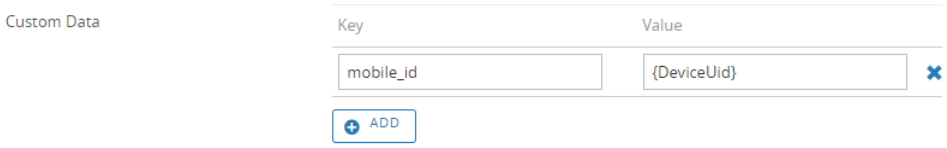
STEP 6 | （選用）（最低版本要求為 GlobalProtect 應用程式 5.0）如果您的 GlobalProtect 部署要求 HIP 與 MDM 整合，請指定唯一裝置識別碼 (UDID) 屬性。

GlobalProtect 支援與 MDM 整合以從 MDM 伺服器取得行動裝置屬性，用於以 HIP 為基礎的原則強制執行。若要使 MDM 整合能夠正常執行，GlobalProtect 應用程式必須向 GlobalProtect 閘道呈現端點的 UDID。UDID 屬性讓 GlobalProtect 應用程式能夠在以 MDM 為基礎的部署中擷取並使用 UDID 資訊。如果您從設定檔中移除 UDID 屬性，將無法再使用 MDM 整合。GlobalProtect 應用程式將產生新的 UDID，但其無法用於整合。

- 如果您使用的是 **Palo Alto Networks GlobalProtect** 網路 **Connection Type**（連線類型），請前往 **VPN** 設定並在廠商組態區域啟用 **Vendor Keys**（廠商金鑰）。將 **Key**（索引鍵）設定為 **`mobile_id`** 並將 **Value**（值）設定為 **`{DeviceUid}`**。



- 如果您使用的是 **Custom**（自訂）網路 **Connection Type**（連線類型），請前往 **VPN** 設定並在連線資訊區域 **ADD**（新增）**Custom Data**（自訂資料）。將 **Key**（索引鍵）設定為 **`mobile_id`** 並將 **Value**（值）設定為 **`{DeviceUid}`**。

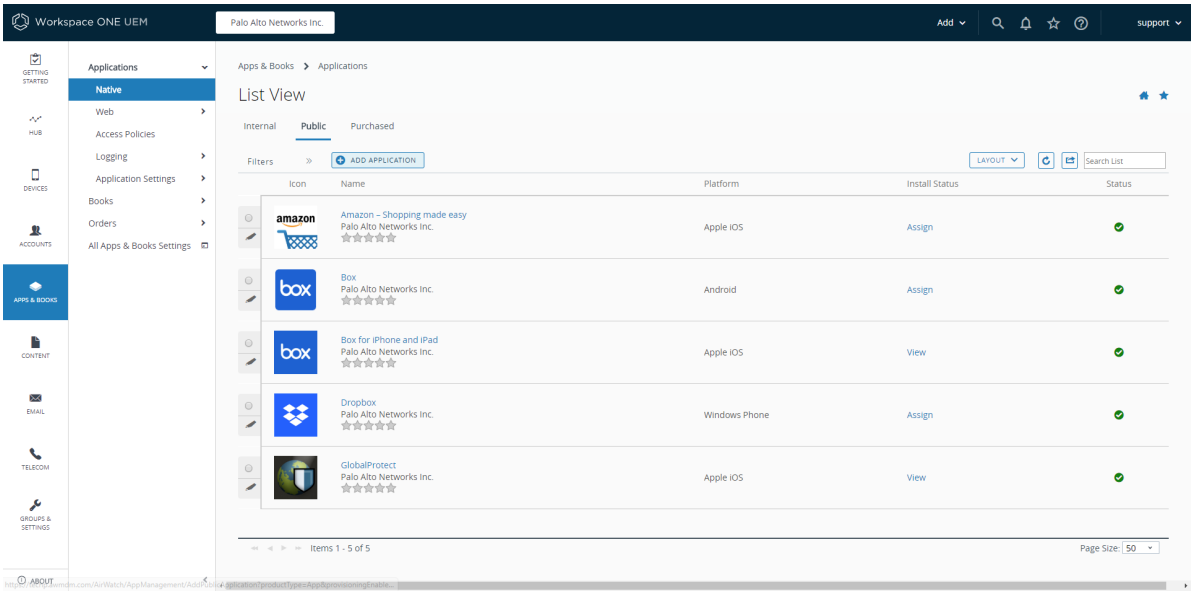


STEP 7 | **SAVE & PUBLISH**（儲存和發佈）您的變更。

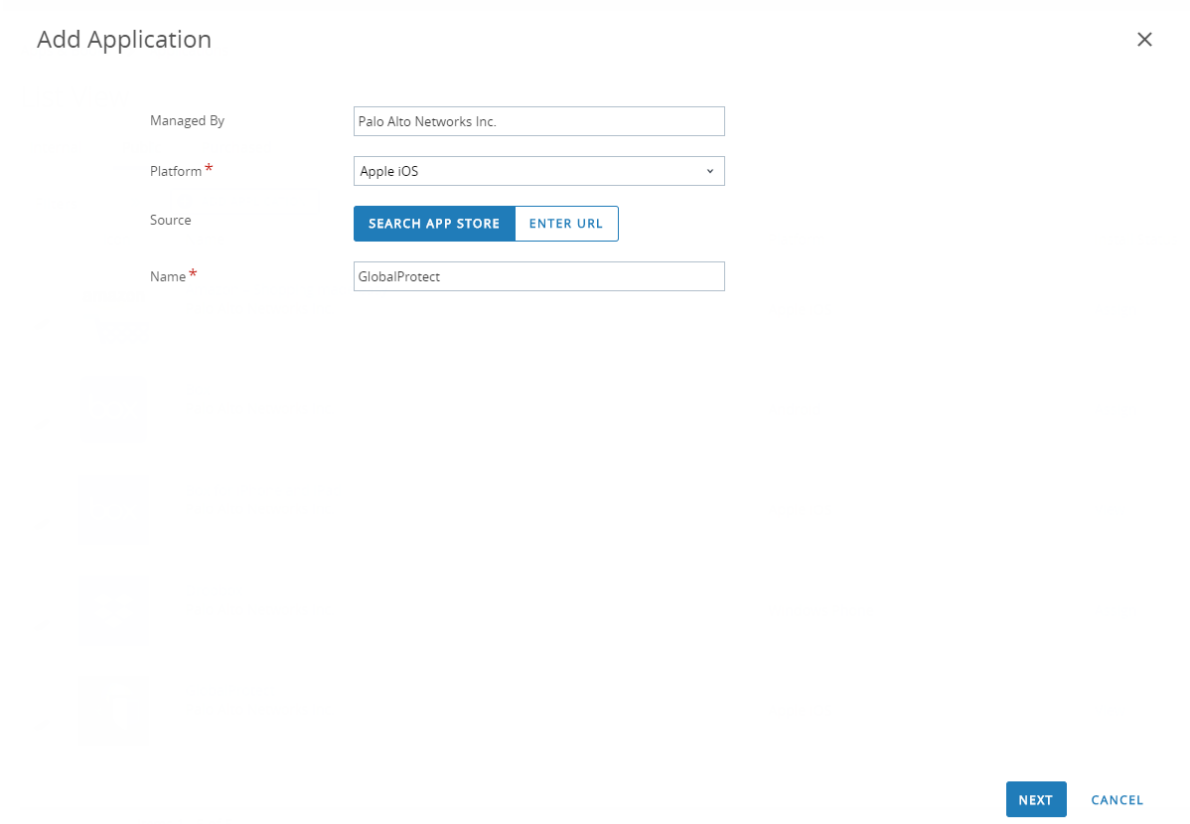
STEP 8 | 為新管理的應用程式設定 per-app VPN 設定，或修改現有受管理應用程式的設定。

設定應用程式設定和啟用 per-app VPN 後，您可以發行應用程式至使用者群組，並啟用此應用程式透過 GlobalProtect VPN 通道傳送流量。

1. 選取 **APPS & BOOKS**（應用程式和書本）> **Applications**（應用程式）> **Native**（原生）> **Public**（公用）。
2. 若要新增應用程式，選取 **ADD APPLICATION**（新增應用程式）。若要修改現有應用程式的設定，在公用應用程式清單（清單檢視）中找到應用程式，然後選取列旁動作功能表內的編輯 (✎) 圖示。

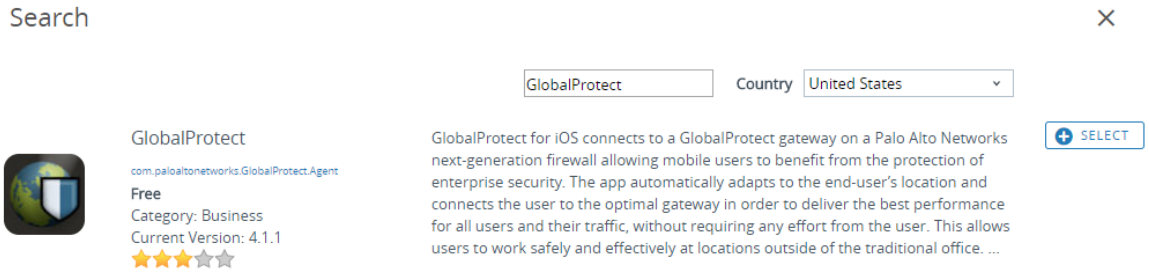


3. 在 **Managed By**（被管理）欄位，選取將管理此應用程式的組織群組。
4. 將 **Platform**（平台）設定為 **Apple iOS**。
5. 選取您用於尋找應用程式的偏好 **Source**（來源）：
   - **SEARCH APP STORE**（搜索應用程式商店）—輸入應用程式的 **Name**（名稱）。
   - **ENTER URL**（輸入 **URL**）—為此應用程式輸入 App Store URL（例如，若要新增 Box 應用程式，輸入 https://itunes.apple.com/us/app/box-for-iphone-and-ipad/id290853822?mt=8&uo=4）。

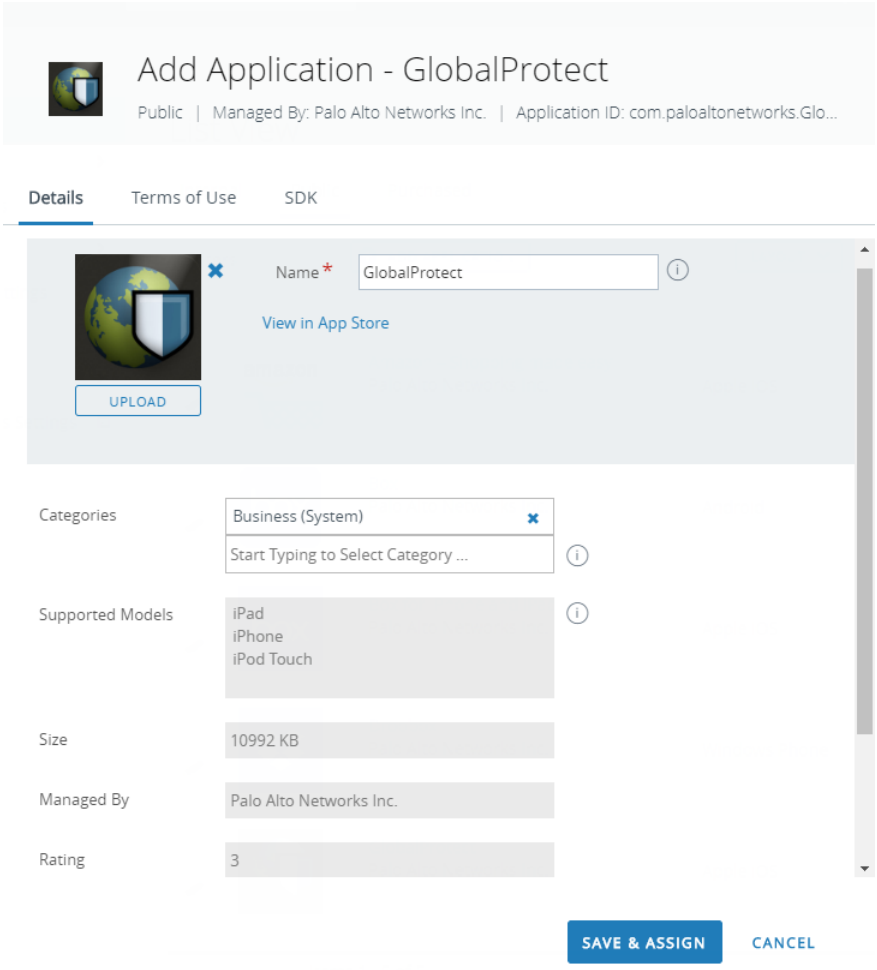


6. 按一下 **NEXT**（下一步）。

   如果您選取了在 App Store 中搜尋應用程式，您還必須從搜尋結果清單中 **Select**（選取）應用程式。

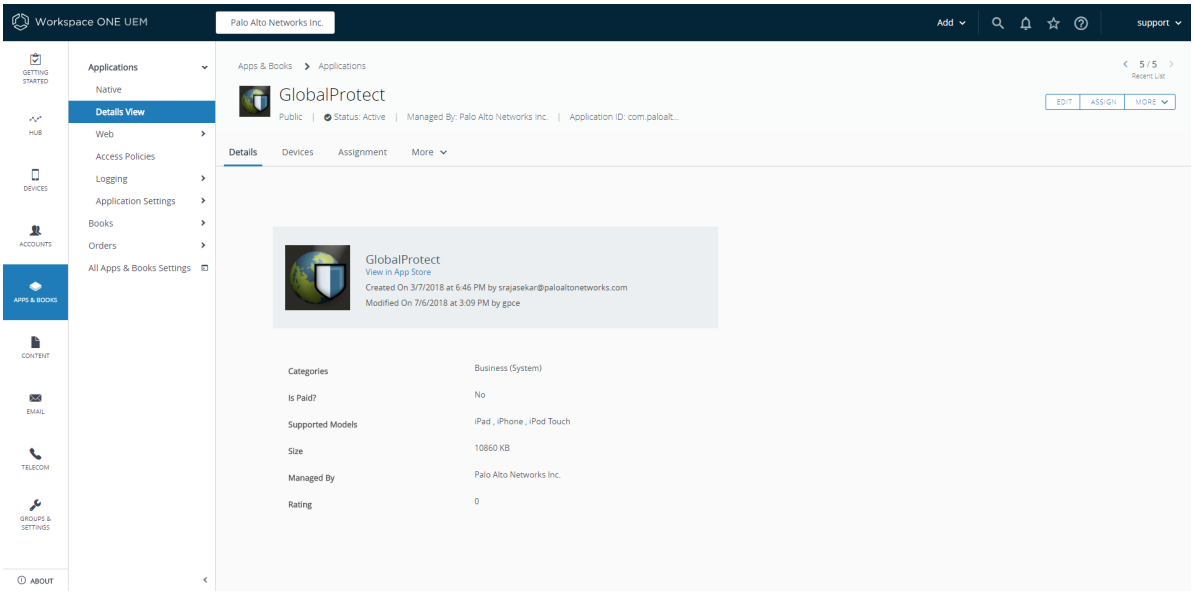


7. 在新增應用程式對話方塊中，請確保應用程式 **Name**（名稱）正確。此名稱將顯示在 AirWatch 應用程式目錄中。
8. （ 選用 ）指派應用程式至預先定義或自訂 **Categories**（類別） 以輕觸存取 AirWatch 應用程式目錄。

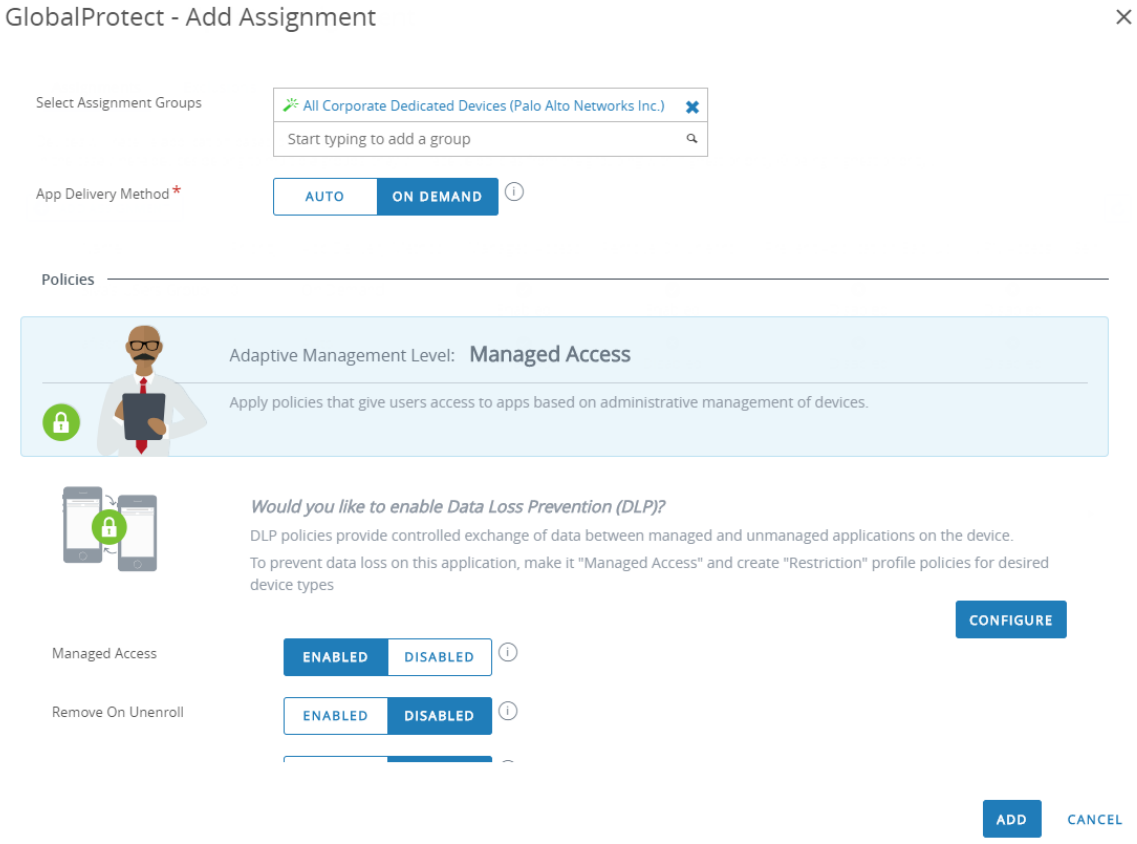


9. **SAVE & ASSIGN**（儲存並指派）新應用程式。

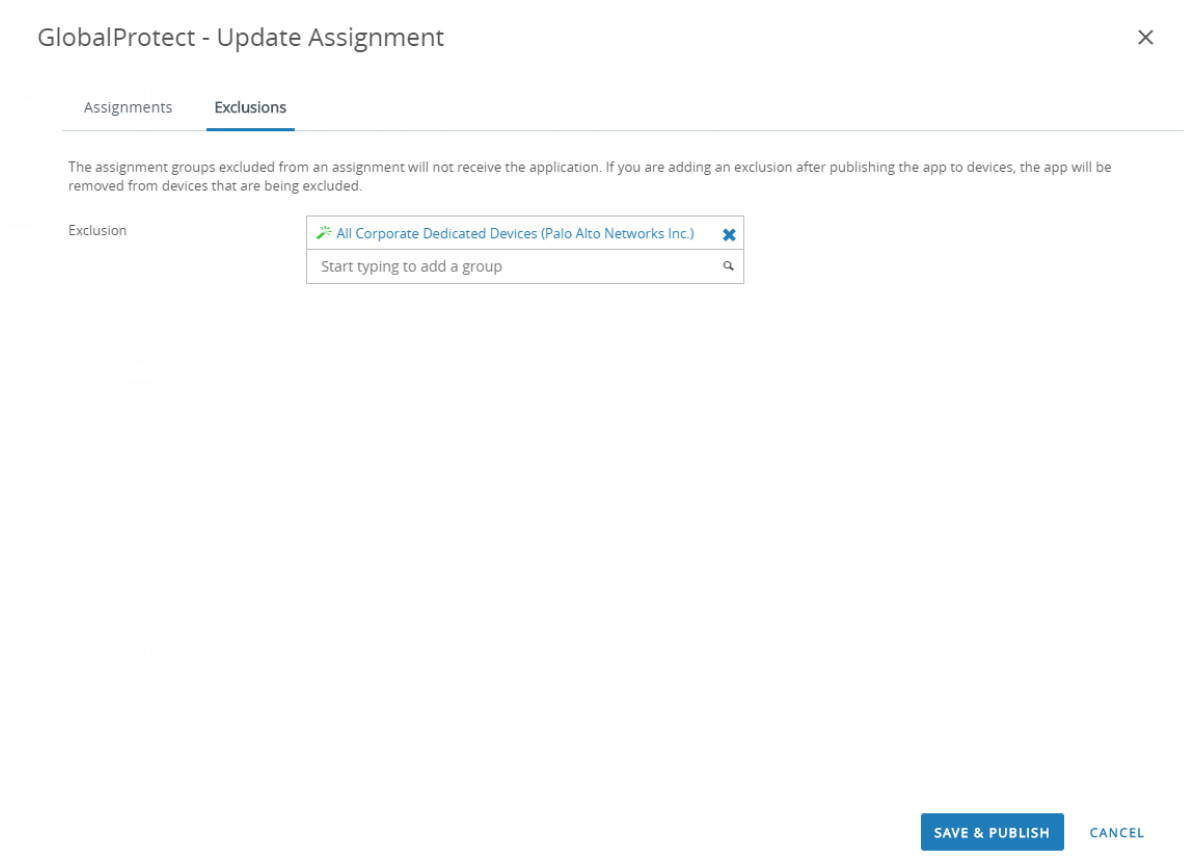
10.從公用應用程式清單（清單檢視）中選取新增的應用程式。
11.從 **Applications**（應用程式）> **Details View**（詳細資料檢視），按一下螢幕右上角的 **ASSIGN**（指派）。



12. 選取 **Assignments**（指派），然後按一下 **ADD ASSIGNMENT**（新增指派）以新增將可存取此應用程式的智慧群組。
    1. 在 **Select Assignment Groups**（選取指派群組）欄位，選取您想要授權存取此應用程式的智慧群組。
    2. 選取 **App Delivery Method**（應用程式傳遞方法）。如果您選取 **AUTO**（自動），應用程式將自動部署至指定的智慧群組。如果您選取 **ON DEMAND**（視需要），則必須手動部署應用程式。
    3. 將 **Managed Access**（管理存取）選項設定為 **ENABLED**（已啟用）。此選項將根據您適用的管理原則，授予使用者此應用程式的存取權限。
    4. 根據需要設定剩餘設定。
    5. **Add**（新增）新指派。



13. （ 選用 ）若要排除某些智慧群組的應用程式存取權限，請選取 **Exclusions**（排除），然後選取您想要從 **Exclusion**（排除） 欄位排除的智慧群組。



14.**SAVE & PUBLISH**（儲存並發行）設定至指派的智慧群組。

透過 *AirWatch* 為 *Android* 端點設定 *Per-App VPN* 組態

您可以透過使用 AirWatch 設定 GlobalProtect VPN 存取，從您的管理行動端點啟用內部資源存取。在 per-app VPN 組態中，您可以指定哪個管理應用程式可透過 GlobalProtect VPN 通道傳送流量。未管理的應用程式將繼續直接連線網際網路，而非透過 GlobalProtect VPN 通道。

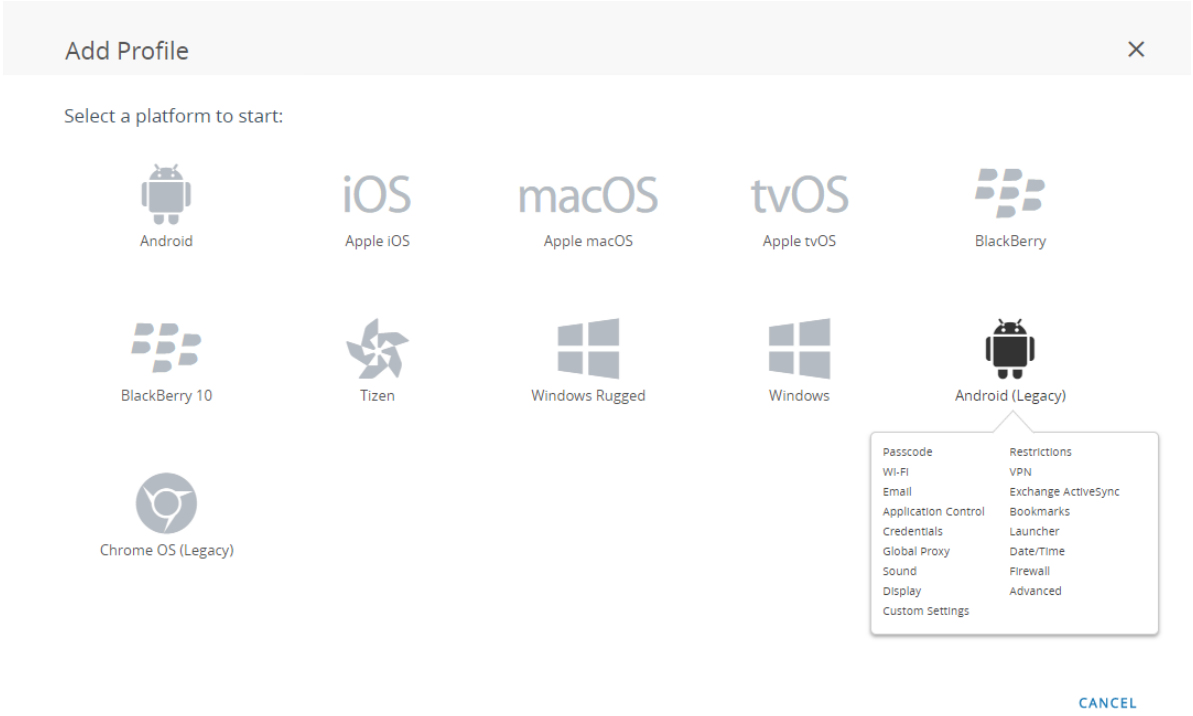
按照下列步驟使用 AirWatch 對 Android 端點設定 Per-App VPN 組態：

STEP 1 | 為 Android 下載 GlobalProtect 應用程式：

- 透過 AirWatch 部署 GlobalProtect 行動應用程式。
- 從 Google Play 直接下載 GlobalProtect 應用程式。

STEP 2 | 從 AirWatch 主控台修改現有 Android 設定檔或新增一個。

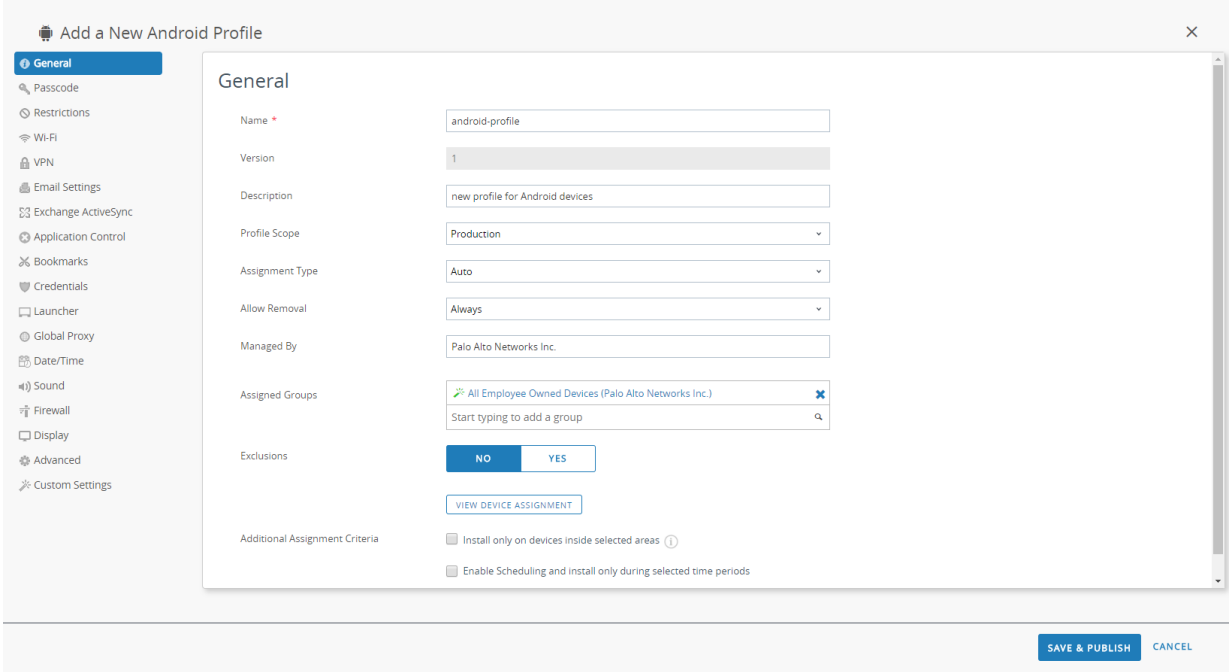
1. 選取 **Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles**（設定檔），然後 **ADD**（新增）新的設定檔。
2. 從平台清單選取 **Android (Legacy)**（**Android**（舊版））。



STEP 3 | 設定**General**（一般）設定：

1. 輸入設定檔的 **Name**（名稱）。
2. （選用）輸入說明設定檔用途的簡短**Description**（描述）。
3. （選用）選取 **Profile Scope**（設定檔範圍），**Production**（生產）、 **Staging**（預備）或 **Both**（二者皆是）。
4. （選用）選取 **Assignment Type**（指派類型）以決定設定檔如何部署至端點。選取 **Auto**（自動）將設定檔自動部署至所有端點，選取 **Optional**（選用）讓一般使用者能從自助式入口網站 (SSP) 安裝設定檔，或手動部署設定檔至個別端點，或選取 **Compliance**（合規性）在一般使用者違反套用於端點的合規性原則時部署設定檔。

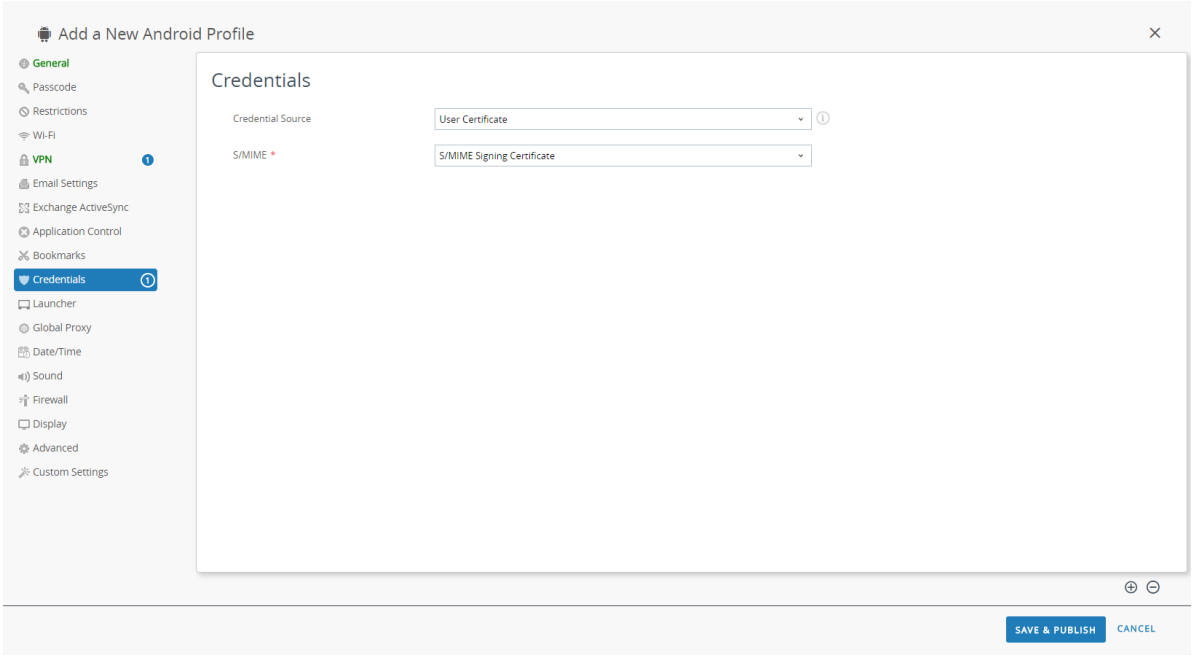
5. （選用）選取 **Allow Removal**（允許移除）以決定一般使用者能否移除設定檔。選取 **Always**（一律）讓一般使用者能在任何時候手動移除設定檔，選取 **Never**（絕不）防止一般使用者移除設定檔，或選取 **With Authorization**（透過授權）讓經過管理員授權的一般使用者能移除設定檔。選取 **With Authorization**（透過授權）會新增必要的密碼。
6. （選用）在 **Managed By**（被管理）欄位，輸入帶有設定檔管理存取的組織群組。
7. （選用）在 **Assigned Groups**（指派的群組）欄位，新增您希望新增設定檔的智慧群組。此欄位包含選項以建立新智慧群組，該智慧群組可透過規格設定用於最小 OS、設備型號、擁有權類別、組織群組等。
8. （選用）表示您是否希望包含任何 **Exclusions**（排除）至此設定檔的指派。如果選取 **Yes**（是），會顯示 **Excluded Groups**（排除群組）欄位，讓您可以選取希望從此設定檔指派中排除的智慧群組。



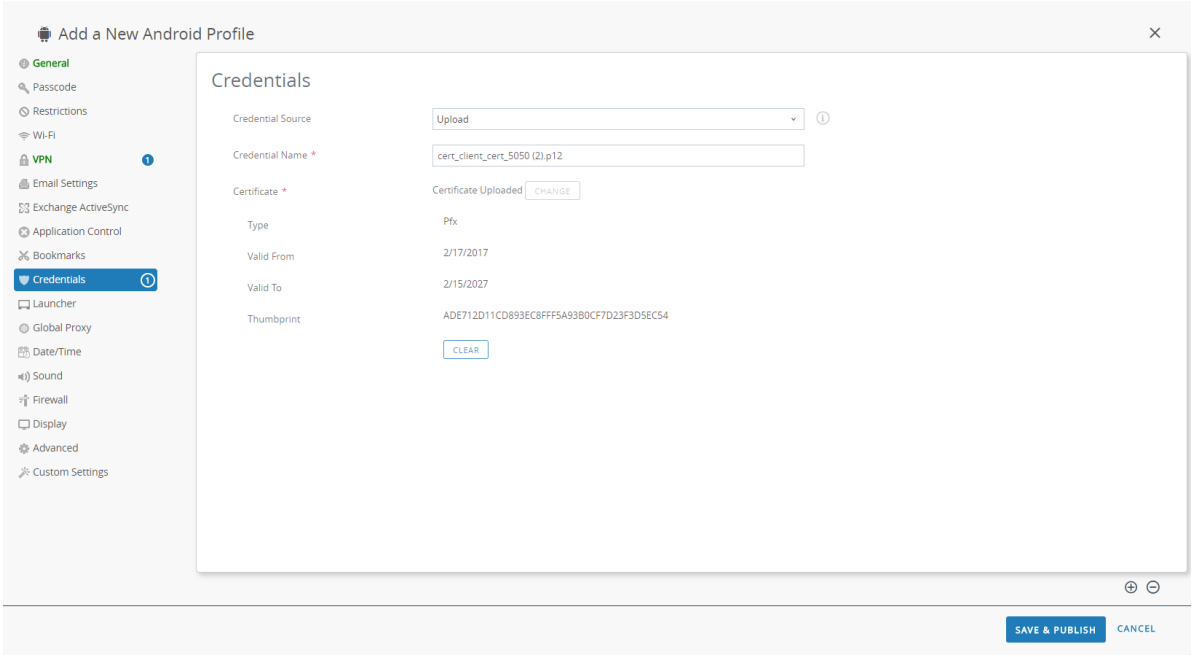
STEP 4 | 設定 **Credentials**（認證） 設定：

所有 *per-app VPN* 組態都需要基於憑證的驗證。

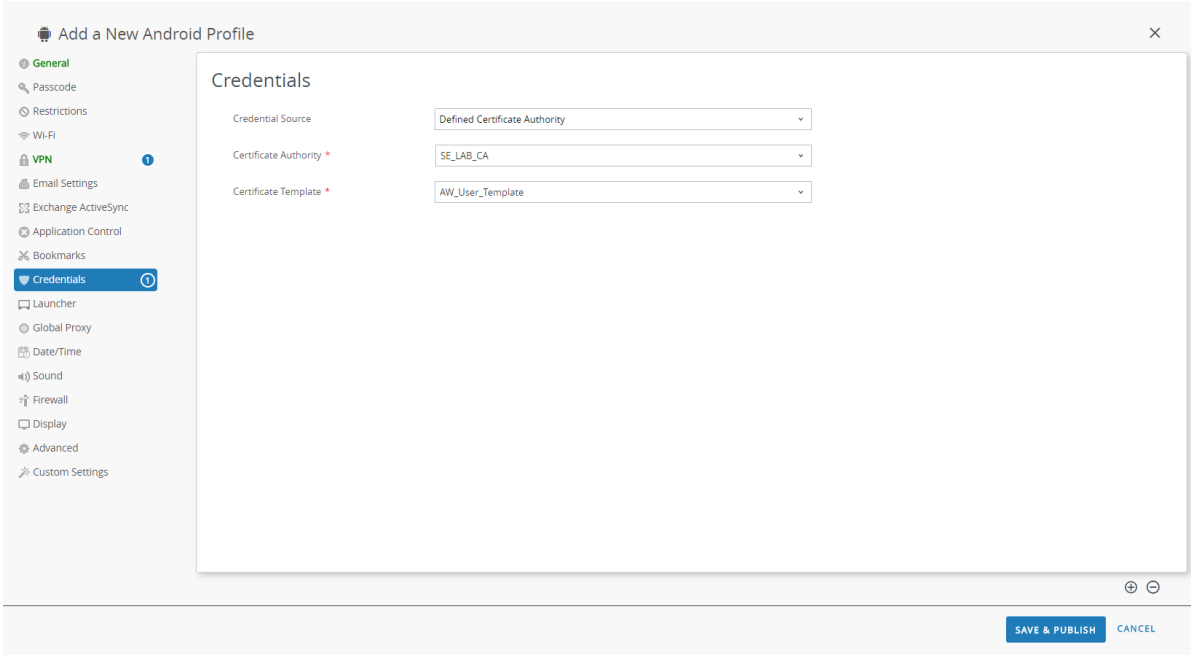
- 若要從 AirWatch 使用者提取用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **User Certificate**（使用者憑證）。
  2. 選取 **S/MIME Signing Certificate**（**S/MIME** 簽署憑證）（預設）。



- 若要手動上載用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **Upload**（上載）。
  2. 輸入 **Credential Name**（認證名稱）。
  3. 按一下 **UPLOAD**（上載）以找到並選取您要上載的憑證。
  4. 選取憑證後，按一下 **SAVE**（儲存）。



- 若要使用預先定義的憑證授權單位和範本：
  1. 將 **Credential Source**（認證來源）設定為 **Defined Certificate Authority**（定義的憑證授權單位）。
  2. 選取您想要取得憑證的 **Certificate Authority**（憑證授權單位）。
  3. 選取憑證授權單位的 **Certificate Template**（憑證範本）。

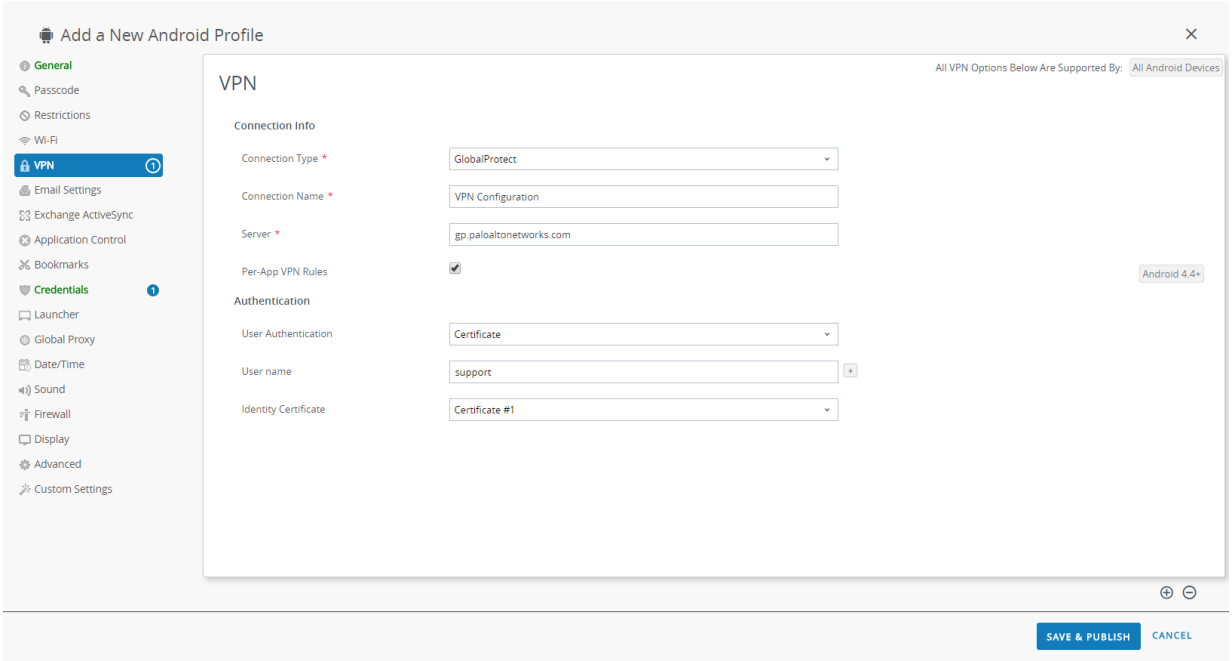


STEP 5 | 設定 **VPN** 設定：

1. 將網路 **Connection Type**（連線類型）設定為 **GlobalProtect**。
2. 輸入要端點顯示的 **Connection Name**（連線名稱）。
3. 在 **Server**（伺服器）欄位，輸入使用者連線的 GlobalProtect 入口網站主機或 IP 位址。
4. 啟用 **Per-App VPN Rules**（**Per-App VPN** 規則） 以通過 GlobalProtect VPN 通道路由傳送受管理應用程式的所有流量。
5. 在驗證區域，將 **User Authentication**（使用者驗證）方法設定為 **Certificate**（憑證）。

   所有 *per-app VPN* 組態都需要基於憑證的驗證。
6. 輸入 VPN 帳戶 **User name**（使用者名稱）或按一下新增 (+) 按鈕以檢視您可以插入的支援查閱值。
7. 出現提示時，請選取 GlobalProtect 將用於驗證使用者的 **Identity Certificate**（識別身分憑證）。**Identity Certificate**（識別身分憑證）與您在 **Credentials**（認證）設定中設定的憑證相同。

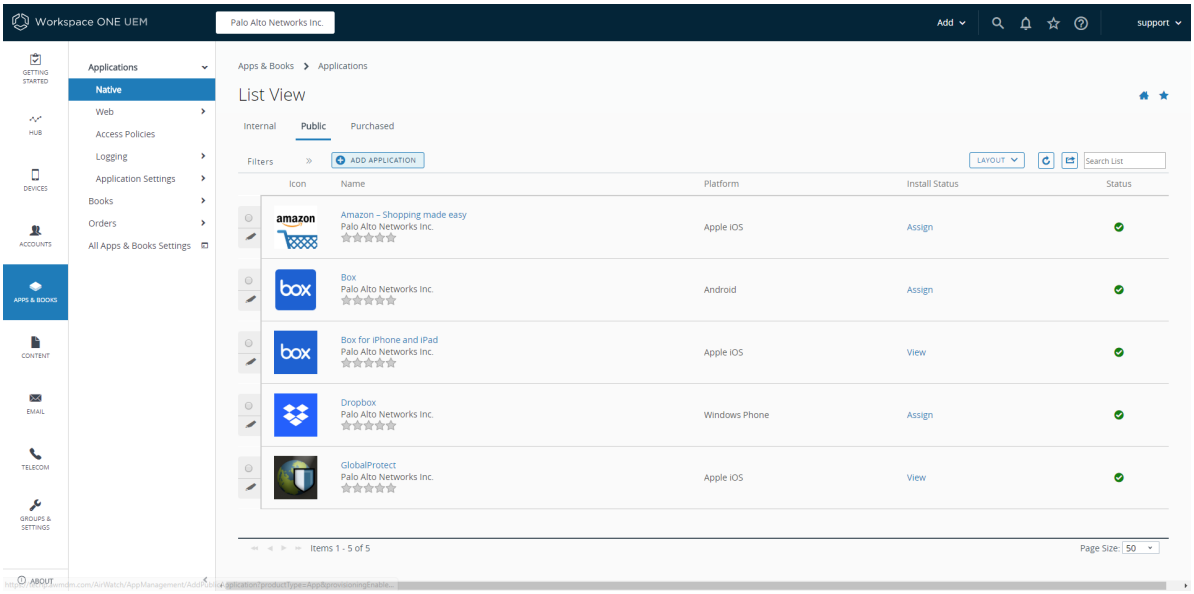


STEP 6 | **SAVE & PUBLISH**（儲存和發佈）您的變更。

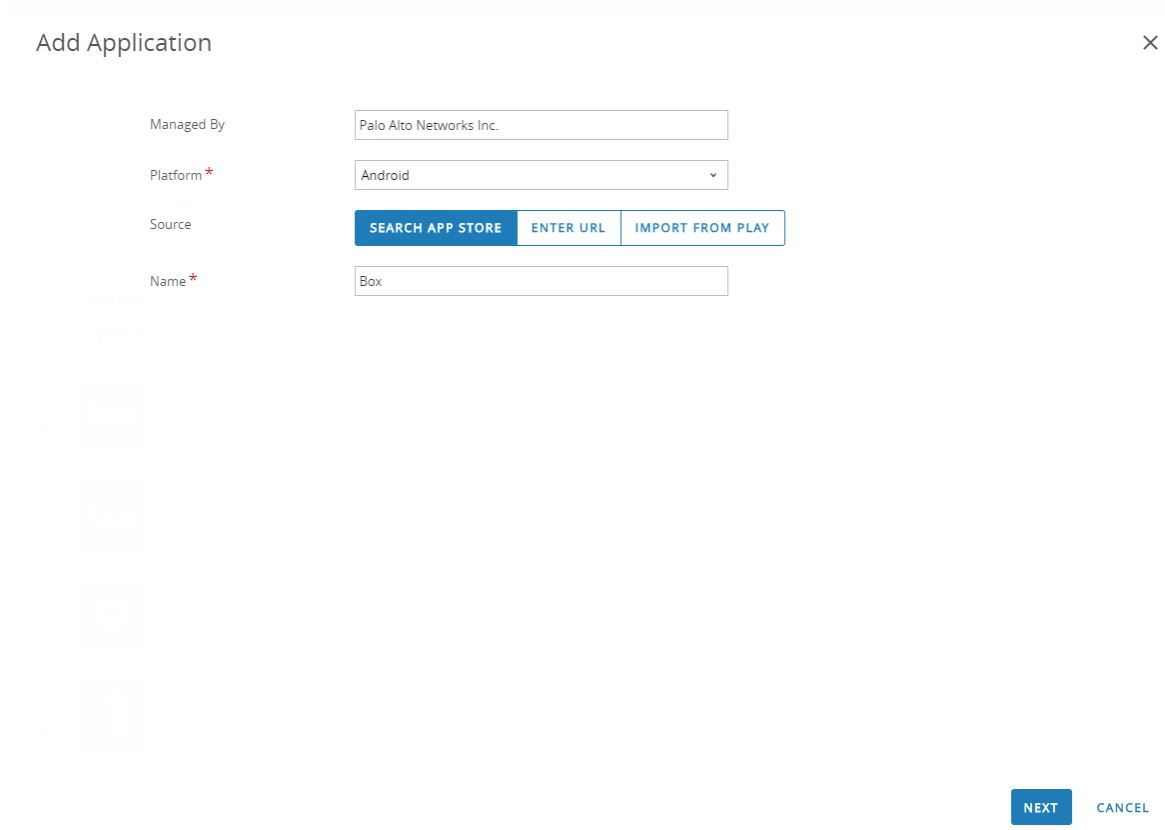
STEP 7 | 為新管理的應用程式設定 per-app VPN 設定，或修改現有受管理應用程式的設定。

設定應用程式設定和啟用 per-app VPN 後，您可以發行應用程式至使用者群組，並啟用此應用程式透過 GlobalProtect VPN 通道傳送流量。

1. 選取 **APPS & BOOKS**（應用程式和書本）> **Applications**（應用程式）> **Native**（原生）> **Public**（公用）。
2. 若要新增應用程式，選取 **ADD APPLICATION**（新增應用程式）。若要修改現有應用程式的設定，在公用應用程式清單（清單檢視）中找到應用程式，然後選取列旁動作功能表內的編輯 () 圖示。

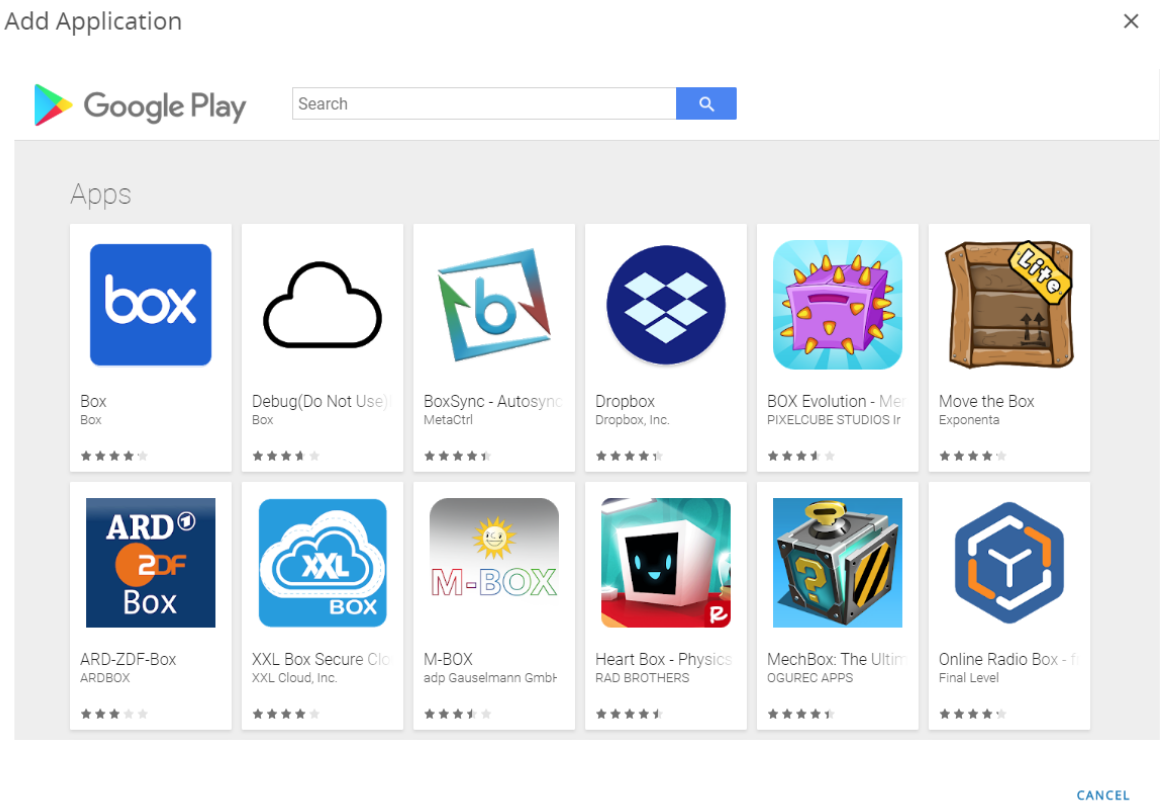


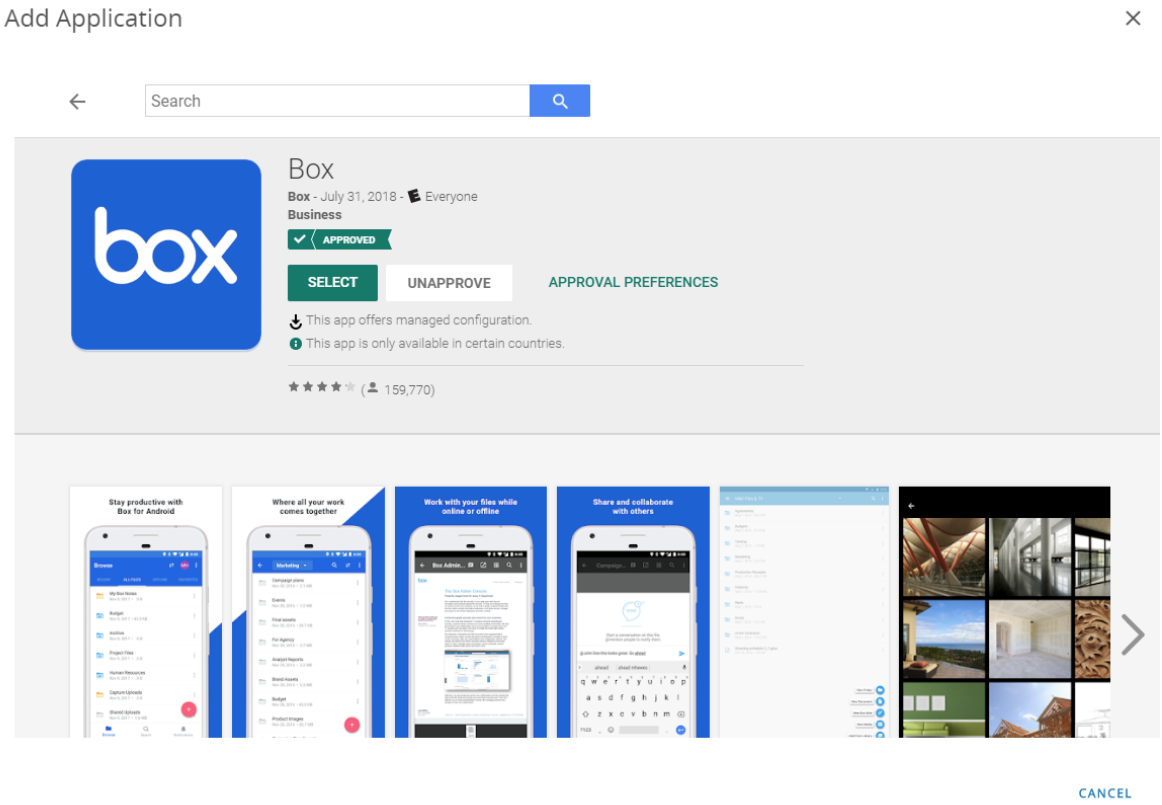
3. 在 **Managed By**（被管理）欄位，選取將管理此應用程式的組織群組。
4. 將 **Platform**（平台）設定為 **Android**。
5. 選取您用於尋找應用程式的偏好 **Source**（來源）：
   - **SEARCH APP STORE**（搜索應用程式商店）—輸入應用程式的 **Name**（名稱）。
   - **ENTER URL**（輸入 **URL**）—為此應用程式輸入 Google Play URL（例如，若要根據 URL 搜尋 Box 應用程式，輸入 https://play.google.com/store/apps/details?id=com.box.android）。
   - **IMPORT FROM PLAY**（從 **PLAY** 匯入）—從 Google Play 匯入公司核准的應用程式。



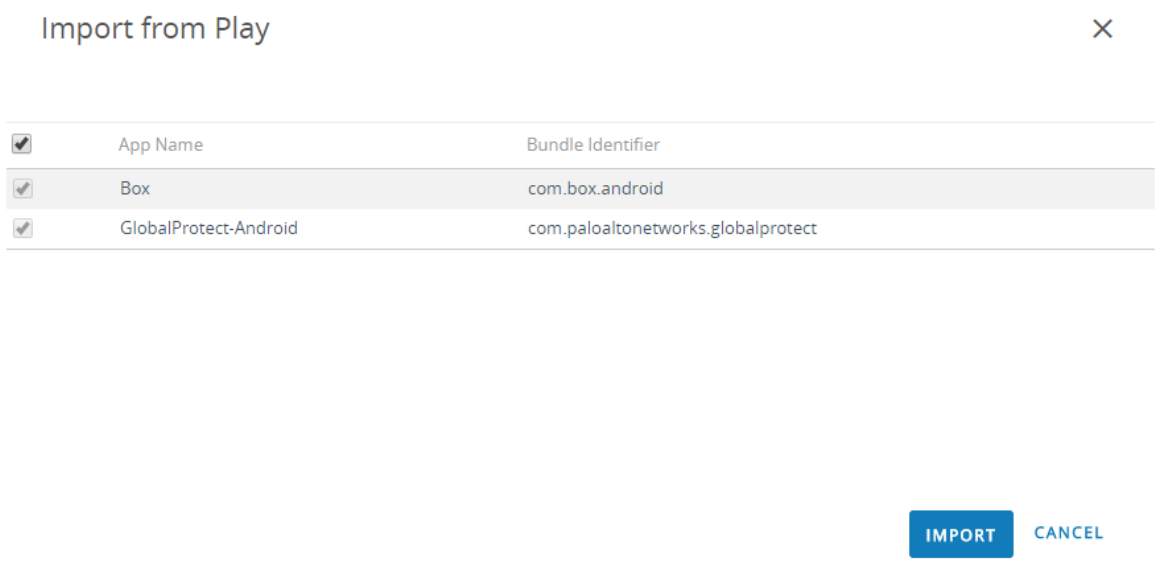
6. 按一下 **NEXT**（下一步）。

如果您選擇了搜尋 Google Play，請按一下搜尋結果清單中的應用程式圖示。如果您的公司尚未核准此應用程式，您必須 **APPROVE**（核准）應用程式。應用程式經過核准後，**SELECT**（選取）此應用程式。

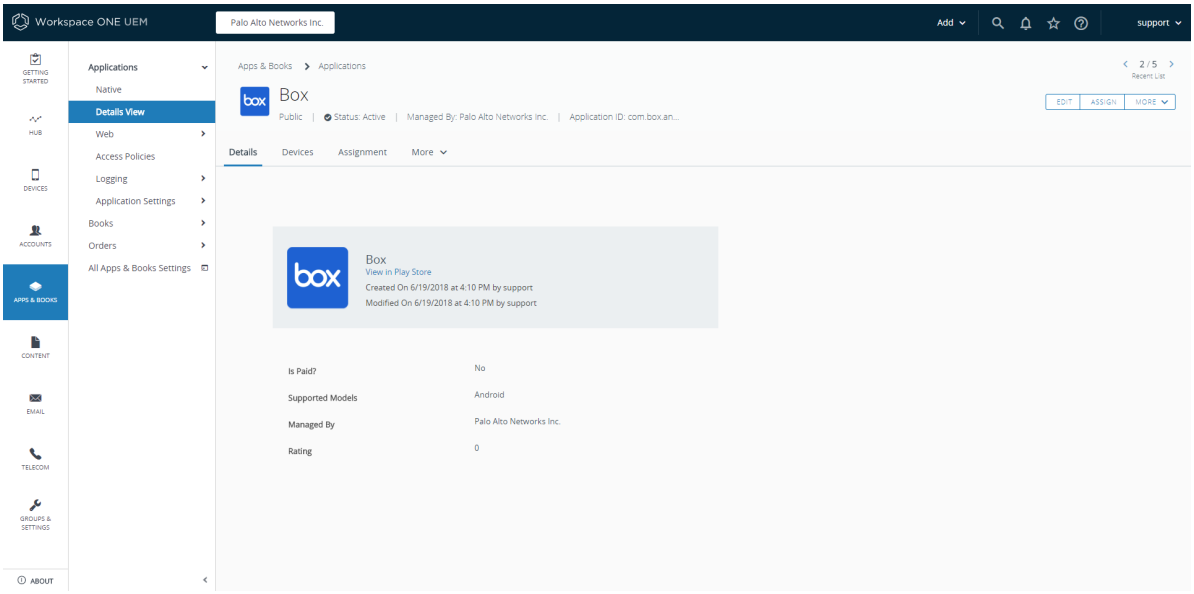




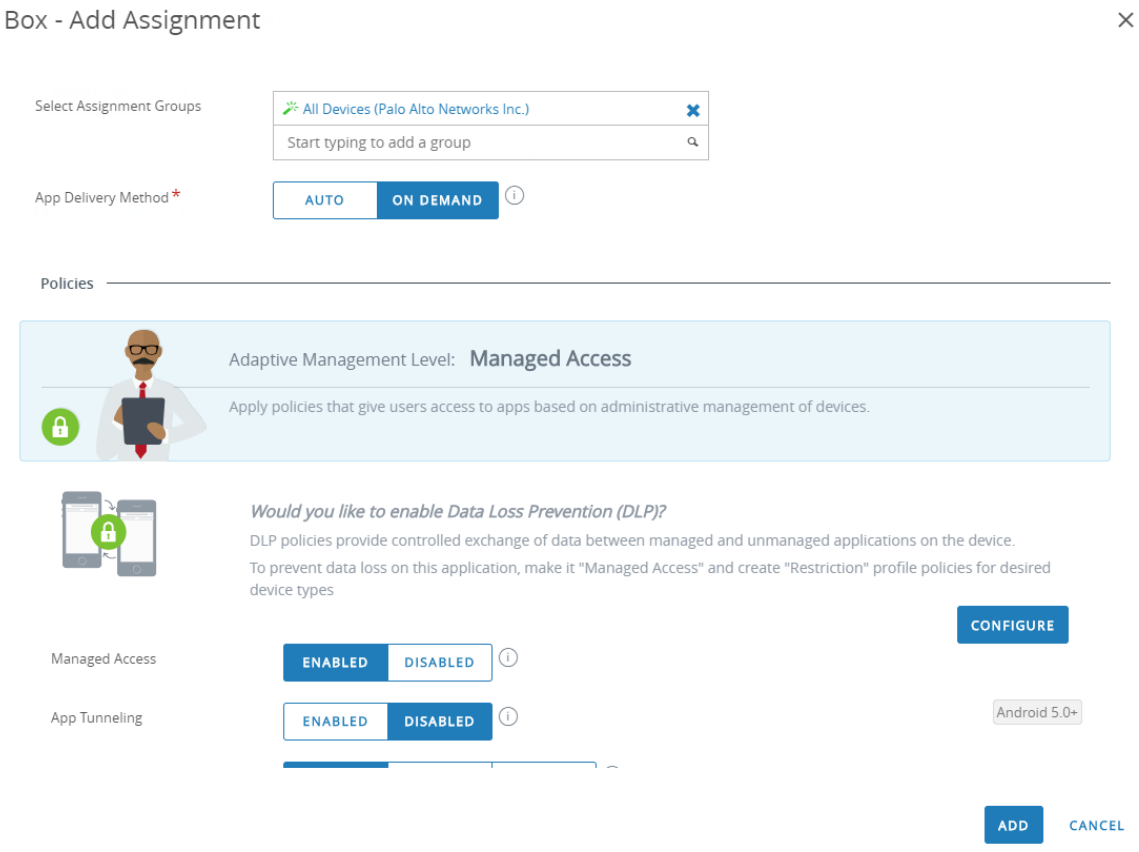
如果您選擇了從 Google Play 匯入應用程式，請從核准的公司應用程式清單中選取應用程式，然後按一下 **Import**（匯入）。如果您未在清單中看到該應用程式，聯絡您的 Android for Work 管理員核准應用程式。



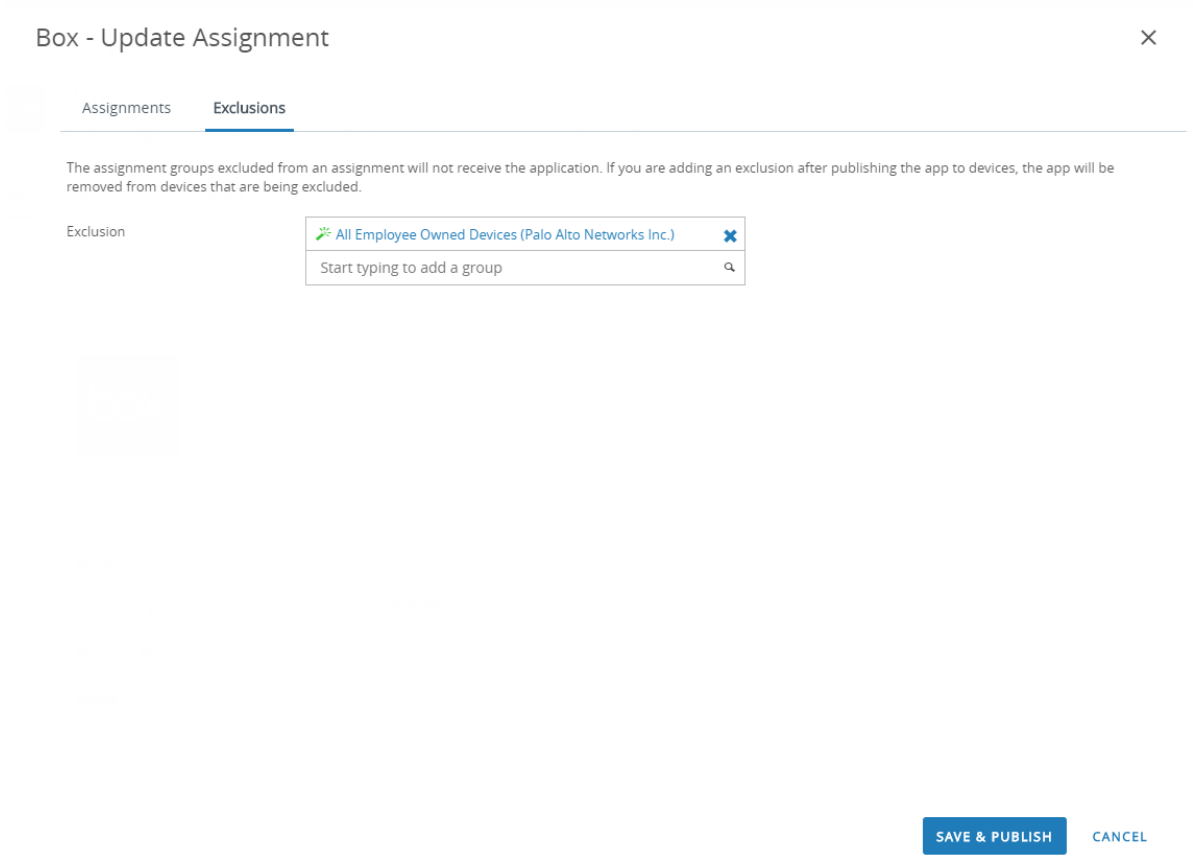
7. 從公用應用程式清單（清單檢視）中選取新增的應用程式。
8. 從 **Applications**（應用程式）> **Details View**（詳細資料檢視），按一下螢幕右上角的 **ASSIGN**（指派）。



9. 選取 **Assignments**（指派），然後按一下 **ADD ASSIGNMENT**（新增指派）以新增將可存取此應用程式的智慧群組。
    1. 在 **Select Assignment Groups**（選取指派群組）欄位，選取您想要授權存取此應用程式的智慧群組。
    2. 選取 **App Delivery Method**（應用程式傳遞方法）。如果您選取 **AUTO**（自動），應用程式將自動部署至指定的智慧群組。如果您選取 **ON DEMAND**（視需要），則必須手動部署應用程式。
    3. 將 **Managed Access**（管理存取）選項設定為 **ENABLED**（已啟用）。此選項將根據您適用的管理原則，授予使用者此應用程式的存取權限。
    4. 根據需要設定剩餘設定。
    5. **Add**（新增）新指派。



10. （ 選用 ）若要排除某些智慧群組的應用程式存取權限，請選取 **Exclusions**（排除），然後選取您想要從 **Exclusion**（排除） 欄位排除的智慧群組。



11.**SAVE & PUBLISH**（儲存並發行）設定至指派的智慧群組。

透過 *AirWatch* 對 *Windows 10 UWP* 端點設定 *Per-App VPN* 組態

您可以透過使用 AirWatch 設定 GlobalProtect VPN 存取，從您的管理行動端點啟用內部資源存取。在 per-app VPN 組態中，您可以指定哪個管理應用程式可透過 GlobalProtect VPN 通道傳送流量。未管理的應用程式將繼續直接連線網際網路，而非透過 GlobalProtect VPN 通道。

由於 *AirWatch* 尚未將 *GlobalProtect* 作為 *Windows* 端點的正式連線供應商，您必須選取替代的 *VPN* 供應商，編輯 *GlobalProtect* 應用程式設定，並根據下列工作流程所述將組態匯入 *VPN* 設定檔。

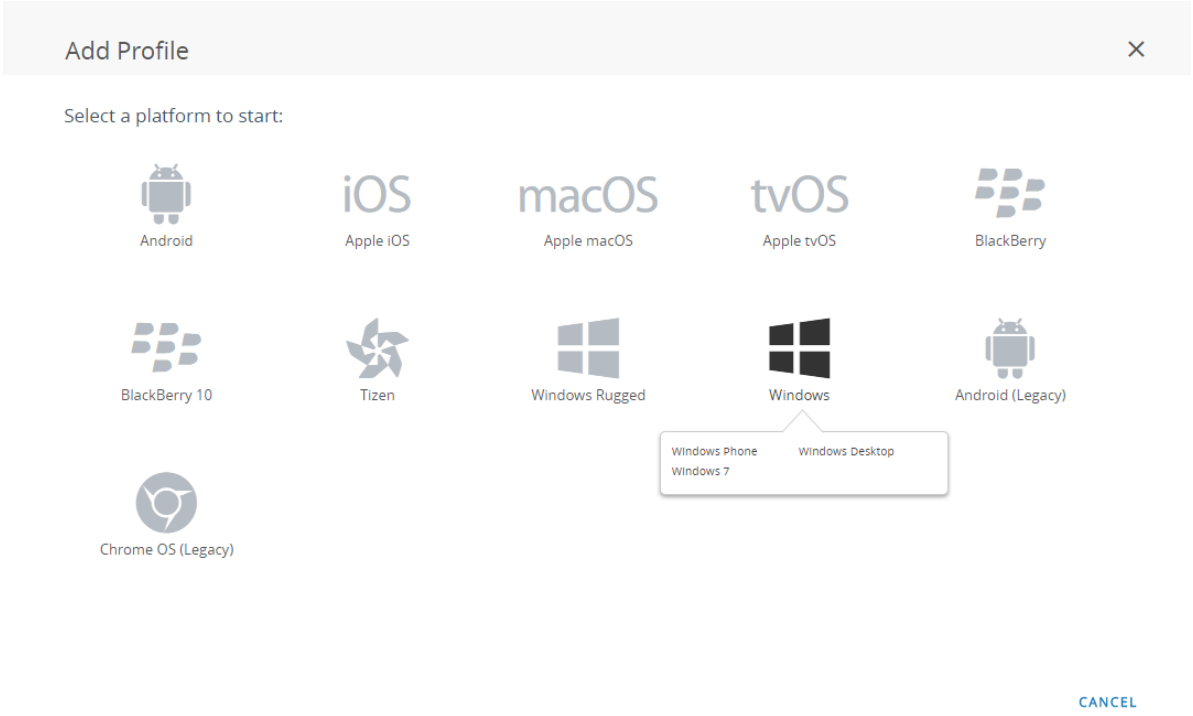
按照下列步驟使用 AirWatch 對 Windows 10 UWP 端點設定 Per-App VPN 組態：

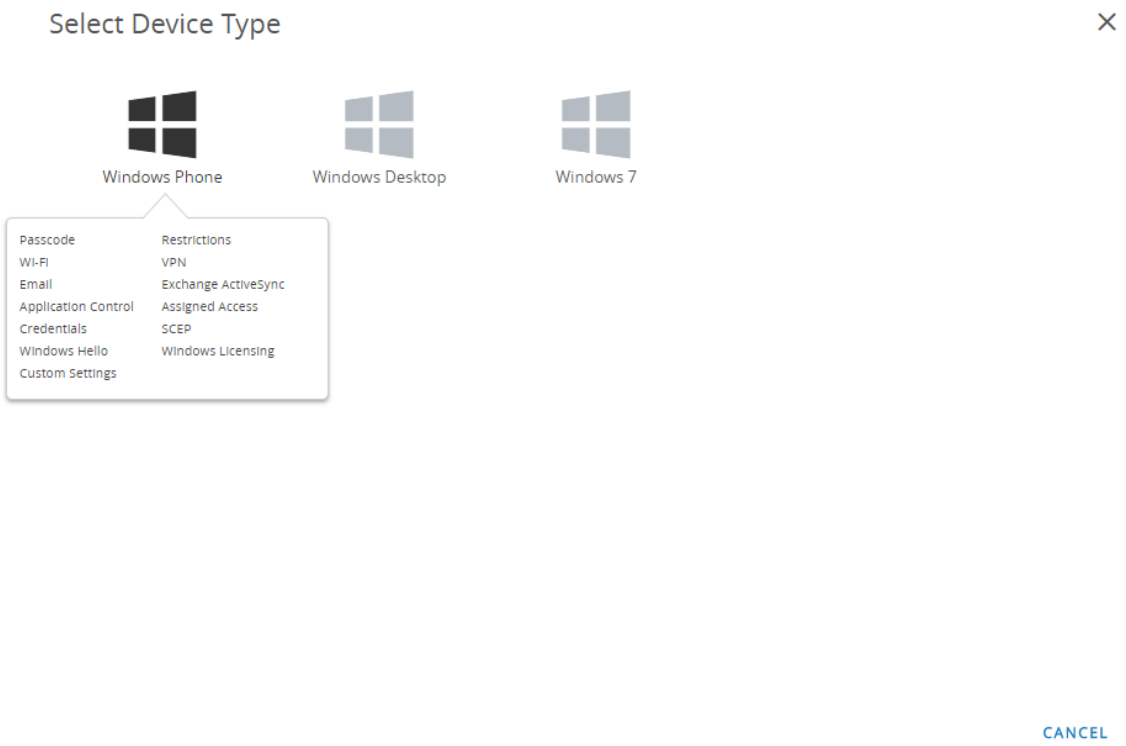
STEP 1 | 為 Windows 10 UWP 下載 GlobalProtect 應用程式：

- 透過 AirWatch 部署 GlobalProtect 行動應用程式。
- 從 Microsoft Store 直接下載 GlobalProtect 應用程式。

STEP 2 | 從 AirWatch 主控台修改現有 Windows 10 UWP 設定檔或新增一個。

1. 選取 **Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles**（設定檔），然後 **ADD**（新增）新的設定檔。
2. 選取 **Windows** 作為平台並選取 **Windows Phone** 作為裝置類型。

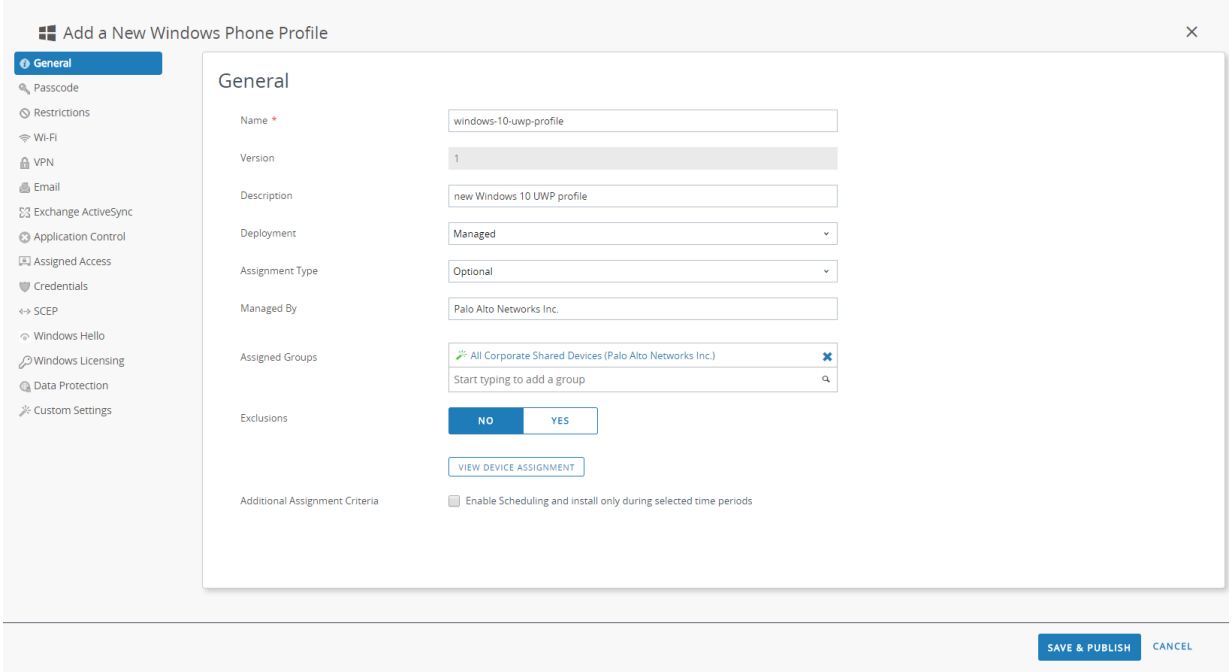




STEP 3 | 設定**General**（一般）設定：

- 輸入設定檔的 **Name**（名稱）。
- （選用）輸入說明設定檔用途的簡短**Description**（描述）。
- （選用）將 **Deployment**（部署）方法設定為 **Managed**（受管理）以使設定檔在取消註冊時自動移除
- （選用）選取 **Assignment Type**（指派類型）以決定設定檔如何部署至端點。選取 **Auto**（自動）將設定檔自動部署至所有端點，選取 **Optional**（選用）讓一般使用者能從自助式入口網站 (SSP) 安裝設定檔，或手動部署設定檔至個別端點，或選取 **Compliance**（合規性）在一般使用者違反套用於端點的合規性原則時部署設定檔。
- （選用）在 **Managed By**（被管理）欄位，輸入帶有設定檔管理存取的組織群組。

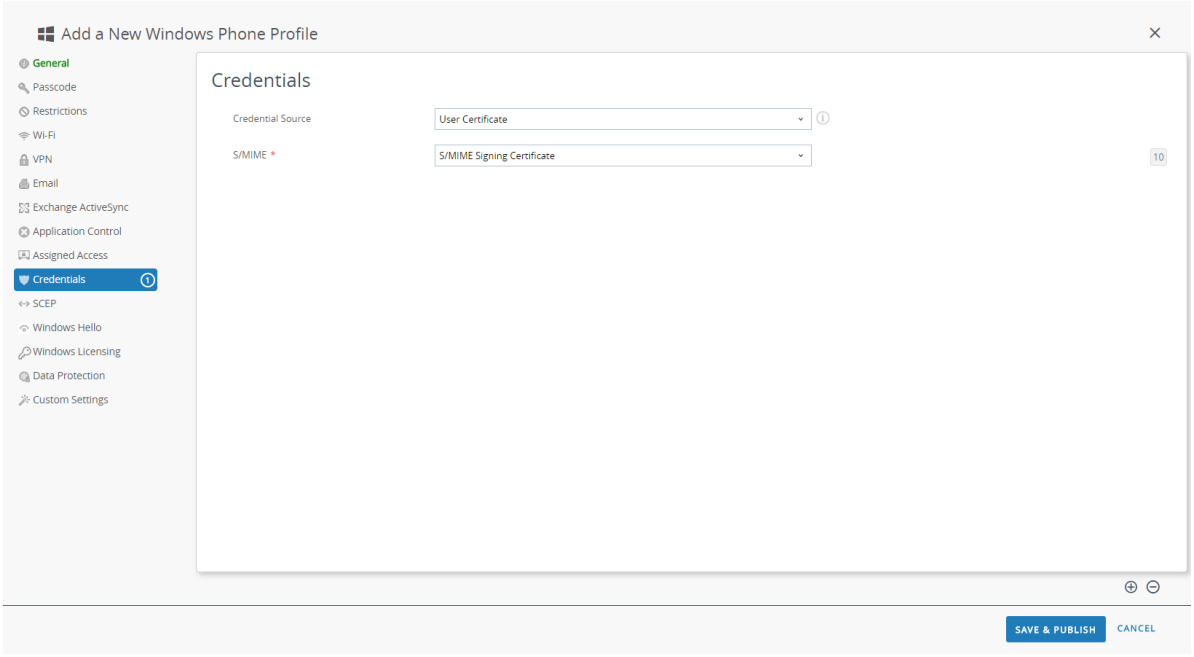
- （選用）在 **Assigned Groups**（指派的群組）欄位，新增您希望新增設定檔的智慧群組。此欄位包含選項以建立新智慧群組，該智慧群組可透過規格設定用於最小 OS、設備型號、擁有權類別、組織群組等。
- （選用）表示您是否希望包含任何 **Exclusions**（排除）至此設定檔的指派。如果選取 **Yes**（是），會顯示 **Excluded Groups**（排除群組）欄位，讓您可以選取希望從此設定檔指派中排除的智慧群組。



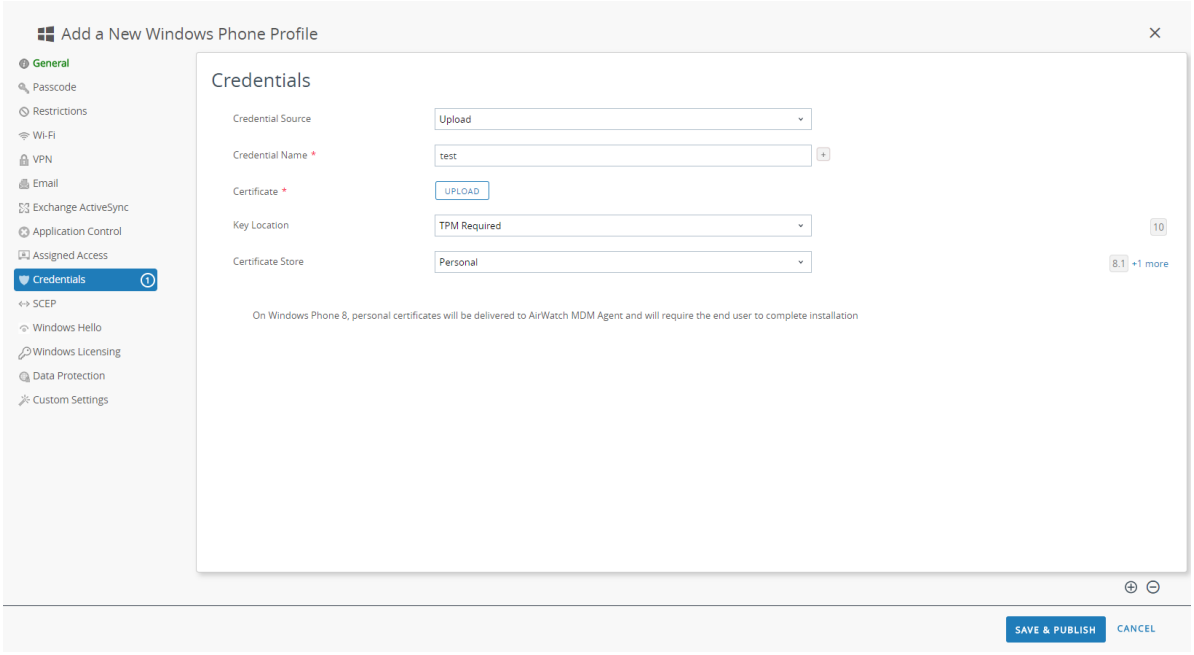
STEP 4 | 設定 **Credentials**（認證） 設定：

所有 *per-app VPN* 組態都需要基於憑證的驗證。

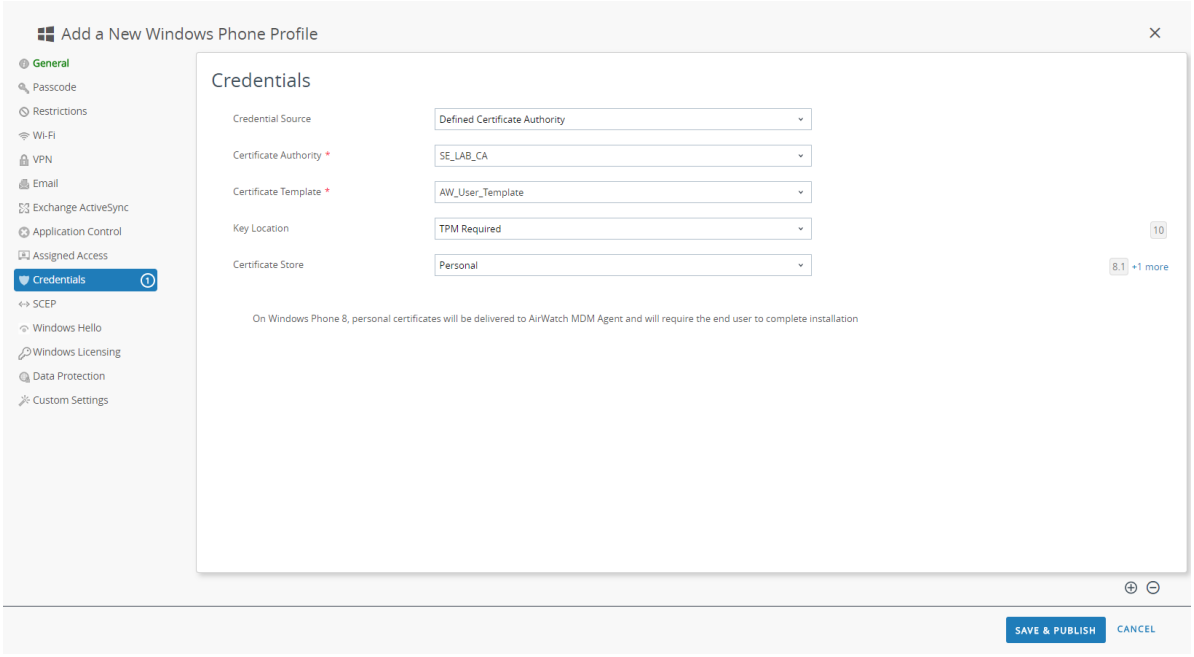
- 若要從 AirWatch 使用者提取用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **User Certificate**（使用者憑證）。
  2. 選取 **S/MIME Signing Certificate**（**S/MIME** 簽署憑證）（預設）。



- 若要手動上載用戶端憑證：
  1. 將 **Credential Source**（認證來源）設定為 **Upload**（上載）。
  2. 輸入 **Credential Name**（認證名稱）。
  3. 按一下 **UPLOAD**（上載）以找到並選取您要上載的憑證。
  4. 選取憑證後，按一下 **SAVE**（儲存）。
  5. 選取您想要儲存憑證私密金鑰的 **Key Location**（金鑰位置）：
     - **TPM Required**（TPM 要求）—在信任的平台模組上儲存私密金鑰。如果信任的平台模組在端點上不可用，則無法安裝私密金鑰。
     - **TPM If Present**（如果存在 **TPM**）—如果在端點上可用，在信任的平台模組上儲存私密金鑰。如果信任的平台模組在端點上不可用，私密金鑰將儲存在端點軟體中。
     - **Software**（軟體）—在端點軟體中儲存私密金鑰。
     - **Passport**（通行證）—儲存私密金鑰至 Microsoft Passport。若要使用此選項，必須在端點上安裝 AirWatch Protection Agent。
  6. 將 **Certificate store**（憑證存放區）設定為 **Personal**（個人）。



- 若要使用預先定義的憑證授權單位和範本：
  1. 將 **Credential Source**（認證來源）設定為 **Defined Certificate Authority**（定義的憑證授權單位）。
  2. 選取您想要取得憑證的 **Certificate Authority**（憑證授權單位）。
  3. 選取憑證授權單位的 **Certificate Template**（憑證範本）。
  4. 選取您想要儲存憑證私密金鑰的 **Key Location**（金鑰位置）：
     - **TPM Required**（**TPM** 要求）—在信任的平台模組上儲存私密金鑰。如果信任的平台模組在端點上不可用，則無法安裝私密金鑰。
     - **TPM If Present**（如果存在 **TPM**）—如果在端點上可用，在信任的平台模組上儲存私密金鑰。如果信任的平台模組在端點上不可用，私密金鑰將儲存在端點軟體中。
     - **Software**（軟體）—在端點軟體中儲存私密金鑰。
     - **Passport**（通行證）—儲存私密金鑰至 Microsoft Passport。若要使用此選項，必須在端點上安裝 AirWatch Protection Agent。
  5. 將 **Certificate store**（憑證存放區）設定為 **Personal**（個人）。



STEP 5 | 設定 **VPN** 設定：

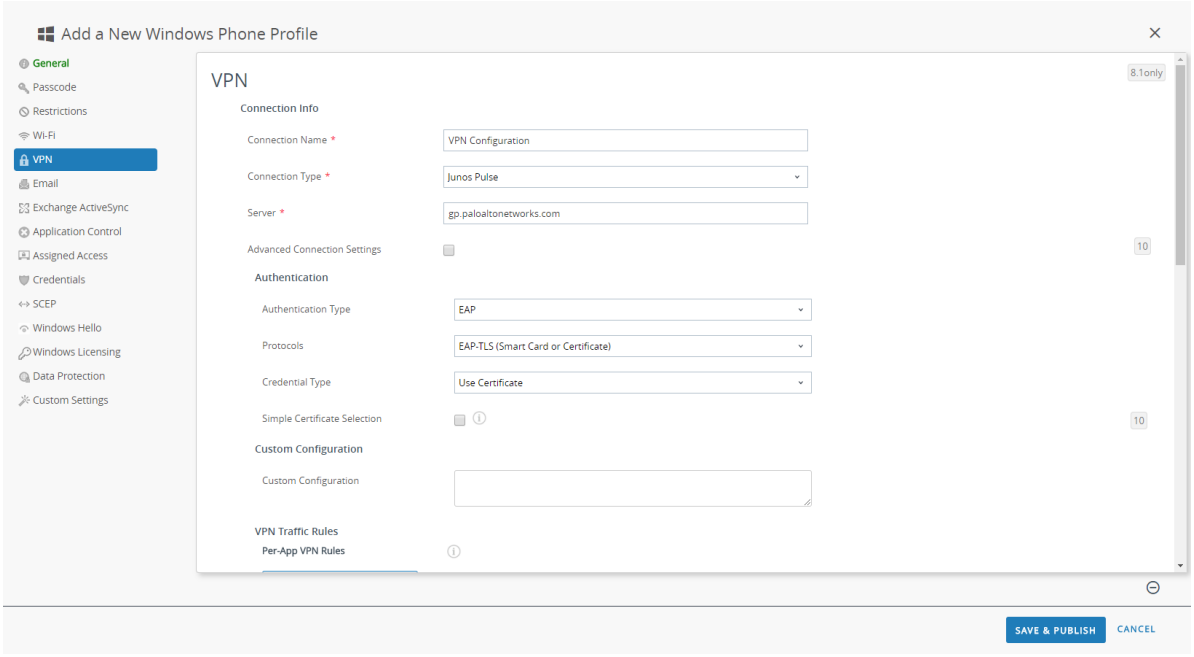
1. 輸入要端點顯示的 **Connection Name**（連線名稱）。
2. 選取替代 **Connection Type**（連線類型）供應商（不選取 **IKEv2**、**L2TP**、**PPTP** 或 **Automatic**（自動），因為其沒有 GlobalProtect VPN 設定檔所需的相關廠商設定）。

   您必須選取替代廠商，因為 *AirWatch* 尚未將 *GlobalProtect* 列為 *Windows* 端點的正式連線供應商。
3. 在 **Server**（伺服器）欄位，輸入使用者連線的 GlobalProtect 入口網站主機或 IP 位址。
4. 在驗證區域，選取基於憑證的 **Authentication Type**（驗證類型）以指定驗證一般使用者的方法。

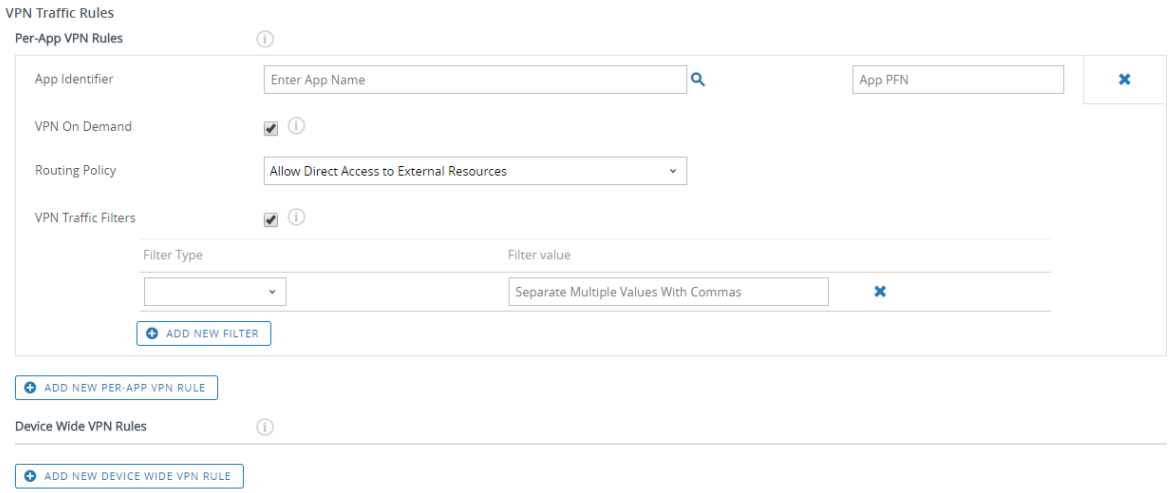
   

   所有 *per-app VPN* 組態都需要基於憑證的驗證。



5. （選用）若要允許 GlobalProtect 儲存使用者認證，請 **ENABLE**（啟用）此選項以在原則區域內 **Remember Credentials**（記住認證）。
6. 在 VPN 流量規則區域內，**ADD NEW PER-APP VPN RULE**（新增 **PER-APP VPN** 規則），為特定的舊版應用程式（通常為 .exe 檔案）或新型應用程式（通常自 Microsoft Store 下載）指定規則。
   1. （選用）啟用 **VPN On Demand**（視需要 **VPN**）以允許 GlobalProtect 連線在應用程式啟動時自動建立。
   2. 選取 **Routing Policy**（路由原則）以指定是否透過 VPN 通道傳送應用程式流量。
   3. （選用）設定特定 **VPN Traffic Filters**（**VPN** 流量篩選條件），只有當符合您定義的特定比對準則（如 IP 位址和連接埠）時才透過 VPN 通道路由應用程式流量。

      透過按一下 **ADD NEW FILTER**（新增篩選條件）來新增比對準則。出現提示時，請輸入 **Filter Name**（篩選條件名稱）和對應的 **Filter Value**（篩選值）。

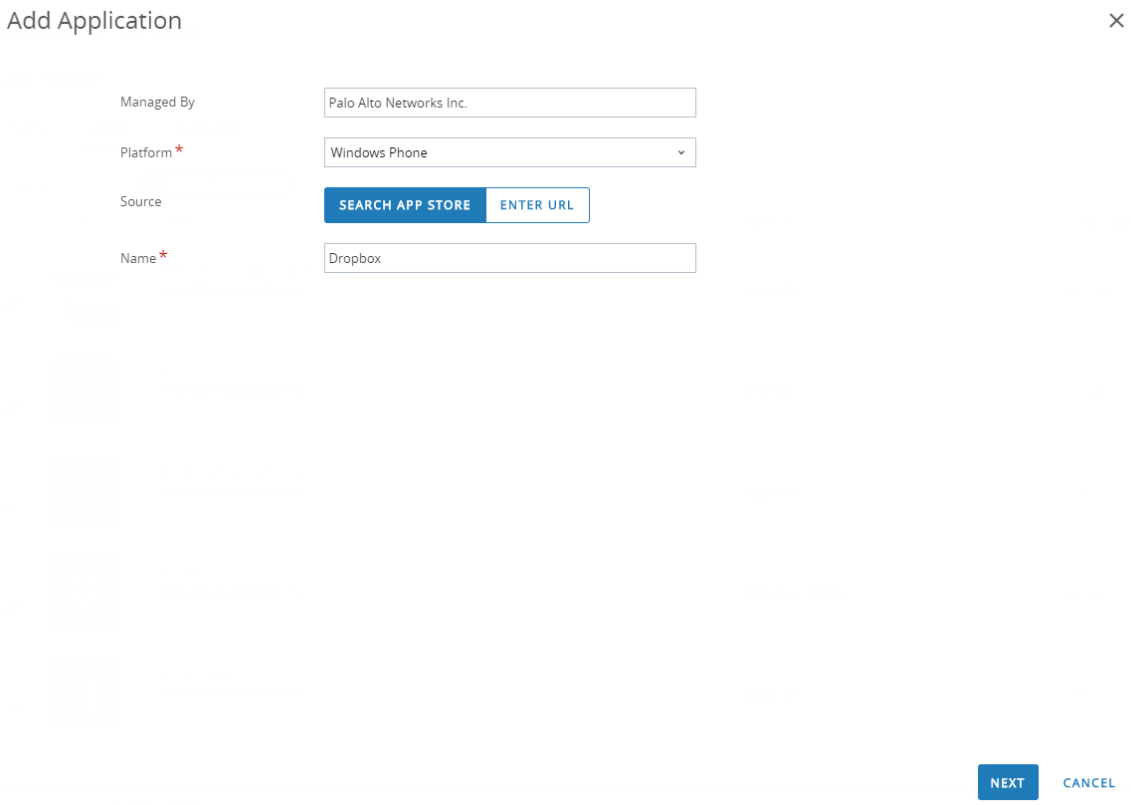


STEP 6 | **SAVE & PUBLISH**（儲存和發佈）您的變更。

STEP 7 | 為新管理的應用程式設定 per-app VPN 設定，或修改現有受管理應用程式的設定。

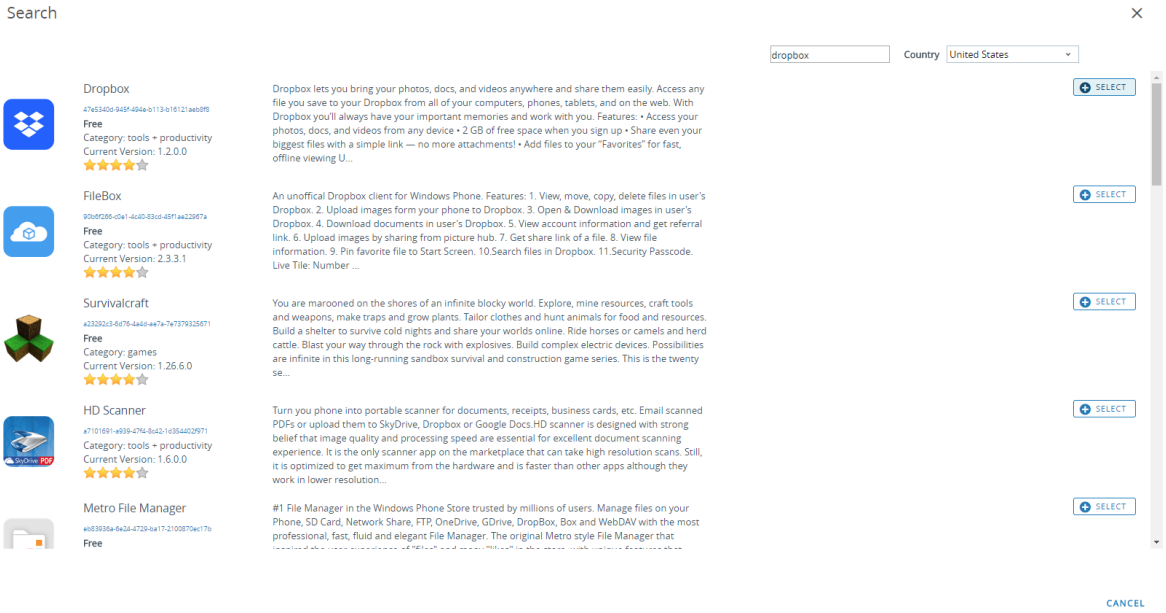
設定應用程式設定和啟用 per-app VPN 後，您可以發行應用程式至使用者群組，並啟用此應用程式透過 GlobalProtect VPN 通道傳送流量。

1. 選取 **APPS & BOOKS**（應用程式和書本）> **Applications**（應用程式）> **Native**（原生）> **Public**（公用）。
2. 若要新增應用程式，選取 **ADD APPLICATION**（新增應用程式）。若要修改現有應用程式的設定，在公用應用程式清單中找到應用程式，然後選取列旁動作功能表內的編輯 () 圖示。
3. 在 **Managed By**（被管理）欄位，選取將管理此應用程式的組織群組。
4. 將 **Platform**（平台）設定為 **Windows Phone**。
5. 選取您用於尋找應用程式的偏好 **Source**（來源）：
   - **SEARCH APP STORE**（搜索應用程式商店）—輸入應用程式的 **Name**（名稱）。
   - **ENTER URL**（輸入 **URL**）—為此應用程式輸入 Microsoft Store URL（例如，若要根據 URL 搜尋 Dropbox 行動應用程式，輸入 https://www.microsoft.com/en-us/p/dropbox-mobile/9wzdncrfj0pk）。

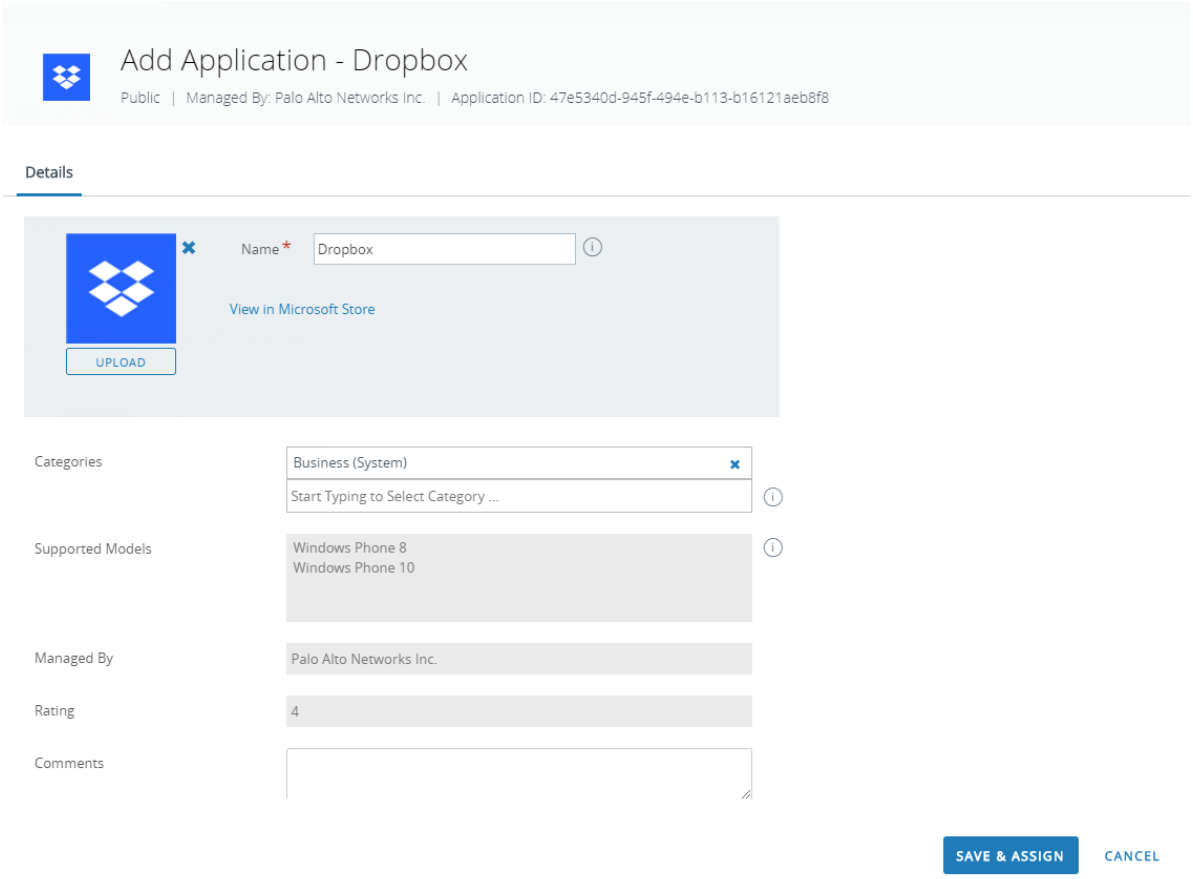


6. 按一下 **NEXT**（下一步）。

   如果您選取了在 Microsoft Store 中搜尋應用程式，您必須從搜尋結果清單中 **SELECT**（選取）應用程式。

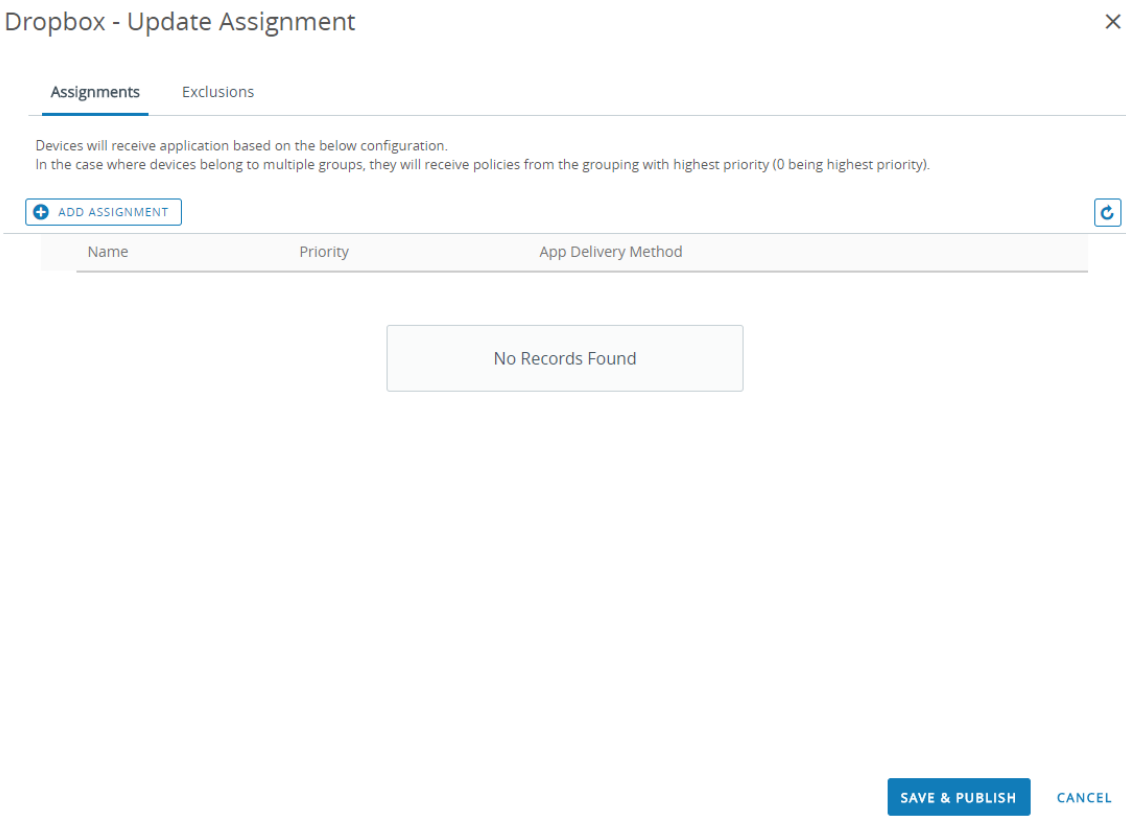


7. 在新增應用程式對話方塊中，請確保應用程式 **Name**（名稱）正確。此名稱將顯示在 AirWatch 應用程式目錄中。
8. （選用）指派應用程式至預先定義或自訂 **Categories**（類別）以輕觸存取 AirWatch 應用程式目錄。

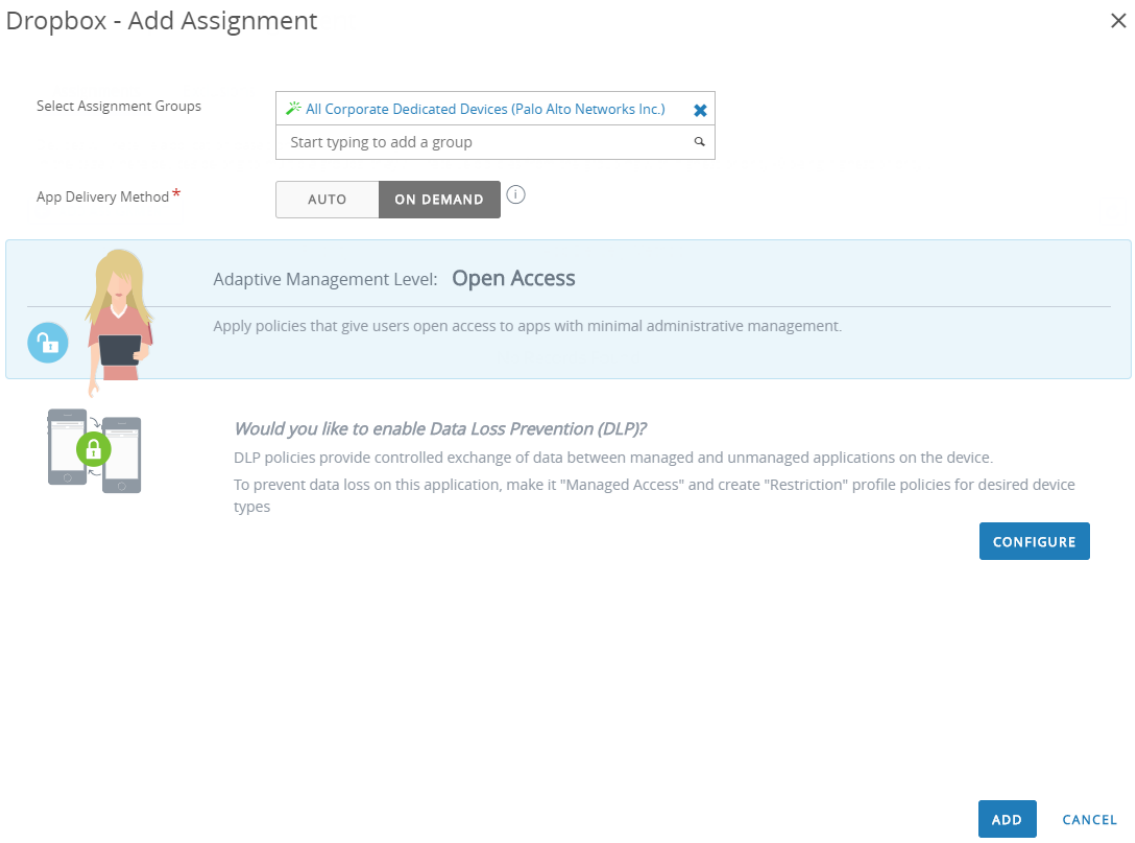


9. **SAVE & ASSIGN**（儲存並指派）新應用程式。

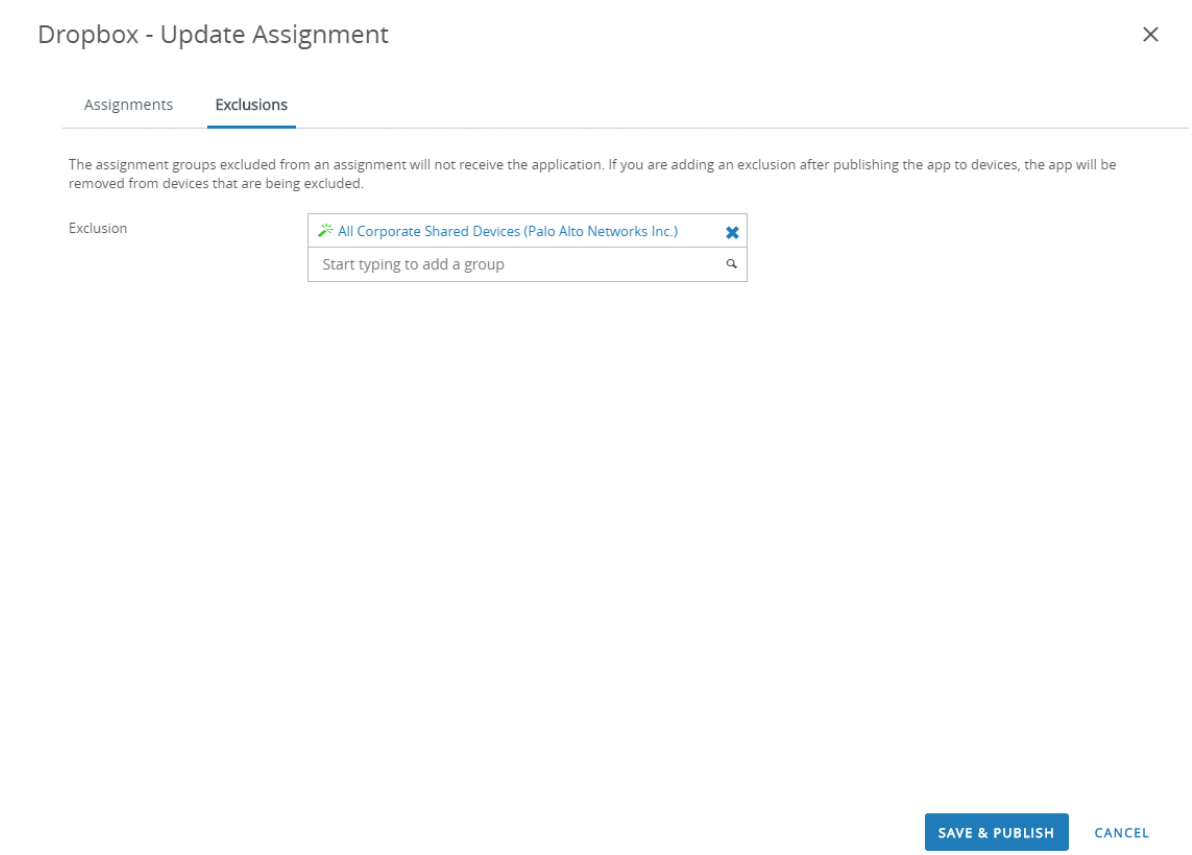
10. 在更新指派對話方塊中，選取 **Assignments**（指派），然後按一下 **ADD ASSIGNMENT**（新增指派）以新增將可存取此應用程式的智慧群組。



1. 在 **Select Assignment Groups**（選取指派群組）欄位，選取您想要授權存取此應用程式的智慧群組。
2. 選取 **App Delivery Method**（應用程式傳遞方法）。如果您選取 **AUTO**（自動），應用程式將自動部署至指定的智慧群組。如果您選取 **ON DEMAND**（視需要），則必須手動部署應用程式。
3. **Add**（新增）新指派。



11. （ 選用 ）若要排除某些智慧群組的應用程式存取權限，請選取 **Exclusions**（排除），然後選取您想要從 **Exclusion**（排除） 欄位排除的智慧群組。



12.**SAVE & PUBLISH**（儲存並發行）設定至指派的智慧群組。

STEP 8 | 若要將連線類型供應商設定為 GlobalProtect，請編輯 XML 內的 VPN 設定檔。

若要最小化原 *XML* 內的其他編輯，在您匯出組態前，檢閱您的 *VPN* 設定檔內的設定。如果您需要在匯出 *VPN* 設定檔後變更設定，您可以在原 *XML* 中進行變更，或在 *VPN* 設定檔中更新設定並再次執行此步驟。

1. 在 **Devices**（裝置）> **Profiles**（設定檔）> **List View**（清單檢視），選取您在之前步驟中新增的設定檔旁的無線電按鈕，然後選取表格頂部的 **</>XML**。AirWatch 會打開設定檔的 XML 檢視。
2. **Export**（匯出）設定檔，然後在您選取的文字編輯器中打開。
3. 為 GlobalProtect 編輯下列設定：

- 在指定 `PluginPackageFamilyName` 的 `LoclURI` 元件中變更元件為：

  <LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>
- 在後續的 `Data` 元件中，變更數值為：

  <Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>

1. 將您的變更儲存至匯出的設定檔。
2. 返回 AirWatch 並選取 **Devices**（裝置）> **Profiles**（設定檔）> **List View**（清單檢視）。
3. 建立（選取 **Add**（新增）> **Add Profile**（新增設定檔）> **Windows** > **Windows Phone**（**Windows** 手機））並命名一個新的設定檔。
4. 選取 **Custom Settings**（自訂設定）> **Configure**（設定），然後複製並粘上編輯的組態。
5. **Save & Publish**（儲存和發佈）您的變更。

STEP 9 | 透過從 **Devices**（裝置）> **Profiles**（設定檔）> **List View**（清單檢視）選取原始設定檔，然後選取 **More Actions**（其他動作）> **Deactivate**（停用），來清除原始設定檔。AirWatch 會將設定檔移動至非使用中清單。

STEP 10 | 測試組態。

透過 **Microsoft Intune** 設定 **Per-App VPN** 組態

Microsoft Intune 是讓您可以從中央位置管理行動端點的雲端企業行動管理平台。GlobalProtect 應用程式提供 Microsoft Intune 在裝置或應用程式等級管理的防火牆和行動端點之間的安全連線。使用 Android 的 GlobalProtect 作為安全連線，可進行對流量的一致檢查和對網路安全政策的強化，以預防行動端點上的威脅。

有關如何使用 Microsoft Intune 設定 Per-App VPN 組態的資訊，請參閱以下幾節：

- 透過 Microsoft Intune 為 iOS 端點設定 Per-App VPN 組態
- 透過 Microsoft Intune 對 Windows 10 UWP 端點設定 Per-App VPN 組態

透過 *Microsoft Intune* 為 *iOS* 端點設定 *Per-App VPN* 組態

您可以透過使用 Microsoft Intune 設定 GlobalProtect VPN 存取，從您的管理行動端點啟用內部資源存取。在 per-app VPN 組態中，您可以指定哪個管理應用程式可透過 VPN 通道路由傳送流量。未管理的應用程式將繼續直接連線網際網路，而非透過 VPN 通道。

按照下列步驟使用 Microsoft Intune 對 iOS 端點設定 Per-App VPN 組態：

STEP 1 | 為 iOS 下載 GlobalProtect 應用程式。

- 透過 Microsoft Intune 部署 GlobalProtect 行動應用程式.
- 從 App Store 直接下載 GlobalProtect 應用程式。

STEP 2 | 新增應用程式至 Microsoft Intune。

您必須將應用程式新增至 Microsoft Intune 才能指派、監控、設定或保護應用程式。

- 將 **App type**（應用程式類型）設定為 **iOS**。
- 新增 iOS 商店應用程式至 Microsoft Intune。

STEP 3 | 為 iOS 設定 per-app VPN 組態。

- 當您建立 per-app VPN 設定檔時，將 **Platform**（平台）設定為 **iOS** 並將 **Connection type**（連線類型）設定為 **Palo Alto Networks GlobalProtect**。
- 當您將應用程式與 VPN 設定檔相關聯時，從 **VPNS**（**VPN**）下拉式清單中選取 per-app VPN 設定檔。

透過 *Microsoft Intune* 對 *Windows 10 UWP* 端點設定 *Per-App VPN* 組態

您可以透過使用 Microsoft Intune 設定 GlobalProtect VPN 存取，從您的管理行動端點啟用內部資源存取。在 per-app VPN 組態中，您可以指定哪個管理應用程式可透過 VPN 通道路由傳送流量。未管理的應用程式將繼續直接連線網際網路，而非透過 VPN 通道。

按照下列步驟使用 Microsoft Intune 對 Windows 10 UWP 端點設定 Per-App VPN 組態：

STEP 1 | 為 Windows 10 UWP 下載 GlobalProtect 應用程式：

- 透過 Microsoft Intune 部署 GlobalProtect 行動應用程式.
- 從 Microsoft Store 直接下載 GlobalProtect 應用程式。

STEP 2 | 設定憑證設定檔。

所有 *per-app VPN* 組態都需要基於憑證的驗證。

STEP 3 | 建立新 Windows 10 UWP VPN 設定檔。

- 將 **Platform**（平台）設定為 **Windows 10** 及更新版本。

STEP 4 | 為 Windows 10 UWP 端點設定 per-app VPN 設定。

- 將 **Connection type**（連線類型）設定為 **Palo Alto Networks GlobalProtect**。
- 在應用程式與流量規則區域，將將 **WIP** 或應用程式與此 **VPN** 相關聯選項設定為將應用程式與此連線相關聯。**Enable**（啟用）此選項以 **Restrict VPN connection to these apps**（限制這些應用程式的 **VPN** 連線），然後 **Add**（新增）您想要使用 VPN 連線的相關應用程式。

透過 **MobileIron** 設定 **Per-App VPN** 組態

MobileIron 是讓您可以從中央控制台管理行動端點的企業行動管理平台。GlobalProtect 應用程式提供 MobileIron 在裝置或應用程式等級管理的防火牆和行動端點之間的安全連線。使用 Android 的 GlobalProtect 作為安全連線，可進行對流量的一致檢查和對網路安全政策的強化，以預防行動端點上的威脅。

有關如何使用 MobileIron 設定 Per-App VPN 組態的資訊，請參閱以下章節：

- 透過 MobileIron 為 iOS 端點設定 Per-App VPN 組態

透過 *MobileIron* 為 *iOS* 端點設定 *Per-App VPN* 組態

您可以透過使用 MobileIron 設定 GlobalProtect VPN 存取，從您的管理行動端點啟用內部資源存取。在 per-app VPN 組態中，您可以指定哪個管理應用程式可透過 VPN 通道路由傳送流量。未管理的應用程式將繼續直接連線網際網路，而非透過 VPN 通道。

按照下列步驟使用 MobileIron 對 iOS 端點設定 Per-App VPN 組態：

STEP 1 | 為 iOS 下載 GlobalProtect 應用程式。

- 透過 MobileIron 部署 GlobalProtect 行動應用程式.
- 從 App Store 直接下載 GlobalProtect 應用程式。

STEP 2 | 新增憑證設定，然後設定憑證設定。

所有 *per-app VPN* 組態都需要基於憑證的驗證。

STEP 3 | 新增 per-app VPN 組態。

- 將設定類型設定為 **Per-app VPN**。

STEP 4 | 為 iOS 設定 per-app VPN 設定。

- 將 **Connection Type**（連線類型）設定為 **Palo Alto Networks GlobalProtect**，然後進行相關設定。

啟用應用程式掃描與 *WildFire* 的整合

透過在 AirWatch 中啟用應用程式掃描，您可以利用關於應用程式的 WildFire® 威脅情報，偵測 Android 端點上的惡意軟體。當啟用時，AirWatch 代理程式遞送安裝在 Android 端點上的應用程式清單至 AirWatch。此情形發生在註冊和端點簽入之後。AirWatch 會定期查詢 WildFire 是否有裁定，並根據裁定對端點採取符合性措施。

STEP 1 | 開始之前，獲得一個 WildFire API 金鑰。如果您尚未獲得 API 金鑰，請聯絡支援部門。

STEP 2 | 從 AirWatch，選取 **Groups & Settings**（群組和設定）> **All Settings**（所有設定）> **Apps**（應用程式）> **App Scan**（應用程式掃描）> **Third Party Integration**（協力廠商整合）。

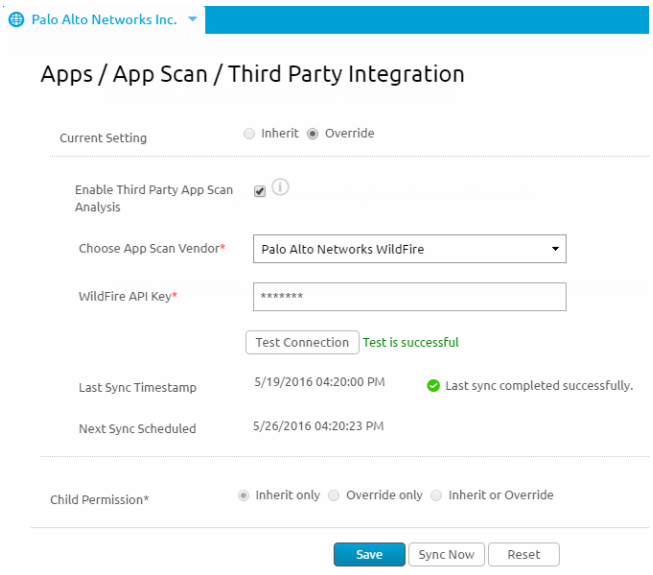
STEP 3 | 選取 **Current Setting:**（目前設定）：覆寫 。

STEP 4 | 選取 **Enable Third Party App Scan Analysis**（啟用協力廠商應用程式掃描分析）以啟用 AirWatch 和 WildFire 之間的通訊。

STEP 5 | 從 **Choose App Scan Vendor**（選取應用程式掃描廠商）下拉式清單中，選取 **Palo Alto Networks WildFire**。

STEP 6 | 輸入您的 WildFire API 金鑰。

STEP 7 | 按一下 **Test Connection**（測試連線），確保 AirWatch 可以與 WildFire 通訊。如果測試失敗，驗證與網際網路的連線，重新輸入 API 金鑰，然後重試。



STEP 8 | **Save**（儲存）變更。AirWatch 排程同步工作與 WildFire 通訊，獲得應用程式雜湊的最新裁定，並定期執行此工作。按一下 **Sync Now**（立即同步）以啟動與 WildFire 的手動同步。

在適用于 *macOS* 端點的 *GlobalProtect* 應用程式上抑制通知

macOS 上的 GlobalProtect 應用程式支援兩種類型的延伸—核心（執行 macOS Catalina 10.15.3 或更舊版本的 macOS 裝置）與系統（執行 macOS Catalina 10.15.4 或更新版本與 GlobalProtect 應用程式 5.1.4 或更新版本的 macOS 裝置）。如果您已在 GlobalProtect 閘道上設定分割通道或執行 GlobalProtect 連線以存取網路（參閱 GlobalProtect 應用程式自訂），GlobalProtect 應用程式上將顯示通知訊息。當使用者存取已啟用這些功能的 GlobalProtect 應用程式時，該訊息會提示使用者在已封鎖載入的 macOS 中啟用核心延伸或系統延伸。

若要允許 GlobalProtect 應用程式使用者在不收到通知的情況下自動載入核心延伸或系統延伸，您可使用支援的行動裝置管理 (MDM) 為該延伸（如 Airwatch）建立原則。

有關如何在適用于 macOS 端點的 GlobalProtect 應用程式上抑制通知，請參閱以下幾節：

- 在適用于 macOS 端點的 GlobalProtect 應用程式中啟用核心延伸
- 在適用于 macOS 端點的 GlobalProtect 應用程式中啟用系統延伸

在適用于 **macOS** 端點的 **GlobalProtect** 應用程式中啟用核心延伸

從 macOS 10.13 開始，Apple 引入了一項軟體變更，要求使用者在使用核心延伸之前必須獲得核准。

雖然使用者可以在 macOS 上手動啟用核心延伸（**System Preferences**（系統偏好設定）> **Security & Privacy**（安全性與隱私），然後選取 **Allow**（允許）核心延伸），您也可以使用 Qualified MDM vendor（合格的 MDM 廠商）建立原則並自動核准核心延伸。Apple 技術說明 TN2450介紹了這一過程。

以下工作流程使用 Airwatch 進行了測試。

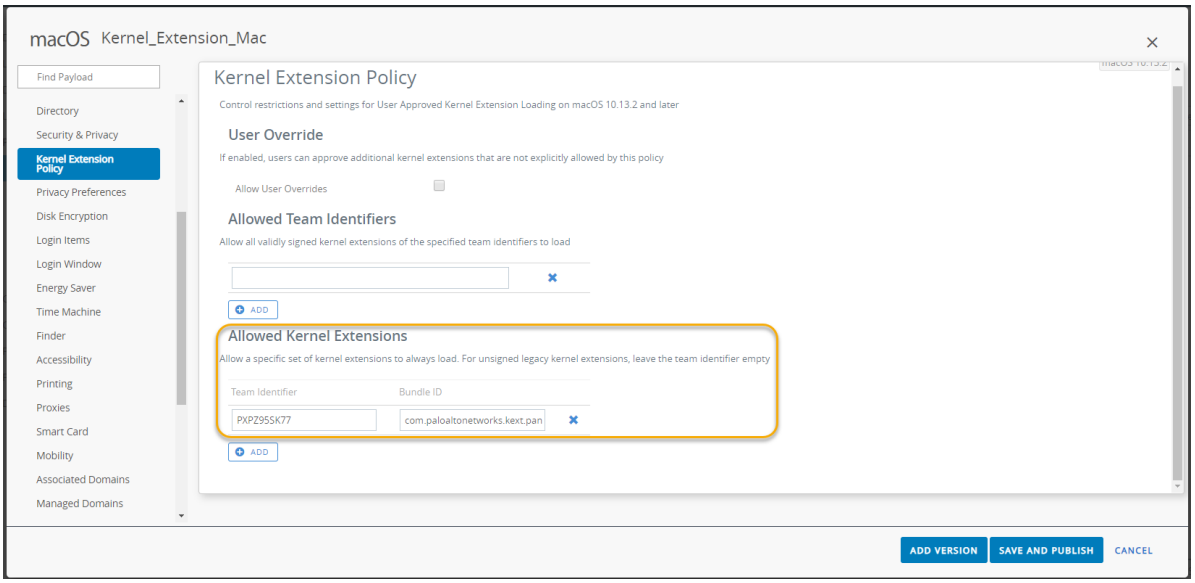
STEP 1 | 建立核心延伸原則。

1. 以管理員身份登入至 AirWatch。
2. 選取 **Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles**（設定檔），然後從下拉式清單中選取 **Add**（新增）> **Add Profile**（新增設定檔）。
3. 在 **Add Profile**（新增設定檔）區域，按一下 **Apple macOS**，然後按一下 **Device Profile**（裝置設定檔）圖示。
4. 在 **General**（一般）區域，指定設定檔的名稱。

您還可在清單中選取現有核心延伸設定檔（**Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles**（設定檔））。

STEP 2 | 新增核心延伸並將相關原則散佈至 macOS 裝置。

1. 選取 **Kernel Extension Policy**（核心延伸原則）。
2. 輸入 GlobalProtect 應用程式使用的團隊識別碼 (**PXPZ95SK77**)。
3. 輸入搭售包 **ID** (**com.paloaltonetworks.kext.pangpd**)。



4. 按一下 **Save and Publish**（儲存並發佈）以儲存變更。

在適用于 macOS 端點的 GlobalProtect 應用程式中啟用系統延伸

從 macOS 10.15.4 開始，Apple 限制了對核心延伸的支援。GlobalProtect 應用程式將使用系統延伸取代核心延伸。使用者必須核准系統延伸才能使用它們。

按照以下步驟進行設定檔設定，以使用 AirWatch 自動核准系統延伸。雖然已使用 AirWatch 對設定進行測試，但您可使用任何合格的 MDM 廠商建立並實作此設定檔。

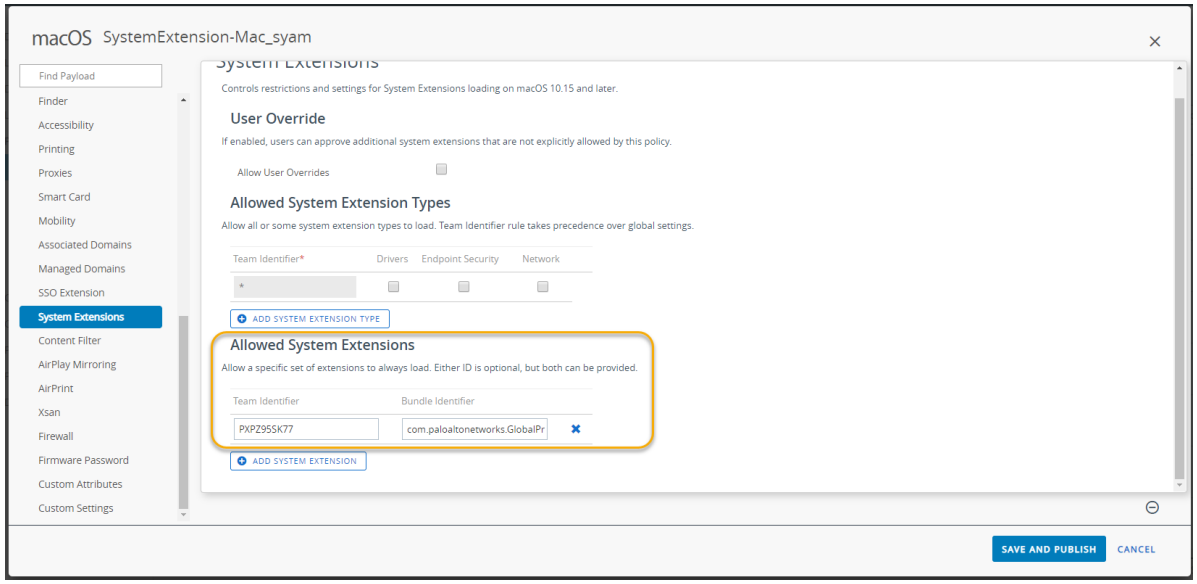
STEP 1 | 建立系統延伸設定檔。

1. 以管理員身份登入至 AirWatch。
2. 選取 **Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles**（設定檔），然後從下拉式清單中選取 **Add**（新增）> **Add Profile**（新增設定檔）。
3. 在 **Add Profile**（新增設定檔）區域，按一下 **Apple macOS**，然後按一下 **Device Profile**（裝置設定檔）圖示。
4. 在 **General**（一般）區域，指定設定檔的名稱。

   您還可在清單中選取現有系統延伸設定檔（**Devices**（裝置）> **Profiles & Resources**（設定檔與資源）> **Profiles**（設定檔））。

STEP 2 | 新增系統延伸。

1. 選取 **System Extensions**（系統延伸）。
2. 輸入 GlobalProtect 應用程式使用的團隊識別碼 (**PXPZ95SK77**)。
3. 輸入搭售包識別碼 (**com.paloaltonetworks.GlobalProtect.client.extension**)



4. 按一下 **Save and Publish**（儲存並發佈）以儲存變更。

透過其他協力廠商 MDM 管理 GlobalProtect 應用程式

若您未使用符合資格的協力廠商 MDM 廠商，您可使用其他協力廠商 MDM 系統部署並管理 GlobalProtect 應用程式：

- 為 iOS 設定 GlobalProtect 應用程式
  - 範例：GlobalProtect iOS 應用程式裝置層次 VPN 組態
  - 範例：GlobalProtect iOS 應用程式應用程式層次 VPN 組態
- 為 Android 設定 GlobalProtect 應用程式
  - 範例：設定 VPN 組態
  - 範例：移除 VPN 組態

為 *iOS* 設定 *GlobalProtect* 應用程式

儘管協力廠商 MDM 系統可讓您推送允許存取公司資源的設定，並提供用來強制執行端點限制的機制，但它無法保護行動端點與它連線的服務之間的連線安全。若要讓應用程式建立安全連線，您必須在端點上啟用 VPN 支援。

下列表格說明了您可以透過協力廠商 MDM 系統設定的典型設定：

setting	說明	值
連線類型	原則啟用的連線類型。	自訂 `SSL`
識別碼	反向 DNS 格式內自訂 SSL VPN 的識別碼。	`com.paloaltonetworks.globalprotect.vpn`
伺服器	GlobalProtect 入口網站的主機名稱或 IP 位址。	`<hostname or IP address>` 例如：`gp.paloaltonetworks.com`
帳戶	驗證連線的使用者帳戶。	`<username>`

setting	說明	值
使用者驗證	連線驗證類型。	憑證 | 密碼
認證	（僅限憑證使用者驗證）驗證連線用認證。	**<credential>** 例如：**clientcredial.p12**
視需要啟用 VPN	（選用）建立連線和需求操作的網域和主機名稱： • 始終建立連線 • 從不建立連線 • 根據需要建立連線	**<domain and hostname and the on-demand action>** 例如： gp.acme.com; 從不建立

範例：GlobalProtect iOS 應用程式裝置層次 VPN 組態

下列範例展示了包含 VPN 裝載的 XML 組態，您可用於確認 iOS GlobalProtect 應用程式的裝置等級 VPN 組態。

```
<?xml version="1.0"
encoding="UTF-8"?> <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
 "http://www.apple.com/DTDs/PropertyList-1.0.dtd"> <plist version="1.0">
 <dict> <key>PayloadContent</key> <array> <dict> <key>PayloadDescription</
key> <string>Configures VPN settings, including authentication.</
string><key>PayloadDisplayName</key> <string>VPN (Sample Device Level
 VPN)</string> <key>PayloadIdentifier</key> <string>Sample Device Level
 VPN.vpn</string> <key>PayloadOrganization</key> <string>Palo Alto Networks</
string> <key>PayloadType</key> <string>com.apple.vpn.managed</string>
 <key>PayloadVersion</key> <integer>1</integer> <key>PayloadUUID</key>
 <string>5436fc94-205f-7c59-0000-011d</string> <key>UserDefinedName</
key> <string>Sample Device Level VPN</string> <key>Proxies</key>
 <dict/> <key>VPNType</key> <string>VPN</string> <key>VPNSubType</key>
 <string>com.paloaltonetworks.GlobalProtect.vpnplugin</string> <key>IPv4</key>
 <dict> <key>OverridePrimary</key> <integer>0</integer> </dict> <key>VPN</
key> <dict> <key>RemoteAddress</key> <string>cademogp.paloaltonetworks.com</
string> <key>AuthName</key> <string></string> <key>DisconnectOnIdle</key>
 <integer>0</integer> <key>OnDemandEnabled</key> <integer>1</integer>
 <key>OnDemandRules</key> <array> <dict> <key>Action</key> <string>Connect</
string> </dict> </array> <key>AuthenticationMethod</key> <string>Password</
string> </dict> <key>VendorConfig</key> <dict> <key>AllowPortalProfile</
key> <integer>0</integer> <key>FromAspen</key> <integer>1</integer>
 </dict> </dict> </array> <key>PayloadDisplayName</key> <string>Sample
 Device Level VPN</string> <key>PayloadOrganization</key> <string>Palo
 Alto Networks</string> <key>PayloadDescription</key> <string>Profile
 Description</string> <key>PayloadIdentifier</key> <string>Sample Device
 Level VPN</string> <key>PayloadType</key> <string>Configuration</string>
 <key>PayloadVersion</key> <integer>1</integer> <key>PayloadUUID</key>
 <string>5436fc94-205f-7c59-0000-011c</string> <key>PayloadRemovalDisallowed</
key> <false/> </dict> </plist>
```

範例：GlobalProtect iOS 應用程式應用程式層次 VPN 組態

下列範例展示了包含 VPN 裝載的 XML 組態，您可用於確認 iOS GlobalProtect 應用程式的應用程式等級 VPN 組態。

```
<?xml version="1.0"
```

```
encoding="UTF-8"?> <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
 "http://www.apple.com/DTDs/PropertyList-1.0.dtd"> <plist version="1.0">
 <dict> <key>PayloadContent</key> <array> <dict> <key>PayloadDescription</
key> <string>Configures VPN settings, including authentication.</
string><key>PayloadDisplayName</key> <string>VPN (Sample App Level VPN)</
string> <key>PayloadIdentifier</key> <string>Sample App Level VPN.vpn</
string> <key>PayloadOrganization</key> <string>Palo Alto Networks</
string> <key>PayloadType</key> <string>com.apple.vpn.managed.applayer</
string> <key>PayloadVersion</key> <integer>1</integer> <key>VPNUUID</key>
 <string>cGFuU2FtcGxlIEFwcCBMZXZlbCBWUE52cG5TYW1wbGUgQXBwIExldmVsIFZQTg==</
string> <key>SafariDomains</key> <array> <string>*.paloaltonetworks.com</
string> </array> <key>PayloadUUID</key> <string>54370008-205f-7c59-0000-01a1</
string> <key>UserDefinedName</key> <string>Sample App Level VPN</string>
 <key>Proxies</key> <dict/> <key>VPNType</key> <string>VPN</string>
 <key>VPNSubType</key> <string>com.paloaltonetworks.GlobalProtect.vpnplugin</
string> <key>IPv4</key> <dict> <key>OverridePrimary</key> <integer>0</
integer> </dict> <key>VPN</key> <dict> <key>RemoteAddress</key>
 <string>cademogp.paloaltonetworks.com</string> <key>AuthName</key>
 <string></string> <key>OnDemandMatchAppEnabled</key> <integer>1</integer>
 <key>OnDemandEnabled</key> <integer>1</integer> <key>DisconnectOnIdle</key>
 <integer>0</integer> <key>AuthenticationMethod</key> <string>Password</
string> </dict> <key>VendorConfig</key> <dict> <key>OnlyAppLevel</
key> <integer>1</integer> <key>AllowPortalProfile</key> <integer>0</
integer> <key>FromAspen</key> <integer>1</integer> </dict> </dict> </
array> <key>PayloadDisplayName</key> <string>Sample App Level VPN</
string> <key>PayloadOrganization</key> <string>Palo Alto Networks</
string> <key>PayloadDescription</key> <string>Profile Description</
string> <key>PayloadIdentifier</key> <string>Sample App Level
 VPN</string> <key>PayloadType</key> <string>Configuration</string>
 <key>PayloadVersion</key> <integer>1</integer> <key>PayloadUUID</key>
 <string>5436fc94-205f-7c59-0000-011c</string> <key>PayloadRemovalDisallowed</
key> <false/> </dict> </plist>
```

為 *Android* 設定 *GlobalProtect* 應用程式

您可以在來自任意協力廠商行動裝置管理 (MDM) 的 Android For Work 端點上部署和設定 GlobalProtect 應用程式，該 MDM 系統支援 Android For Work 應用程式資料限制。

在 Android 端點上，流量根據 GlobalProtect 閘道上的存取路由，經過 VPN 通道路由傳送。從管理 Android for Work 端點的協力廠商 MDM，您可以進一步透過 VPN 通道精簡路由傳送的流量。

在端點由企業擁有的情況下，端點擁有者管理整個端點，包括該端點上安裝的所有應用程式。依預設，所有安裝的應用程式根據閘道上定義的存取路由，經過 VPN 通道傳送流量。

在自帶裝置 (BYOD) 的情況下，端點非企業擁有，並使用工作設定檔來區分商業和個人應用程式。依預設，僅工作設定檔內被管理的應用程式根據閘道上定義的存取路由，經過 VPN 通道傳送流量。安裝在端點個人部分的應用程式不可通過 VPN 通道傳送流量，該 VPN 通道由工作設定檔內安裝的管理 GlobalProtect 應用程式設定。

要從較小的應用程式組路由傳送流量，您可以啟用 Per-App VPN 讓 GlobalProtect 僅路由傳送來自特定管理應用程式的流量。對於 Per-App VPN，您可以透過允許名單或封鎖名單的方法，指定特定管理應用程式經過 VPN 通道執行路由傳送。

作為 VPN 組態的一部分，您也可以指定使用者如何連線 VPN。當您設定連線方法為 **user-logon**（使用者登入）時，GlobalProtect 應用程式將自動建立連線。當您設定連線方法為 **on-demand**（根據需要）時，使用者必須手動啟動連線。

在 *MDM* 中定義的 *VPN* 連線方法會優先於在 *GlobalProtect* 入口網站組態中定義的連線方法。

自動移除 VPN 組態會恢復 GlobalProtect 應用程式至原始組態設定。

若要設定 Android 的 GlobalProtect 應用程式，設定下列 Android 應用程式限制。

金鑰	值類型	說明	範例
入口網站	字串	入口網站的 IP 位址或完全合格的網域名稱 (FQDN)。	**10.1.8.190**
使用者名稱	字串	使用者的使用者名稱。	**john**
密碼	字串	使用者的密碼。	**Passwd!234**
mobile_id	字串	在協力廠商 MDM 服務中設定的行動 ID 可唯一地識別行動裝置。GlobalProtect 使用此行動 ID 擷取裝置資訊。	**5188a8193be43f42d332dde5cb2c941e**
憑證	字串 (in Base64)	用戶端憑證用於驗證代理程式和入口網站。	**DAFDSaweEWQ23wDSAFD....**
client_certificate_passphrase	字串	與用戶端憑證相關聯的金鑰。	**PA$$W0RD$123**
app_list	字串	Per-App VPN 的組態。以允許清單或封鎖清單開始字串，後接應用程式名稱，並用分號分隔。允許清單指定使用 VPN 通道進行網路通訊的應用程式。其他未在允許清單內的應用程式的網路流量，或明示位於封鎖清單內的部分，不經過 VPN 通道。	允許清單 | 封鎖清單：**com.google.calendar; com.android.email; com.android.chrome**
connect_method	字串	使用者登入使用其 windows 認證將使用者自動連線至 GlobalProtect 入口網站或依需求將使用者手動連線至閘道。	使用者登入 | 視需要
remove_vpn_config_via_restriction	布林值	永久移除所有 GlobalProtect VPN 組態資訊。	真 | 假

範例：設定 **VPN** 組態

```
private static String RESTRICTION_PORTAL = "portal"; private
 static String RESTRICTION_USERNAME = "username"; private static
 String RESTRICTION_PASSWORD = "password"; private static String
 RESTRICTION_CONNECT_METHOD = "connect_method"; private static String
 RESTRICTION_CLIENT_CERTIFICATE = "client_certificate"; private static String
 RESTRICTION_CLIENT_CERTIFICATE_PASSPHRASE = "client_certificate_passphrase";
 private static String RESTRICTION_APP_LIST = "app_list"; private static
 String RESTRICTION_REMOVE_CONFIG = "remove_vpn_config_via_restriction";
 Bundle config = new Bundle(); config.putString(RESTRICTION_PORTAL,
 "192.168.1.1"); config.putString(RESTRICTION_USERNAME,
 "john"); config.putString(RESTRICTION_PASSWORD, "Passwd!234");
```

```
config.putString(RESTRICTION_CONNECT_METHOD, "user-logon");
config.putString(RESTRICTION_CLIENT_CERTIFICATE, "DAFDSaweEWQ23wDSAFD....");
config.putString(RESTRICTION_CLIENT_CERTIFICATE_PASSPHRASE,
"PA$$W0RD$123"); config.putString(RESTRICTION_APP_LIST, "allow
list:com.android.chrome;com.android.calendar"); DevicePolicyManager dpm
= (DevicePolicyManager) getSystemService(Context.DEVICE_POLICY_SERVICE);
dpm.setApplicationRestrictions(EnforcerDeviceAdminReceiver.getComponentName(this),
"com.paloaltonetworks.globalprotect", config);
```

範例：移除 VPN 組態

```
Bundle config = new Bundle(); config.putBoolean(RESTRICTION_REMOVE_CONFIG,
 true ); DevicePolicyManager dpm = (DevicePolicyManager)
 getSystemService(Context.DEVICE_POLICY_SERVICE);
 dpm.setApplicationRestrictions(EnforcerDeviceAdminReceiver.
 getComponentName(this),"com.paloaltonetworks.globalprotect", config);
```

適用于 *IoT* 裝置的 *GlobalProtect*

藉助適用于 IoT 的 GlobalProtect，您可以保護來自 IoT 裝置的流量，並將安全性原則執行延伸至 IoT 裝置。設定適用于 IoT 的 GlobalProtect 後，GlobalProtect 應用程式會使用用戶端憑證及使用者名稱和密碼（選用）對 GlobalProtect 入口網站和閘道進行驗證。成功驗證後，GlobalProtect 應用程式將建立 IPSec 通道。如果使用 IPSec 的連線不成功，您可以設定 GlobalProtect 應用程式以回復到 SSL 通道。請參閱《Palo Alto Networks 相容性矩陣》，取得 IoT 裝置 OS 支援的功能清單。

> 適用于 IoT 的 GlobalProtect 的要求：
> 為 IoT 裝置設定 GlobalProtect 入口網站與閘道
> 在 Android 裝置上安裝適用于 IoT 的 GlobalProtect
> 在 Raspbian 裝置上安裝適用于 IoT 的 GlobalProtect
> 在 Ubuntu 裝置上安裝適用于 IoT 的 GlobalProtect
> 在 Windows 裝置上安裝適用于 IoT 的 GlobalProtect

適用于 IoT 的 GlobalProtect 的要求：

適用于 IoT 的 GlobalProtect 具有下列要求：

- 訂閱 Prisma Access 或 GlobalProtect
- 防火牆執行 PAN-OS 9.1（立即升級）
- 執行下列作業系統：
  - Android
  - Raspbian
  - Ubuntu
  - Windows IoT 企業版
- 128MB RAM
- 4GB 存儲空間
- x86 與 ARMv7 或 ARMv5 processor處理器
- 使用 CLI 或 WebDM 中的 snap 應用程式包進行安裝

為 IoT 裝置設定 GlobalProtect 入口網站與閘道

STEP 1 | 檢閱 適用于 IoT 的 GlobalProtect 的要求：。

STEP 2 | 設定 GlobalProtect 閘道以支援適用于 IoT 的 GlobalProtect 應用程式。

1. 完成設定 GlobalProtect 閘道的必要工作。。
2. 為支援適用于 IoT 的 GlobalProtect 應用程式的每個閘道安裝 GlobalProtect 訂閱。若您使用 Prisma Access，則無需 GlobalProtect 訂閱。
3. 為 IoT 裝置自訂閘道組態：

   設定閘道時，可指定專門用於 IoT 的用戶端驗證設定。例如，您可設定 Windows 與 macOS 端點，以使用雙因素驗證並要求 IoT 裝置使用基於憑證的驗證。

   您還可為 IoT 裝置設定支援的網路與用戶端設定（如特定 IP 集區、存取路和分割通道）。

   1. 選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道），然後選取或 **Add**（新增）閘道組態。
   2. 為 IoT 裝置新增用戶端驗證組態：
      1. 選取 **Authentication**（驗證）並 **Add**（新增）用戶端驗證組態。
      2. 輸入 **Name**（名稱）以標識用戶端驗證組態，將 **OS**（作業系統）設為 **IoT**，指定用於在此閘道上進行使用者驗證的 **Authentication Profile**（驗證設定檔）。選擇啟用用戶端憑證驗證的設定檔。
      3. 按一下 **OK**（確定）。
   3. 若要設定僅適用于 IoT 端點的特定用戶端設定，請設定新的用戶端設定組態：
      1. 選取 **Agent**（代理程式）並 **Add**（新增）用戶端設定組態。
      2. 根據需要設定用戶端驗證設定。
      3. 選取 **User/User Group**（使用者/使用者群組），然後 **Add**（新增）作業系統並選取 **IoT**。
      4. 按一下 **OK**（確定）。
   4. 按一下 **OK**（確定）。
   5. **Commit**（提交）組態。

STEP 3 | 設定入口網站以支援適用于 IoT 裝置的 GlobalProtect 應用程式。

若要支援 IoT 裝置，您必須設定一個或多個 GlobalProtect 應用程式可以連線至的閘道，然後設定入口網站與應用程式設定。入口網站可以傳送組態資訊及關於此應用程式可用閘道的資訊。收到來自 GlobalProtect 入口網站的組態后，應用程式會發現用戶端組態中列出的閘道並選取最佳閘道。按照下列工作流程設定 GlobalProtect 入口網站以支援適用于 IoT 裝置的 GlobalProtect 應用程式。

1. 若您尚未完成設定 GlobalProtect 入口網站的必要工作，請先完成。
2. 定義 IoT 裝置的用戶端設定以對入口網站進行驗證。
   1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後選取入口網站組態。
   2. 設定使用者存取入口網站時，適用 IoT 裝置的用戶端驗證設定：
      1. 選取 **Authentication**（驗證），然後 **Add**（新增）用戶端驗證組態。
      2. 輸入 **Name**（名稱）以標識用戶端驗證組態，將 **OS**（作業系統）設為 **IoT**，指定用於在此入口網站上進行使用者驗證的 Authentication Profile（驗證設定檔）。選擇啟用用戶端憑證驗證的設定檔。
3. 自訂 IoT 裝置的代理程式組態。

修改現有組態還是建立新組態取決于您的環境。例如，如果您使用的是作業系統特定的閘道或想要收集特定于 IoT 裝置的主機資訊，則可以考慮建立親的代理程式組態。

有關支援功能的資訊，請參閱《Palo Alto Networks 相容性矩陣》，取得 IoT 裝置作業系統支援的功能清單。

1. 定義 GlobalProtect 代理程式組態：
2. 選取 **Agent**（代理程式），然後選取現有的或 **Add**（新增）入口網站代理程式組態。
3. 為 IoT 裝置設定驗證設定。
4. 選取 **User/User Group**（使用者/使用者群組），然後新增 **OS**（作業系統）並選取 **IoT**。
5. 指定使用此組態的使用者可以連線的外部閘道。
6. （選用）選取應用程式並自訂適用于 IoT 的 GlobalProtect 應用程式的適用入口網站設定。GlobalProtect 應用程式將捨弃任何不適用于 IoT 的設定。如需作業系統支援的功能清單，請參閱《Palo Alto Networks 相容性矩陣》，取得 IoT 裝置作業系統支援的功能清單。
7. 按兩下 **OK**（確定）。
8. **Commit**（提交）組態。

4. 在 IoT 裝置上執行原則（**Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件））。

   您現在可以使用特定于 IoT 裝置的主機資訊建立 HIP 物件，並將其用於任何 HIP 設定檔中的比對條件。然後您可使用 HIP 設定檔作為原則規則中的比對條件，以執行相應的安全性原則。

   1. 選取 **General**（一般）> **Host Info**（主機資訊）> **OS**（作業系統）。
   2. 選取 **Contains**（包含）> **IoT**。
   3. 按一下 **OK**（確定）。
   4. 根據需要建立其他 HIP 物件。
   5. 設定以 HIP 為基礎的原則強制執行。

STEP 4 | 安裝並設定適用於 IoT 的 GlobalProtect 應用程式。

使用 IoT 裝置作業系統的隨附說明。

- 在 Android 裝置上安裝適用于 IoT 的 GlobalProtect
- 在 Raspbian 裝置上安裝適用于 IoT 的 GlobalProtect
- 在 Ubuntu 裝置上安裝適用于 IoT 的 GlobalProtect
- 在 Windows 裝置上安裝適用于 IoT 的 GlobalProtect

在 Android 裝置上安裝適用于 IoT 的 GlobalProtect

若要在 Android 裝置上使用適用于 IoT 的 GlobalProtect，您必須將應用程式與 GlobalProtect 組態作為系統應用程式建立到 Android 作業系統映像中。若要讓 GlobalProtect 在無周邊模式中執行，您必須使用 GlobalProtect 應用程式包部署預先設定檔案。

STEP 1 | 在 Android OS 映像中新增 GlobalProtect.apk 作為預建系統應用程式。

1. 從 Support Site（支援站點），選取 **Updates**（更新）> **Software Updates**（軟體更新），然後下載 GlobalProtect APK。
2. 將 `android_src_tree_root/packages/app/` 目錄中的 APK 檔案解碼。

   解碼器將應用程式解壓縮到 GlobalProtect 資料夾中。
3. 在 GlobalProtect 資料夾中，建立 `Android.mk` 檔案。此檔案定義了編碼器將用於建立系統的來源與共用庫。

   編輯檔案以包含：

```
LOCAL_PATH := $(call my-dir) include $(CLEAR_VARS) LOCAL_MODULE_TAGS :=
 optional LOCAL_MODULE := GlobalProtect LOCAL_SRC_FILES :=
 $(LOCAL_MODULE).apk LOCAL_MODULE_CLASS := APPS LOCAL_MODULE_SUFFIX :=
 $(COMMON_ANDROID_PACKAGE_SUFFIX) LOCAL_CERTIFICATE := PRESIGNED include
 $(BUILD_PREBUILT)
```

4. 對於 `android_src_tree_root/vendor/` 中的任何其他 MK 檔案，請新增以下行：

```
PRODUCT_PACKAGES += GlobalProtect
```

5. 根據 IoT 裝置支援的 CPU 架構，新增 libgpjni.so 至 `/system/lib` 或 `/system/lib64`。在 apktool 將 GlobalProtect.apk 解碼後，可從 lib 目錄擷取 libgpjni.so 檔案。

STEP 2 | 修改 Android Framework 原始碼以對 VPN 連線的權限請求彈出式視窗預先授權。

編輯 `android_src_tree_root/frameworks/base/services/core/java/com/android/server/connectivity/Vpn.java` 檔案以包含下列代碼區段：

```
private boolean isVpnUserPreConsented(String packageName) { if
 (“com.paloaltonetworks.globalprotect”.equals(packageName)){ Log.v(TAG, "IoT,
 isVpnUserPreConsented always true"); return true; } AppOpsManager appOps
 = (AppOpsManager) mContext.getSystemService(Context.APP_OPS_SERVICE); //
 Verify that the caller matches the given package
 and has permission to activate VPNs. return
 appOps.noteOpNoThrow(AppOpsManager.OP_ACTIVATE_VPN,Binder.getCallingUid(),
 packageName) == AppOpsManager.MODE_ALLOWED; } }
```

STEP 3 | 自訂 Android 行為以在 Android 8.0 及更新版本的通知列中禁用 GlobalProtect 圖示。

編輯 `android_src_tree_root/frameworks/base/services/core/java/com/android/server/am/ActiveServices.java` 檔案以包含下列代碼區段。

```
if ( r.packageName.equals("com.paloaltonetworks.globalprotect") )
 { Slog.d(TAG, "not to show the foreground service running notification for
 IoT"); } else { r.postNotification(); }
```

STEP 4 | 設定您想為 Android IoT 裝置預先部署的 VPN 設定。

1. 以下列格式建立設定檔案 (`globalprotect.conf`) 并編輯 GlobalProtect 入口網站的 IP 位址及驗證設定：用戶名稱與密碼，或用戶端憑證路徑 (client-cert-path) 及密碼檔案 (client-cert-passphrase)。

   基於使用者名稱-密碼的驗證

   ```
   <?xml version="1.0" encoding="UTF-8"?> <GlobalProtect> <PanSetup>
    <Portal>192.168.1.23</Portal> </PanSetup> <Settings> <head-less>yes</
   head-less> <os-type>IoT</os-type> <username>user1</username>
    <password>mypassw0rd</password> <log-path-service>/home/gptest/Desktop/
   data/gps</log-path-service> <log-path-agent>/home/gptest/Desktop/data/
   gpadata</log-path-agent> </Settings> </GlobalProtect>
   ```

   基於用戶端-憑證的驗證

   ```
   <?xml version="1.0" encoding="UTF-8"?> <GlobalProtect> <PanSetup>
    <Portal>192.168.1.23</Portal> </PanSetup> <Settings> <head-less>yes</
   head-less> <os-type>IoT</os-type> <client-cert-path>/home/gptest/Desktop/
   data/pan_client_cert.pfx</client-cert-path> <client-cert-passphrase>/
   home/gptest/Desktop/data/pan_client_cert_passcode.dat</client-cert-
   passphrase> <username>user1</username> <password>paloalto</password> <log-
   path-service>/home/gptest/Desktop/data/gps</log-path-service> <log-path-
   agent>/home/gptest/Desktop/data/gpadata</log-path-agent> </Settings> </
   GlobalProtect>
   ```

2. 以 Base64 格式編碼 `globalprotect.conf` 檔案并將其儲存至 `android_src_tree_root/system/config/` 目錄。

   如果需要，您可以將檔案儲存至其他位置。但是，您必須在 `android_src_tree_root/assets/gp_conf_location.txt` 檔案中編輯此設定的位置。

STEP 5 | 建立 GlobalProtect APK 檔案。

STEP 6 | 簽署 GlobalProtect APK 檔案。

STEP 7 | 將新的 OS 推送至 Android 裝置，作為系統映像的一部份，然後將新的 OS 推送至 Android 裝置。

在 Raspbian 裝置上安裝適用于 IoT 的 GlobalProtect

若要在 Raspbian 裝置上安裝適用于 IoT 的 GlobalProtect，請完成以下步驟。

適用于 *Raspbian* 和 *Ubuntu IoT* 裝置的 *GlobalProtect* 僅支援 *Arm* 架構。

STEP 1 | 從 Support Site（支援站點），選取 **Updates**（更新）> **Software Updates**（軟體更新），然後下載適用于您 OS 的 GlobalProtect 包。

STEP 2 | 安裝適用於 IoT 的 GlobalProtect 應用程式。

在 IoT 裝置上，使用 **sudo dpkg -i GlobalProtect_deb_arm<*version*>.deb** 命令安裝此軟體。

```
sudo dpkg -i GlobalProtect_deb_arm-5.1.0.0-84.deb
```

之後若要解除安裝此軟體，則使用 ***sudo dpkg -P globalprotect*** 命令。

STEP 3 | 設定您想為 Raspbian IoT 裝置預先部署的 VPN 設定。

1. 在 `client-cert` 路徑中，以 pcks12 格式匯入憑證，并以 .pfx 為副檔名儲存檔案（例如 **pan_client_cert.pfx**）。
2. 在 `client-cert-passphrase` 路徑中，以 .dat 為副檔名儲存密碼檔案（例如 **pan_client_cert_passcode.dat**）
3. 在 `log-path-service` 路徑中，如果您沒有使用 PanGPS 的預設路徑（例如 `/opt/paloaltonetworks/globalprotect`），請確保 `log-setting` 路徑資料夾與 `opt/paloaltonetworks` 下的 globalprotect 資料夾具有相同權限。
4. 以下列格式建立 `/opt/paloaltonetworks/globalprotect/pangps.xml` 預先部署設定檔案并編輯 GlobalProtect 入口網站的 IP 位址及驗證設定：使用者名稱與密碼，或用戶端憑證路徑 (**client-cert-path**) 及密碼檔案 (**client-cert-passphrase**)。您也可指定用於儲存 GlobalProtect 服務的選用資料夾 (**log-path-service**) 及代理程式 (**log-path-agent**) 日誌。

```
<?xml version="1.0" encoding="UTF-8"?> <GlobalProtect> <PanSetup>
 <Portal>192.168.1.160</Portal> //預先部署的入口網站位址 </PanSetup> <PanGPS> </
PanGPS> <Settings> <portal-timeout>5</portal-timeout> <connect-timeout>5</
connect-timeout> <receive-timeout>30</receive-timeout> <os-type>IoT</
os-type> //預先部署的 IoT OS 類型。如果沒有此頁籤，GP 將自動偵測 OS 類型。<head-
less>yes</head-less> //預先部署的無頭模式 <username>abc</username> //選用預
先部署的使用者名稱 <password>xyz</password> //選用預先部署的密碼 <client-cert-
path>cli_cert_path</client-cert-path> //選用預先部署的用戶端憑證 (p12) 路
徑 <client-cert-passphrase>cli_cert_passphrase_path< /client-cert-
passphrase> //選用預先部署的用戶端憑證密碼檔案路徑 <log-path-service>/tmp/gps</
log-path-service> //選用預先部署的 PanGPS 日誌資料夾 <log-path-agent>/tmp/
gpa</log-path-agent> //選用預先部署的 PanGPA 和 globalprotect CLI 日誌資料夾 </
Settings> </GlobalProtect>
```

STEP 4 | 重新啟動 GlobalProtect 程序以使預先部署設定生效。

STEP 5 | 在您部署 IoT 裝置後，可以根據需要使用 **globalprotect collect-log** 命令收集日誌。

```
user@raspbianhost:~/Desktop/data$ globalprotect collect-log 支援檔案將儲存至 /
home/gptest/.GlobalProtect/GlobalProtectLogs.tgz
```

STEP 6 | （選用）如果驗證方法是使用者名稱/密碼與用戶端憑證驗證的組合，則確保用戶端憑證的 **CommonName** 與使用者名稱相符。

在 Ubuntu 裝置上安裝適用于 IoT 的 GlobalProtect

若要在 Ubuntu 裝置上安裝適用于 IoT 的 GlobalProtect，請完成以下步驟。

適用于 *Raspbian* 和 *Ubuntu IoT* 裝置的 *GlobalProtect* 僅支援 *Arm* 架構。

STEP 1 | 從 Support Site（支援站點），選取 **Updates**（更新）> **Software Updates**（軟體更新），然後下載適用于您 OS 的 GlobalProtect 包。

STEP 2 | 安裝適用於 IoT 的 GlobalProtect 應用程式。

在 IoT 裝置上，使用 **sudo dpkg -i GlobalProtect_deb-*<version>*.deb** 命令安裝此軟體。

```
user@linuxhost:~$ sudo dpkg -i GlobalProtect_deb-4.1.0.0-19.deb
```

之後若要解除安裝此軟體，則使用 ***sudo dpkg -P globalprotect*** 命令。

STEP 3 | 設定您想為 Ubuntu IoT 裝置預先部署的 VPN 設定。

1. 在 `client-cert` 路徑中，以 pcks12 格式匯入憑證，並以 .pfx 為副檔名儲存檔案（例如 **pan_client_cert.pfx**）。
2. 在 `client-cert-passphrase` 路徑中，以 .dat 為副檔名儲存密碼檔案（例如 **pan_client_cert_passcode.dat**）
3. 在 `log-path-service` 路徑中，如果您沒有使用 PanGPS 的預設路徑（例如 `/opt/paloaltonetworks/globalprotect`），請確保 `log-setting` 路徑資料夾與 `opt/paloaltonetworks` 下的 globalprotect 資料夾具有相同權限。
4. 以下列格式建立 `/opt/paloaltonetworks/globalprotect/pangps.xml` 預先部署設定檔案並編輯 GlobalProtect 入口網站的 IP 位址及驗證設定：用戶名稱與密碼，或用戶端憑證路徑 (**client-cert-path**) 及密碼檔案 (**client-cert-passphrase**)。您也可指定用於儲存 GlobalProtect 服務的選用資料夾 (**log-path-service**) 及代理程式 (**log-path-agent**) 日誌。

```
<?xml version="1.0" encoding="UTF-8"?> <GlobalProtect> <PanSetup>
 <Portal>192.168.1.160</Portal> //預先部署的入口網站位址 </PanSetup> <PanGPS> </
PanGPS> <Settings> <portal-timeout>5</portal-timeout> <connect-timeout>5</
connect-timeout> <receive-timeout>30</receive-timeout> <os-type>IoT</
os-type> //預先部署的 IoT OS 類型。如果沒有此頁籤，GP 將自動偵測 OS 類型。<head-
less>yes</head-less> //預先部署的無頭模式 <username>abc</username> //選用預
先部署的使用者名稱 <password>xyz</password> //選用預先部署的密碼 <client-cert-
path>cli_cert_path</client-cert-path> //選用預先部署的用戶端憑證 (p12) 路
徑 <client-cert-passphrase>cli_cert_passphrase_path< /client-cert-
passphrase> //選用預先部署的用戶端憑證密碼檔案路徑 <log-path-service>/tmp/gps</
log-path-service> //選用預先部署的 PanGPS 日誌資料夾 <log-path-agent>/tmp/
gpa</log-path-agent> //選用預先部署的 PanGPA 和 globalprotect CLI 日誌資料夾 </
Settings> </GlobalProtect>
```

STEP 4 | 重新啟動 GlobalProtect 程序以使預先部署設定生效。

STEP 5 | 在您部署 IoT 裝置後，可以根據需要使用 **globalprotect collect-log** 命令收集日誌。

```
user@linuxhost:~$ globalprotect collect-log 支援檔案將儲存至 /home/
gptest/.GlobalProtect/GlobalProtectLogs.tgz
```

STEP 6 | （選用）如果驗證方法是使用者名稱/密碼與用戶端憑證驗證的組合，則確保用戶端憑證的 **CommonName** 與使用者名稱相符。

在 Windows 裝置上安裝適用于 IoT 的 GlobalProtect

執行 Windows 10 IoT 的裝置可以使用 GlobalProtect 應用程式。利用您組織的散佈方法，例如 Microsoft 系統中心設定管理器 (SCCM)，在執行 Windows 10 IoT 企業版的 IoT 裝置上部署和安裝 GlobalProtect 應用程式。

GlobalProtect Windows IoT 部署支援基於憑證的驗證。您必須在本機機器存放區的所有 IoT 裝置上安裝用於進行驗證的憑證。如果 IoT 裝置有多個具有相同根 CA 的憑證，則 GlobalProtect 將使用 IoT 裝置的本機機器存放區中的第一個憑證進行驗證；確保您的憑證在裝置中的順序正確。

下列各節說明如何在執行 Windows IoT 的裝置上安裝 GlobalProtect 應用程式：

- 在 IoT 裝置上下載並安裝 MSIEXEC 檔案。
- 在 IoT 裝置上修改登錄機碼（隨選或一直開啟）
- 在 IoT 裝置上修改登錄機碼（一直開啟，預先登入）

在 IoT 裝置上下載並安裝 MSIEXEC 檔案。

您可下載並安裝 `msiexec.exe` 檔案至 IoT 裝置，為隨選連線方法或一直開啟連線方法安裝 GlobalProtect 應用程式。您將使用與在非 IoT 裝置上相同的方法來部署 msiexec.exe 檔案。

在 IoT 裝置上修改登錄機碼（隨選或一直開啟）

您必須將 OS 類型指定為 IoT，裝置類型指定為無周邊，及入口網站位址。您也可以指定使用者名稱與密碼（選用）。如果您未指定使用者名稱與密碼，則 GlobalProtect 會使用基於憑證的驗證。

您可對隨選連線方法或一直開啟連線方法使用下列安裝方法：

- 指定 OS 類型（必填）：

  登錄子機碼：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  名稱：os 類型

  類型：REG_SZ

  資料：IoT
- 指定無周邊 IoT 裝置（必填）：

  登錄子機碼：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  名稱：無周邊

  類型：REG_SZ

  資料：yes
- 指定入口網站位址（必填）：

  登錄子機碼：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  名稱：入口網站

  類型：REG_SZ

  資料：輸入 GlobalProtect 入口網站的 IP 位址或 FQDN。

- 指定使用者名稱（選用）：

  登錄子機碼：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  名稱：使用者名稱

  類型：REG_SZ

  資料：輸入用於 IoT 裝置的使用者名稱。
- 指定密碼（選用）：

  登錄子機碼：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  名稱：密碼

  類型：REG_SZ

  資料：輸入用於 IoT 裝置的密碼。

在 IoT 裝置上修改登錄機碼（一直開啟，預先登入）

您必須指定入口網站位址、預先登入逾時值及僅限服務值。您必須刪除 GlobalProtect 值以防止 IoT 裝置在系統重新啟動時自動啟動應用程式介面。預先登入 VPN 通道未與使用者名稱關聯，因為使用者尚未登入。

您可對預先登入（一直開啟）連線方法或一直開啟連線方法使用下列安裝方法：

- 指定入口網站位址（必填）：

  登錄子機碼：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  名稱：入口網站

  類型：REG_SZ

  資料：輸入 GlobalProtect 入口網站的 IP 位址或 FQDN。
- 指定預先登入值（必填）：

  登錄子機碼：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  名稱：預先登入

  類型：REG_SZ

  資料：1
- 指定僅限服務值（必填）：

  登錄子機碼：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  名稱：僅限服務

  類型：REG_SZ

  資料：yes
- 刪除 GlobalProtect 值（必填）：

  登錄子機碼：`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

  名稱：GlobalProtect

  類型：REG_SZ

主機資訊

雖然您的公司網路邊界可能有迫切的安全性需求，但您的網路真的只與存取該網路的端點一樣安全。隨著現今工作者的行動性越來越高，經常需要從各種場所（機場、咖啡廳、旅館）與各種端點（公司佈建裝置與個人裝置）存取公司資源，您必須以符合邏輯的方式將網路安全性擴展至您的端點，才能確保全面性、一致性的安全性強制執行。GlobalProtect™ 主機資訊設定檔 (HIP) 功能可讓您收集有關端點安全性狀態的資訊（例如是否已安裝最新安全性修補程式與防毒定義、是否已啟用磁碟加密、端點是否已遭 Jailbreak 或 Root 或是否正在執行您組織中所需要的特定軟體，而做出決定的基礎，是以允許還是拒絕存取以嚴格遵守您所定義之主機原則的特定主機為準。

以下幾節提供在原則強制執行中使用主機資訊的相關資訊。

> 關於主機資訊
> 設定以 HIP 為基礎的原則強制執行
> 從端點收集應用程式與處理資料
> 重新散佈 HIP 報告
> 封鎖設備存取
> 設定 Windows 的 User-ID 代理程式以收集主機資訊

關於主機資訊

GlobalProtect 應用程式的其中一項工作是收集關於其執行所在主機的資訊。然後應用程式會在成功連線時將此主機資訊交付至 GlobalProtect 閘道。閘道會將應用程式所交付的原始主機資訊與您已定義的任何 HIP 物件和 HIP 設定檔相比對。如果發現相符，它會在 HIP 比對日誌中產生項目。此外，如果在原則規則中發現 HIP 設定檔的相符項，則會強制執行對應的安全原則。

針對原則強制執行使用主機訊息設定檔會啟用精細安全性，其可確保在獲得允許存取您的網路資源之前，存取您的關鍵資源的遠端主機能夠受到適當維護並嚴格遵守您的安全性標準。例如，在允許存取最敏感的資料系統之前，您可能需要確定存取資料的主機是否已在其硬碟上啟用加密。如果端點系統已啟用加密，您可以建立僅允許存取應用程式的安全性規則來強制執行此原則。此外，針對不遵守此規則的端點，您可以建立通知訊息，警示使用者為什麼遭到拒絕存取並將使用者連結至檔案共用區，使用者可以在此存取遺失加密軟體的安裝程式（當然，為了允許使用者存取該檔案共用區，您必須建立對應的安全規則，來允許存取符合該特定 HIP 設定檔之主機的特定共用區）。

- GlobalProtect 應用程式收集的資料為何？
- 閘道如何使用主機資訊來強制執行原則？
- 使用者如何知道他們的系統是否相容？
- 我如何獲得端點狀態的可見度？

GlobalProtect 應用程式收集的資料為何？

依預設，GlobalProtect 應用程式會收集關於在端點上執行之一般使用者安全性套件的廠商特定資料（如 OPSWAT 全球合作項目所編輯）並將此資料報告給 GlobalProtect 閘道以供用於原則強制執行。

由於安全性軟體必須持續發展以確保一般使用者能夠受到保護，GlobalProtect 閘道授權也可讓您取得 GlobalProtect 資料檔案的動態更新，並針對每個套件提供最新的修補程式與軟體版本。

依預設，應用程式會收集關於下列資訊類別的資料，以協助識別主機的安全性狀態：

表 **8:** 表格：資料收集類別

類別	收集的資料
總言	關於主機本身的資訊，包括主機名稱、登入網域、作業系統、應用程式版本與電腦所屬的網域（針對 Windows 系統）。 對於 *Windows* 端點的網域，*GlobalProtect* 應用程式會收集為 `ComputerNameDnsDomain` 定義的網域，這是為本機電腦及與本機電腦關聯的叢集指派的 *DNS* 網域。這是在 *HIP* 比對日誌詳細資訊（*Monitor*（監控）> *Logs*（日誌）> *HIP Match*（*HIP* 比對））中為 *Windows* 端點的 *Domain*（網域）顯示的資料）。
行動裝置	行動裝置的相關資訊，包含裝置名稱、登入網域、作業系統、應用程式版本和關於裝置連線至的網路之資訊。此外，GlobalProtect 會收集裝置是否已遭 Root 或 Jailbreak 的資訊。 若要收集行動裝置屬性並在 *HIP* 強制性原則中使用它們的話，*GlobalProtect* 就需要一個 *MDM* 伺服器。*GlobalProtect* 目前支援 *HIP* 與 *AirWatch MDM* 伺服器的整合。

類別	收集的資料
	對於 AirWatch 所管理的裝置，GlobalProtect 應用程式所收集的主機資訊可以透過 AirWatch 服務所收集的額外資訊來補充。對於可從 AirWatch 擷取的屬性清單，請參閱設定 Windows 的 User-ID 代理程式以收集主機資訊。
修補程式管理	關於在主機上啟用與/或安裝之任何修補程式管理軟體及是否有任何遺失修補程式的資訊。 如果您要在 *HIP* 物件中為遺失修補程式設定 *Severity*（嚴重性）值作為比對條件（*Objects*（物件）> *GlobalProtect* > *HIP Objects*（*HIP* 物件）> *<hip-object>* > *Patch Management*（修補程式管理）> *Criteria*（準則）），請使用 *GlobalProtect* 嚴重性值和 *OPSWAT* 嚴重性評等之間的下列對應，以瞭解每個值表示的意思： • ***0***—低 • ***1***—中 • ***2***—重要 • ***3***—重要
防火牆	關於在主機上安裝與/或啟用之任何防火牆的資訊。
反惡意軟體	關於在端點上啟用與/或安裝之任何防毒或反間諜軟體、是否已啟用即時保護、病毒定義版本、上次掃描時間、廠商與產品名稱的資訊。 GlobalProtect 使用 OPSWAT 技術偵測和評估端點上的 協力廠商安全應用程式。透過整合 OPSWAT OESIS 架構，GlobalProtect 讓您可以評估端點的合規狀態。例如，您可以定義 HIP 物件和 HIP 設定檔，確認端點上特定廠商的防毒軟體版本，並確保具有最新的病毒定義檔案。 *OPSWAT* 無法在 *macOS* 端點上偵測 *Gatekeeper* 安全性功能的下列反惡意軟體資訊： • *Engine Version*（引擎版本） • *Definition Version*（定義版本） • *Date*（日期） • *Last Scanned*（上次掃描時間）
磁碟備份	關於是否已安裝磁碟備份軟體、上次備份時間，以及軟體的廠商與產品名稱的資訊。
磁碟加密	關於是否已安裝磁碟加密軟體、針對加密設定了哪些磁碟機與/或路徑，以及軟體的廠商與產品名稱的資訊。
資料遺失防範	關於是否安裝與/或啟用資料遺失防範 (DLP) 軟體以防止敏感公司資訊流出公司網路，或儲存在可能不安全裝置上的資訊。此資訊僅會從 Windows 端點收集。
憑證	關於端點上安裝的機器憑證之資訊。
自訂檢查	關於是否存在特定登錄機碼（僅限 Windows）、屬性清單 (plists)（僅限 macOS）、OR 作業系統程序及使用者空間應用程式程序的資訊。

您可以將某些資訊類別排除於在某些主機上收集之外，以節省 CPU 循環與改善回應時間。為此，在入口網站建立代理程式組態，然後排除您沒有興趣的類別（**Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> <*portal-config*> > **Agent**（代理程式）> <*agent-config*> > **Data Collection**（資料收集））。例如，如果不打算根據端點是否執行磁碟備份軟體來建立原則，您可以排除該類別以防止應用程式收集有關磁碟備份的任何資訊。

您還可以將資訊排除於在個人端點上收集之外，以提供使用者隱私。例如，您可以排除安裝在端點上未由協力廠商行動裝置管理員管理的應用程式清單。

閘道如何使用主機資訊來強制執行原則？

儘管應用程式會取得相關資訊，以說明會從下載自入口網站的用戶端組態處收集哪些資訊，您仍可在閘道上建立 HIP 物件與 HIP 設定檔，來定義您想要監控與/或用於強制執行原則的主機屬性有哪些：

- **HIP** 物件—比對準則，可用於篩選掉您針對應用程式所報告的原始資料強制執行原則時，所慣用的主機資訊。例如，雖然原始主機資料可能包含端點上安裝的數個防毒套件的相關資訊，但您可能只會在組織內使用一種您慣用的特殊應用程式。在此情況中，您將建立 HIP 物件以符合您想要強制施行的特定應用程式。

  若要判斷需要的 HIP 物件，最好的方法是決定要如何使用收集的主機資訊來強制執行原則。請注意，HIP 物件本身只會建立封鎖，讓您建立在安全原則中使用的 HIP 設定檔。因此，您可能需要維持單純的物件，符合某種情況，例如，呈現特殊類型的必要軟體、特定網域中的成員資格，或呈現特定的端點作業系統。利用這種做法，您可以靈活建立極精細的（且極強大的）HIP 擴張原則。
- **HIP** 設定檔—一起評估的 HIP 物件集合，適用於監控或安全原則強化。建立 HIP 設定檔時，您可以使用布林邏輯來結合先前建立的 HIP 物件（以及其他 HIP 設定檔），如此在針對導出的 HIP 設定檔評估流量時，就會得到符合或不符合結果。如果有符合項，則將執行對應的原則規則。如果沒有符合項，則針對下一個規則，及使用任何其他原則比對準則來評估流量。

與流量日誌（僅在有原則相符時才會建立日誌項目）不同，每當應用程式所提交的原始資料與您所定義的 HIP 物件與/或 HIP 設定檔相符時，HIP 比對日誌就會產生項目。久而久之（在將 HIP 設定檔附加至安全原則之前），這便會使 HIP 比對日誌成為監控網路中端點狀態的良好資源，以協助您精準決定需要強制執行的原則有哪些。請參閱設定以 HIP 為基礎的原則強制執行，以取得如何建立 HIP 物件與 HIP 設定檔，及將其作為原則比對準則的詳細資訊。

使用者如何知道他們的系統是否相容？

依預設，不會為一般使用者提供有關原則決定（作為啟用 HIP 之安全性規則的強制執行結果）的任何資訊。不過，當特定 HIP 設定檔相符與/或不相符時，您可以設定要顯示的 HIP 通知訊息來啟用此功能。

至於決定何時顯示訊息（即，當使用者的設定與原則中的 HIP 設定檔相符或不相符時是否顯示訊息），主要視您的原則與 HIP 相符（或不相符）對使用者有何意義而定。也就是說，相符是否表示使用者獲授與網路資源的完整存取權？或者表示由於不相容問題而限制其存取權？

舉例而言，請考量下列情況：

- 如果未安裝所需的公司防毒與反間諜軟體套件，您可以建立相符的 HIP 設定檔。在此情況下，您可能需要為比對 HIP 設定檔的使用者建立 HIP 通知訊息，告訴他們需要安裝軟體（並選擇性地提供使用者可以存取對應軟體安裝程式之檔案共用區的連結）。
- 如果已安裝那些相同的應用程式，您可以建立相符的 HIP 設定檔。在這種情況下，您可能需要為與設定檔不相符的使用者建立訊息，並指示這些使用者前往安裝套件的位置。

請參閱設定以 HIP 為基礎的原則強制執行，以取得如何建立 HIP 物件與 HIP 設定檔，及用於定義 HIP 通知訊息的詳細資訊。

我如何獲得端點狀態的可見度？

只要端點連線到 GlobalProtect，應用程式就會對閘道呈現其 HIP 資料。接著閘道會使用此資料來判定主機會比對哪些 HIP 物件和/或 HIP 設定檔。閘道會針對每個符合的項目產生 HIP 比對日誌項目。與流量日誌（僅在有原則相符時才會建立日誌項目）不同，每當應用程式所提交的原始資料與您所定義的 HIP 物件與/或 HIP 設定檔相符時，HIP 比對日誌就會產生項目。久而久之（在將 HIP 設定檔附加至安全原則之前），這便會使 HIP 比對日誌成為監控網路中端點狀態的良好資源，以協助您精準決定需要強制執行的原則有哪些。

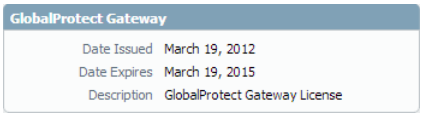
由於 HIP 比對日誌只有在主機狀態符合您所建立的 HIP 物件時才會產生，因此為了獲得端點狀態的完整可見度，您必須建立多個 HIP 物件，以記錄符合特定狀態之端點的 HIP 比對符合項目（為了強制執行安全性原則），及記錄不符合之端點的 HIP 比對符合項目（為了可見度）。例如，假設您想要防止沒有安裝防毒或反間諜軟體的端點連線到網路。在此情況中，您將建立一個符合已安裝特定防毒或反間諜軟體之主機的物件。透過將此物件包含在 HIP 設定檔中，並將它附加到允許從您的 VPN 區域存取的安全性原則規則，您可以確保只有受到防毒或反間諜軟體保護的主機能夠連線。

在此範例中，您將無法檢視哪些端點不符合 HIP 比對日誌中的此需求。如果您要檢視日誌中未安裝防毒或反間諜軟體的端點，讓您可以追蹤這些使用者，您也可以建立一個 HIP 物件，使其符合防毒或反間諜軟體未安裝的條件。由於此物件僅供日誌記錄之用，因此不需要將它新增至 HIP 設定檔或附加到安全性原則規則。

設定以 HIP 為基礎的原則強制執行

若要在原則強制執行中啟用主機資訊的使用，您必須完成下列步驟。如需 HIP 功能的詳細資訊，請參閱關於主機資訊。

STEP 1 | 確認 HIP 檢查的授權正確。

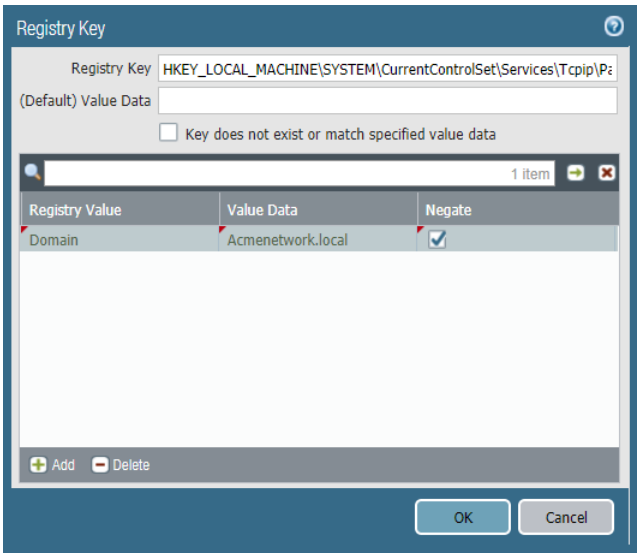


若要使用 HIP 功能，您必須購買 GlobalProtect 使用授權，並在將執行 HIP 檢查的每個閘道上安裝 GlobalProtect 使用授權。若要確認每個入口網站與閘道上的授權狀態，請選取 **Device**（裝置）> **Licenses**（授權）。

如果您沒有所需授權，請聯絡 Palo Alto Networks 銷售工程師或零售商。如需授權的詳細資訊，請參閱關於 GlobalProtect 授權。

STEP 2 | （選用）定義應用程式所要收集的任何自訂主機資訊。例如，如果廠商和/或產品清單不含建立 HIP 物件所需要的任何應用程式，您可以建立自訂檢查以讓您判定該應用程式是否已安裝（具有對應的登錄或 Plist 機碼）或正在執行（具有對應的執行中程序）。

步驟 *2* 與 *3* 會假設您已設定 *GlobalProtect* 入口網站。如果您尚未設定入口網站，請參閱設定 GlobalProtect 入口網站存取權以取得指示。



1. 在代管 GlobalProtect 入口網站的防火牆上，選取**Network**（網路）> **GlobalProtect** > **Portals**（入口網站）。
2. 選取您要修改的入口網站組態。
3. 在 **Agent**（代理程式）頁籤上，選取您要新增自訂 HIP 檢查的目標代理程式組態，或 **Add**（新增）新代理程式組態。
4. 選取 **Data Collection**（資料收集），然後啟用選項以 **Collect HIP Data**（收集 **HIP** 資料）。
5. 在 **Custom Checks**（自訂檢查）下，定義您要從執行此代理程式組態之主機收集的下列資料：
   - 若要收集有關特定登錄機碼的資訊：在 **Windows** 頁籤上，**Add**（新增）**Registry Key**（登錄機碼）名稱，以收集 **Registry Key**（登錄機碼）區域內的資料。若要限制特定 **Registry Value**（登錄值）的資料收集，**Add**（新增）然後定義特定登錄值。按一下 **OK**（確定）以儲存設定。

- 若要收集關於執行中處理程序的資訊：選取適當頁籤（**Windows** 或 **Mac**）然後 **Add**（新增）程序至 **Process List**（處理程序清單）。輸入您想讓應用程式收集相關資訊的處理程序名稱。
- 若要收集有關特定屬性清單的資訊：在 **Mac** 頁籤上，**Add**（新增）**Plist** 以收集資料。若要限制特定索引鍵值的資料收集，**Add**（新增）**Key**（索引鍵）值。按一下 **OK**（確定）以儲存設定。

6. 如果這是新代理程式組態，請視需要定義 GlobalProtect 代理程式組態。
7. 按一下 **OK**（確定）來儲存組態。
8. **Commit**（提交）變更。

STEP 3 | （選用）從收集中排除類別。

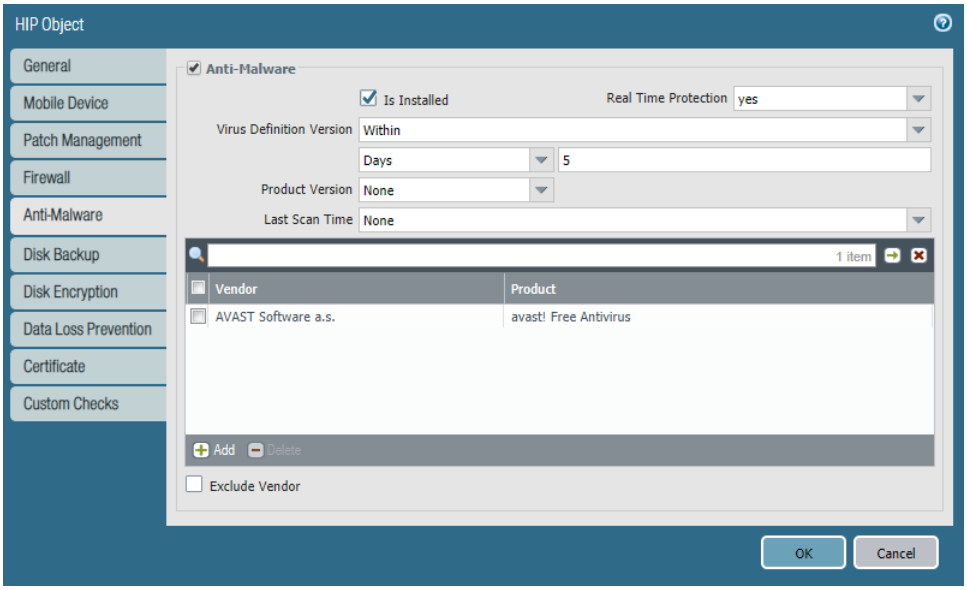
1. 在代管 GlobalProtect 入口網站的防火牆上，選取**Network**（網路）> **GlobalProtect** > **Portals**（入口網站）。
2. 選取您要修改的入口網站組態。
3. 在 **Agent**（代理程式）頁籤上，選取您要從中排除類別的代理程式組態，或按一下 **Add**（新增）一個新的。
4. 選取 **Data Collection**（資料收集），然後確認已啟用 **Collect HIP Data**（收集 **HIP** 資料）。
5. 在 **Exclude Categories**（排除類別）下，**Add**（新增）一個新的排除類別。
6. 從下拉式清單中選取要排除的 **Category**（類別）。
7. （選用）如果您要從所選類別中排除特定廠商與/或產品，而不是排除整個類別，請按一下 **Add**（新增）。在編輯廠商對話方塊中，選取您要排除的 **Vendor**（廠商），然後按一下 **Add**（新增）以排除該廠商的特定產品。完成定義該廠商時，請按一下 **OK**（確定）。您可以將多個廠商與產品新增至排除清單。
8. 針對您要排除的每個類別，重複步驟 5-7。
9. 如果這是新代理程式組態，請視需要定義 GlobalProtect 代理程式組態。
10. 按一下 **OK**（確定）來儲存組態。
11. **Commit**（提交）變更。

STEP 4 | 建立 HIP 物件以篩選應用程式所收集的原始主機資料。

若要判斷需要的 HIP 物件，最好的方法是決定要如何使用收集的主機資訊來強制執行原則。請注意，HIP 物件本身只會建立封鎖，讓您建立在安全原則中使用的 HIP 設定檔。因此，您可能需要維持單純的物件，符合某個項目，例如，呈現特殊類型的必要軟體、特定網域中的成員資格，或呈現特定的作業系統。利用這種做法，您可以靈活建立極精細的（且極強大的）HIP 擴張原則。

如需有關特定 *HIP* 類別或欄位的詳細資訊，請參閱線上說明。

1. 在代管 GlobalProtect 閘道的防火牆上（如果您打算在多個閘道之間共享 HIP 物件，則在 Panorama 上），選取 **Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件），然後 **Add**（新增）新的 HIP 物件。
2. 輸入物件的 **Name**（名稱）。
3. 針對您想要比對的主機資訊類別選取所對應的頁籤，並選取核取方塊來啟用要與類別比對的物件。例如，若要建立尋找有關防毒或反間諜軟體資訊的物件，請選取 **Anti-Malware**（防惡意軟體）頁籤，然後選取 **Anti-Malware**（防惡意軟體）核取方塊來啟用對應欄位。完成欄位以定義所需比對準則。例如，下圖顯示如果當端點已安裝 AVAST Free Antivirus 軟體應用程式、已啟用 **Real Time Protection**（即時保護），並且已在最近 5 天內更新病毒定義時，建立要比對 HIP 物件的方法。



針對您要在此物件中比對的每個類別重複此步驟。如需詳細資訊，請參閱 表格：資料收集類別 。

4. （選用）設定要與端點的擁有權類別或合規狀態比對的標籤。

   例如，您可以建立要與員工所擁有端點比對的標籤，以防止使用者在自己的個人端點上存取敏感的網路資源。

   Windows 適用的 User-ID 代理程式會查詢 MDM 伺服器，取得下列資訊：

   - 行動裝置合規狀態：
   - 行動裝置所屬的智慧群組（擁有權類別）。

   User-ID 代理程式會將此資訊轉換為併入 HIP 報告的標籤。您可以根據這些標籤值建立 HIP 物件，以在網路的端點上強制執行 HIP 式安全原則。如需詳細資訊，請參閱設定 Windows 的 User-ID 代理程式以收集主機資訊。

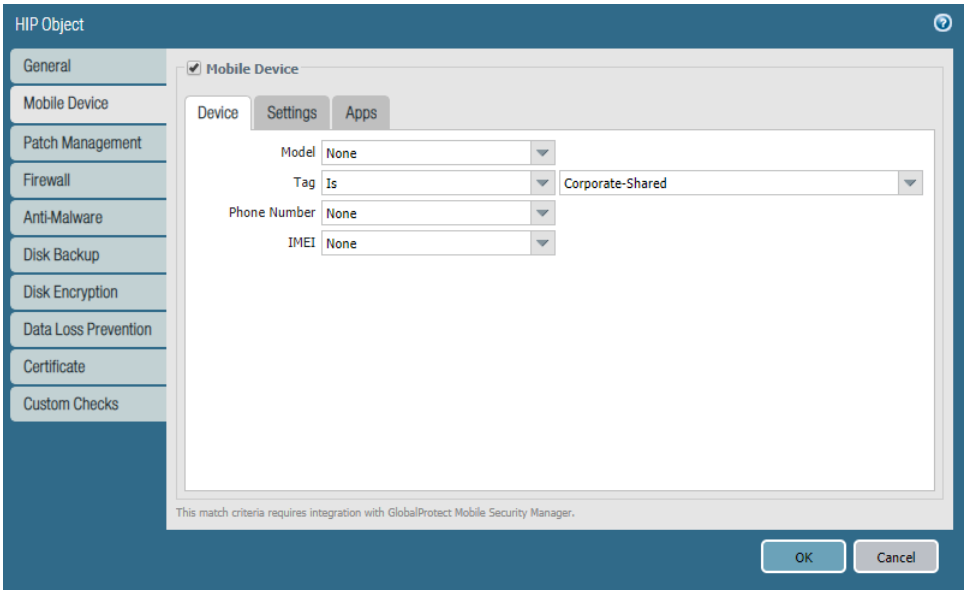
   1. 選取 **Mobile Device**（行動裝置）核取方塊以啟用 **Mobile Device**（行動裝置）設定組態。
   2. 在 **Device**（裝置）頁籤上，從 **Tag**（標籤）下拉式清單選取比對運算子（例如 **Contains**（包含）或 **Is Not**（非））。
   3. （選用）出現提示時，輸入下列擁有權類別值之一：

      擁有權類別表示該端點的擁有者。

      - 員工擁有的
      - 公司專用的
      - 公司共享的
   4. （選用）出現提示時，輸入下列合規狀態值之一：

      合規狀態表示端點是否符合定義的安全性原則。

      - 符合標準的
      - 未符合標準的
      - 不可用的

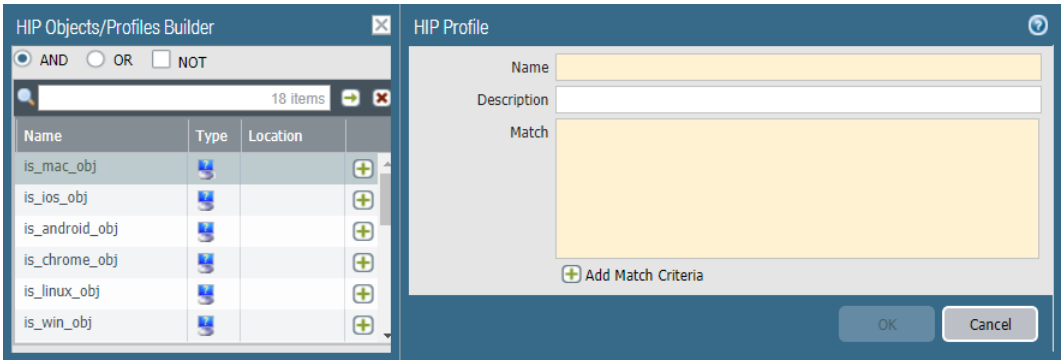


5. 按一下 **OK**（確定）來儲存 HIP 物件。
6. 重複這些步驟來建立您需要的其他每種 HIP 物件。
7. **Commit**（提交）變更。

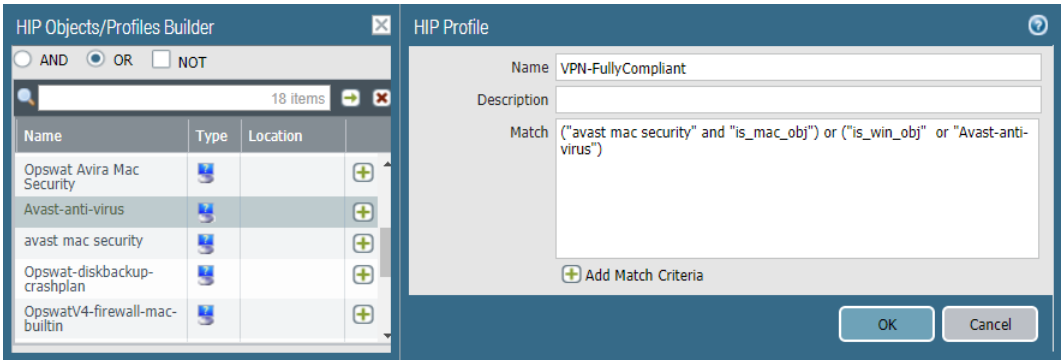
STEP 5 | 建立您打算在原則中使用的 HIP 設定檔。

建立 HIP 設定檔時，您可以使用布林邏輯來結合先前建立的 HIP 物件（以及其他 HIP 設定檔），如此在針對導出的 HIP 設定檔評估流量時，就會得到符合或不符合結果。如果有符合項，則將執行對應的原則規則；如果沒有符合項，則針對下一個規則，及使用任何其他原則比對準則來評估流量。

1. 在代管 GlobalProtect 閘道的防火牆上（如果您打算在多個閘道之間共享 HIP 設定檔，則在 Panorama 上），選取 **Objects**（物件）> **GlobalProtect** > **HIP Profiles**（**HIP** 設定檔），然後 **Add**（新增）新的 HIP 設定檔。
2. 輸入 **Name**（名稱）和 **Description**（說明）來識別設定檔。
3. 按一下**Add Match Criteria**（新增比對準則）開啟 [HIP 物件/設定檔建立器]。
4. 選取要作為比對準則的 HIP 物件或設定檔，然後按一下新增圖示 ()，將它移至 [HIP 設定檔] 對話方塊的 **Match**（比對）文字方塊。若只有當物件中的準則對流量而言不為 true 時，方允許 HIP 設定檔將物件評估為符合，請先選取 **NOT** 核取方塊再新增物件。



5. 為正在建立的設定檔繼續新增比對準則，確定在每次加法之間選取適當的布林運算子選項按鈕（**AND** 或 **OR**）；再次提醒您，請在適當的情況下使用 **NOT** 核取方塊。
6. 若是建立複雜的布林運算式，則必須在**Match**（比對）文字方塊中，於適當的位置手動新增括號，確保使用所要的邏輯來評估 HIP 設定檔。例如，下列 HIP 設定檔將比對具有 FileVault 磁碟加密（適用於 macOS 作業系統）或 TrueCrypt 磁碟加密（適用於 Windows 系統），且屬於必要的網域，並已安裝 Symantec 防毒用戶端之主機的流量：

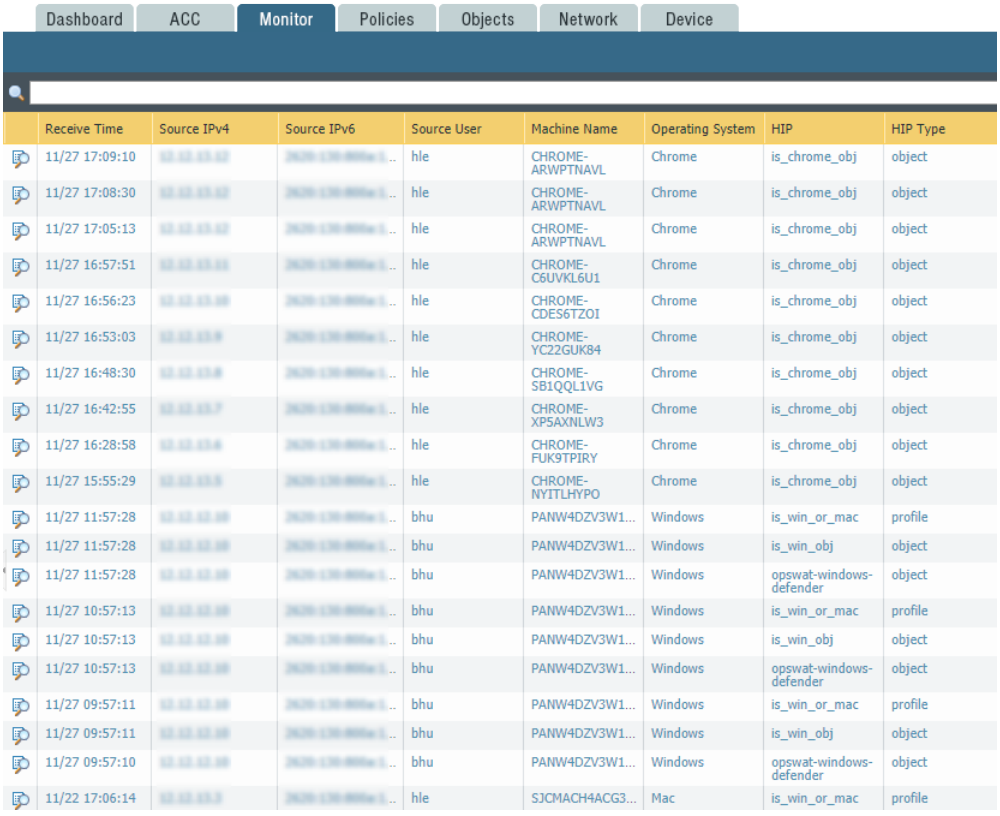


7. 新增所有比對準則後，請按一下 **OK**（確定）來儲存設定檔。
8. 重複這些步驟來建立您需要的其他每種 HIP 設定檔。
9. **Commit**（提交）變更。

STEP 6 | 確認您所建立的 HIP 物件與 HIP 設定檔是否如預期一樣與 GlobalProtect 流量相符。

不妨將監控 *HIP* 物件與設定檔，視為一種為主機端點監控安全性狀態與活動的方法。久而久之，透過監控主機資訊，您將能夠更加瞭解安全性與相容性的問題發生在何處，並可以使用此資訊引導自己建立有用的原則。如需詳細資訊，請參閱我如何獲得端點狀態的可見度？

在 GlobalProtect 使用者連線的目標閘道上，選取 **Monitor**（監控）> **Logs**（記錄）> **HIP Match**（**HIP** 比對）。此日誌顯示，當針對定義的 HIP 物件與 HIP 設定檔評估應用程式所報告的原始 HIP 資料時，閘道所識別的所有相符項。與其他日誌不同，要記錄 HIP 比對並不需要安全原則相符項。



Receive Time	Source IPv4	Source IPv6	Source User	Machine Name	Operating System	HIP	HIP Type
11/27 17:09:10	[redacted]	[redacted]	hle	CHROME-ARWPTNAVL	Chrome	is_chrome_obj	object
11/27 17:08:30	[redacted]	[redacted]	hle	CHROME-ARWPTNAVL	Chrome	is_chrome_obj	object
11/27 17:05:13	[redacted]	[redacted]	hle	CHROME-ARWPTNAVL	Chrome	is_chrome_obj	object
11/27 16:57:51	[redacted]	[redacted]	hle	CHROME-C6UVKL6U1	Chrome	is_chrome_obj	object
11/27 16:56:23	[redacted]	[redacted]	hle	CHROME-CDES6TZOI	Chrome	is_chrome_obj	object
11/27 16:53:03	[redacted]	[redacted]	hle	CHROME-YC22GUK84	Chrome	is_chrome_obj	object
11/27 16:48:30	[redacted]	[redacted]	hle	CHROME-SB1QQL1VG	Chrome	is_chrome_obj	object
11/27 16:42:55	[redacted]	[redacted]	hle	CHROME-XP5AXNLW3	Chrome	is_chrome_obj	object
11/27 16:28:58	[redacted]	[redacted]	hle	CHROME-FUK9TPIRY	Chrome	is_chrome_obj	object
11/27 15:55:29	[redacted]	[redacted]	hle	CHROME-NYITLHYPO	Chrome	is_chrome_obj	object
11/27 11:57:28	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	is_win_or_mac	profile
11/27 11:57:28	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	is_win_obj	object
11/27 11:57:28	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	opswat-windows-defender	object
11/27 10:57:13	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	is_win_or_mac	profile
11/27 10:57:13	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	is_win_obj	object
11/27 10:57:13	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	opswat-windows-defender	object
11/27 09:57:11	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	is_win_or_mac	profile
11/27 09:57:11	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	is_win_obj	object
11/27 09:57:10	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	opswat-windows-defender	object
11/22 17:06:14	[redacted]	[redacted]	hle	SJCMACH4ACG3...	Mac	is_win_or_mac	profile

STEP 7 | 在包含需要以 HIP 為基礎之存取控制來傳送要求的 GlobalProtect 使用者來源區域中啟用 User-ID。您必須啟用 User-ID，即使您不打算使用使用者識別功能，否則防火牆不會產生任何 HIP 比對日誌項目也是如此。

1. 選取 **Network**（網路）> **Zones**（區域）。
2. 在要啟用 User-ID 的區域中，按一下**Name**（名稱）。
3. **Enable User Identification**（啟用使用者識別），然後按一下 **OK**（確定）。

STEP 8 | 在您的閘道上建立啟用 HIP 的安全性規則。

最佳做法是，您應在新增 HIP 設定檔之前建立安全性規則，並測試它們是否符合預期流量（根據來源與目的地準則）。透過此做法，您可更好地確定在原則內啟用 HIP 之規則的適當位置。

1. 選取 **Policies**（原則）> **Security**（安全性）並選取您要新增 HIP 設定檔的目標規則。
2. 在 **Source**（來源）頁籤上，確保 **Source Zone**（來源地區）是您為其啟用 User-ID 的區域。
3. 在 **User**（使用者）頁籤上，**Add**（新增）用於識別使用者的 **HIP Profiles**（**HIP** 設定檔）（您可新增最多 63 個 HIP 設定檔至一條規則）。
4. 按一下 **OK**（確定）來儲存規則。
5. **Commit**（提交）變更。

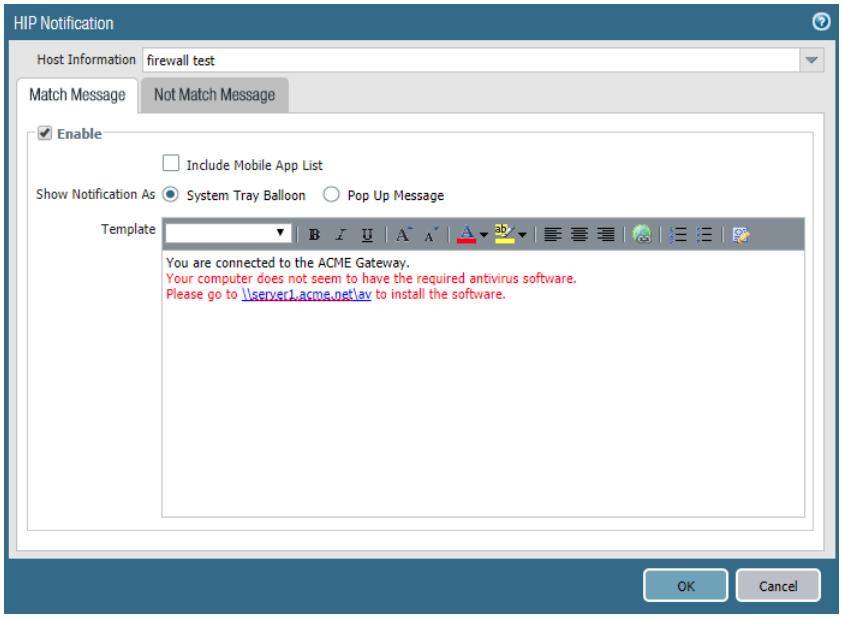
		Source				Destination	
Name	Tags	Zone	Address	User	HIP Profile	Zone	Address
iOSApps	none	corp-vpn	any	known-user	is iOS	trust	any

STEP 9 | 定義當使用 HIP 設定檔強制執行安全性規則時，一般使用者會看到的通知訊息。

至於決定要何時顯示通知訊息（即，當使用者的設定與原則中的 HIP 設定檔相符或不相符時是否顯示訊息），主要視您的原則與 HIP 相符（或不相符）對使用者有何意義而定。也就是說，相符是否表示使用者獲授與網路資源的完整存取權？或者表示由於不相容問題而限制其存取權？

例如，假設您所建立的 HIP 設定檔，會在所需的公司防毒與反間諜軟體套件未安裝時相符。在此情況下，您可能需要為比對 HIP 設定檔的使用者建立 HIP 通知訊息，告訴他們需要安裝軟體。或者，如果在已安裝那些相同應用程式的情況下，您的 HIP 設定檔相符，則您可能需要為與設定檔不相符的使用者建立訊息。

1. 在代管 GlobalProtect 閘道的防火牆上，選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）。
2. 選取您要新增 HIP 通知訊息的閘道組態。
3. 選取 **Agent**（代理程式）> **HIP Notification**（**HIP** 通知），然後按一下 **Add**（新增）。
4. 從 **Host Information**（主機資訊）下拉式清單選取套用此訊息的 HIP 設定檔。
5. 當對應的 HIP 設定檔已進行比對或未比對時，根據您是否要顯示此訊息，選取 **Match Message**（符合訊息）或 **Not Match Message**（不符合訊息）。在某些情況下，您可能需要根據您正在比對的物件與原則的目的，來為相符與非相符項目建立訊息。
6. **Enable**（啟用）**Match Message**（符合訊息）或 **Not Match Message**（不符合訊息），然後選取您要將訊息顯示為 **Pop Up Message**（快顯訊息）還是 **System Tray Balloon**（系統匣球形文字說明）。
7. 在 **Template**（範本）文字方塊中輸入訊息文字，然後按一下 **OK**（確定）。文字方塊提供文字的 WYSIWYG 檢視與 HTML 來源檢視，您可以使用 **Source Edit**（來源編輯）圖示在這兩種檢視之間切換。工具列也提供各種格式化文字與建立外部文件超連結的選項（例如直接將使用者連結至所需軟體程式的下載 URL）。

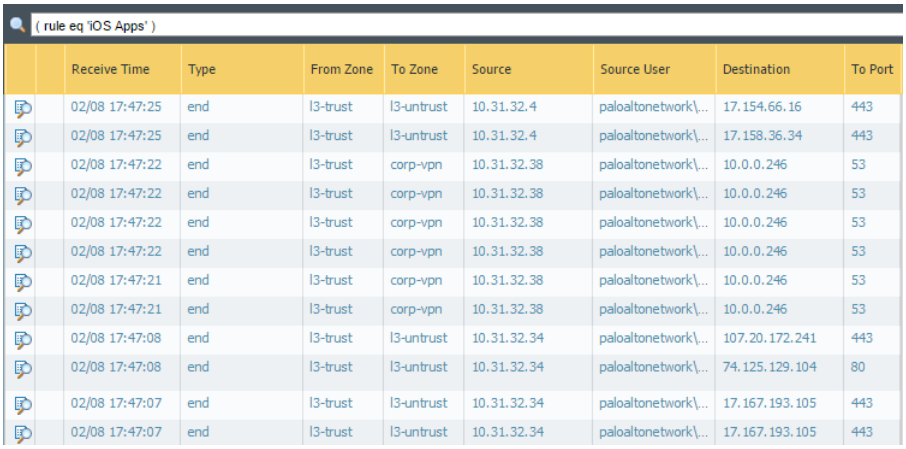


8. 針對每個要定義的訊息重複此程序。
9. **Commit**（提交）變更。

STEP 10 | 確認您的 HIP 設定檔是否如預期一樣正常。

您可以使用流量日誌監控達到了啟用 HIP 的原則的流量：

1. 在代管閘道的防火牆上，選取 **Monitor**（監控）> **Logs**（記錄）> **Traffic**（流量）。
2. 篩選日誌以僅顯示與包含您打算監控之 HIP 設定檔的規則相符的流量。例如，若要搜尋與名為「iOS 應用程式」之安全性規則相符的流量，您應在篩選文字方塊中輸入 **(rule eq 'iOS Apps')**，如下所示：



從端點收集應用程式與處理資料

Windows 登錄與 macOS plist 可分別用於為 Windows 與 macOS 作業系統設定和儲存設定。您可以建立自訂檢查，讓您判定該應用程式在 Windows 或 macOS 端點上是否已安裝（具有對應的登錄或 Plist 機碼）或正在執行（具有對應的執行中程序）。啟用自訂檢查以指示 GlobalProtect 應用程式收集特定的登錄資訊（從 Windows 端點收集登錄機碼與登錄機碼值）或偏好設定清單 (Plist) 資訊（從 macOS 端點收集 Plist 與 Plist 索引鍵）。您定義要在自訂檢查中收集的資料會包含在 GlobalProtect 應用程式所收集的原始 主機資訊 資料中，然後在應用程式連線時提交到 GlobalProtect 閘道。

若要監控透過自訂檢查收集的資料，您可以建立 HIP 物件。接著，您可以將 HIP 物件新增至 HIP 設定檔，以使用收集到的資料來比對端點流量，並強制執行安全性規則。閘道可使用 HIP 物件（比對在自訂檢查中定義的資料），以篩選由應用程式提交的原始主機資訊。當閘道將端點資料與 HIP 物件比對時，系統會為資料產生 HIP 比對日誌項目。HIP 設定檔也允許閘道將收集到的資料與安全性規則比對。如果使用 HIP 設定檔作為安全性原則規則的準則，則閘道將會在符合的流量上強制執行安全性規則。

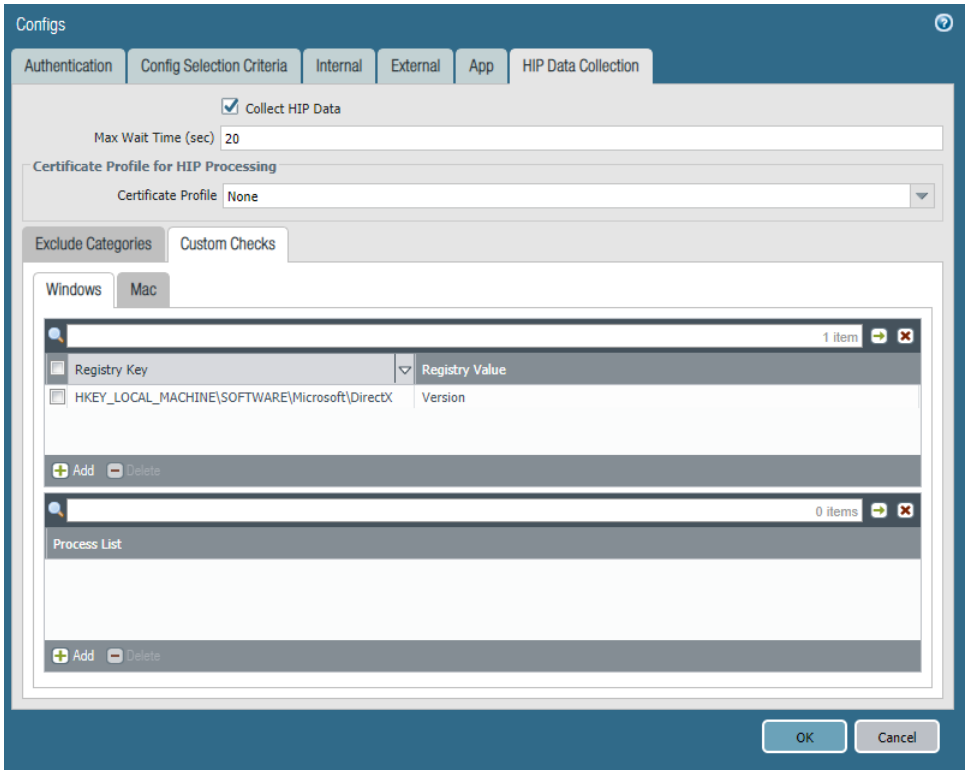
使用下列步驟可啟用自訂檢查以收集 Windows 與 macOS 端點的資料。此工作流程還包括一些選用的步驟，可為自訂檢查建立 HIP 物件與 HIP 設定檔，讓您能夠使用端點資料作為安全性原則的比對準則，來監控、識別流量並採取動作。

如需直接從 *Windows* 登錄或全域 *macOS plist* 定義應用程式設定的詳細資訊，請參閱明顯部署應用程式設定。

STEP 1 | 允許 GlobalProtect 應用程式從 Windows 端點收集 Windows 登錄資訊，從 macOS 端點收集 plist 資訊。所收集的資訊類型可包括應用程式是否已安裝在端點上，或是該應用程式的特定屬性或特性。

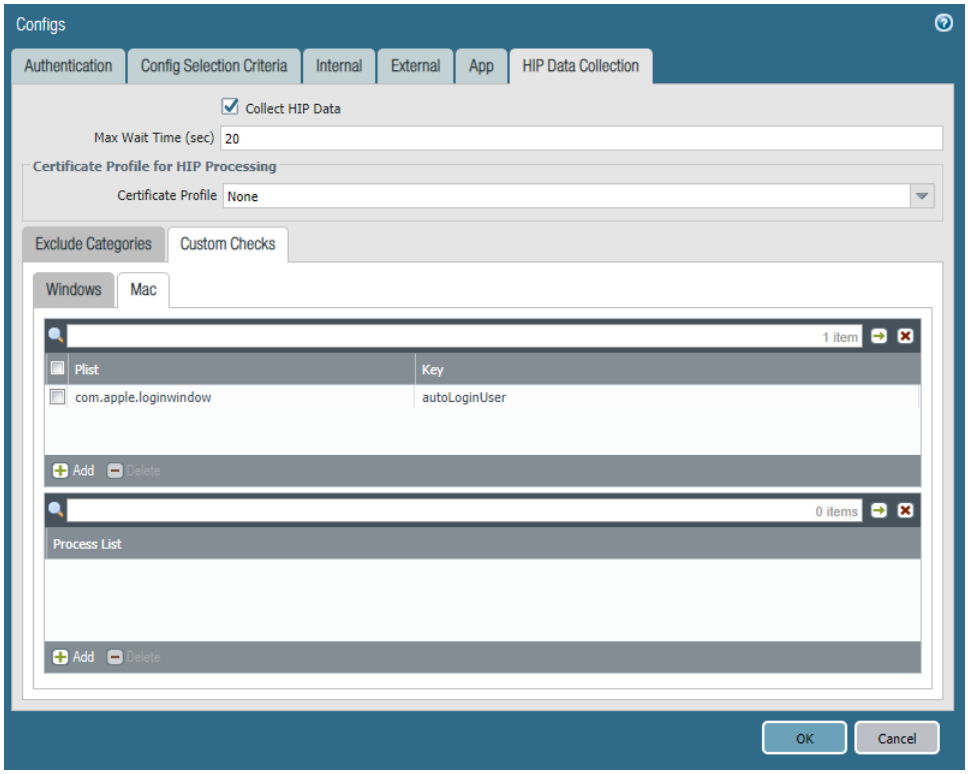
從 Windows 端點收集資料：

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）。
2. 選取現有入口網站組態或 **Add**（新增）一個。
3. 在 **Agent**（代理程式）頁籤上，選取您要修改的代理程式組態或 **Add**（新增）一個新的。
4. 選取 **HIP Data Collection**（**HIP** 資料收集）。
5. 啟用 GlobalProtect 應用程式以 **Collect HIP Data**（收集 **HIP** 資料）。
6. 選取 **Custom Checks**（自訂檢查）> **Windows**，然後 **Add**（新增）您要收集相關資訊的 **Registry Key**（登錄機碼）。如果您想要將資料收集限制在登錄機碼內包含的值，請新增對應的 **Registry Value**（登錄值）。

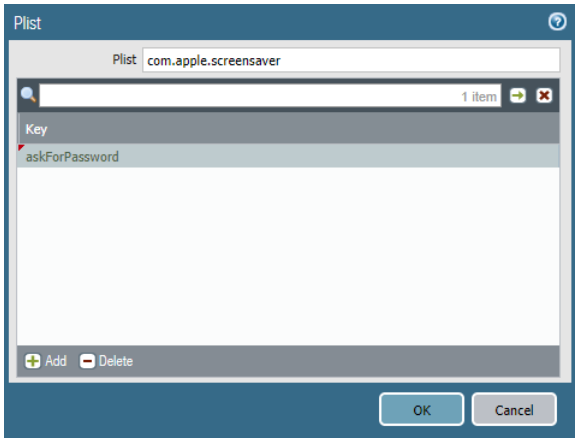


從 macOS 端點收集資料：

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）。
2. 選取現有入口網站組態或 **Add**（新增）一個。
3. 在 **Agent**（代理程式）頁籤上，選取您要修改的代理程式組態或 **Add**（新增）一個新的。
4. 選取 **HIP Data Collection**（**HIP** 資料收集）。
5. 啟用 GlobalProtect 應用程式以 **Collect HIP Data**（收集 **HIP** 資料）
6. 選取 **Custom Checks**（自訂檢查）> **Mac**，然後 **Add**（新增） 您要收集相關資訊的 **Plist** 及對應的 plist **Key**（索引鍵），以判定應用程式是否已安裝。



例如，**Add**（新增）**Plist** `com.apple.screensaver` 和 **Key**（索引鍵）`askForPassword`，以收集在螢幕保護程式開始後是否需要密碼才能喚醒 macOS 端點的資訊：



STEP 2 | （選用）檢查端點上是否正在執行特定的處理程序。

1. 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）。
2. 選取現有入口網站組態或 **Add**（新增）一個。
3. 在 **Agent**（代理程式）頁籤上，選取您要修改的代理程式組態或 **Add**（新增）一個新的。
4. 選取 **HIP Data Collection**（**HIP** 資料收集）。
5. 啟用 GlobalProtect 應用程式以 **Collect HIP Data**（收集 **HIP** 資料）
6. 選取 **Custom Checks**（自訂檢查）> **Windows** 或 **Mac**。
7. 將您要收集相關資訊的處理程序名稱 **Add**（新增）至 **Process List**（處理程序清單）。

STEP 3 | 儲存自訂檢查。

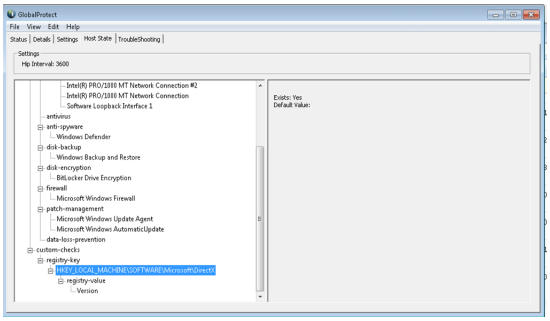
按一下 **OK**（確定）並 **Commit**（提交）變更。

STEP 4 | 確認 GlobalProtect 應用程式正從端點收集在自訂檢查中定義的資料。

對於 Windows 端點：

1. 透過按一下系統匣圖示來啟動適用於 Windows 端點的 GlobalProtect 應用程式。GlobalProtect 狀態面板將開啟。
2. 按一下設定 (

) 圖示以開啟設定功能表。
3. 選取 **Settings**（設定）以開啟 **GlobalProtect** 設定面板。
4. 選取 **Host Profile**（主機設定檔）頁籤以檢視 GlobalProtect 應用程式從端點收集的資訊。確認 **custom-checks**（自訂檢查）下拉式清單會顯示您針對收集定義的資料。



對於 macOS 端點：

1. 透過按一下系統匣圖示來啟動適用於 macOS 端點的 GlobalProtect 應用程式。GlobalProtect 狀態面板將開啟。
2. 按一下設定 (

) 圖示以開啟設定功能表。
3. 選取 **Settings**（設定）以開啟 **GlobalProtect** 設定面板。
4. 選取 **Host Profile**（主機設定檔）頁籤以檢視 GlobalProtect 應用程式從端點收集的資訊。確認 **custom-checks**（自訂檢查）下拉式清單會顯示您針對收集定義的資料。

STEP 5 | （選用）建立 HIP 物件來比對登錄機碼 (Windows) 或 plist (macOS)，讓您能夠篩選從 GlobalProtect 應用程式收集的原始主機資訊以監控要進行自訂檢查的資料。

透過針對自訂檢查資料定義的 HIP 物件，閘道將比對從應用程式提交到 HIP 物件的原始資料，系統會針對該資料產生 HIP 比對日誌項目（**Monitor**（監控）> **HIP Match**（**HIP** 比對））。

針對 Windows 和 macOS 端點：

1. 選取 **Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件）。
2. 選取現有 HIP 物件或 **Add**（新增）一個。
3. 在 **Custom Checks**（自訂檢查）頁籤上，選取核取方塊以啟用 **Custom Checks**（自訂檢查）。

僅對於 Windows 端點：

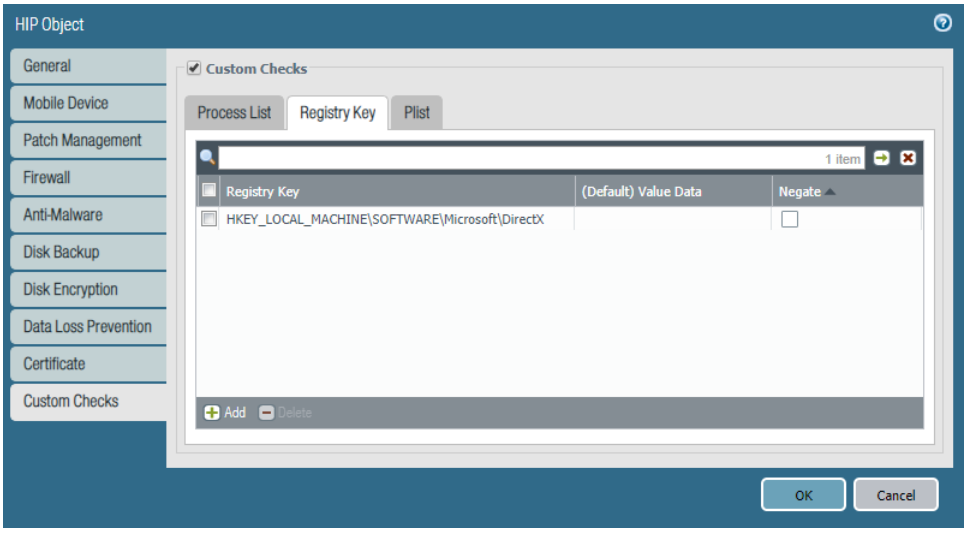
1. 若要檢查 Windows 端點的特定登錄機碼，請選取 **Custom Checks**（自訂檢查）> **Registry Key**（登錄機碼），然後 **Add**（新增）要與之比對的登錄機碼。出現提示時，輸入 **Registry Key**（登錄機碼），然後設定下列選項之一：
   - 若要與登錄機碼的預設值資料進行比對，請輸入 **(Default) Value Data**（預設（值資料））。
   - 若要比對沒有指定登錄機碼的端點，請選取 **Key does not exist or match the specified value data**（機碼不存在或不符合指定的值資料）。

不要同時設定 *(Default) Value Data*（預設（值資料））與 *Key does not exist or match the specified value data*（機碼不存在或不符合指定的值資料）選項。

2. 若要與登錄機碼內的特定值進行比對，請選取 **Custom Checks**（自訂檢查）> **Registry Key**（登錄機碼），然後 **Add**（新增）要與之比對的登錄機碼。出現提示時，輸入 **Registry Key**（登錄機碼）。按一下 **Add**（新增），然後設定下列選項之一：
   - 若要與登錄機碼內的特定值進行比對，請輸入 **Registry Value**（登錄值）和對應 **Value Data**（值資料）。
   - 若要比對沒有指定登錄機碼的端點，請輸入 **Registry Value**（登錄值），然後選取 **Negate**（否定）核取方塊。

   若要使用此選項，請不要為 *Registry Key*（登錄機碼）輸入任何 *Value Data*（值資料）。

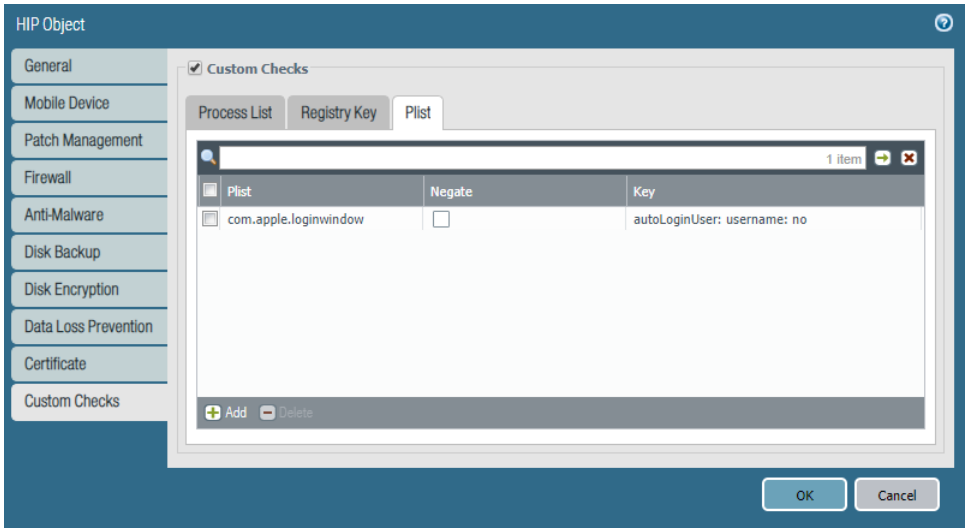
   若您為登錄機碼新增多個登錄值，*GlobalProtect* 閘道將檢查所有端點以查看所有指定登錄值。



3. 按一下 **OK**（確定）來儲存 HIP 物件。您可以在下一次設備簽入時 **Commit**（提交）變更，以檢視 **HIP Match**（**HIP** 比對）日誌中的資料，或繼續進行步驟 6。

僅對於 macOS 端點：

1. 若要檢查 macOS 端點以查看特定 plist，請選取 **Plist**，然後 **Add**（新增）要檢查的 plist。出現提示時，輸入 **Plist** 的名稱。如果您想要比對沒有指定 plist 的 macOS 端點，請啟用 **Plist does not exist**（**Plist** 不存在）選項。
2. 若要與 plist 內的特定機碼-值配對進行比對，請選取 **Plist**，然後 **Add**（新增）要檢查的 plist。出現提示時，輸入 **Plist** 的名稱，然後 **Add**（新增）**Key**（機碼）及要比對的對應 **Value**（值）。或者如果您想要識別沒有特定索引鍵與值的端點，請在新增 **Key**（索引鍵）與 **Value**（值）後，選取 **Negate**（否定）。



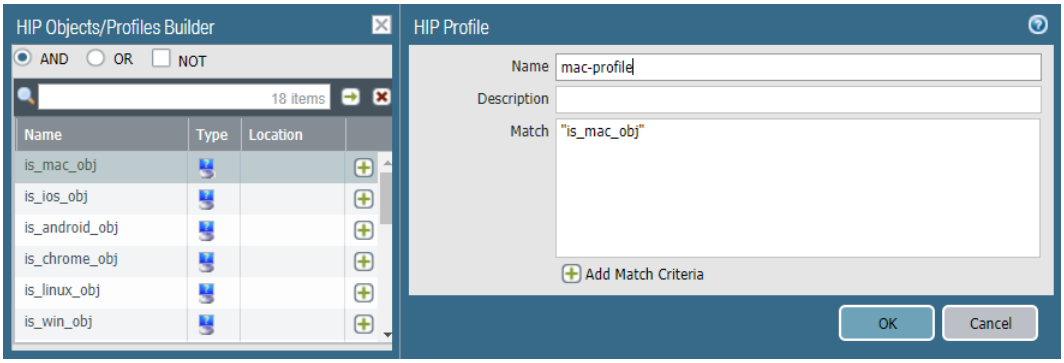
3. 按一下 **OK**（確定）來儲存 HIP 物件。您可以在下一次設備簽入時 **Commit**（提交）變更，以檢視 **HIP Match**（**HIP** 比對）日誌中的資料，或繼續進行步驟 6。

STEP 6 | （選用）建立 HIP 設定檔以允許針對流量評估 HIP 物件。

HIP 設定檔可新增至安全性原則，以額外比對符合該原則的流量。將流量與 HIP 設定檔比對後，會在流量上強制執行安全性原則規則。

如需建立 HIP 設定檔的詳細資訊，請參閱設定 HIP 型原則強化。

1. 選取 **Objects**（物件）> **GlobalProtect** > **HIP Profiles**（**HIP** 設定檔）。
2. 選取現有 HIP 設定檔或 **Add**（新增）一個。
3. 按一下**Add Match Criteria**（新增比對準則）開啟 [HIP 物件/設定檔建立器]。
4. 選取要作為比對準則的 **HIP object**（**HIP** 物件），然後按一下新增（ ）圖示，將它移至 [HIP 設定檔] 的 **Match**（比對）區域。
5. 當您將物件新增至新的 HIP 設定檔後，按一下 **OK**（確定），然後 **Commit**（提交）變更。



STEP 7 | 將 HIP 設定檔新增至安全性原則，讓使用自訂檢查收集的資料可用於比對流量與採取動作。

選取 **Policies**（原則）> **Security**（安全性），然後選取現有的安全性原則或 **Add**（新增）一個。在 **User**（使用者）頁籤上，將 **HIP Profiles**（**HIP** 設定檔）**Add**（新增）至該原則。如需安全性原則元件的詳細資訊，及如何使用安全性原則以比對流量與採取動作，請參閱安全性原則。

重新散佈 HIP 報告

為確保主機資訊設定檔 (HIP) 原則執行的一致性及簡化原則管理，您可向企業內的其他閘道、防火牆、專用日誌收集器 (DLC) 及 Panorama 設備散佈從 GlobalProtect 應用程式收到（及傳送至內部或外部 GlobalProtect 閘道）的 HIP 報告。在下列情況下，重新散佈 HIP 報告非常實用：

- 您想要對內部和外部 GlobalProtect 閘道套用一致的原則。
- 您想要對通過多個防火牆的特定使用者之流量套用一致的 HIP 原則。

若要重新散佈 HIP 報告，請使用與 重新散佈 User-ID 資訊 相同的部署建議和最佳做法。

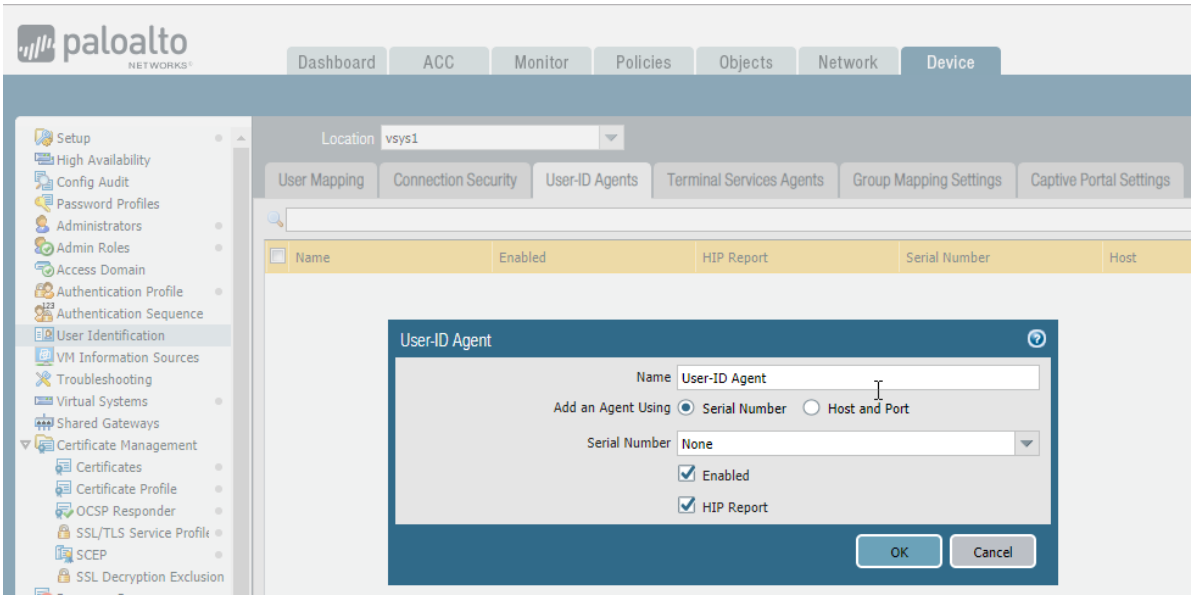
按照下列步驟設定 HIP 報告重新散佈。

STEP 1 | 設定以 HIP 為基礎的原則強制執行 針對閘道與防火牆。

STEP 2 | 設定 HIP 報告重新散佈。

1. 選取 **Device**（裝置）> **User Identification**（使用者識別）> **User-ID Agents**（**User-ID** 代理程式）。
2. 選取現有 User-ID 代理程式或 **Add**（新增）一個。

   代理程式必須為 *Palo Alto Networks* 新一代防火牆、*GlobalProtect* 閘道、*DLC* 或 *Panorama* 設備。
3. 選取 **HIP Report**（**HIP** 報告）。



4. 按一下 **OK**（確定）。

STEP 3 | 如果您使用 GlobalProtect 防火牆或閘道散佈 HIP 報告，請確保用於重新散佈 HIP 報告之防火牆或閘道上的群組對應設定與設定 User-ID 之防火牆或閘道上的下列屬性相符。

如果您使用 *Panorama* 設備或 *DLC* 散佈 *HIP* 報告，請略過此步驟。

- 設定 HIP 報告重新散佈防火牆或閘道上的使用者屬性以與 User-ID 防火牆或閘道上的使用者屬性相符。

  例如，如果用於 HIP 報告重新散佈之防火牆或閘道的 **Primary attribute**（主要屬性）為 sAMAccountName 且 **Alternate Username 1**（替代使用者名稱 **1**）為使用者主體名稱 (UPN)，請確保在設定 User-ID 的防火牆或閘道上設定相同值。

  屬性順序不必相同；例如，如果 *HIP* 報告重新散佈防火牆的 *Primary attribute*（主要屬性）為 *sAMAccountName* 且 *Alternate Username 1*（替代使用者名稱 *1*）為 *UPN*，您可將 *User-ID* 防火牆的 *Alternate Username*（替代使用者名稱）設為 *sAMAccountName*，*Primary attribute 1*（主要屬性 *1*）設為 *UPN*。
- 如果部署時在群組對應中設定了使用者網域，則須設定 HIP 報告重新散佈防火牆或閘道上的使用者網域屬性以與 User-ID 防火牆或閘道上的使用者網域屬性相符。使用者網域屬性必須在所有防火牆與閘道中保持一致。
- 在 HIP 報告重新散佈防火牆或閘道上設定通用使用者群組（防火牆與閘道上連線至相同驗證伺服器並擷取相同使用者群組的使用者群組）以與 User-ID 防火牆或閘道上的使用者群組相符。

STEP 4 | 使用與 將 User-ID 資訊重新散佈至受管理的防火牆 相同的工作流程將 HIP 報告重新散佈至受管理的 Panorama 設備、閘道、防火牆及虛擬系統。

封鎖端點存取

當使用者遺失可對您的網路提供 GlobalProtect 存取的端點，端點被盜，或者使用者離開您的組織時，您可以透過將該端點置於封鎖清單中，以封鎖該端點對您網路的存取。

封鎖清單對邏輯網路位置而言屬於本機（在此範例中為 vsys 1）並且每個位置可包含最多 1000 部端點。因此，您可以為每個代管 GlobalProtect 部署的位置建立獨立的封鎖清單。

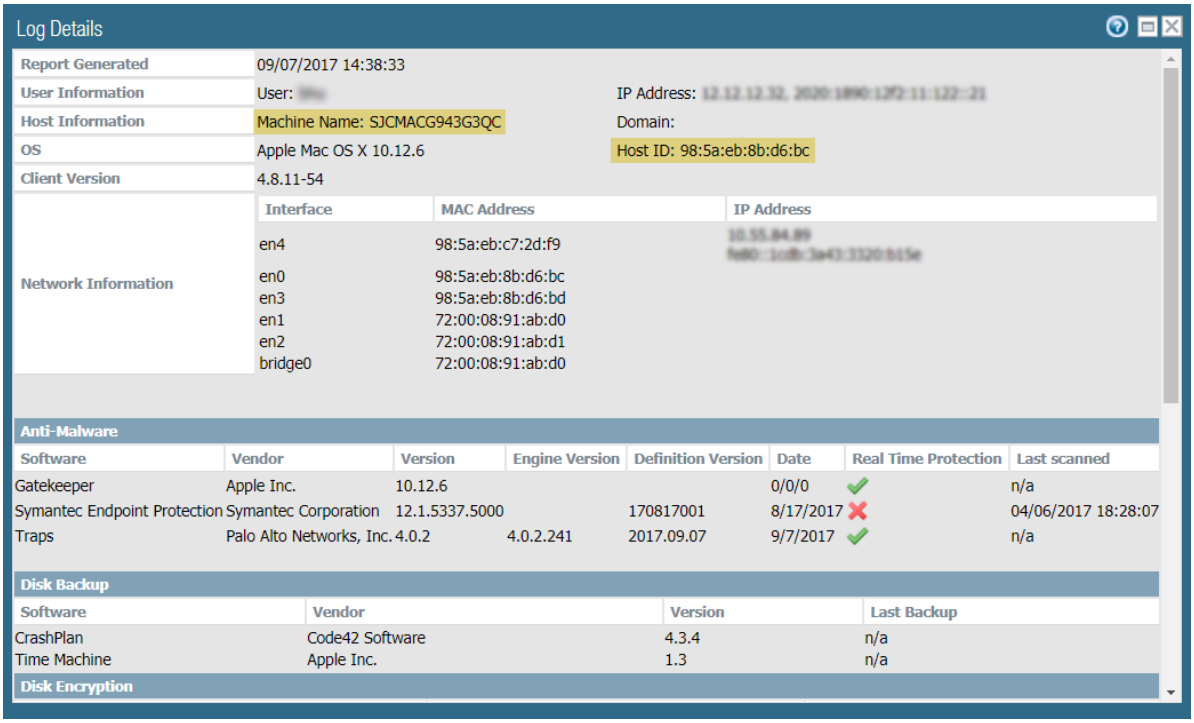
STEP 1 | 識別您想要封鎖的端點主機 ID。

主機 ID 是 GlobalProtect 為了識別主機所指派的唯一 ID。主機 ID 值會依端點類型而有所不同：

- Windows—Windows 登錄中儲存的機器 GUID (HKEY_Local_Machine\Software\Microsoft\Cryptography\MachineGuid)
- macOS—第一個內建實體網路介面的 MAC 位址
- Android—Android ID
- iOS—UDID
- Chrome—GlobalProtect 所指派的唯一英數字串，長度為 32 個字元

如果您不知道主機 ID，可以在 HIP 比對日誌中將 user-ID 關聯到主機 ID：

1. 選取 **Monitor**（監控）> **Logs**（日誌）> **HIP Match**（**HIP** 比對）。
2. 針對與端點相關聯的來源使用者，篩選 HIP 比對日誌。
3. 開啟 HIP 比對日誌，在 **OS**（作業系統）> **Host ID**（主機 **ID**）下識別主機 ID，並選擇性地在 **Host Information**（主機資訊）> **Machine Name**（機器名稱）下識別主機名稱。

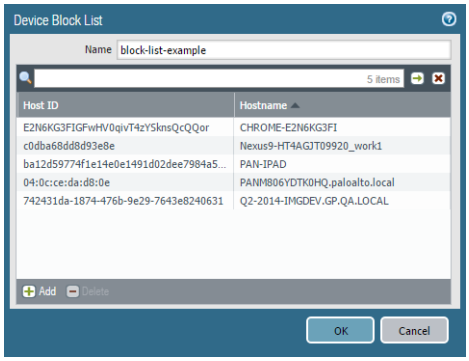


STEP 2 | **建立設備封鎖清單。**

您無法使用 *Panorama* 範本來推送設備封鎖清單至防火牆。

1. 選取 **Network**（網路） > **GlobalProtect** > **Device Block List**（設備封鎖清單） 並 **Add**（新增） 一個設備封鎖清單。
2. 輸入清單的描述性 **Name**（名稱）。
3. 針對具有多個 Virtual System（虛擬系統，VSYS）的防火牆，選取 **Location**（位置）（VSYS 或 **Shared**（共用））， 您可在其中使用設定檔。

STEP 3 | **新增設備至封鎖清單。**



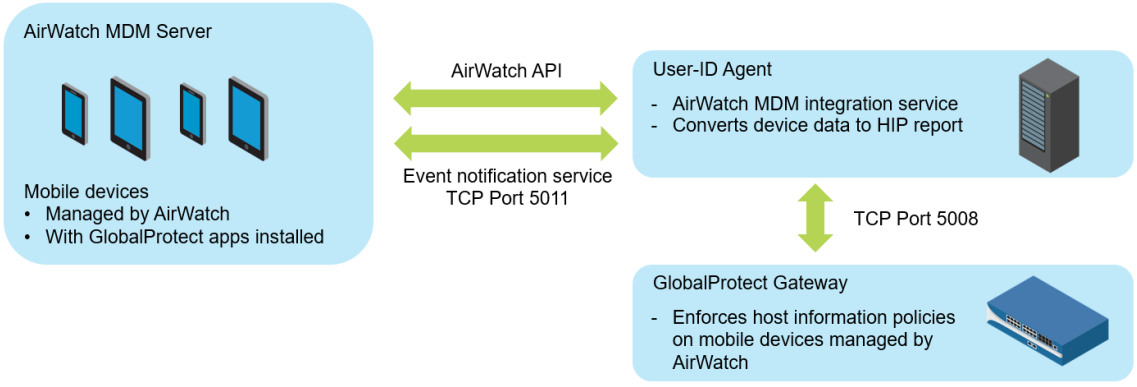
1. **Add**（新增）端點。為您要封鎖的端點輸入主機 ID（必要）和主機名稱（選用）。
2. 視需要 **Add**（新增）其他端點。
3. 按一下 **OK**（確定）來儲存並啟動封鎖清單。

設備封鎖清單不需要提交且立即啟用。

設定 Windows 的 User-ID 代理程式以收集主機資訊

以 Windows 為基礎的 User-ID 代理程式已經過擴充，以支援新的 AirWatch MDM 整合服務。此服務讓 GlobalProtect 能使用服務所收集的主機資訊，在由 AirWatch 管理的裝置上強制執行以 HIP 為基礎的原則。AirWatch MDM 整合服務會作為以 Windows 為基礎的 User-ID 代理程式的一部分來執行，使用 AirWatch API 來收集由 VMware AirWatch 管理的行動端點資訊，並將此資料轉譯為主機資訊。

對於由 *AirWatch* 管理的 *Android* 端點，此功能支援 *Android for Work* 端點，但不支援其他類型的 *Android* 端點。



MDM 整合概要

內含以 Windows 為基礎的 User-ID 代理程式 MDM 整合服務會對 AirWatch MDM 伺服器執行完整的 HIP 查詢以擷取行動裝置的完整主機資訊。行動裝置上的 GlobalProtect 應用程式也會將 HIP 資訊傳送給閘道，而閘道會將來自 GlobalProtect 應用程式與 MDM 整合服務的資訊合併。執行 GlobalProtect 應用程式的行動裝置與 GlobalProtect 閘道連線時，GlobalProtect 可以使用主機資訊設定檔套用安全性原則。

您可將 MDM 整合服務設定為在規律間隔擷取 AirWatch 裝置資訊並將此資訊推送至 GlobalProtect 閘道。此外，該服務可以監控 AirWatch 事件通知並在 AirWatch 事件發生時（例如合規性變更）時擷取更新的裝置資訊。

收集的資訊

下表顯示如何將從 AirWatch 管理端點所收集的資訊轉換為 HIP 報告屬性。系統會自動執行對應。

AirWatch 屬性	HIP 報告屬性
裝置資訊	
序號	序號

AirWatch 屬性	HIP 報告屬性
MacAddress	wifimac
Imei	IMEI
作業系統	版本
Model	型號
DeviceFriendlyName	devname
IsSupervised	supervised
Udid（唯一裝置識別碼）	udid
使用者名稱	使用者
前次註冊時間	註冊時間
平台	os
註冊狀態	由 MDM 管理
前次看見時間	前次檢查時間
合規性狀態 （User-ID 代理程式 8.0.3 或更新版本）	符合標準的 未符合標準的 不可用的
擁有權 （User-ID 代理程式 8.0.3 或更新版本）	員工擁有的 公司專用的 公司共享的
安全性資訊	
已啟用資料保護	磁碟已加密
密碼是否存在	密碼已設定
密碼是否符合標準	符合標準的密碼
網路資訊	
資料漫遊已啟用	資料漫遊中
GPS 座標	
緯度	緯度
經度	經度

AirWatch 屬性	HIP 報告屬性
範例時間	最後一個位置的時間
應用程式詳細資料	
應用程式名稱	應用程式名稱
版本	版本
應用程式識別碼	封裝

系統需求

AirWatch MDM 整合服務需要下列軟體：

軟體	最低支援版本
使用者識別代理程式	8.0.1
PAN-OS	7.1.0
適用於 Android 的 GlobalProtect 應用程式	4.0.0
適用於 iOS 的 GlobalProtect 應用程式	4.0.1
AirWatch 伺服器	8.4.7.0
Windows 伺服器	2008 與 2012 具 User-ID 代理程式 8.0.4 和 PAN-OS 8.0.4 的 2016

設定 GlobalProtect 以擷取主機資訊

使用下列指示設定 GlobalProtect，從 AirWatch 管理的裝置中擷取主機資訊。

STEP 1 | 安裝 User-ID 代理程式。User-ID 代理程式所在位置，必須能啟用至 VMware AirWatch 行動裝置管理 (MDM) 系統的安全連線。

AirWatch MDM 整合服務包含在以 Windows 為基礎的 User-ID 代理程式中。

STEP 2 | 在以 Windows 為基礎的 User-ID 代理程式和 GlobalProtect 閘道之間設定 SSL 驗證。

設定 SSL 驗證時，請確保：

- 在以 Windows 為基礎的 User-ID 代理程式上設定的伺服器憑證，具有與 User-ID 代理程式主機的主機名稱/IP 位址相同的通用名稱 (CN)。
- 伺服器憑證受到防火牆信任（包含在防火牆 MDM 設定中的受信任 CA 清單）。
- 必須將防火牆上設定的 MDM 用戶端憑證的根憑證授權單位 (CA) 憑證，匯入 Windows 伺服器的 Windows 信任存放區。

1. 取得伺服器憑證和私密金鑰，以便在以 Windows 為基礎的 User-ID 代理程式和 GlobalProtect 閘道之間進行驗證。憑證套件必須是包含 PEM 憑證、完整憑證鏈和私密金鑰的 PEM 格式。
2. 開啟以 Windows 為基礎的 User-ID 代理程式，並選取 **Server Certificate**（伺服器憑證）。
3. **Add**（新增）伺服器憑證。

- **Browse**（瀏覽）至憑證檔案並 **Open**（開啟）檔案以上傳憑證到以 Windows 為基礎的 User-ID 代理程式。
- 輸入憑證的 **Private Key Password**（私密金鑰）。
- 按一下 **OK**（確定）。

代理程式會驗證憑證是否有效，並將私密金鑰的加密密碼儲存在主機的 Windows 憑證存放區。

如果安裝成功，關於憑證的詳細資訊（包括通用名稱、到期日和簽發者）會顯示在 **Server Certificate**（伺服器憑證）頁籤上。

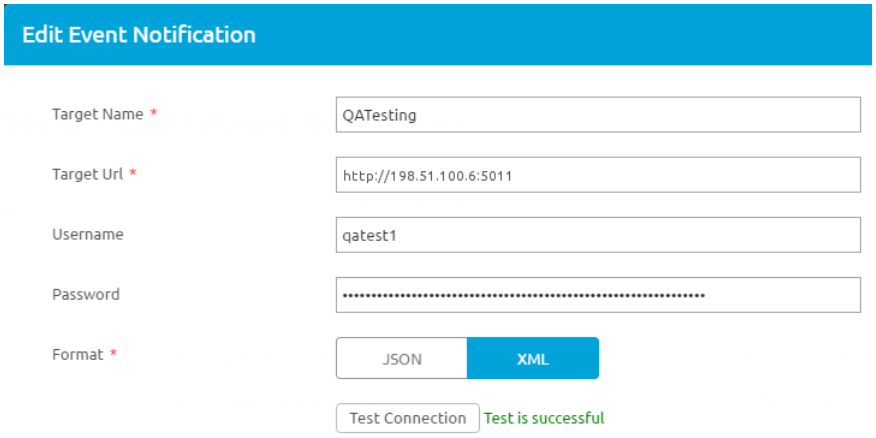
1. 重新啟動以 Windows 為基礎的 User-ID 代理程式。

STEP 3 | 設定以 Windows 為基礎的 User-ID 代理程式上之 MDM 整合服務。

1. 選取以 Windows 為基礎的 User-ID 代理程式中之 **MDM Integration**（**MDM** 整合）。
2. 指定要進行 TCP 通訊的 **Gateway Connection TCP Port**（閘道連線 **TCP** 連接埠）。以 Windows 為基礎的 User-ID 代理程式將在此連接埠接聽所有 MDM 相關的訊息。預設連接埠為 5008。若要變更連接埠，請指定 1 到 65535 的數字。
3. 在 **Setup**（設定）頁籤上按一下 **Edit**（編輯）。
4. 針對 **MDM Vendor**（**MDM** 廠商）選取 **AirWatch**。

STEP 4 | 指定 **MDM Event Notification**（**MDM** 事件通知）設定以監控並收集 AirWatch 事件（例如，裝置註冊、裝置抹除和合規性變更）。當事件發生時，MDM 整合服務會從 AirWatch API 取得已更新的裝置資訊，並將此資訊推送至所有已設定的 GlobalProtect 閘道。

對於 *MDM Event Notification*（*MDM* 事件通知），請確保您在此處輸入的值，也已設定在 *AirWatch* 主控台下的 *Groups & Settings*（群組與設定）> *All Settings*（所有設定）> *System*（系統）> *Advanced*（進階）> *API* > *Event Notifications*（事件通知）。

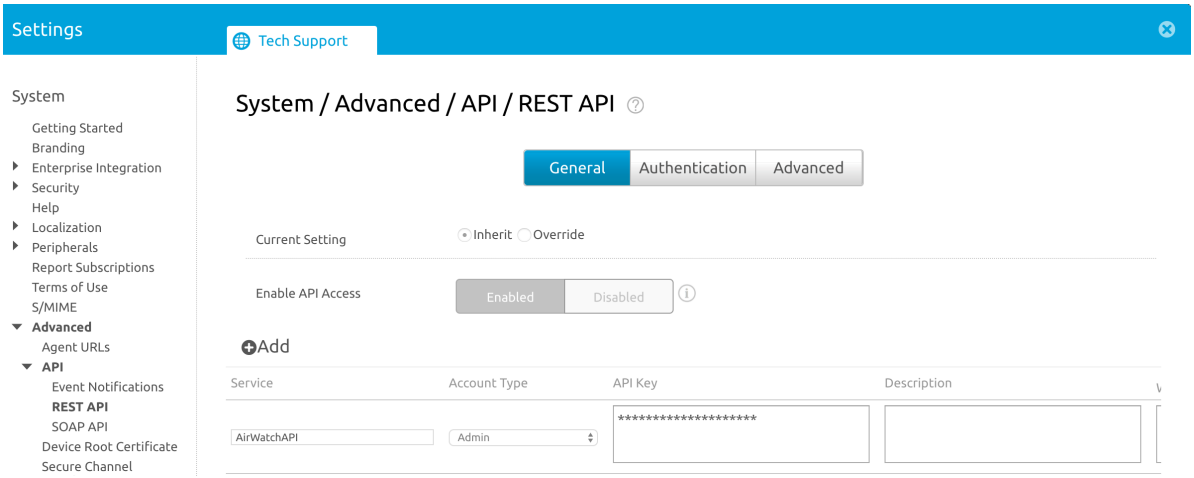


- 請設定 **TCP Port**（**TCP** 連接埠）以便與事件通知服務通訊。使用此格式：`http://<external_hostname>/<ip_address>:<port>` where `<ip-address>` 是 MDM 整合服務的 IP 位址。預設連接埠為 5011。若要變更連接埠，請指定 1 到 65535 的數字。
- 對於事件通知，請輸入驗證接下來的要求所需之 **Username**（使用者名稱）和 **Password**（密碼）憑證。

- 輸入 **Permitted Ip**（允許使用的 **IP**）位址來存取 MDM 事件。此為以逗號分隔的 IP 位址（張貼 MDM 事件的位址）清單。例如，AirWatch 伺服器的 IP 位址：如需取得指定哪個 IP 位址的指示，請聯絡 AirWatch 支援團隊。

STEP 5 | 新增 **MDM API Authentication**（**MDM API** 驗證）設定以與 AirWatch API 連線。

- 輸入 AirWatch MDM 伺服器的 **Server Address**（伺服器位址），以 Windows 為基礎的 User-ID 代理程式連線將會連線至該伺服器。例如 `api.awmdm.com`。
- 輸入憑證存取 AirWatch MDM API 所需的 **Username**（使用者名稱）和 **Password**（密碼）。
- 輸入 **Tenant Code**（租戶代碼）。這是存取 AirWatch MDM API 所需，唯一的十六進位代碼。在 AirWatch 主控台，您可以在 t **System**（系統）> **Advanced**（進階）> **API** > **REST API** > **API Key**（**API** 金藥）找到租戶代碼。



- 輸入 **Mobile Device State Retrieval Interval**（行動裝置狀態擷取間隔）。此設定會控制從 AirWatch 管理的裝置擷取主機資訊的頻繁程度。預設時間間隔為 30 分鐘。若要變更間隔，請指定 1 到 600 的數字。

STEP 6 | **Commit**（提交）您的變更。

STEP 7 | 按一下 **Test Connection**（測試連線）以確認以 Windows 為基礎的 User-ID 代理程式可以連線至 AirWatch API。

STEP 8 | 設定 GlobalProtect 閘道與 MDM 整合服務通訊，以擷取受 AirWatch 管理裝置的 HIP 報告。

1. 在 PAN-OS Web 介面，選取 **Network**（網路）> **GlobalProtect** > **MDM**。
2. **Add**（新增）下列有關 MDM 整合服務的資訊。

- **Name**（名稱）—輸入 MDM 整合服務的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
- （選用）選取閘道所屬的虛擬系統。
- **Server**（伺服器）—輸入 Airwatch MDM 整合服務上介面的 IP 位址或 FQDN，閘道將連線該介面以擷取 HIP 報告。確定具有此介面的服務路由。
- **Connection Port**（連線連接埠）—輸入連線連接埠，MDM 整合服務將在該連接埠接聽 HIP 報告要求。預設連接埠為 5008。若要變更連接埠，請指定 1 到 65535 的數字。
- **Client Certificate**（用戶端憑證）—選取在建立 HTTPS 連線時，將向 MDM 整合服務出示的閘道之用戶端憑證。您可以從下拉式選單選取用戶端憑證，或匯入新的用戶端憑證。**Certificate Purpose**（憑證用途）必須指出其為用戶端驗證憑證。

用戶端憑證的根憑證授權單位 *(CA)* 憑證，必須匯入 *Windows* 伺服器的 *Windows* 信任存放區，該伺服器已安裝以 *Windows* 為基礎的 *User-ID* 代理程式。

1. **Add**（新增）根 CA 憑證，該憑證與 MDM 整合服務主機上安裝的伺服器憑證相關聯。您需要根 CA 憑證以及伺服器憑證，來建立閘道和 MDM 整合服務之間的安全連線。您可以從下拉式選單選取根 CA 憑證，或匯入新的憑證。
2. 按一下 **OK**（確定）。
3. **Commit**（提交）您的變更。

STEP 9 | 請檢查您的連線，確保已將 AirWatch 裝置數據傳輸到 GlobalProtect。

1. 開啟以 Windows 為基礎的 User-ID 代理程式並選取 **MDM Integration**（**MDM** 整合）> **Mobile Devices**（行動裝置）。您應該可以看見唯一裝置 ID 和所有 AirWatch 管理的裝置使用者名稱清單。
2. （選用）您可以 **Filter**（篩選）此清單以找出 **Mobile Device**（行動裝置）。
3. （選用）。選取裝置 ID 清單中的裝置，然後按一下 **Retrieve Device State**（擷取裝置狀態）已擷取關於裝置的最新資訊，並查看其如何對應至 GlobalProtect 閘道上的主機資訊設定檔。

對 MDM 整合服務進行疑難排解

如果您對事件通知有問題或無法對 AirWatch REST API 進行驗證，請依照這些指示。

- MDM 整合服務不會接收 AirWatch MDM 伺服器的事件通知。
  1. 將 **Debug**（偵錯）選項（在 **File**（檔案）功能表）設定為 **Debug**（偵錯）或 **Verbose**。
  2. 前往 Windows 伺服器上的 User-ID 代理程式安裝資料夾，然後開啟 `MaDebug` 檔案。尋找與以下類似的訊息：

```
The address x.x.x.x is not in the permitted ip list for event
 notifications.
```

3. 新增此 IP 位址作為 **Permitted IP**（允許的 **IP**）位址（**MDM Integration**（**MDM** 整合）> **Setup**（設定）> **Permitted IP**（允許的 **IP**））。

- 對 Airwatch REST API 的驗證是不成功的。

  請確保以下事項：

  - 用於 MDM 整合服務以對 AirWatch MDM 服務進行驗證的認證是有效的。
  - 用於存取 Airwatch REST API 的使用者帳戶有 API 存取權和對資料的唯讀權限（最低）以供行動裝置與 AirWatch 管理的使用者使用。
  - 租用戶碼 (API 金鑰) 與使用者帳戶正確建立關聯。移除所有未使用的 API 金鑰。

認證

當您啟用 FIPS-CC 模式時，適用於 Windows 和 macOS 端點的 GlobalProtect™ 應用程式符合聯邦資訊處理標準 (FIPS 140-2) 與通用準則 (CC) 的要求。這些安全性憑證可確保符合一系列安全性保證和功能標準，通常美國政府機構和其他國內外受管制行業要求提供。關於產品認證和協力廠商憑證的詳細資訊，請參閱 Palo Alto Networks 憑證 頁面。

有關如何在 FIPS-CC 模式下設定適用於 Windows 和 macOS 端點的 GlobalProtect 應用程式並對其進行疑難排解的資訊，請參閱以下幾節。

- 啟用並驗證 FIPS-CC 模式
- FIPS-CC 安全性功能
- 對 FIPS-CC 模式進行疑難排解

啟用並驗證 FIPS-CC 模式

您可透過下列方法啟用並驗證 GlobalProtect 應用程式的 FIPS-CC 模式：

- 使用 Windows 登錄來啟用並驗證 FIPS-CC 模式
- 使用 macOS 屬性清單來啟用並驗證 FIPS-CC 模式

若要修改 *Windows* 登錄或 *macOS plist*，您在 *Windows* 或 *macOS* 中必須擁有管理員帳戶。

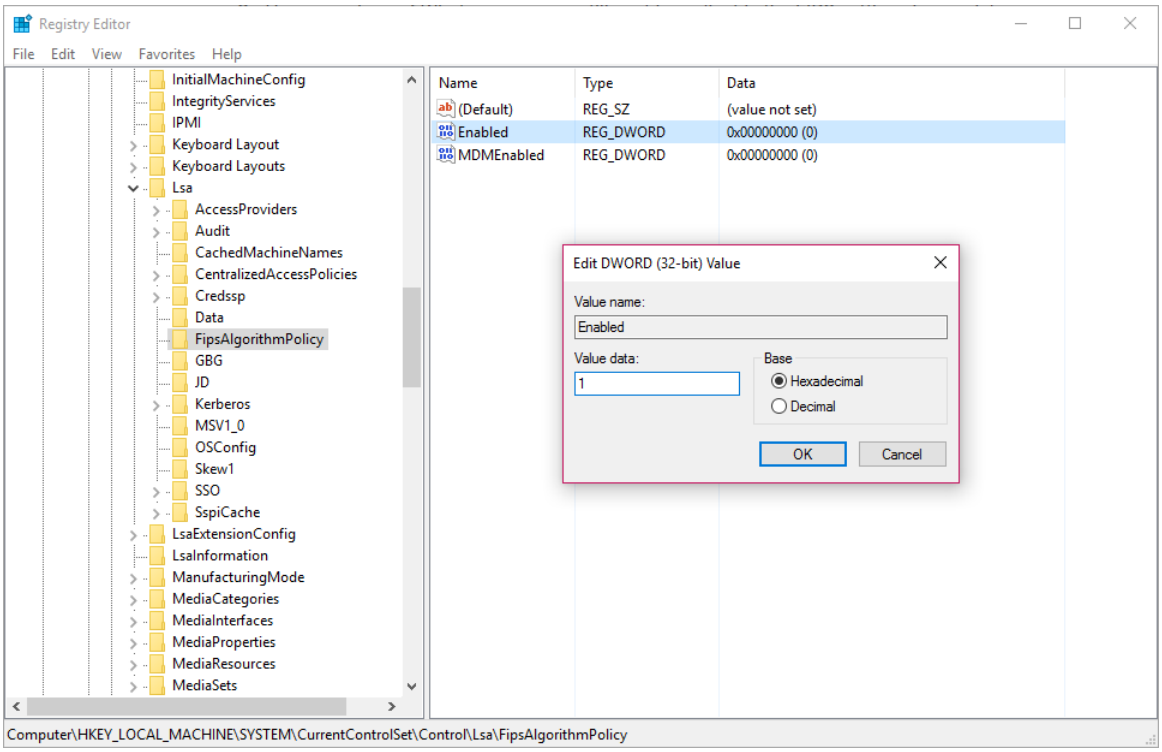
使用 Windows 登錄來啟用並驗證 FIPS-CC 模式

在 Windows 端點上，按照下列步驟使用 Windows 登錄 啟用並驗證 GlobalProtect™ 的 FIPS-CC 模式：

STEP 1 | 在 Windows 作業系統中啟用 FIPS 模式。

若要啟用 GlobalProtect 的 FIPS-CC 模式，您必須先在 Windows 作業系統中啟用 FIPS 模式，以確保 Windows 端點符合 FIPS 140-2 標準。

1. 啟動命令提示。
2. 輸入 **`regedit`** 以開啟 Windows 登錄。
3. 在 Window 登錄中，前往：`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\`。
4. 以滑鼠右鍵按一下 **Enabled**（已啟用）登錄值並 **Modify**（修改）該值。
5. 若要啟用 FIPS 模式，請將 **Value Data**（值資料）設為 **1**。預設值 **0** 表示 FIPS 模式已停用。

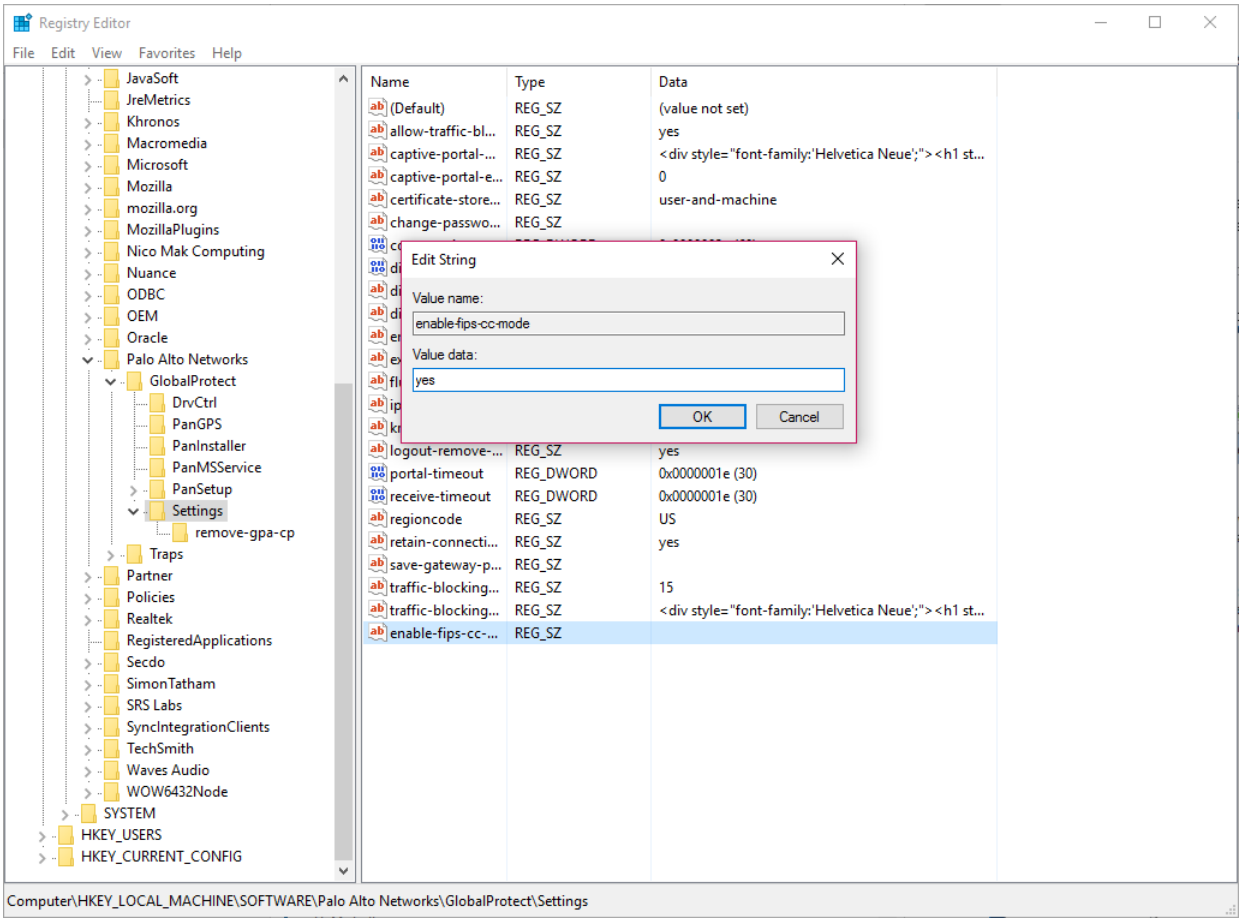


6. 按一下 **OK**（確定）。
7. 重新啟動端點。

STEP 2 | 啟用 GlobalProtect 的 FIPS-CC 模式。

FIPS-CC 模式啟用後便無法停用。若要在非 *FIPS-CC* 模式下執行 *GlobalProtect*，一般使用者必須解除安裝然後重新安裝 *GlobalProtect* 應用程式。這會從 *Windows* 登錄中清除所有 *FIPS-CC* 模式設定。

1. 啟動命令提示。
2. 輸入 **`regedit`** 以開啟 Windows 登錄。
3. 在 Window 登錄中，前往：`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\`。
4. 按一下 **Edit**（編輯），然後選取 **New**（新）> **String Value**（字串值）。
5. 出現提示時，將新登錄值的 **Name**（名稱）指定為 **`enable-fips-cc-mode`**。
6. 以滑鼠右鍵按一下新登錄值並 **Modify**（修改）該值。
7. 若要啟用 FIPS 模式，請將 **Value Data**（值資料）設為 **`yes`**。
8. 按一下 **OK**（確定）。

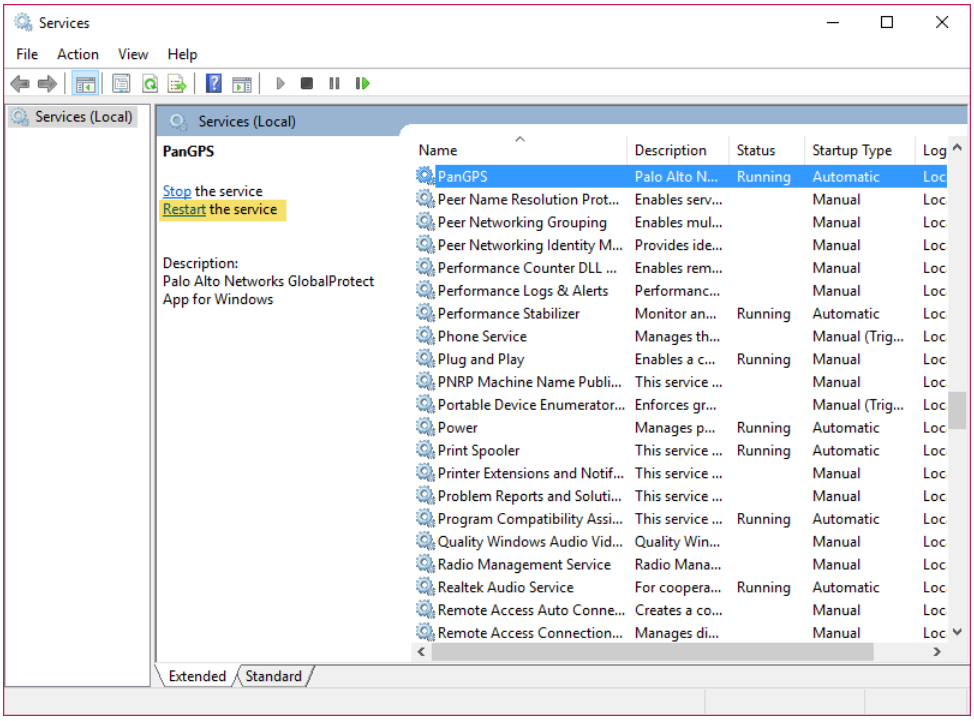


STEP 3 | 重新啟動 GlobalProtect。

若要使 GlobalProtect 應用程式在 FIPS-CC 模式下初始化，必須透過下列方法之至重新啟動 GlobalProtect：

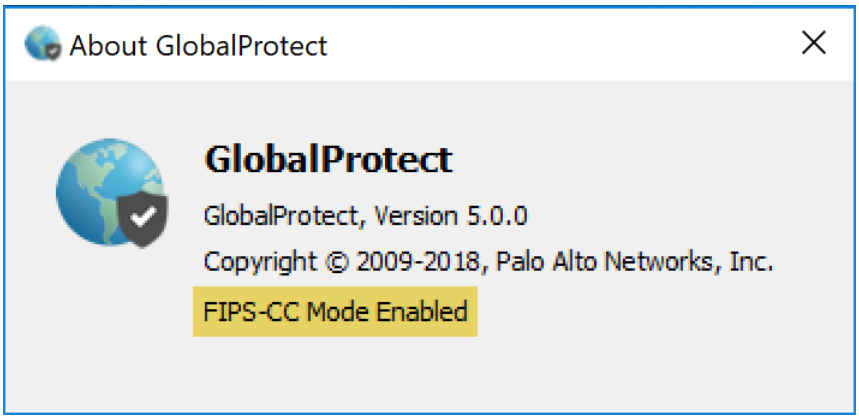
- 重新啟動端點。
- 重新啟動 GlobalProtect 應用程式與 GlobalProtect 服務 (PanGPS)：
  1. 啟動命令提示。
  2. 輸入 **`services.msc`** 以開啟 Windows 服務管理器。
  3. 從服務清單中，選取 **PanGPS**。

4. **Restart**（重新啟動）服務。



STEP 4 | 確認已在 GlobalProtect 應用程式上啟用 FIPS-CC 模式。

1. 啟動 GlobalProtect 應用程式。
2. 從狀態面板中，開啟設定對話方塊 ( )。
3. 選取 **About**（關於）。
4. 確認已啟用 FIPS-CC 模式。如果 FIPS-CC 模式已啟用，「關於」對話方塊將顯示 `FIPS-CC Mode Enabled`（`FIPS-CC 模式已啟用`）狀態。



使用 macOS 屬性清單來啟用並驗證 FIPS-CC 模式

在 macOS 端點上，按照下列步驟使用 macOS plist（屬性清單）啟用並驗證 GlobalProtect™ 的 FIPS-CC 模式：

若要啟用 *GlobalProtect* 的 *FIPS-CC* 模式，您的 *macOS* 端點必須符合 *FIPS 140-2* 標準。依預設，*macOS* 作業系統的 *FIPS* 模式在執行 *macOS 10.8* 及更新版本的端點上自動啟用。

STEP 1 | 打開 GlobalProtect Plist 檔案，找到 GlobalProtect 自訂設定。

1. 啟動 plist 編輯器，例如 Xcode。
2. 在 plist 編輯器中，開啟以下 plist 檔案：/程式庫/偏好設定/com.paloaltonetworks.GlobalProtect.settings.plist。
3. 找到 GlobalProtect 設定字典：/Palo Alto Networks/GlobalProtect/設定。

   如果設定字典不存在，則建立一個。您可將每個機碼新增至設定字典作為字串。

STEP 2 | 啟用 GlobalProtect 的 FIPS-CC 模式。

FIPS-CC 啟用後便無法停用。若要在非 *FIPS-CC* 模式下執行 *GlobalProtect*，一般使用者必須解除安裝然後重新安裝 *GlobalProtect* 應用程式。這會從 *macOS plist* 中清除所有 *FIPS-CC* 模式設定。

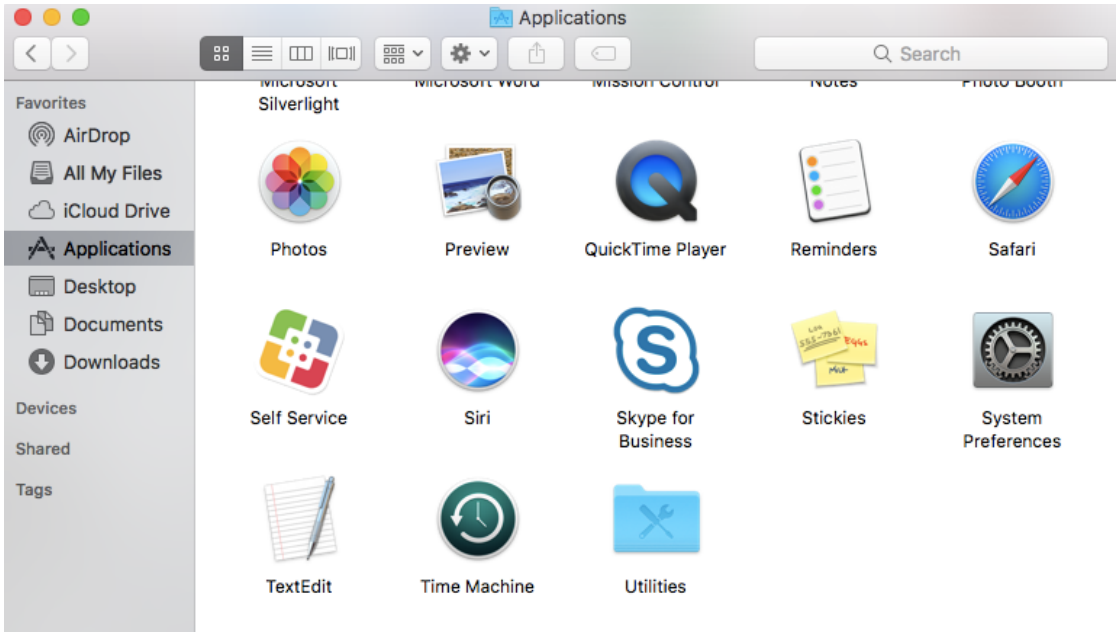
在設定字典中，新增下列機碼-值配對以啟用 FIPS-CC 模式：

```
<key>enable-fips-cc-mode</key>
<string>yes</string>
```

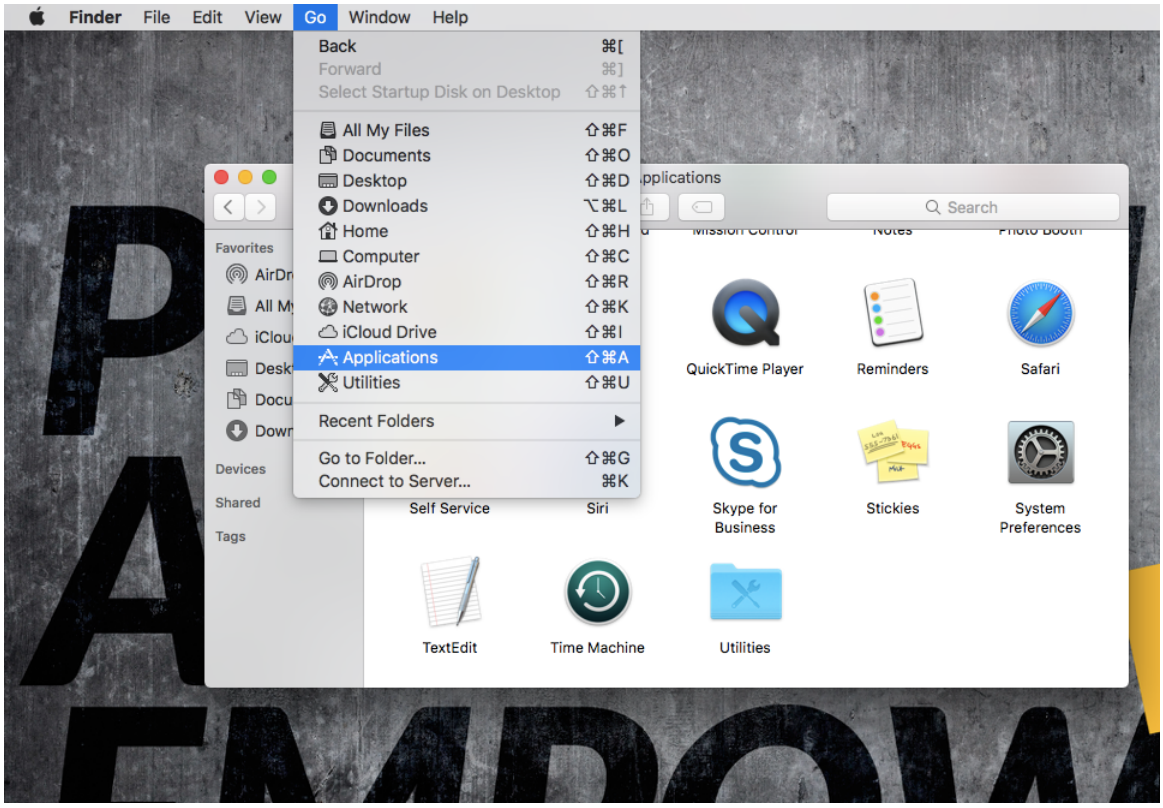
STEP 3 | 重新啟動 GlobalProtect。

若要使 GlobalProtect 應用程式在 FIPS-CC 模式下初始化，必須透過下列方法之至重新啟動 GlobalProtect：

- 重新啟動端點。
- 重新啟動 GlobalProtect 應用程式與 GlobalProtect 服務 (PanGPS)：
  1. 啟動查找器。
  2. 開啟應用程式資料夾：
     - 從查找器側列中，選取 **Applications**（應用程式）。



     - 如果您在查找器側列中沒有看到 **Applications**（應用程式），可從查找器功能表列選取 **Go**（移至）> **Applications**（應用程式）。



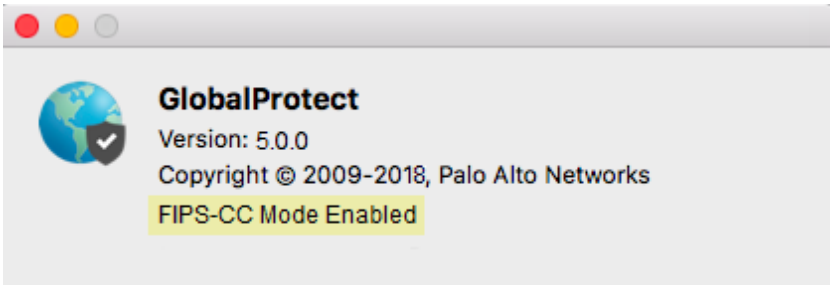
若要在查找器側列中顯示 *Applications*（應用程式），可從查找器功能表列選取 *Finder*（查找器）> *Preferences*（偏好設定）。從查找器偏好設定中，選取 *Sidebar*（側列），然後啟用此選項以顯示 *Applications*（應用程式）。

3. 開啟公用程式資料夾。
4. 啟動終端。
5. 執行下列命令：

```
username>$ launchctl unload -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangpa.plist username>$ launchctl unload -
S Aqua /Library/LaunchAgents/com.paloaltonetworks.gp.pangps.plist
 username>$ launchctl load -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangpa.plist username>$ launchctl load -S
 Aqua /Library/LaunchAgents/com.paloaltonetworks.gp.pangps.plist
```

STEP 4 | 確認已在 GlobalProtect 應用程式上啟用 FIPS-CC 模式。

1. 啟動 GlobalProtect 應用程式。
2. 從狀態面板中，開啟設定對話方塊 ( )。
3. 選取 **About**（關於）。
4. 確認已啟用 FIPS-CC 模式。如果 FIPS-CC 模式已啟用，「關於」對話方塊將顯示 `FIPS-CC Mode Enabled`（`FIPS-CC 模式已啟用`）狀態。



FIPS-CC 安全性功能

當您啟用 GlobalProtect 的 FIPS-CC 模式時，下列安全性功能將對 Windows 與 macOS 端點上的所有 GlobalProtect 應用程式執行。

- 您必須使用 TLS 或 IPSec 加密 GlobalProtect 應用程式與閘道之間的所有 VPN 通道。
- 設定 IPSec VPN 時，您必須在 IPSec 設定期間選取出現的加密套件選項。
- 設定 IPSec VPN 通道時，您可指定下列加密演算法之一：
  - AES-CBC-128（採用 SHA1 驗證演算法）
  - AES-GCM-128
  - AES-GCM-256
- 伺服器與用戶端憑證都必須使用下列特徵碼演算法之一：
  - RSA 2048 位元（或更高）
  - ECDSA P-256
  - ECDSA P-384
  - ECDSA P-521

  此外，您還必須使用 SHA256、SHA384 或 SHA512 等特徵碼雜湊演算法。

對 FIPS-CC 模式進行疑難排解

如果您在啟用 FIPS-CC 模式後遇到問題，可參閱以下幾節以幫助排解這些疑難問題。

- 檢視並收集 GlobalProtect 日誌
- 解決 FIPS-CC 模式問題

檢視並收集 GlobalProtect 日誌

您可在 GlobalProtect™ 日誌中檢視關於 FIPS-CC 問題的詳細資訊。

按照下列步驟檢視或收集 GlobalProtect 日誌：

STEP 1 | 啟動 GlobalProtect 應用程式。

STEP 2 | 從狀態面板中，開啟設定對話方塊 ( )。

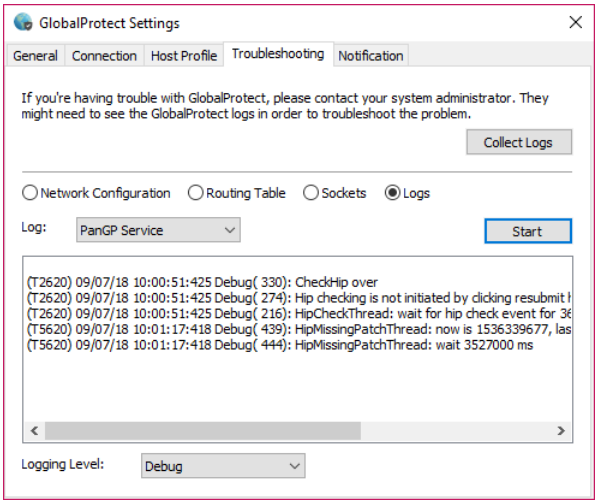
STEP 3 | 選取 **Settings**（設定）。

STEP 4 | 從 GlobalProtect 設定面板中，選取 **Troubleshooting**（疑難排解）。

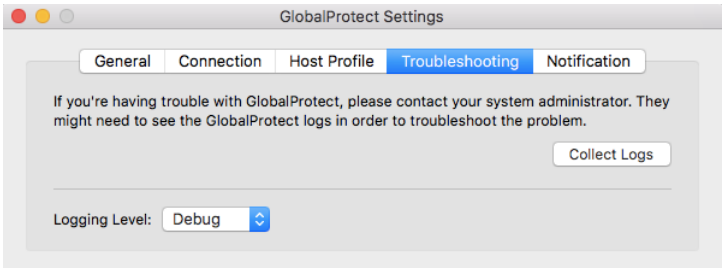
STEP 5 | 選取 **Logging Level**（日誌記錄層級）。

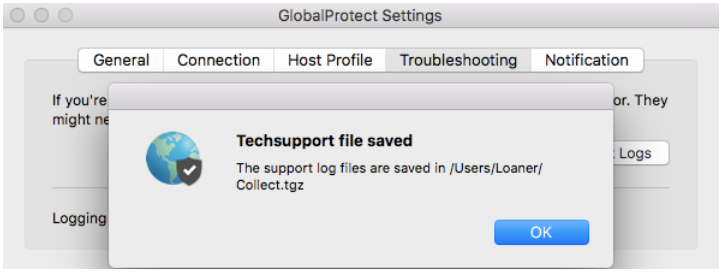
STEP 6 | （選用—僅限 Windows）檢視您的 GlobalProtect 日誌：

1. 選取 **Logs**（日誌）。
2. 選擇 **Log**（日誌）類型。
3. **Start**（開始）收集日誌。



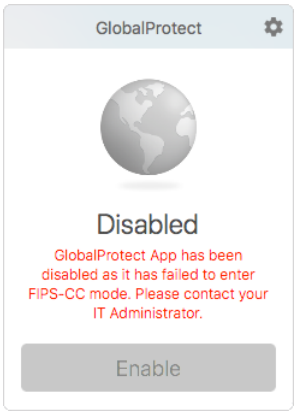
STEP 7 | （選用）**Collect Logs**（收集日誌）以傳送給 GlobalProtect 管理員進行疑難排解。

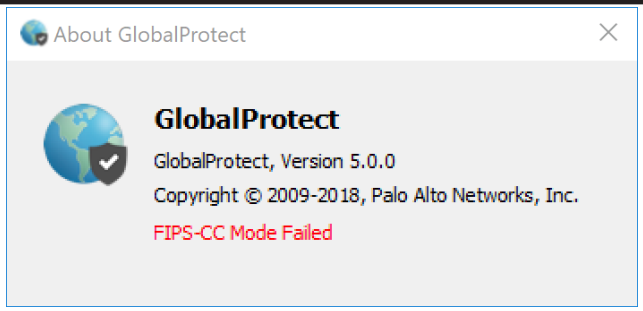




解決 FIPS-CC 模式問題

下表說明了可能的 FIPS-CC 模式問題與相應解決方案。如果您遇到任何下表未列出的問題，請聯絡 GlobalProtect™ 管理員尋求疑難排解協助。

問題	說明	解決方案
由於 FIPS 開機自測或完整性測試失敗，GlobalProtect 應用程式無法在 FIPS-CC 模式下初始化。	當您啟用 FIPS-CC 模式後，GlobalProtect 應用程式會在應用程式初始化及系統或應用程式重新啟動期間執行 FIPS 開機自測與完整性測試。如果其中一個測試失敗，GlobalProtect 應用程式將停用，且 About（關於）視窗將顯示 `FIPS-CC` 模式失敗錯誤訊息： 	重新啟動應用程式以清除錯誤狀態。如果問題仍然存在，請解除安裝然後重新安裝應用程式。

問題	說明	解決方案
		
由於 FIPS 條件自測失敗，GlobalProtect 應用程式無法在 FIPS-CC 模式下建立連線。	當 GlobalProtect 應用程式在 FIPS-CC 模式下初始化後，將執行 FIPS 條件自測。如果自測失敗，GlobalProtect 應用程式將終止工作階段並保持中斷連線。	若要建立 GlobalProtect 連線，您必須重新對 GlobalProtect 入口網站進行驗證。

如果 *GlobalProtect* 無法在 *FIPS-CC* 模式下初始化或連線，您可存取 *GlobalProtect* 設定面板中的 *Troubleshooting*（疑難排解）頁籤以檢視和收集用於疑難排解的日誌。*GlobalProtect* 成功連線之前，所有其他頁籤均不可用。

GlobalProtect 快速設定

以下幾節提供設定某些通用 GlobalProtect™ 部署的逐步指示：

遠端存取 VPN（驗證設定檔）

遠端存取 GlobalProtect VPN 中，GlobalProtect 入口網站與閘道均設定於 **ethernet1/2**，且 ethernet1/2 也正是 GlobalProtect 使用者連線的實體介面。使用者連線並向入口網站與閘道驗證之後，端點會從其虛擬介面卡建立通道（已為其指定與閘道 tunnel.2 設定相關聯之 IP 配發範圍中的 IP 位址—在此範例中為 10.31.32.3-10.31.32.118）。由於 GlobalProtect VPN 通道在個別 **corp-vpn** 區域終止，因此您能夠看到連線流量，並且能夠為遠端使用者量身訂製安全政策。

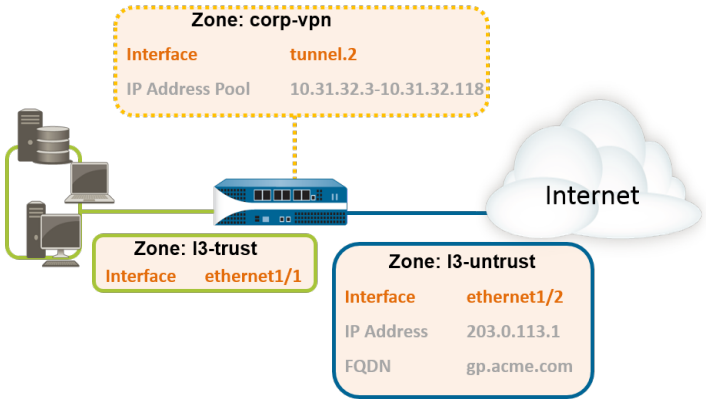


圖 5: 遠端存取的 **GlobalProtect VPN**

STEP 1 | 為 GlobalProtect 建立介面與區域。

針對所有介面設定使用 *default*（預設）虛擬路由器，以防必須建立內部區域路由。

- 選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路）。將 **ethernet1/2** 設定為 Layer 3 Ethernet 介面，且 IP 位址為 203.0.113.1，然後將其指定給 **l3-untrust Security Zone**（安全性區域）與預設 **Virtual Router**（虛擬路由器）。
- 建立將 IP 位址 **203.0.113.1** 對應至 **gp.acme.com** 的 DNS「A」記錄。
- 選取 **Network**（網路）> **Interfaces**（介面）> **Tunnel**（通道），然後 **Add**（新增）**tunnel.2** 介面。將通道介面 **Add**（新增）至名為 **corp-vpn** 的新 **Security Zone**（安全性區域），然後將其指定至預設 **Virtual Router**（虛擬路由器）。
- 在 **corp-vpn** 區域上啟用使用者識別。

STEP 2 | 建立安全政策來啟用 corp-vpn 區域與 l3-trust 區域之間的流量，以讓您存取內部資源。

1. 選取 **Policies**（原則）> **Security**（安全性），然後按一下 **Add**（新增）新的規則。
2. 以此為例，您可以定義設定如下的規則：
   - **Name**（名稱）（**General**（一般）頁籤）—VPN 存取
   - **Source Zone**（來源區域）（**Source**（來源）頁籤）—corp-vpn
   - **Destination Zone**（目的地區域）（**Source**（目的地）頁籤）—l3-trust

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 3 | 使用下列方法之一獲得介面伺服器憑證，裝載 GlobalProtect 入口網站和閘道：

- （建議）從廣為人知的協力廠商 CA 匯入伺服器憑證。

- 使用入口網站上的根 CA，以建立自我簽署伺服器憑證。

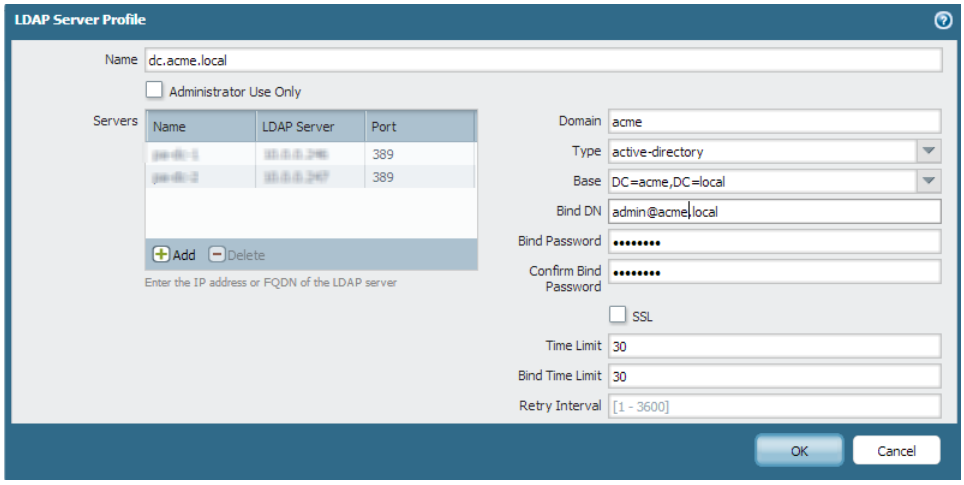
選取 **Device**（新增）> **Certificate Management**（憑證管理）> **Certificates**（憑證）來管理憑證，如下：

- 取得伺服器憑證。由於入口網站與閘道在相同介面上，因此可將相同的伺服器憑證用於這兩個元件。
- 憑證的 CN 必須符合 FQDN `gp.acme.com`。
- 若要讓使用者連線至入口網站而不接收憑證錯誤，請使用公開 CA 中的伺服器憑證。

STEP 4 | 建立伺服器設定檔

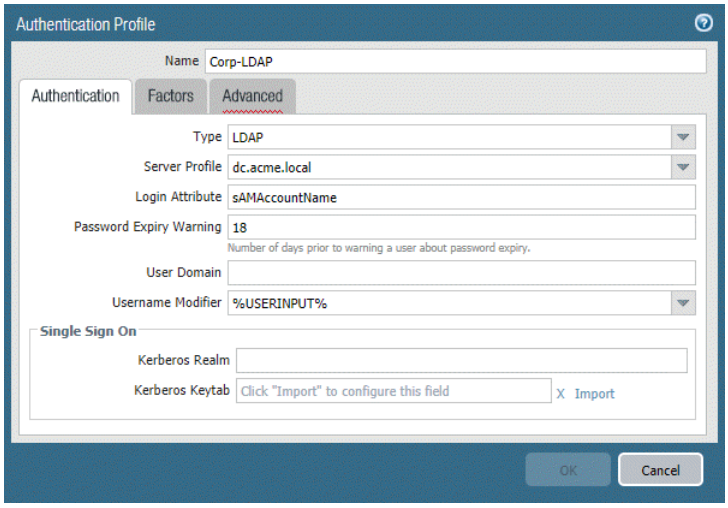
伺服器設定檔會指示防火牆連線至驗證伺服器的方式。支援本機、RADIUS、Kerberos、SAML 與 LDAP 驗證方法。此範例顯示用於針對 Active Directory 驗證使用者的 LDAP 驗證設定檔。

建立用於連線至 LDAP 伺服器的伺服器設定檔（**Device**（裝置）> **Server Profiles**（伺服器設定檔）> **LDAP**）。



STEP 5 | （選用）建立驗證設定檔。

將伺服器設定檔附加至驗證設定檔（**Device**（裝置）> **Authentication Profile**（驗證設定檔））。



STEP 6 | 設定 GlobalProtect 閘道。

選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道），然後 **Add**（新增）下列設定：

IP Address（IP 位址）—**`ethernet1/2`**

IP 位址—203.0.113.1

Server Certificate（伺服器憑證）—GP-server-cert.pem issued by GoDaddy

Authentication Profile（驗證設定檔）—Corp-LDAP

Tunnel Interface（通道介面）—tunnel.2

IP Pool（IP 集區）—10.31.32.3 - 10.31.32.118

STEP 7 | 設定 GlobalProtect 入口網站。

選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後 **Add**（新增）下列設定：

1. 設定 GlobalProtect 入口網站存取權。

   IP Address（IP 位址）—ethernet1/2

   IP 位址—203.0.113.1

   Server Certificate（伺服器憑證）—GP-server-cert.pem issued by GoDaddy

   Authentication Profile（驗證設定檔）—Corp-LDAP
2. 定義 GlobalProtect 用戶端驗證組態：

   Connect Method（連線方法）—On-demand（由使用者手動初始的連線）

   External Gateway Address（外部閘道位址）—gp.acme.com

STEP 8 | 部署 GlobalProtect 應用程式軟體。

選取 **Device**（裝置）> **GlobalProtect Client**（GlobalProtect 用戶端）。按照程序在入口網站裝載應用程式更新。

STEP 9 | （選用）啟用對 GlobalProtect 行動應用程式的使用。

購買並安裝 GlobalProtect 訂閱（**Device**（裝置）> **Licenses**（授權））來啟用對應用程式的使用。

STEP 10 | 儲存 GlobalProtect 設定。

按一下 **Commit**（交付）。

遠端存取 VPN（憑證設定檔）

對於憑證驗證，使用者必須出示有效的用戶端憑證，識別至 GlobalProtect 入口網站或閘道的使用者。除了憑證本身外，入口網站或閘道可使用憑證設定檔確定遞送憑證的使用者是否是發出憑證的使用者。

當作用戶端憑證為驗證的唯一方法使用時，使用者出示的憑證必須在其中一個憑證欄位中包含使用者名稱；使用者名稱通常會對應至憑證之 [主旨] 欄位中的通用名稱 (CN)。

如成功驗證，GlobalProtect 應用程式會建立具有閘道的通道，並會在閘道的通道設定中為其指定 IP 配發範圍中的 IP 位址。若要從 **corp-vpn** 區域對工作階段啟用以使用者為基礎的政策強制執行，憑證中的使用者名稱會對應至由閘道所指定的 IP 位址。如果安全性原則除使用者名稱外還需要網域名稱，憑證設定檔內的指定網域值可附加至使用者名稱。

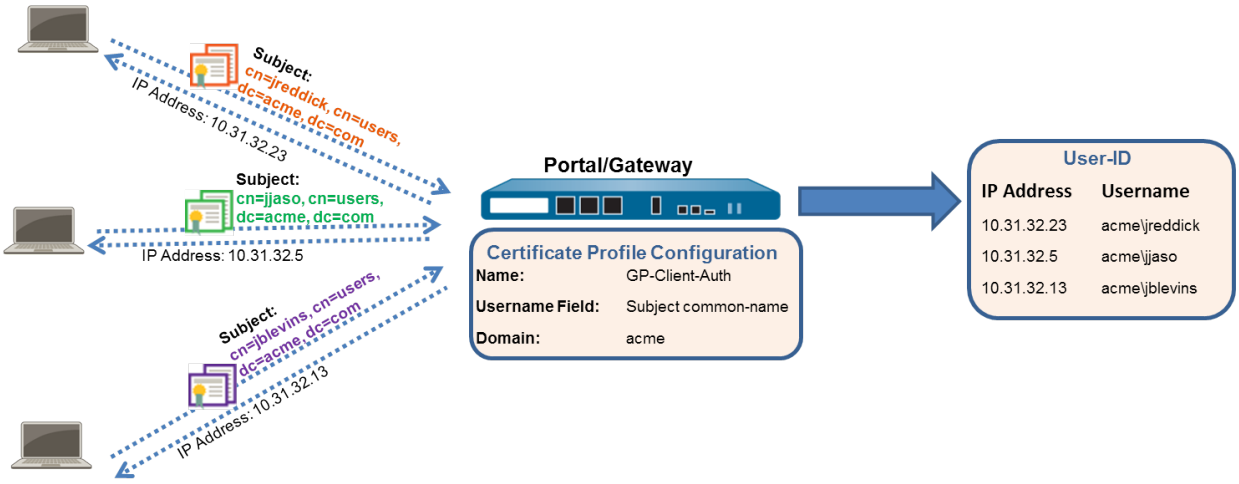


圖 6: GlobalProtect 用戶端憑證驗證設定

此快速設定使用相同的拓撲作為遠端存取的 GlobalProtect VPN。唯一的設定差異是，此設定只使用用戶端憑證驗證，而非針對外部驗證伺服器驗證使用者。

STEP 1 | 為 GlobalProtect 建立介面與區域。

針對所有介面設定使用 *default*（預設）虛擬路由器，以防必須建立內部區域路由。

- 選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路）。將 **ethernet1/2** 設定為 Layer 3 Ethernet 介面，且 IP 位址為 **203.0.113.1**，然後將其指定給 **l3-untrust Security Zone**（安全性區域）與預設 **Virtual Router**（虛擬路由器）。
- 建立將 IP 位址 **203.0.113.1** 對應至 **gp.acme.com** 的 DNS「A」記錄。

- 選取 **Network**（網路）> **Interfaces**（介面）> **Tunnel**（通道），然後 **Add**（新增）**tunnel.2** 介面。將通道介面新增至名為 `corp-vpn` 的新 **Security Zone**（安全性區域），然後將其指定至預設 **Virtual Router**（虛擬路由器）。
- 在 **corp-vpn** 區域上啟用使用者識別。

STEP 2 | 建立安全政策來啟用 **corp-vpn** 區域與 **l3-trust** 區域之間的流量，以讓您存取內部資源。

1. 選取 **Policies**（原則）> **Security**（安全性），然後按一下 **Add**（新增）新的規則。
2. 以此為例，您可以定義設定如下的規則：
   - **Name**（名稱）（**General**（一般）頁籤）—**VPN Access**
   - **Source Zone**（來源區域）（**Source**（來源）頁籤）—**corp-vpn**
   - **Destination Zone**（目的地區域）（**Source**（目的地）頁籤）—**l3-trust**

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 3 | 使用下列方法之一獲得介面伺服器憑證，裝載 GlobalProtect 入口網站和閘道：

- （建議）從廣為人知的協力廠商 CA 匯入伺服器憑證。
- 使用入口網站上的根 CA，以建立自我簽署伺服器憑證。

選取 **Device**（新增）> **Certificate Management**（憑證管理）> **Certificates**（憑證）來管理憑證，如下：

- 取得伺服器憑證。由於入口網站與閘道在相同介面上，因此可將相同的伺服器憑證用於這兩個元件。
- 憑證的 CN 必須符合 FQDN `gp.acme.com`。
- 若要讓使用者連線至入口網站而不接收憑證錯誤，請使用公開 CA 中的伺服器憑證。

STEP 4 | 將用戶端憑證發出至 GlobalProtect 用戶端和端點。

1. 使用您的企業 PKI 或公開 CA 將唯一的用戶端憑證發出給每個 GlobalProtect 使用者。
2. 在端點的個人憑證存放區中安裝憑證。

STEP 5 | 建立用戶端憑證設定檔。

1. 選取 **Device**（裝置）> **Certificates Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。**Add**（新增）新的憑證設定檔，然後輸入設定檔 **Name**（名稱），例如 **GP-client-cert**。
2. 從 **Username Field** 下拉式清單中選取主旨。
3. 在 **CA Certificates**（**CA** 憑證）區域，**Add**（新增）簽發用戶端憑證的 CA 憑證。按兩下 **OK**（確定）。

STEP 6 | 設定 GlobalProtect 閘道。

請參閱在遠端存取的 GlobalProtect VPN 中顯示的拓樸圖表。

選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道），然後 **Add**（新增）下列設定：

IP Address（**IP** 位址）—**ethernet1/2**

IP Address（**IP** 位址）—**203.0.113.1**

Server Certificate（伺服器憑證）—**GP-server-cert.pem issued by GoDaddy**

Certificate Profile（憑證設定檔）—**GP-client-cert**

Tunnel Interface（通道介面）—**tunnel.2**

IP Pool（**IP** 集區）—**10.31.32.3 - 10.31.32.118**

STEP 7 | 設定 GlobalProtect 入口網站。

選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後 **Add**（新增）下列設定：

1. 設定 GlobalProtect 入口網站存取權。

   IP Address（**IP** 位址）—`ethernet1/2`

   IP Address（**IP** 位址）—`203.0.113.1`

   Server Certificate（伺服器憑證）—`GP-server-cert.pem issued by GoDaddy`

   Certificate Profile（憑證設定檔）—`GP-client-cert`
2. 定義 GlobalProtect 代理程式組態：

   Connect Method（連線方法）—`On-demand`（由使用者手動初始的連線）

   External Gateway Address（外部閘道位址）—`gp.acme.com`

STEP 8 | 部署 GlobalProtect 應用程式軟體。

選取 **Device**（裝置）> **GlobalProtect Client**（**GlobalProtect** 用戶端）。按照程序在入口網站裝載應用程式更新。

STEP 9 | （選用）啟用對 GlobalProtect 行動應用程式的使用。

購買並安裝 GlobalProtect 訂閱（**Device**（裝置）> **Licenses**（授權））來啟用對應用程式的使用。

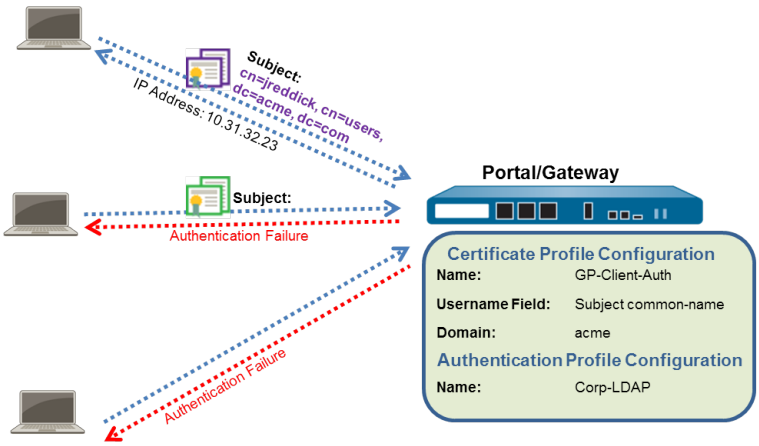
STEP 10 | 儲存 GlobalProtect 設定。

按一下 **Commit**（交付）。

使用雙因素驗證的遠端存取 VPN

如果您透過驗證設定檔和憑證設定檔設定 GlobalProtect 入口網站或閘道（可以同提供雙因素驗證），一般使用者在獲得存取權之前必須透過兩個設定檔獲得驗證。對於入口網站驗證而言，這表示在憑證的初始入口網站連線之前，必須將其預先部署至端點。此外，使用者所出示的用戶端憑證必須與憑證設定檔中所定義的憑證相符

- 如果憑證設定檔未指定使用者名稱欄位（將 **Username Field**（使用者名稱欄位）設定為 **None**（無）），用戶端憑證將不需要使用者名稱。在這種情況下，針對驗證設定檔進行驗證時，使用者必須提供使用者名稱。
- 如果憑證設定檔指定使用者名稱欄位，使用者出示的憑證必須在對應欄位中包含使用者名稱。例如，如果憑證設定檔指定使用者名稱欄位為 **Subject**（主旨），則使用者出示的憑證必須在通用名稱欄位中包含值，否則驗證將失敗。此外，當需要使用者名稱欄位時，如果使用者嘗試輸入認證以對驗證設定檔進行驗證，則會自動將憑證之使用者名稱欄位中的值填入為使用者名稱。如果您不想強制使用者使用憑證中的使用者名稱驗證，請不要在憑證設定檔中指定使用者名稱欄位。



此快速設定使用相同的拓撲作為遠端存取的 GlobalProtect VPN。但是，在此設定中，使用者必須對憑證設定檔與驗證設定檔進行驗證。如需雙因素驗證特定類型的詳細資訊，請參閱下列主題：

- 透過憑證和驗證設定檔啟用雙因素驗證
- 使用一次性密碼 (OTP) 啟用雙因素驗證
- 使用智慧卡啟用雙因素驗證
- 使用軟體權杖應用程式啟用雙因素驗證

使用下列程序設定帶雙因素驗證的遠端 VPN 存取。

STEP 1 | 為 GlobalProtect 建立介面與區域。

針對所有介面設定使用 *default*（預設）虛擬路由器，以防必須建立內部區域路由。

- 選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路）。將 **ethernet1/2** 設定為 **Layer3** Ethernet 介面，且 IP 位址為 `203.0.113.1`，然後將其指定給 `l3-untrust` **Security Zone**（安全性區域）與預設 **Virtual Router**（虛擬路由器）。
- 建立將 IP 位址 `203.0.113.1` 對應至 `gp.acme.com` 的 DNS「A」記錄。
- 選取 **Network**（網路）> **Interfaces**（介面）> **Tunnel**（通道），然後 **Add**（新增）**tunnel.2** 介面。將通道介面新增至名為 `corp-vpn` 的新 **Security Zone**（安全性區域），然後將其指定至預設 **Virtual Router**（虛擬路由器）。

- 在 **corp-vpn** 區域上啟用使用者識別。

STEP 2 | 建立安全政策來啟用 **corp-vpn** 區域與 **l3-trust** 區域之間的流量，以讓您存取內部資源。

1. 選取 **Policies**（原則）> **Security**（安全性），然後按一下 **Add**（新增）以建立新的規則。
2. 以此為例，您可以定義設定如下的規則：
   - **Name**（名稱）（**General**（一般）頁籤）—**VPN Access**
   - **Source Zone**（來源區域）（**Source**（來源）頁籤）—**corp-vpn**
   - **Destination Zone**（目的地區域）（**Source**（目的地）頁籤）—**l3-trust**

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 3 | 使用下列方法之一獲得介面伺服器憑證，裝載 GlobalProtect 入口網站和閘道：

- （建議）從廣為人知的協力廠商 CA 匯入伺服器憑證。
- 使用入口網站上的根 CA，以建立自我簽署伺服器憑證。

選取 **Device**（新增）> **Certificate Management**（憑證管理）> **Certificates**（憑證）來管理憑證，如下：

- 取得伺服器憑證。由於入口網站與閘道在相同介面上，因此可將相同的伺服器憑證用於這兩個元件。
- 憑證的 CN 必須符合 FQDN **gp.acme.com**。
- 若要讓使用者連線至入口網站而不接收憑證錯誤，請使用公開 CA 中的伺服器憑證。

STEP 4 | 將用戶端憑證發出至 GlobalProtect 用戶端和端點。

1. 使用您的企業 PKI 或公開 CA 將唯一的用戶端憑證發出給每個 GlobalProtect 使用者。
2. 在端點的個人憑證存放區中安裝憑證。

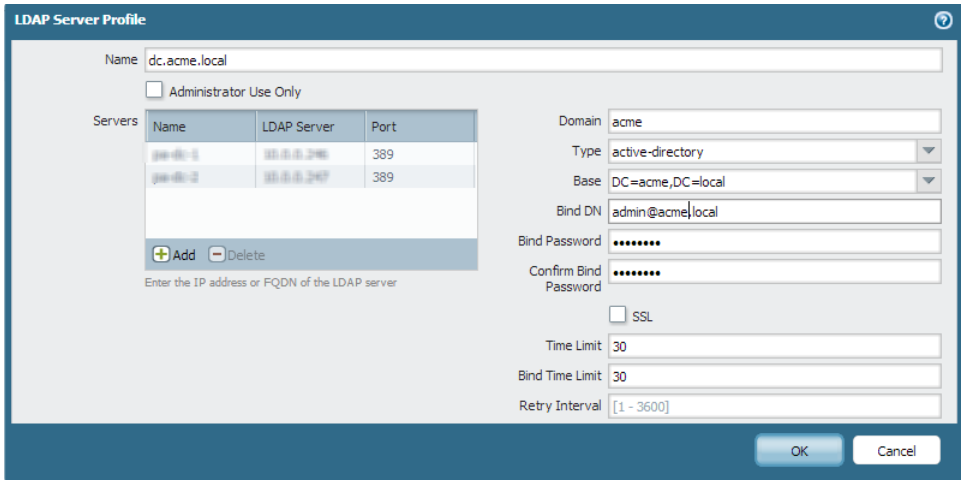
STEP 5 | 建立用戶端憑證設定檔。

1. 選取 **Device**（裝置）> **Certificates Management**（憑證管理）> **Certificate Profile**（憑證設定檔）。**Add**（新增）新的憑證設定檔，然後輸入設定檔 **Name**（名稱），例如 **GP-client-cert**。
2. 指定取得將用來驗證一般使用者之使用者名稱的位置。
   - 從使用者—如果您想讓一般使用者在對驗證設定檔中所指定的服務進行驗證時提供使用者名稱，請選取 **None**（無）作為 **Username Field**（使用者名稱欄位）。
   - 從憑證—如果您想從憑證擷取使用者名稱，請選取 **Subject**（主旨）作為 **Username Field**（使用者名稱欄位）。如果您使用此選項，當提示使用者登入入口網站/閘道時，包含在憑證中的 CN 將自動填入使用者名稱欄位。需要使用者使用該使用者名稱登入。
3. 在 **CA Certificates**（**CA** 憑證）區域，**Add**（新增）簽發用戶端憑證的 CA 憑證。按兩下 **OK**（確定）。

STEP 6 | 建立伺服器設定檔

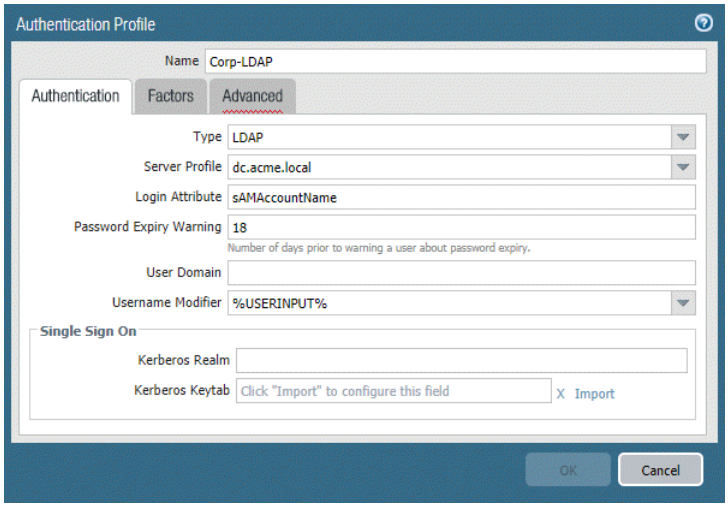
伺服器設定檔會指示防火牆連線至驗證伺服器的方式。支援本機、RADIUS、Kerberos、SAML 與 LDAP 驗證方法。此範例顯示用於針對 Active Directory 驗證使用者的 LDAP 驗證設定檔。

建立用於連線至 LDAP 伺服器的伺服器設定檔（**Device**（裝置）> **Server Profiles**（伺服器設定檔）> **LDAP**）。



STEP 7 | （選用）建立驗證設定檔。

將伺服器設定檔附加至驗證設定檔（**Device**（裝置）**Authentication Profile**（驗證設定檔））。



STEP 8 | 設定 GlobalProtect 閘道。

請參閱在遠端存取的 GlobalProtect VPN 中顯示的拓樸圖表。

選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道），然後 **Add**（新增）下列設定：

IP Address（IP 位址）—`ethernet1/2`

IP Address（IP 位址）—`203.0.113.1`

Server Certificate（伺服器憑證）—`GP-server-cert.pem issued by GoDaddy`

Certificate Profile（憑證設定檔）—`GP-client-cert`

Authentication Profile（驗證設定檔）—`Corp-LDAP`

Tunnel Interface（通道介面）—`tunnel.2`

IP Pool（IP 集區）—`10.31.32.3 - 10.31.32.118`

STEP 9 | 設定 GlobalProtect 入口網站。

選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後 **Add**（新增）下列設定：

1. 設定 GlobalProtect 入口網站存取權。

   IP Address（**IP** 位址）—**ethernet1/2**

   IP Address（**IP** 位址）—**203.0.113.1**

   Server Certificate（伺服器憑證）—**GP-server-cert.pem issued by GoDaddy**

   Certificate Profile（憑證設定檔）—**GP-client-cert**

   Authentication Profile（驗證設定檔）—**Corp-LDAP**
2. 定義 GlobalProtect 代理程式組態：

   Connect Method（連線方法）—**On-demand**（由使用者手動初始的連線）

   External Gateway Address（外部閘道位址）—**gp.acme.com**

STEP 10 | 部署 GlobalProtect 應用程式軟體。

選取 **Device**（裝置）> **GlobalProtect Client**（**GlobalProtect** 用戶端）。。按照程序在入口網站裝載應用程式更新。

STEP 11 | （選用）明顯部署應用程式設定。

從入口網站設定部署應用程式設定還有一種可行的方法，即直接透過 Windows 登錄或全域 macOS plist 定義設定。您可以在使用者登入端點並連線至 GlobalProtect 入口網站之前，部署包括指定入口網站 IP 位址或啟用 GlobalProtect 以啟動 VPN 通道的設定範例。僅在 Windows 端點上，您也可以透過 MSIEXEC 安裝程式進行設定。如需其他資訊，請參閱可自訂應用程式設定。

STEP 12 | （選用）啟用對 GlobalProtect 行動應用程式的使用。

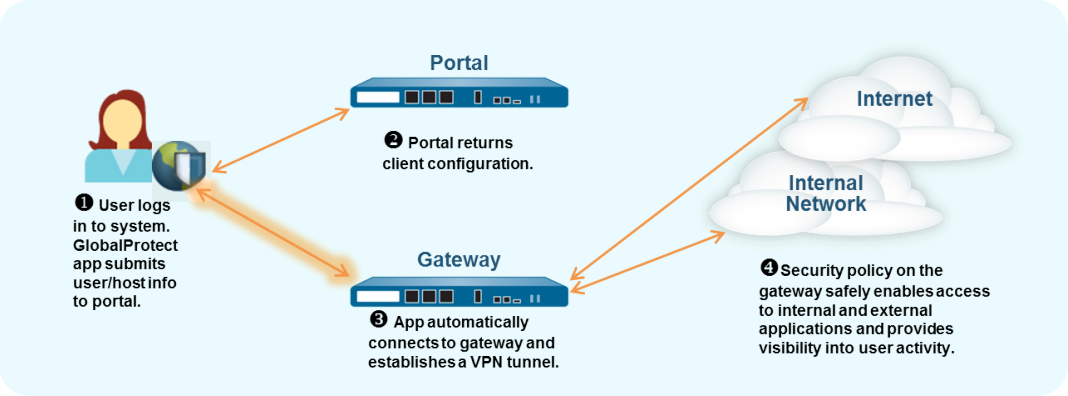
購買並安裝 GlobalProtect 訂閱（**Device**（裝置）> **Licenses**（授權））來啟用對應用程式的使用。

STEP 13 | 儲存 GlobalProtect 設定。

按一下 **Commit**（交付）。

一直開啟 VPN 設定

在「一直開啟」的 GlobalProtect 設定中，應用程式會連線至 GlobalProtect 入口網站（在使用者登入時），以提交使用者與主機資訊，並接收用戶端組態。然後應用程式會自動連線並建立至入口網站所傳遞用戶端組態中指定閘道的 VPN 通道，如下圖所示：



若要將下列遠端存取 VPN 設定其中之一切換為一直開啟設定，您只需變更連線方法即可：

- 遠端存取 VPN（驗證設定檔）
- 遠端存取 VPN（憑證設定檔）
- 使用雙因素驗證的遠端存取 VPN

使用下列步驟將一個遠端存取 VPN 設定切換為一直開啟設定。

STEP 1 | 選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後選取入口網站組態。

STEP 2 | 在 **Agent**（代理程式）頁籤上，選取您要修改的代理程式組態。

STEP 3 | 選取 **App**（應用程式），然後將 **Connect Method**（連線方法）設定為 **User-logon (Always On)**（使用者登入（一直開啟））。

STEP 4 | 按一下 **OK**（確定）儲存代理程式組態。

STEP 5 | 針對您要修改的每個代理程式組態，重複步驟 2-4。

STEP 6 | 按一下**OK**（確定）儲存入口網站組態，然後**Commit**（提交）變更。

使用預先登入的遠端存取 VPN

預登入 是在使用者登入之前建立 VPN 通道的連線方法。預登入的目的是驗證端點（而非使用者），然後讓網域指令碼或其他工作可以在端點開啟後盡快運行。電腦憑證讓端點能夠建立通向 GlobalProtect 閘道的 VPN 通道。電腦憑證讓端點能夠建立通向 GlobalProtect 閘道的 VPN 通道。IT 管理員的普通做法是在使用者端點預備階段安裝電腦憑證。

預登入 VPN 通道無使用者名稱關聯，因為使用者尚未登入。若要允許端點可在信任區域內存取資源，您必須建立與預登入使用者相符的原則。這些原則應該只允許存取啟動系統所需的基本服務，例如 DHCP、DNS、Active Directory（例如變更過期密碼）、防毒與/或作業系統更新服務。在使用者閘道驗證向後，GlobalProtect 應用程式會將 VPN 通道重新指派至該使用者（防火牆上的 IP 位址對應從預登入端點變為已驗證使用者）。

Windows 7 與 Windows 10 端點的 GlobalProtect 認證提供者登入畫面還會在使用者登入之前顯示預登入連線狀態，這會讓一般使用者確定登入時其是否能夠存取網路資源。如果 GlobalProtect 應用程式偵測到內部端點，則登入畫面會顯示內部預登入連線狀態。如果 Globalprotect 應用程式偵測到外部端點，則登入畫面會顯示已連線或 未連線預登入連線狀態。

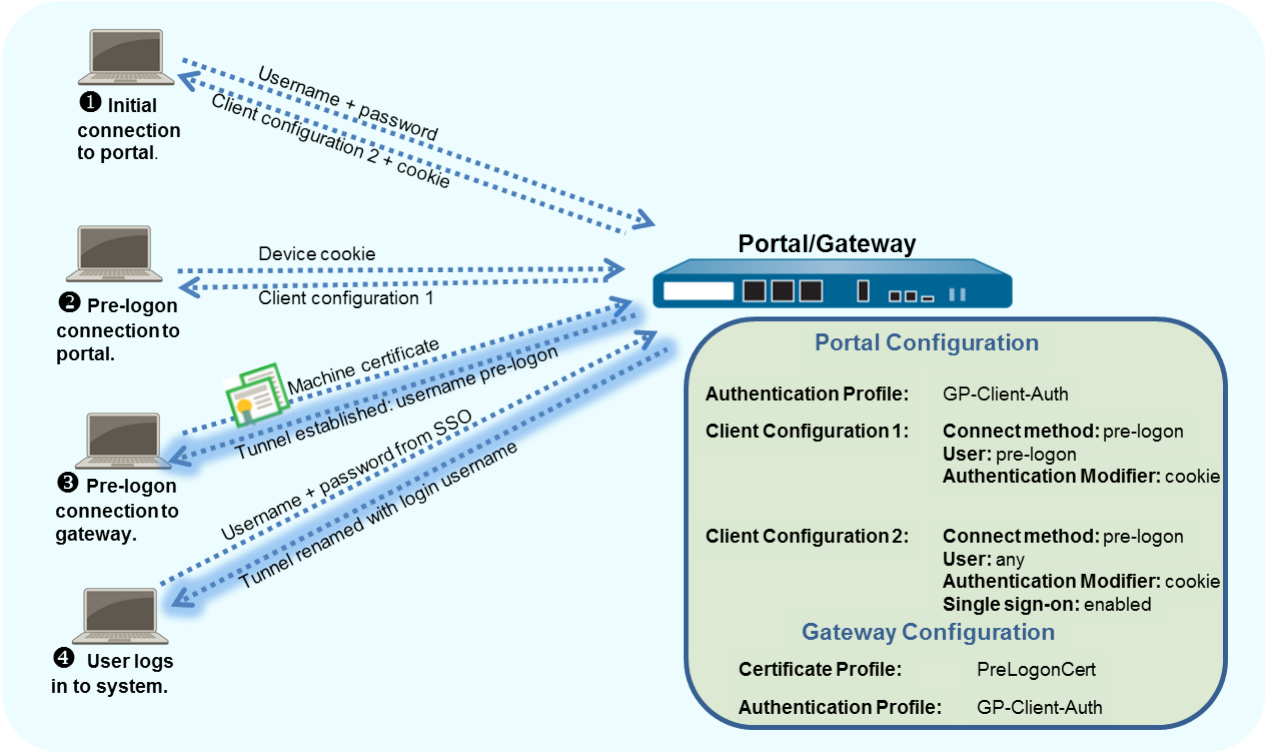
透過預登入連線時，*Windows* 端點的行為與 *macOS* 端點不同。在 *macOS* 端點上，預登入通道在使用者登入時被卸除，並建立一個新通道。

當使用者請求新連線時，入口網站透過驗證設定檔驗證使用者。入口網站也可使用可選用的憑證設定檔，驗證用戶端憑證（如果組態包含用戶端憑證）。在此情況下，憑證必須識別使用者。在驗證後，入口網站確定端點的 GlobalProtect 組態是否為當前狀態。如果入口網站組態變更，其推送更新的組態至端點。

如果入口網站上的組態，或閘道包含基於 cookie 的驗證，入口網站或閘道在端點上安裝加密的 cookie。之後，入口網站或閘道使用 cookie 驗證使用者，並重新整理代理程式組態。如果代理程式組態設定檔包含 cookie 驗證以外的預登入連線方法，GlobalProtect 元件可使用 cookie 進行預登入。

如果使用者不曾登入端點（例如無周邊端點）或需要在使用者之前未登入的系統上執行預先登入連線，您可以讓端點啟動預先登入通道，而不連線到入口網站以下載預先登入組態。要實現此操作，您必須透過在 Windows 登錄或 macOS Plist 中建立項目，取代預設行為。

GlobalProtect 端點將連線至在組態中指定的入口網站、使用其電腦憑證（如在閘道上設定之憑證設定檔所指定）驗證端點，並建立 GlobalProtect 連線。當一般使用者隨後登入機器時，且如果單一登入 (SSO) 已在代理程式組態中啟用，使用者名稱和密碼將在使用者登入時被擷取。如果 SSO 未在代理程式組態中啟用，或端點上不支援 SSO（例如，macOS 系統），則使用者的認證必須儲存在應用程式中（**Save User Credentials**（儲存使用者認證）選項必須設定為 **Yes**（是））。成功驗證閘道之後，通道將會重新命名 (Windows) 或重建 (macOS)，並強制執行以使用者與群組為基礎的原則。



此範例使用遠端存取的 GlobalProtect VPN 中所顯示的 GlobalProtect 拓撲。

STEP 1 | 為 GlobalProtect 建立介面與區域。

針對所有介面設定使用 *default*（預設）虛擬路由器，以防必須建立內部區域路由。

- 在此範例中，請選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路）頁籤，然後進行下列設定：
  1. 選取 **ethernet1/2**。
  2. 從 **Interface Type**（介面類型）下拉式清單中選取 **Layer 3**。
  3. 在 **Config**（設定）頁籤上，**Assign interface to**（將介面指定為）預設 **Virtual Router**（虛擬路由器）和 **`l3-untrust`** **Security Zone**（安全性區域）。
  4. 在 **IPv4** 頁籤上，按一下 **Add**（新增）以選取 **`203.0.113.1`** IP 位址（或與 **`203.0.113.1`** 對應的物件）或新增 **New Address**（新位址）以建立新物件與位址對應（將位址類型保留為 **Static**（靜態））。例如，建立將 IP 位址 **`203.0.113.1`** 對應至 **`gp.acme.com`** 的 **`DNS`**「**`A`**」記錄。
- 選取 **Network**（網路）> **Interfaces**（介面）> **Tunnel**（通道）以 **Add**（新增）新的通道介面。
  1. 對於 **Interface Name**（介面名稱），則輸入 **`tunnel.2`**。
  2. 在 **Config**（設定）頁籤上，**Assign Interface To**（將介面指定為）名為 **`corp-vpn`** 的新 **Security Zone**（安全性區域）和預設 **Virtual Router**（虛擬路由器）。
- 在 **`corp-vpn`** 區域上啟用使用者識別。

STEP 2 | 建立安全性原則規則。

此組態需要下列原則（**Policies**（原則）> **Security**（安全性））：

1. **Add**（新增）可讓預先登入使用者存取啟動端點所需之基本服務的規則，例如驗證服務、DNS、DHCP 與 Microsoft 更新。
2. **Add**（新增）規則以否認預先登入使用者對所有其他目的地和應用程式的存取權。
3. **Add**（新增）任何其他規則以讓不同使用者或使用者群組能夠存取特定目的地與應用程式。請依照 最佳做法網際網路閘道安全性原則 建議來建立這些規則。

STEP 3 | 使用下列方法之一獲得介面伺服器憑證，裝載 GlobalProtect 入口網站和閘道：

- （建議）從廣為人知的協力廠商 CA 匯入伺服器憑證。
- 使用入口網站上的根 CA，以建立自我簽署伺服器憑證。

選取 **Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）來管理憑證，條件如下：

- 取得伺服器憑證。由於入口網站與閘道在相同介面上，因此可將相同的伺服器憑證用於這兩個元件。
- 憑證的 CN 必須符合 FQDN `gp.acme.com`。
- 若要讓端點連線至入口網站而不接收憑證錯誤，請使用公開 CA 中的伺服器憑證。

STEP 4 | 針對將連線至 GlobalProtect 的每個端點產生電腦憑證，然後將憑證匯入至每個電腦上的個人憑證存放區。

雖然您可以針對每個端點產生自我簽署憑證，但最佳作法是使用您自己的公開金鑰基礎結構 (PKI) 來將憑證發出並散佈至端點。

1. 將用戶端憑證發出至 GlobalProtect 用戶端和端點。
2. 在端點的個人憑證存放區中安裝憑證。（Windows 上的本機電腦存放區或 macOS 端點上的系統金鑰鏈）

STEP 5 | 從發出電腦憑證的 CA 將信任的根 CA 憑證匯入至入口網站與閘道：

您無須匯入私人金鑰。

1. 下載 Base64 格式的 CA 憑證。
2. 使用下列步驟將憑證匯入至裝載入口網站或閘道的每個防火牆：
   1. 選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證），然後 **Import**（匯入）憑證。
   2. 輸入作為用戶端 CA 憑證識別的 **Certificate Name**（憑證名稱）。
   3. **Browse**（瀏覽）從 CA 下載的 **Certificate File**（憑證檔案）。
   4. 將 **File Format**（檔案格式）設定為 **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**）。
   5. 按一下 **OK**（確定）儲存您的憑證。
   6. 在 **Device Certificates**（裝置憑證）頁籤上，選取剛才匯入的憑證。
   7. 選取 **Trusted Root CA**（信任根 **CA**）核取方塊，然後按一下 **OK**（確定）。

STEP 6 | 在裝載 GlobalProtect 閘道的每個防火牆上，建立憑證設定檔以識別要用來驗證電腦憑證的 CA 憑證。

如果您要使用用戶端憑證驗證來在使用者登入系統時對其進行驗證，請確保在憑證設定檔中除了參考發出電腦憑證的 CA 憑證之外，也參考發出用戶端憑證的 CA 憑證（若這兩個憑證不同）。

1. 選取 **Device**（設備）> **Certificates**（憑證）> **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔），然後 **Add**（新增）新的憑證設定檔。
2. 輸入用來識別設定檔的 **Name**（名稱），例如 **`PreLogonCert`**。
3. 將 **Username Field**（使用者名稱欄位）設定為 **None**（無）。
4. （選用）如果您也將使用用戶端憑證驗證來在登入時驗證使用者，請新增發出用戶端憑證的 CA 憑證（若其與發出電腦憑證的 CA 憑證不同）。
5. 在 **CA Certificates**（**CA** 憑證）欄位中，**Add**（新增）CA 憑證。
6. 選取您在步驟 5 中匯入的受信任根 **CA Certificate**（**CA** 憑證），然後按一下 **OK**（確定）。
7. 按一下 **OK**（確定）來儲存設定檔。

STEP 7 | 設定 GlobalProtect 閘道。

請參閱在遠端存取的 GlobalProtect VPN 中顯示的拓樸圖表。

雖然您必須針對閘道的預先登入存取建立憑證設定檔，但您可以將用戶端憑證驗證或以驗證設定檔為基礎的驗證用於登入使用者。在此範例中，會使用用來針對入口網站驗證使用者的相同 LDAP 設定檔。

1. 選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道），然後 **Add**（新增）下列閘道設定：

   IP Address（**IP** 位址）—**`ethernet1/2`**

   IP Address（**IP** 位址）—**`203.0.113.1`**

   Server Certificate（伺服器憑證）—**`GP-server-cert.pem issued by GoDaddy`**

   Certificate Profile（憑證設定檔）—**`PreLogonCert`**

   Authentication Profile（驗證設定檔）—**`Corp-LDAP`**

   Tunnel Interface（通道介面）—**`tunnel.2`**

   IP Pool（**IP** 集區）—**`10.31.32.3 - 10.31.32.118`**
2. **Commit**（提交）閘道設定。

STEP 8 | 設定 GlobalProtect 入口網站。

設定 **Device**（裝置）詳情（網路參數、憑證服務設定檔和驗證伺服器憑證）。

選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後 **Add**（新增）下列入口網站設定：

設定 GlobalProtect 入口網站存取權。

IP Address（**IP** 位址）—**`ethernet1/2`**

IP Address（**IP** 位址）—**`203.0.113.1`**

Server Certificate（伺服器憑證）—**`GP-server-cert.pem issued by GoDaddy`**

Certificate Profile（憑證設定檔）—**`None`**

Authentication Profile（驗證設定檔）—`Corp-LDAP`

STEP 9 | 為預登入使用者和登入使用者定義 GlobalProtect 代理程式組態。

使用單一組態，如果您想要預登入使用者在登入前後存取相同閘道。

若要預登入使用者在登入前後使用不同閘道，請建立兩個組態設定檔。在此第一個組態的 **User/User Group**（使用者/使用者群組）中，選取 **pre-logon**（預登入）篩選器。透過預登入，入口網站首先驗證端點（非使用者），以設定連線（儘管預登入參數與使用者關聯）。之後，入口網站在使用者登入時對其進行驗證。

在入口網站驗證使用者後，其部署第二個組態。在此情況下，**User/User Group**（使用者/使用者群組）為 **any**（任何）。

最佳作法是，在第二個組態中啟用 *SSO*，以確保當使用者登入端點時，立即將正確的使用者名稱報告給閘道。若未啟用 *SSO*，將使用 *Agent*（代理程式）設定面板中儲存的使用者名稱。

選取 **GlobalProtect** 入口網站組態 視窗中的 **Agent**（代理程式） 頁籤（**Network**（網路） > **GlobalProtect** > **Portals**（入口網站） > **<portal-config>**），然後 **Add**（新增） 下列設定之一：

- 在預登入使用者登入前後使用相同的閘道：

Use single sign-on（使用單一登入）—**enabled**

Connect Method（連線方法）—預先登入

External Gateway Address（外部閘道位址）—**gp1.acme.com**

User/User Group（使用者/使用者群組）—**any**

Authentication Override（驗證取代）—透明驗證使用者和組態重新整理的 Cookie 驗證

- 在預登入使用者登入前後，使用分割閘道：

第一個代理程式組態：

Connect Method（連線方法）—預先登入

External Gateway Address（外部閘道位址）—**gp1.acme.com**

User/User Group（使用者/使用者群組）—預先登入

Authentication Override（驗證取代）—透明驗證使用者和組態重新整理的 Cookie 驗證

第二個代理程式組態：

Use single sign-on（使用單一登入）—**enabled**

Connect Method（連線方法）—預先登入

External Gateway Address（外部閘道位址）—**gp2.acme.com**

User/User Group（使用者/使用者群組）—**any**

Authentication Override（驗證取代）—透明驗證使用者和組態重新整理的 Cookie 驗證

請確保預先登入組態是設定清單中的第一個設定。如果不是，請選取它，然後按一下 **Move Up**（上移）。

STEP 10 | 儲存 GlobalProtect 設定。

按一下 **Commit**（交付）。

STEP 11 | （選用）如果使用者不會登入設備（例如無周邊裝置）或需要使用者之前未登入的端點上執行預先登入連線，可在端點上建立 **Prelogon** 登錄項目。

您還必須預先部署預設入口網站 *IP* 位址。

如需關於登錄設定的更多資訊，請參閱明顯部署應用程式設定。

1. 前往下列 Windows 登錄位置以檢視 GlobalProtect 設定清單：

   `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`
2. 選取 **Edit**（編輯） > **New**（新） > **String Value**（字串值） 以建立下列登錄項目：

- 建立名稱為 **Prelogon** 的 **String Value**（字串值），且值為 **1**。此設定啟用 GlobalProtect 以在使用者登入端點之前啟動連線。
- 建立名稱為 **Portal** 的 **String Value**（字串值）入口網站，指定 GlobalProtect 端點預設入口網站的 IP 位址或主機名稱。

GlobalProtect 多閘道設定

在下方的 GlobalProtect 多閘道拓撲中，第二外部閘道已新增至組態。在此拓撲中，您必須設定其他防火牆才能裝載第二個 GlobalProtect 閘道。當您新增將由入口網站部署的用戶端組態時，您還可以為不同用戶端組態指定不同閘道或允許存取所有閘道。

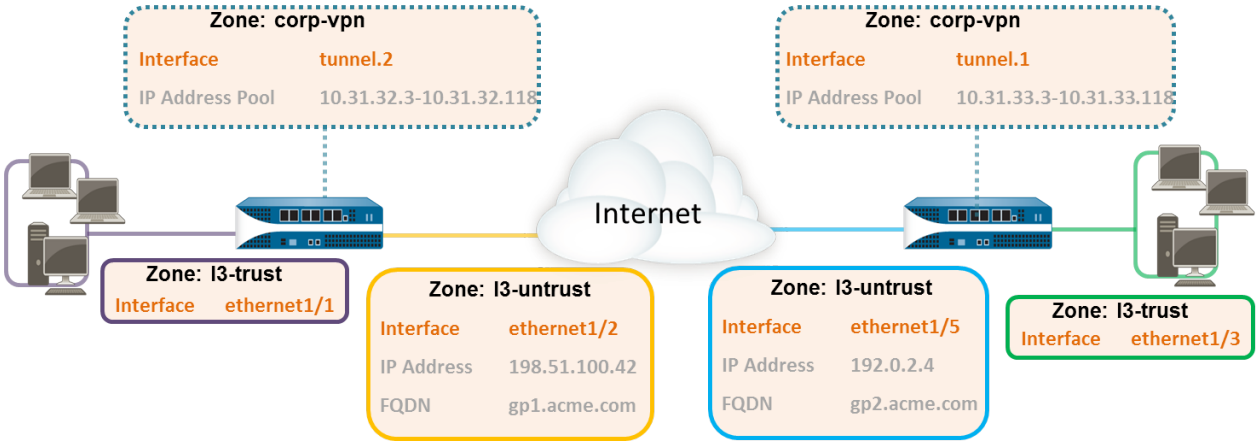


圖 7: GlobalProtect 多閘道拓撲

如果用戶端組態包含多個閘道，應用程式將嘗試連線至其用戶端組態中所列出的所有閘道。應用程式將使用優先順序與回應時間來決定要連線的目標閘道。僅當高優先順序閘道的回應時間大於所有閘道平均回應時間時，應用程式將連線至低優先順序閘道。如需更多訊息，請參閱多個閘道組態中的閘道優先順序。

STEP 1 | 為 GlobalProtect 建立介面與區域。

在此設定中，您必須在裝載閘道的每個防火牆上設定介面。

針對所有介面設定使用 *default*（預設）虛擬路由器，以防必須建立內部區域路由。

在裝載入口網站/閘道 (gw1) 的防火牆上：

- 選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路），然後選取 **ethernet1/2**。
- 將 **ethernet1/2** 設定為 Layer 3 Ethernet 介面，且 IP 位址為 `198.51.100.42`，然後將其指定給 `l3-untrust` **Security Zone**（安全性區域）與 `default` **Virtual Router**（虛擬路由器）。
- 建立將 IP 位址 `198.51.100.42` 對應至 `gp1.acme.com` 的 DNS「A」記錄。
- 選取 **Network**（網路）> **Interfaces**（介面）> **Tunnel**（通道），然後 **Add**（新增）`tunnel.2` 介面。將介面新增至名為 `corp-vpn` 的新 **Security Zone**（安全性區域）。然後再將該介面指定給`default` **Virtual Router**（虛擬路由器）。
- 在 `corp-vpn` 區域上啟用使用者識別。

在裝載第二個閘道 (gw2) 的防火牆上：

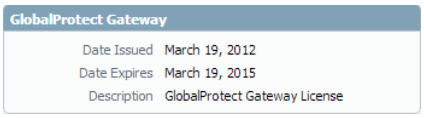
- 選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路），然後選取 **ethernet1/2**。

- 將 **ethernet1/5** 設定為 Layer 3 Ethernet 介面，且 IP 位址為 **192.0.2.4**，然後將其指定給 **l3-untrust Security Zone**（安全性區域）與 **default Virtual Router**（虛擬路由器）。
- 建立將 IP 位址 **192.0.2.4** 對應至 **gp2.acme.com** 的 DNS「A」記錄。
- 選取 **Network**（網路）> **Interfaces**（介面）> **Tunnel**（通道），然後 **Add**（新增）**tunnel.1** 介面。將介面新增至名為 **corp-vpn** 的新 **Security Zone**（安全性區域）。然後再將該介面指定給預設 **Virtual Router**（虛擬路由器）。
- 在 **corp-vpn** 區域上啟用使用者識別。

STEP 2 | 如果您的一般使用者將在行動端點上使用 GlobalProtect 應用程式，或者您想要使用已啟用 HIP 的安全性原則，您需要購買並在各個閘道上安裝 GlobalProtect 訂閱。

購買 GlobalProtect 訂閱並收到啟動碼之後，請在裝載入口網站的防火牆上安裝授權，如下所示：

1. 選取 **Device**（裝置）> **Licenses**（授權）。
2. 選取 **Activate feature using authorization code**（使用授權碼啟動功能）。
3. 出現提示時，請輸入 **Authorization Code**（授權碼），然後按一下 **OK**（確定）。
4. 確認授權已成功啟動：



STEP 3 | 在裝載 GlobalProtect 閘道的每個防火牆上建立安全性原則。

此設定需要安全性原則來啟用 **corp-vpn** 區域與 **l3-trust** 區域之間的流量，以讓您存取內部資源（**Policies**（原則）> **Security**（安全性））。

STEP 4 | 使用下列建議獲得每個介面的伺服器憑證，裝載 GlobalProtect 入口網站和閘道：

- （在裝載入口網站或入口網站/閘道的防火牆上）從廣為人知的協力廠商 CA 匯入伺服器憑證。
- （在僅裝載閘道的防火牆上）使用入口網站上的根 CA，以建立自我簽署伺服器憑證。

在代管入口網站/閘道或閘道的每個防火牆上，選取 **Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）來管理憑證，如下：

- 取得裝載入口網站/gw1 之介面的伺服器憑證。由於入口網站與閘道位於相同介面上，因此您必須使用相同的伺服器憑證。憑證的 CN 必須符合 FQDN `gp1.acme.com`。若要讓端點連線至入口網站而不接收憑證錯誤，請使用公開 CA 中的伺服器憑證。
- 取得裝載 gw2 之介面的伺服器憑證。由於此介面只裝載閘道，因此您可以使用自我簽署的憑證。憑證的 CN 必須符合 FQDN `gp2.acme.com`。

STEP 5 | 定義您將對入口網站與閘道驗證使用者的方式。

必要時，您可以使用憑證設定檔與/或驗證設定檔的任何組合來確保入口網站與閘道的安全性。入口網站與個別閘道也可以使用不同的驗證結構描述。如需逐步指示，請參閱以下幾節：

- 設定外部驗證（驗證設定檔）
- 設定用戶端憑證驗證（憑證設定檔）
- 設定雙因素驗證（權杖或以 OTP 為基礎）

然後，您必須參考您在入口網站與閘道設定中定義的憑證設定檔與/或驗證設定檔。

STEP 6 | 設定 GlobalProtect 閘道。

下列範例顯示 GlobalProtect 多閘道拓撲中所示之 gp1 與 gp2 的設定。

在代管 gp1 的防火牆上，選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）。進行閘道設定，如下所示：

IP Address（**IP** 位址）—**ethernet1/2**

IP Address（**IP** 位址）—**198.51.100.42**

Server Certificate（伺服器憑證）—**GP1-server-cert.pem issued by GoDaddy**

Tunnel Interface（通道介面）—**tunnel.2**

IP Pool（**IP** 集區）—**10.31.32.3 - 10.31.32.118**

在代管 gp2 的防火牆上，選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）。進行閘道設定，如下所示：

IP Address（**IP** 位址）—**ethernet1/2**

IP Address（**IP** 位址）—**192.0.2.4**

Server Certificate（伺服器憑證）—自我簽署的憑證，**GP2-server-cert.pem**

Tunnel Interface（通道介面）—**tunnel.1**

IP Pool（**IP** 集區）—**10.31.33.3 - 10.31.33.118**

STEP 7 | 設定 GlobalProtect 入口網站。

選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）。進行入口網站設定，如下所示：

1. 設定 GlobalProtect 入口網站存取權。

   IP Address（**IP** 位址）—**ethernet1/2**

   IP Address（**IP** 位址）—**198.51.100.42**

   Server Certificate（伺服器憑證）—**GP1-server-cert.pem issued by GoDaddy**
2. 定義 GlobalProtect 代理程式組態：

   您所建立的用戶端組態數取決於您的特定存取需求，包括您是否需要以使用者/群組為基礎的原則與/或已啟用 HIP 的原則強制執行。

STEP 8 | 部署 GlobalProtect 代理程式軟體。

選取 **Device**（裝置）> **GlobalProtect Client**（**GlobalProtect** 用戶端）。

在此範例中，依照程序在入口網站裝載應用程式更新。

STEP 9 | 儲存 GlobalProtect 設定。

在裝載入口網站與閘道的防火牆上 **Commit**（提交）組態。

內部 HIP 檢查與使用者存取的 GlobalProtect

當與 User-ID 與/或 HIP 檢查搭配使用時，內部閘道可提供安全準確的方法，來由使用者與/或裝置狀態識別及控制流量，取代其他網路存取控制 (NAC) 服務。內部閘道在需要關鍵資源之驗證存取權的敏感環境中非常有用。

在只有內部閘道的設定中，必須使用使用者登入（一直開啟）設定所有端點；不支援視需要模式。還建議您將所有用戶端組態設定為使用單一登入 (SSO)。另外，由於內部主機不需要建立與閘道之間的通道連線，因此會使用端點上實體網路介面卡的 IP 位址。

在此快速設定中，內部閘道可強制執行以群組為基礎的原則，讓工程群組中的使用者能夠存取內部來源控制與錯誤資料庫，並讓財務群組中的使用者能夠存取 CRM 應用程式。所有已驗證的使用者都可以存取內部 Web 資源。此外，在閘道上設定的 HIP 設定檔會檢查每個主機，以確保符合內部維護需求，例如，是否已安裝最新的安全性修補程式、是否已啟用磁碟加密，或是否已安裝所需軟體。

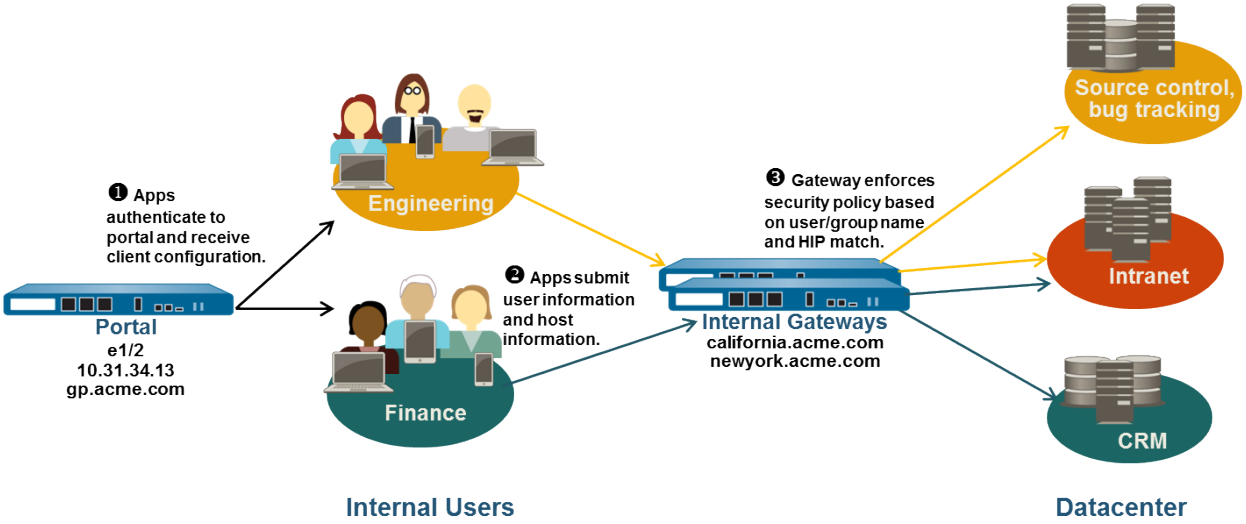


圖 8: GlobalProtect 內部閘道設定

使用下列步驟設定 GlobalProtect 內部閘道。

STEP 1 | 為 GlobalProtect 建立介面與區域。

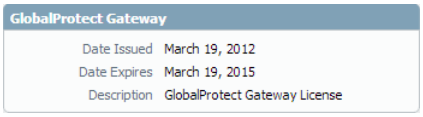
在此設定中，您必須在裝載入口網站與/或閘道的每個防火牆上設定介面。由於此設定僅使用內部閘道，因此您必須在內部網路上設定每個介面的入口網站與閘道。

針對所有介面設定使用 *default*（預設）虛擬路由器，以防建立內部區域路由。

在裝載入口網站/閘道的每個防火牆上：

1. 選取要裝載入口網站/閘道的 Ethernet 連接埠，然後在 **l3-trust Security Zone**（安全性區域）中設定具有 IP 位址的 Layer3 介面（**Network**（網路）> **Interfaces**（介面）> **Ethernet**）。
2. 在 **l3-trust** 區域上 **Enable User Identification**（啟用使用者識別）。

STEP 2 | 如果您的任何一般使用者將在行動裝置上存取 GlobalProtect 應用程式，或您要使用已啟用 HIP 的安全性原則，請購買並在各個裝載內部閘道的防火牆上安裝 GlobalProtect 訂閱。



購買 GlobalProtect 訂閱並收到啟動碼之後，請在裝載閘道的防火牆上安裝 GlobalProtect 訂閱，如下所示：

1. 選取 **Device**（裝置）> **Licenses**（授權）。
2. 選取 **Activate feature using authorization code**（使用授權碼啟動功能）。
3. 出現提示時，請輸入 **Authorization Code**（授權碼），然後按一下 **OK**（確定）。
4. 確認授權已成功啟動。

如果您沒有所需授權，請聯絡 Palo Alto Networks 銷售工程師或零售商。如需授權的詳細資訊，請參閱關於 GlobalProtect 授權。

STEP 3 | 取得 GlobalProtect 入口網站與每個 GlobalProtect 閘道的伺服器憑證。

為了初次連線至入口網站，端點必須信任用來簽發入口網站伺服器憑證的根 CA 憑證。您可以在初次入口網站連線之前，使用入口網站上的自我簽署憑證，並將根 CA 憑證部署至端點，或者從信任的 CA 取得入口網站的伺服器憑證。

您可以針對閘道使用自我簽署的憑證。

建議的工作流程如下所示：

1. 在裝載入口網站的防火牆上：
    1. 從已知的協力廠商 CA 匯入伺服器憑證。
    2. 建立用來針對 GlobalProtect 元件簽發自我簽署憑證的根 CA 憑證。
    3. 使用入口網站上的根 CA，以建立自我簽署伺服器憑證。為每個閘道重複此步驟。
2. 在裝載內部閘道的每個防火牆上，部署自我簽署的伺服器憑證。

STEP 4 | 定義您將對入口網站與閘道驗證使用者的方式。

必要時，您可以使用憑證設定檔與/或驗證設定檔的任何組合來確保入口網站與閘道的安全性。入口網站與個別閘道也可以使用不同的驗證結構描述。如需逐步指示，請參閱以下幾節：

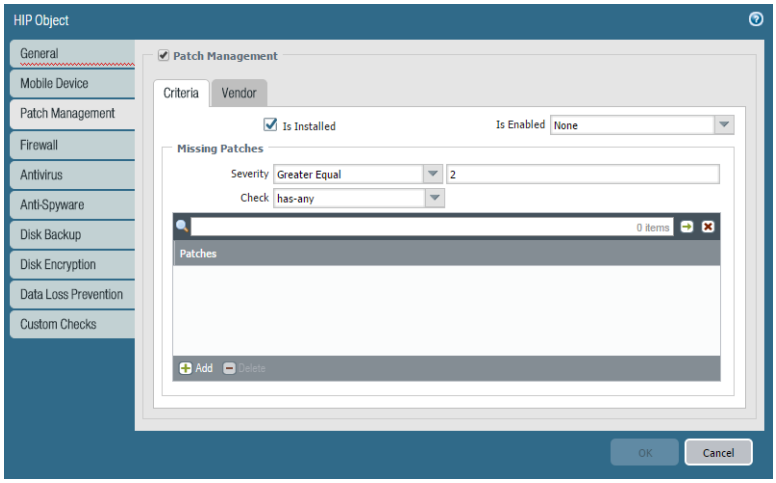
- 設定外部驗證（驗證設定檔）
- 設定用戶端憑證驗證（憑證設定檔）
- 設定雙因素驗證（權杖或以 OTP 為基礎）

然後，您必須參考您在入口網站與閘道設定中定義的憑證設定檔與/或驗證設定檔。

STEP 5 | 建立針對閘道存取權強制執行安全原則所需的 HIP 設定檔。

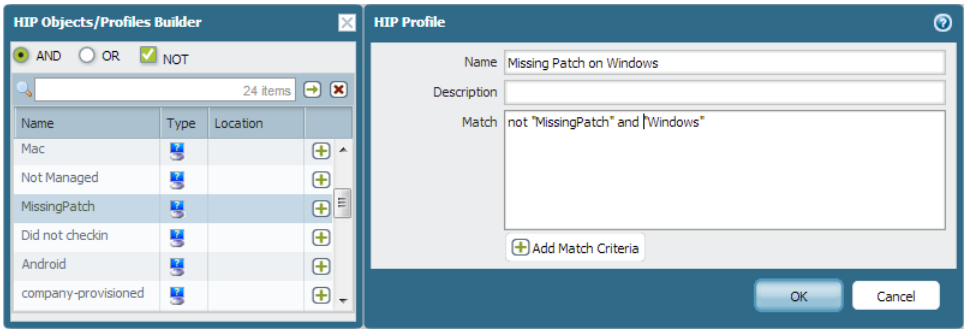
如需 HIP 比對的詳細資訊，請參閱主機資訊。

1. 建立 HIP 物件以篩選應用程式所收集的原始主機資料。例如，如果您想要防止不具備所需最新修補程式的使用者連線，您可以建立 HIP 物件，來比對其是否已安裝修補程式管理軟體，以及所有具備特定嚴重性的修補程式是否為最新狀態。



2. 建立您打算在原則中使用的 HIP 設定檔。

   例如，如果您要確保只有具有最新修補程式的 Windows 使用者可以存取內部應用程式，您可以附加下列 HIP 設定檔，來比對有否遺失修補程式的主機：



STEP 6 | 設定內部閘道。

選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道），然後選取現有的內部閘道或 **Add**（新增）新的閘道。進行下列閘道設定：

- 介面
- **IP** 位址
- 伺服器憑證
- **Authentication Profile**（驗證設定檔）及/或 **Configuration Profile**（組態設定檔）

請注意，不需要在閘道設定中設定用戶端（除非您想要設定 HIP 通知），因為不需要通道連線。如需建立閘道設定的逐步指示，請參閱設定 GlobalProtect 閘道。

STEP 7 | 設定 GlobalProtect 入口網站。

雖然之前的所有設定都可以使用 *User-logon (Always On)*（使用者登入（一直開啟））或 *On-demand (Manual user initiated connection)*（視需要（手動使用者起始連線））連線方法，但內部閘道設定必須一律開啟，因此需要採用 *User-logon (Always On)*（使用者登入（一直開啟））連線方法。

選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後選取現有的入口網站或 **Add**（新增）新的入口網站。設定入口網站，如下所示：

1. 設定 GlobalProtect 入口網站存取權。

   IP Address（**IP** 位址）—**`ethernet1/2`**

IP Address（**IP** 位址）—**10.31.34.13**

Server Certificate（伺服器憑證）—**GP-server-cert.pem issued by GoDaddy** 含 **CN=gp.acme.com**

2. 定義 GlobalProtect 用戶端驗證組態：

   Use single sign-on（使用單一登入）—**enabled**

   Connect Method（連線方法）—**User-logon (Always On)**

   Internal Gateway Address（內部閘道位址）—**california.acme.com, newyork.acme.com**

   User/User Group（使用者/使用者群組）—**any**

3. **Commit**（提交）入口網站設定。

STEP 8 | 部署 GlobalProtect 應用程式軟體。

選取 **Device**（裝置）> **GlobalProtect Client**（**GlobalProtect** 用戶端）。

在此範例中，使用程序以在入口網站裝載應用程式更新。

STEP 9 | 在您的閘道上建立已啟用 HIP 與/或以使用者/群組為基礎的安全性規則。

針對此範例新增下列安全性規則：

1. 選取 **Policies**（原則）> **Security**（安全性），然後按一下 **Add**（新增）。
2. 在 **Source**（來源）頁籤上，設定 **Source Zone**（來源區域）為 **l3-trust**。
3. 在 **User**（使用者）頁籤上，新增要比對的 HIP 設定檔與使用者/群組。
   - 在 **HIP Profiles**（**HIP** 設定檔）區域中按一下 **Add**（新增），然後選取 HIP 設定檔 **MissingPatch**。
   - **Add**（新增）**Source User**（來源使用者）群組（財務或工程，這視您要建立的規則而定）。
4. 按一下 **OK**（確定）來儲存規則。
5. **Commit**（提交）閘道設定。

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	CRM access	none	l3-trust	any	Finance	Missing Patch ...	l3-trust	any	sap	application-default	✓
2	Eng access	none	l3-trust	any	Engineering	Missing Patch ...	l3-trust	any	bugzilla perforce	application-default	✓

混合的內部與外部閘道設定

在 GlobalProtect 混合的內部與外部閘道設定中，您可以為 VPN 存取與敏感內部資源的存取設定單獨的閘道。在使用此設定的情況下，GlobalProtect 應用程式可執行內部主機偵測，來確定它位於內部網路還是外部網路。如果應用程式確定它位於外部網路，便會嘗試連線至其用戶端組態中所列的外部閘道，然後會與具有最高優先順序及最短回應時間的閘道建立連線。

如果您將所有外部閘道設定為僅手動閘道，但將 *GlobalProtect* 連線方法設定為 *User-Logon (Always On)*（使用者登入（一直開啟））或 *Pre-Logon (Always On)*（預登入（一直開啟）），則 *GlobalProtect* 應用程式不會自動連線至任何外部閘道。*GlobalProtect* 將保持未連線狀態，直至外部使用者手動建立閘道連線。此行為可讓您部署 *GlobalProtect* 來為內部使用者衍生 *User-ID*，同時針對外部使用者支援視需要 *VPN* 行為。

由於安全原則是在每個閘道上單獨定義的，因此您可以精細控制外部與內部使用者可以存取的資源。此外，您還可以透過設定入口網站，以根據使用者/群組成員資格或 HIP 設定檔比對，部署不同的用戶端組態，來精細控制使用者可以存取的閘道。

在此範例中，會將入口網站與全部三個閘道（一個外部閘道與兩個內部閘道）部署在不同的防火牆上。位於 gpvpn.acme.com 的外部閘道提供對於公司網路的遠端 VPN 存取，而內部閘道則根據群組成員資格提供對於敏感資料中心資源的精細存取權。此外，HIP 檢查可用來確保存取資料中心的主機具有最新的安全性修補程式。

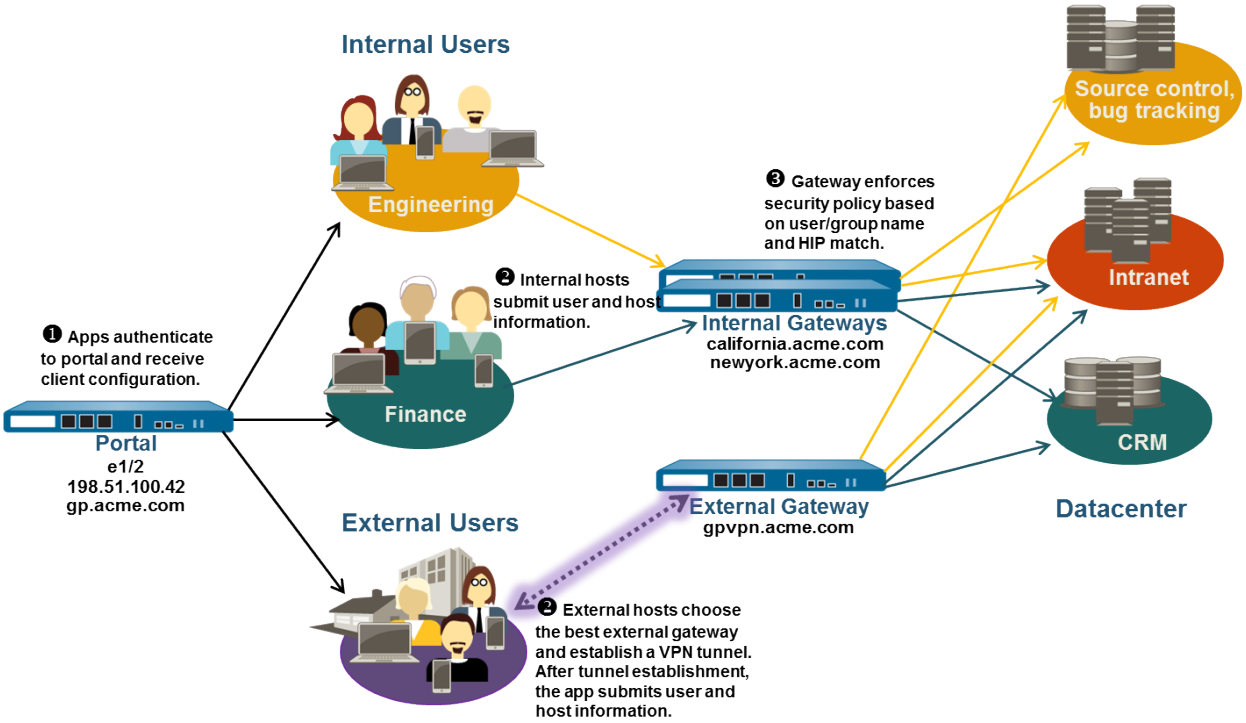


圖 9: 具有內部與外部閘道的 **GlobalProtect** 部署

使用下列步驟設定內部和外部 GlobalProtect 閘道混合。

STEP 1 | 為 GlobalProtect 建立介面與區域。

在此設定中，您必須在裝載入口網站的防火牆與裝載閘道的每個防火牆上設定介面。

在您已設定 *GlobalProtect* 入口網站或閘道的介面上，請勿附加允許 *HTTP*、*HTTPS*、*Telnet* 或 *SSH* 的介面管理設定檔，因為這會啟用從網際網路存取管理介面的存取權。請遵照保護管理存取權的最佳做法，來確保您可以保障防火牆的管理存取權，以防攻擊成功。

針對所有介面設定使用 *default*（預設）虛擬路由器，以防必須建立內部區域路由。

在裝載入口網站閘道 (gp.acme.com) 的防火牆上：

- 選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet** 並將 **ethernet1/2** 設定為 Layer 3 Ethernet 介面，且 IP 位址為 **198.51.100.42**。將其指定到 **l3-untrust Security Zone**（安全性區域）和預設 **Virtual Router**（虛擬路由器）。
- 建立將 IP 位址 198.51.100.42 對應至 gp.acme.com 的 DNS「A」記錄。

- 選取 **Network**（網路）> **Interfaces**（介面）> **Tunnel**（通道），然後 **Add**（新增）`tunnel.2` 介面。將其指定到名為 `corp-vpn` 的 **Security Zone**（安全性區域）和預設 **Virtual Router**（虛擬路由器）。
- 在 corp-vpn 區域上啟用使用者識別。

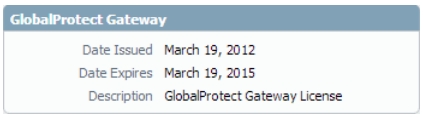
在裝載外部閘道 (gpvpn.acme.com) 的防火牆上：

- 選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet** 並將 **ethernet1/2** 設定為 Layer 3 Ethernet 介面，且 IP 位址為 `192.0.2.4`。將其指定到 `l3-untrust` **Security Zone**（安全性區域）和預設 **Virtual Router**（虛擬路由器）。
- 建立將 IP 位址 192.0.2.4 對應至 gpvpn.acme.com 的 DNS "A" 記錄。
- 選取 **Network**（網路）> **Interfaces**（介面）> **Tunnel**（通道），然後 **Add**（新增）`tunnel.3` 介面。將其指定到名為 `corp-vpn` 的 **Security Zone**（安全性區域）和預設 **Virtual Router**（虛擬路由器）。
- 在 corp-vpn 區域上啟用使用者識別。

在裝載內部閘道（california.acme.com 與 newyork.acme.com）的防火牆上：

- 選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet** 並在內部網路設定帶 IP 位址的 Layer 3 Ethernet 介面。將其指定到 `l3-trust` **Security Zone**（安全性區域）和預設 **Virtual Router**（虛擬路由器）。
- 建立對應內部 IP 位址 california.acme.com 與 newyork.acme.com 的 DNS「A」記錄。
- 在 l3-trust 區域上啟用使用者識別。

STEP 2 | 如果您的一般使用者將在行動端點上使用 GlobalProtect 應用程式，或者您想要使用已啟用 HIP 的安全性原則，您需要購買並在各個裝載（內部和外部）閘道的防火牆上安裝 GlobalProtect 訂閱。



購買 GlobalProtect 訂閱並收到啟動碼之後，請在裝載閘道的防火牆上安裝 GlobalProtect 訂閱：

1. 選取 **Device**（裝置）> **Licenses**（授權）。
2. 選取 **Activate feature using authorization code**（使用授權碼啟動功能）。
3. 出現提示時，請輸入 **Authorization Code**（授權碼），然後按一下 **OK**（確定）。
4. 確認授權與使用授權已成功啟動。

如果您沒有所需授權，請聯絡 Palo Alto Networks 銷售工程師或零售商。如需授權的詳細資訊，請參閱關於 GlobalProtect 授權。

STEP 3 | 取得 GlobalProtect 入口網站與每個 GlobalProtect 閘道的伺服器憑證。

為了初次連線至入口網站，端點必須信任用來簽發入口網站伺服器憑證的根 CA 憑證。

您可以在閘道上使用自我簽署憑證，並在用戶端組態中將根 CA 憑證部署至應用程式。最佳做法是在裝載入口網站的防火牆上產生所有憑證，然後將其部署至閘道。

建議的工作流程如下所示：

1. 在裝載入口網站的防火牆上：
    1. 從已知的協力廠商 CA 匯入伺服器憑證。
    2. 建立用來針對 GlobalProtect 元件簽發自我簽署憑證的根 CA 憑證。
    3. 使用入口網站上的根 CA，以建立自我簽署伺服器憑證。為每個閘道重複此步驟。
2. 在裝載內部閘道的每個防火牆上：
    - 部署自我簽署的伺服器憑證。

STEP 4 | 定義您將對入口網站與閘道驗證使用者的方式。

您可以使用憑證設定檔與/或驗證設定檔的任何組合來確保入口網站與閘道的安全性。入口網站與個別閘道也可以使用不同的驗證結構描述。如需逐步指示，請參閱以下幾節：

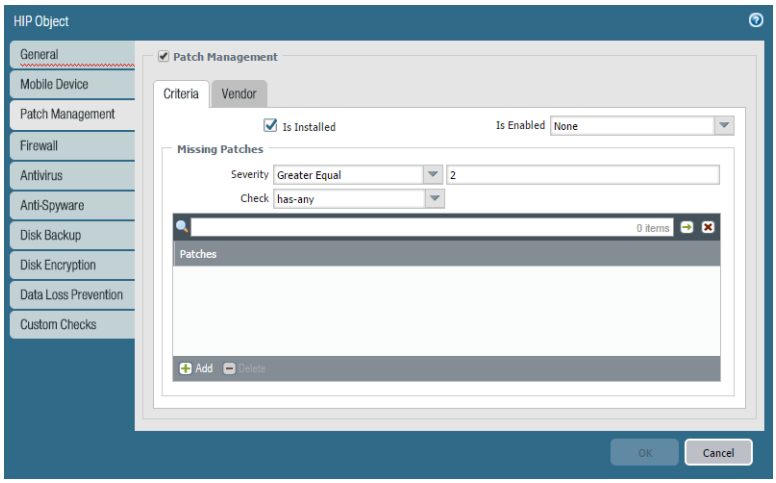
- 設定外部驗證（驗證設定檔）
- 設定用戶端憑證驗證（憑證設定檔）
- 設定雙因素驗證（權杖或以 OTP 為基礎）

然後，您必須參考您在入口網站與閘道設定中定義的憑證設定檔與/或驗證設定檔。

STEP 5 | 建立針對閘道存取權強制執行安全原則所需的 HIP 設定檔。

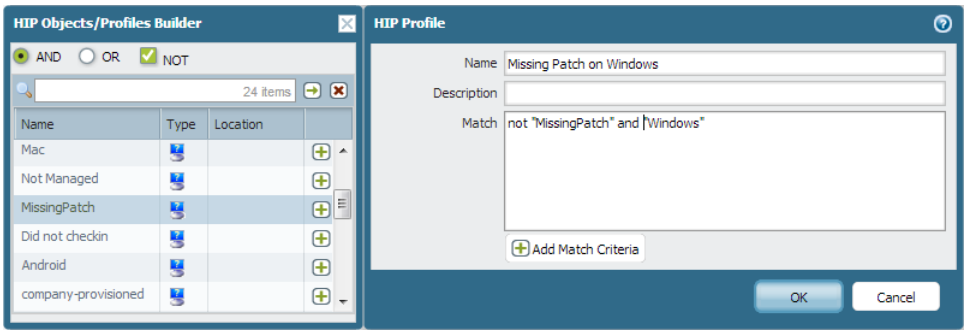
如需 HIP 比對的詳細資訊，請參閱主機資訊。

1. 建立 HIP 物件以篩選應用程式所收集的原始主機資料。例如，如果您想要防止所出現的使用者不具備所需的最新修補程式，您可以建立 HIP 物件，來比對其是否已安裝修補程式管理軟體，以及所有具備特定嚴重性的修補程式是否為最新狀態。



2. 建立您打算在原則中使用的 HIP 設定檔。

例如，如果您要確保只有具有最新修補程式的 Windows 端點可以存取內部應用程式，您可以附加下列 HIP 設定檔，來比對有否遺失修補程式的主機：



STEP 6 | 設定內部閘道。

選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道），然後透過下列設定 **Add**（新增）閘道組態：

- 介面
- **IP** 位址
- 伺服器憑證

- **Authentication Profile**（驗證設定檔）及/或 **Configuration Profile**（組態設定檔）

請注意，不需要在閘道設定中設定用戶端組態（除非您想要設定 HIP 通知），因為不需要通道連線。如需建立閘道設定的逐步指示，請參閱設定 GlobalProtect 閘道。

STEP 7 | 設定 GlobalProtect 入口網站。

雖然此範例顯示如何建立要部署至所有應用程式的單一用戶端組態，但您也可以針對不同的使用方式建立單獨的設定，然後根據使用者/群組名稱與/或執行應用程式的端點作業系統對其進行部署。

選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站），然後 **Add**（新增）下列入口網站組態：

1. 設定 GlobalProtect 入口網站存取權。

   IP Address（IP 位址）—**ethernet1/2**

   IP Address（IP 位址）—**10.31.34.13**

   Server Certificate（伺服器憑證）—**GP-server-cert.pem issued by GoDaddy** 含 **CN=gp.acme.com**
2. 定義 GlobalProtect 用戶端驗證組態：

   Internal Host Detection（內部主機偵測）—**enabled**

   Use single sign-on（使用單一登入）—**enabled**

   Connect Method（連線方法）—**User-logon (Always On)**

   External Gateway Address（外部閘道位址）—**gpvpn.acme.com**

   Internal Gateway Address（內部閘道位址）—**california.acme.com, newyork.acme.com**

   User/User Group（使用者/使用者群組）—任何
3. **Commit**（提交）入口網站設定。

STEP 8 | 部署 GlobalProtect 應用程式軟體。

選取 **Device**（裝置）> **GlobalProtect Client**（GlobalProtect 用戶端）。

在此範例中，使用程序以在入口網站裝載應用程式更新。

STEP 9 | 在每個閘道上建立安全性原則規則，以安全地為您的 VPN 使用者啟用應用程式存取權。

- 建立安全性原則（**Policies**（原則）> **Security**（安全性））來啟用 corp-vpn 區域與 l3-trust 區域之間的流量。
- 建立 HIP 已啟用且以使用者/群組為基礎的原則規則，以啟用您內部資料中心資源的精確存取權。
- 針對可見度，建立允許所有使用者透過 Web 瀏覽存取 l3-untrust 區域的規則，並使用預設安全性設定檔來保護您不受已知威脅的攻擊。

			Source				Destination					
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	CRM access	none	corp-vpn l3-trust	any	Finance	Missing Patch ...	l3-trust	any	sap	application-default		none
2	Eng access	none	corp-vpn l3-trust	any	Engineering	Missing Patch ...	l3-trust	any	bugzilla perforce	application-default		none
3	GP access	none	corp-vpn l3-trust	any	any	any	l3-untrust	any	web-browsing	application-default		

STEP 10 | 儲存 GlobalProtect 設定。

Commit（提交）入口網站與閘道組態。

網頁驗證與強制執行 GlobalProtect 以進行網路存取

在大部分實例中，行動使用者連線至啟用了被控制的入口網站的 Wi-Fi 網路，如在咖啡店、機場和酒店所使用的 Wi-Fi。僅在使用者登入被控制的入口網站後，方可存取網際網路。使用者可以透過基於瀏覽器的入口網站登入頁面登入，或基於作業系統的被控制的入口網站助理，使用如名稱和電子郵箱位址之類的識別碼登入。透過此設定，您可以限制使用者登入被控制的入口網站的時間。如果使用者成功登入，且網際網路可存取，GlobalProtect 應用自動建立連線。如果使用或則未能在指定時間內登入，所有流量將被封鎖。

要進一步降低網路收到安全威脅的影響，您也可以 為網路存取強制使用 GlobalProtect。當您啟用此選項時，GlobalProtect 封鎖所有網路流量直至應用程式連線至 GlobalProtect 閘道。所有流量都需要經過 VPN 隧道進行檢查和原則強制執行，從而讓您可以保持完全的可見度和對使用者流量的控制。

基於被控制的入口網站的存在以及網路存取是否需要 GlobalProtect 連線，使用者必須遵照特定的工作流程存取網路：

網頁驗證	強制執行 GlobalProtectfor 網路存取	工作流程
是	是	如果網路存取需要 GlobalProtect 連線，且您的終端使用者也必須登入被控制的入口網站以存取網際網路，他們必須使用下列步驟存取網路： 1. 連線至 Wi-Fi 網路。 在您連線至 Wi-Fi 網路後，GlobalProtect 自動偵測被控制的入口網站。如果您的管理員設定了被控制入口網站偵測消息，GlobalProtect 應用通知您必須登入被控制的入口網站以存取網路。 管理員也可以設定被控制入口網站偵測消息顯示的時間。 2. 使用以下選項之一登入被控制入口網站： • 打開 Web 瀏覽器，透過被控制入口網站登入頁面登入。 • 透過端點作業系統內置的原生被控制入口網站助理登入。 如果登入被控制入口網站成功，網際網路可存取，且 GlobalProtect 應用自動連線。如果應用未立即連線，且您的管理員設定流量封鎖通知消息，以說明您必須連線至 GlobalProtect 進行網路存取，其將在連線建立之前顯示此消息。 管理員也可以設定流量封鎖通知顯示的時間。 如果被控制入口網站登入失敗，且被控制入口網站登入頁面超時，或 GlobalProtect 無法建立連線，您將無法使用網路。要重新啟動入口網站登入並重新出發被控制入口網站登入時間，啟動 GlobalProtect 應用然後從應用設置功能表選取 **Refresh Connection**（重新整理連線）()。

網頁驗證	強制執行 GlobalProtectfor 網路存取	工作流程
是	否	如果您的終端使用者必須登入被控制入口網站以存取網際網路，但網路存取無需 GlobalProtect 連線，則其必須透過下列步驟存取網路： 1. 連線至 Wi-Fi 網路。 在您連線至 Wi-Fi 網路後，GlobalProtect 自動偵測被控制的入口網站。 2. 使用以下選項之一登入被控制入口網站： • 打開 Web 瀏覽器，透過被控制入口網站登入頁面登入。 • 透過端點作業系統內置的原生被控制入口網站助理登入。 如果登入成功且網際網路可存取，則 GlobalProtect 應用自動連線。
否	是	如果網路存取需要 GlobalProtect 連線，但您的終端使用者無需登入被控制的入口網站以存取網際網路，他們必須連線至 Wi-Fi 網路。一旦連線至 Wi-Fi 且可存取網際網路，GlobalProtect 應用自動連線。 如果應用未立即連線，且您的管理員設定流量封鎖通知消息，以說明您必須連線至 GlobalProtect 進行網路存取，其將在連線建立之前顯示此消息。如果 GlobalProtect 無法建立連線，您將無法存取網路。您必須透過斷開連線，然後重新連線至 Wi-Fi 網路、重新啟動端點或重新整理 GlobalProtect 連線的方式，重新啟動網路探索。

使用以下步驟自定義被控制入口網站設置，並說明網路存取是否需要 GlobalProtect 連線：

僅當您透過一直開啟連線方法設定 *GlobalProtect* 時，設定 *Enforce GlobalProtect for Network Access*（為網路存取強制使用 *GlobalProtect*）選項。

STEP 1 | 設定 GlobalProtect 入口網站存取權.

STEP 2 | 定義 GlobalProtect 代理程式組態.

STEP 3 | 自訂 GlobalProtect 應用程式.

- 要確保 GlobalProtect 連線一直開啟，將 **Connect Method**（連線方法）設定為 **User-logon (Always On)**（使用者登入（一直開啟））。
- 如果您的使用者必須登入被控制入口網站以存取網際網路，您可以透過設定以下選項，自定義被控制入口網站設置：
  - 在 **Captive Portal Exception Timeout (sec)**（被控制的入口網站例外逾時）（秒）欄位中，輸入使用者可登入被控制入口網站的時間（以秒為單位）（範圍為 0 至 3600 秒；預設為 0 秒）。如果使用者未在此時段內登入，網頁驗證登入頁面將逾時，且使用者將無法使用網路。
  - 要啟用 GlobalProtect 應用以通知使用者何時偵測被控制入口網站，將 **Display Captive Portal Detection Message**（顯示被控制入口網站偵測消息）設為 **Yes**（是）。
    - 在 **Captive Portal Notification Delay (sec)**（被控制的入口網站通知延遲）（秒）欄位中，輸入 GlobalProtect 應用顯示被控制入口網站偵測消息顯示時間（以秒為單位）（範圍為 1 至 120 秒；預設為 5 秒）。GlobalProtect 在偵測到網頁驗證之後，但在網際網路可連線之前啟動此計時器。

- 自定義 GlobalProtect 偵測到被控制入口網站時顯示的 **Captive Portal Detection Message**（被控制入口網站偵測消息）。

- 要強制所有網路流量周遊 GlobalProtect VPN 隧道，設定下列選項：
  - 將 **Enforce GlobalProtect for Network Access**（為網路存取強制使用 **GlobalProtect**）選項設為 **Yes**（是）。
  - 要啟用 GlobalProtect 應用通知使用者網路存取需要 GlobalProtect 連線，將 **Display Traffic Blocking Notification Message**（顯示流量封鎖通知訊息）設為 **Yes**（是）。當網際網路可存取，而 GlobalProtect 連線建立之前，GlobalProtect 應用顯示此消息。
    - 在 **Traffic Blocking Notification Delay (sec)**（流量封鎖通知延遲）（秒）欄位中，輸入 GlobalProtect 應用顯示流量封鎖通知消息顯示時間（以秒為單位）（範圍為 5 至 120 秒；預設為 15 秒）。在網際網路可存取後，GlobalProtect 啟動此計時器。
    - 自定義當網路存取需要 GlobalProtect 連線時顯示的 **Traffic Blocking Notification Message**（流量封鎖通知消息）。此消息必須是 512 個字元或更少。

STEP 4 | **Commit**（提交）變更。

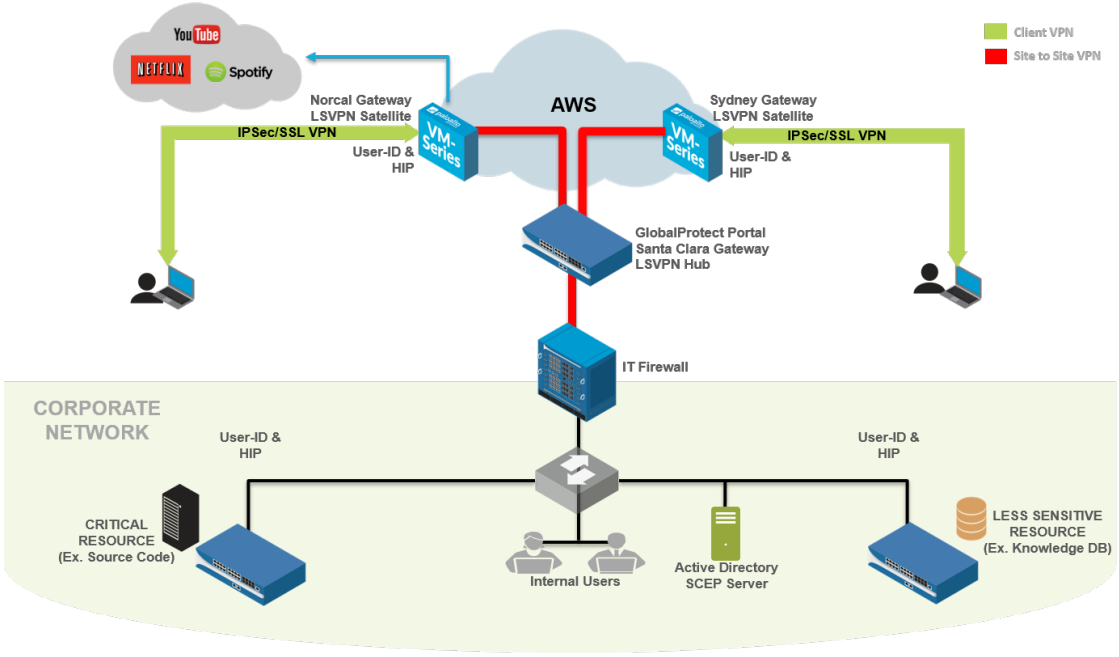
GlobalProtect 架構

此部分概述了部署 GlobalProtect™ 的範例參考架構，可保護網際網路流量並提供對公司資源的安全存取。

本部分中所述的參考架構和指南提供了普通部署案例。在採用此架構之前，識別您的公司安全性、基礎設施管理和一般使用者體驗要求，以及基於這些要求部署 GlobalProtect。

儘管各企業的要求可能不同，您可以利用本文中的普通原理和設計考慮，以及最佳做法組態指南來滿足您的企業安全需求。

GlobalProtect 參考架構拓撲



- GlobalProtect 入口網站
- GlobalProtect 閘道

GlobalProtect 入口網站

在此拓撲中，共置空間內的 PA-3020 可作為 GlobalProtect 入口網站。

員工和承包商可透過雙因素驗證 (2FA) 驗證入口網站，該驗證包括 Active Directory (AD) 認證和一個一次性密碼 (OTP)。入口網站基於使用者和群組成員資格以及作業系統，部署 GlobalProtect 用戶端組態。

透過設定分割入口網站套用於小群組或試驗使用者組的用戶端組態，您可以在將其用於更多使用者前測試其功能。任何包含新功能的用戶端組態—如 Enforce GlobalProtect 或 Simple Certificate Enrollment Protocol (SCEP) 功能（透過 PAN-OS 7.1 和後續更新內容實現可用性）—在試驗組態中先被啟用，並透過試驗使用者驗證，之後再用於其它使用者。

GlobalProtect 入口網站也將組態推送至 GlobalProtect 衛星。此組態包括 GlobalProtect 閘道，此閘道衛星可連線並建立站台對站台通道。

GlobalProtect 閘道

共置空間（上文提及）內的 PA-3020 也可以作為 GlobalProtect 閘道（Santa Clara Gateway）。Amazon Web Services (AWS) 和 Microsoft Azure 公共雲端內部署的 10 個其他閘道。這些 AWS 和 Azure 閘道的部署地區或 POP 位置部署基於全球的員工分佈。

- **Santa Clara Gateway**—員工和承包商可透過 2FA 驗證 Santa Clara Gateway（位於共置空間內的 PA-3020）。此閘道需要使用者提供其 Active Directory 認證及其 OTP。由於此閘道保護敏感資源，其作為僅手動閘道設定。結果是，使用者不會自動連線至此閘道，而必須手動選取連線的閘道。例如，當使用者連線至 AWS-Norcal 時，其非僅手動閘道，部分敏感內部資源無法存取。使用者必須手動切換並透過 Santa Clara Gateway 驗證以存取這些資源。

此外，Santa Clara Gateway 作為大規模 VPN (LSVPN) 通道終止點設定，用於 AWS 和 Azure 內的閘道衛星連線。Santa Clara Gateway 也被設定為在公司總部內，設置內部協定安全 (IPSec) 通道至 IT 防火牆。此通道提供對公司總部內資源的存取。

- **Amazon Web Services** 和 **Microsoft Azure** 內的閘道—此閘道需要 2FA：用戶端憑證和 Active Directory 認證。GlobalProtect 入口網站散佈用戶端憑證，此憑證用於透過 GlobalProtect SCEP 功能驗證這些閘道。

  公共雲端內的這些閘道也可作為 GlobalProtect 衛星。其與 GlobalProtect 入口網站通訊，下載衛星組態，並建立與 Santa Clara Gateway 的站台對站台通道。GlobalProtect 衛星透過序號進行初始驗證，然後透過憑證進行後續驗證。
- 公司總部內閘道—在公司總部內，有三道防火牆作為 GlobalProtect 閘道使用。這些是內部閘道，且不要求端點設定通道。使用者透過其 Active Directory 認證驗證這些閘道。這些內部閘道使用 GlobalProtect 識別 User-ID 並收集來自端點的主機資訊設定檔 (HIP)。

若要讓一般使用者盡可能獲得無縫體驗，您可以設定這些內部閘道以透過 *SCEP* 提供的憑證，或透過 *Kerberos* 服務票證驗證使用者。

GlobalProtect 參考架構功能

一般使用者體驗

遠端（公司網路外）連線至 AWS 或 Azure 中閘道之一的一般使用者。當您設定 GlobalProtect 入口網站用戶端組態時，指派相同的優先順序至閘道。透過此組態，使用者連線的閘道視乎通道設定期間，端點上測量的每條閘道 SSL 回應時間。

例如，澳洲的使用者通常會連線至 AWS-雪梨閘道。使用者連線至 AWS-雪梨後，GlobalProtect 應用程式將所有流量從端點傳送至 AWS-雪梨防火牆進行檢查。GlobalProtect 透過 AWS-雪梨閘道直接遞送流量至公共網際網路網站，並透過 AWS-雪梨閘道和 Santa Clara Gateway 之間的站台對站台通道傳送流量至公司資源，然後透過 IPsec 站台對站台通道至公司總部。此架構被設計用於減少使用者存取網際網路時遇到的延遲。如果 AWS-雪梨閘道（或靠近雪梨的任何閘道）無法觸及，GlobalProtect 應用程式將迂迴網際網路流量至公司總部的防火牆，並造成延遲問題。

Active Directory 伺服器位於公司網路內。當遠端使用者驗證時，GlobalProtect 應用程式透過 AWS/Azure 中的站台對站台通道遞送驗證請求至 Santa Clara Gateway。該閘道隨後透過 IPsec 站台對站台通道轉送請求至公司總部內的 Active Directory 伺服器。

若要減少遠端使用者驗證和通道設定的時間，可考慮複製 *Active Directory* 伺服器並使其在 *AWS* 中可用。

公司網路內的一般使用者在登入後立即驗證三個內部閘道。GlobalProtect 應用程式遞送 HIP 報告至這些內部閘道。當使用者在公司網路上的辦公室內時，必須滿足 User-ID 和 HIP 要求，以存取工作時的任何資源。

管理與記錄

在此部署中，您可以從部署於共置空間的 Panorama 管理並設定所有防火牆。

若要提供一致的安全，AWS 和 Azure 內的所有防火牆使用相同的安全原則和組態。若要簡化閘道組態，Panorama 也會使用一個設備群組和一個範本。在此部署中，所有閘道轉送記錄至 Panorama。讓您可以從中央位置監控網路流量或故障排除問題，而無需您登入各防火牆。

當需要更新軟體時，您可以使用 Panorama 部署軟體更新至所有防火牆。Panorama 首先更新一或兩道防火牆，並在更新剩餘防火牆之前確認升級是否成功。

監控與高可用性

若要在此部署中監控防火牆，您可以使用 Nagios，這是一種開放原始碼伺服器、網路和記錄監控軟體。設定 Nagios 以定期確認來自入口網站和閘道預登入頁面的回應，並當回應與預期不符時，遞送警報。您也可以設定 GlobalProtect 簡易網路管理通訊協定 (SNMP) 管理資訊庫 (MIB) 物件以監控閘道使用。

在此部署中，僅有一個 GlobalProtect 入口網站實例。如果入口網站不可用，新使用者（之前從未連線至入口網站）將無法連線至 GlobalProtect。但是，現有使用者可以使用快取的入口網站用戶端組態連線至閘道之一。

AWS 內的多虛擬機 (VM) 防火牆被設定為 GlobalProtect 找到以提供閘道備援。因此，無需設定閘道為高可用性 (HA) 對。

GlobalProtect 參考架構組態

若要讓您的部署與參考架構一致，請檢閱下列組態檢查清單。

- 閘道設定
- 入口網站設定
- 原則設定

閘道設定

- 停用分割通道。若要停用分割通道，確保沒有在 **Agent**（代理程式）> **Client Settings**（用戶端設定）> **Split Tunnel**（分隔通道）設定中指定的存取路由。請參閱設定 GlobalProtect 閘道。
- 在 **Agent**（代理程式）> **Client Settings**（用戶端設定）> **Split Tunnel**（分隔通道）中啟用 **No direct access to local network**（無直接本機網路存取）。請參閱設定 GlobalProtect 閘道。
- 啟用閘道以 **Accept cookie for authentication override**（接受驗證取代 **cookie**）。請參閱設定 GlobalProtect 閘道。

入口網站設定

- 將 **Connect Method**（連線方法）設定為 **Always-on (User logon)**（一直開啟（使用者登入））。請參閱自訂 GlobalProtect 應用程式。
- 設定 **Use Single Sign-On**（使用單一登入）（僅 Windows）為 **Yes**（是）。請參閱自訂 GlobalProtect 應用程式。
- 將入口網站設定為 **Save User Credentials**（儲存使用者認證）（將值設定為 **Yes**（是））。請參閱定義 GlobalProtect 代理程式組態。
- 啟用入口網站以 **Accept cookie for authentication override**（接受驗證取代 **cookie**）。請參閱定義 GlobalProtect 代理程式組態。
- 將 **Cookie Lifetime**（**Cookie** 存留時間）設定為 20 小時。請參閱定義 GlobalProtect 代理程式組態。
- **Enforce GlobalProtect**（強制執行 **GlobalProtect**）以進行網路存取請參閱自訂 GlobalProtect 應用程式。
- 強制執行網路存取 **GlobalProtect** 啟用時，允許使用者使用密碼來停用 GlobalProtect 應用程式。請參閱自訂 GlobalProtect 應用程式。
- 設定 **Internal Host Detection**（內部主機偵測）。請參閱定義 GlobalProtect 代理程式組態。
- 在資料收集中啟用 **Collect HIP Data**（收集 **HIP** 資料）選項。請參閱定義 GlobalProtect 代理程式組態。
- 散佈並安裝 SSL 解密用的 SSL 轉送代理程式 CA 憑證。請參閱定義 GlobalProtect 代理程式組態。

原則設定

- 基於最佳做法網際網路閘道安全性原則設定所有防火牆以使用安全原則和設定檔在此參考部署中，包括共置空間內的 Santa Clara Gateway 和 AWS/Azure 公共雲端內的閘道。
- 啟用 AWS 和 Azure 內所有閘道上的 SSL 解密。
- 在 AWS 中為所有閘道設定 基於原則的轉送規則，以透過 Santa Clara Gateway 轉送流量至特定網站。這確保了如 www.stubhub.com 和 www.lowes.com 之類封鎖來自 AWS IP 位址範圍流量的網站仍可以在使用者連線至 AWS 中的閘道時可以存取。

GlobalProtect 密碼編譯

關於 GlobalProtect 加密選擇

GlobalProtect 支援 IPsec 和 SSL 通道模式。GlobalProtect 也支援讓 GlobalProtect 應用程式能夠在使用 SSL 通道之前，一律先嘗試設定 IPsec 通道的功能，且會要求 GlobalProtect 應用程式這樣做。透過 IPsec 通道，GlobalProtect 應用程式會使用 SSL/TLS 來交換加密和驗證演算法及金鑰。GlobalProtect 用於保障 SSL/TLS 通道安全的加密套件選擇，取決於：

- 閘道所接受的 **SSL/TLS** 版本—對於使用 SSL/TLS 設定檔的應用程式，GlobalProtect 入口網站和閘道可以限制其所能使用的加密套件清單。在防火牆上，您可以透過指定憑證與受允許的通訊協定版本來建立 SSL/TLS 設定檔，以及將該設定檔關聯至 GlobalProtect 入口網站和閘道。
- 閘道伺服器憑證的演算法—端點的作業系統會決定 GlobalProtect 應用程式要包含在 Client Hello 訊息中的加密套件。只要 GlobalProtect 應用程式包含閘道偏好使用的加密套件，閘道就會選取該加密套件用於 SSL 工作階段。在 Client Hello 訊息內的加密套件順序不會影響對加密套件的選擇：閘道會根據 SSL/TLS 服務設定檔、閘道伺服器憑證的演算法以及其偏好清單來選取加密套件。您可以從 GlobalProtect 閘道驗證設定中選取服務設定檔。

GlobalProtect 應用程式與閘道間的加密交換

下圖顯示在建立 VPN 通道時，在 GlobalProtect 閘道和 GlobalProtect 應用程式之間所進行的加密交換。

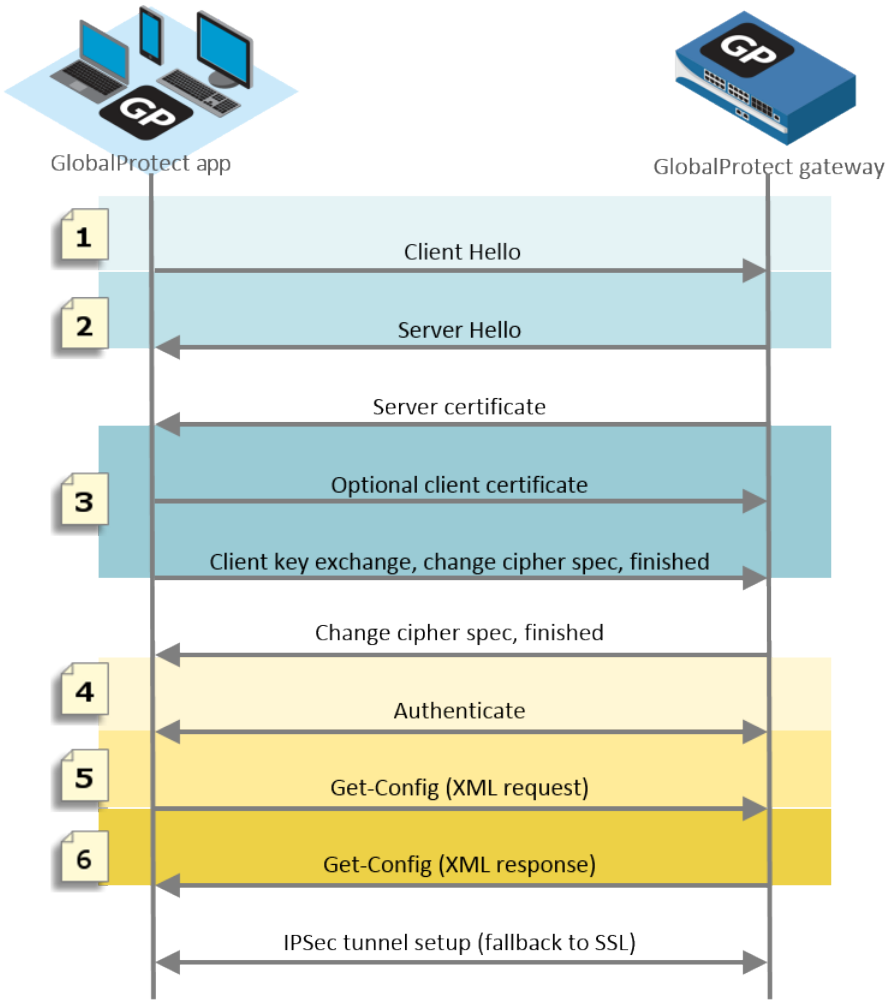


圖 10: 應用程式和閘道之間的加密交換

以下表格更詳細地描述了這些階段。

表 9: 應用程式和閘道之間的加密交換

通訊階段	說明
1。Client Hello	應用程式擁有取決於端點作業系統的加密套件清單。
2.Server Hello	閘道選取應用程式所提出的加密套件。當選取加密以設置通道時，閘道會略過應用程式所擁有的加密套件編號和順序，反之會依賴閘道伺服器憑證的 SSL/TLS 版本和演算法，以及閘道偏好的清單（如關於 GlobalProtect 加密選項中所述）。
3.選用的用戶端憑證	閘道可以選擇性要求要使用的應用程式用戶端憑證，以信任使用者或端點的身分。

通訊階段	說明
4.SSL 工作階段	在設定 SSL/TLS 工作階段後，應用程式會透過閘道驗證並請求閘道設定（取得組態請求）。若要請求設定，應用程式會提出加密和驗證演算法以及其他設定，例如偏好的通道介面 IP 位址。閘道根據 GlobalProtect IPSec 加密設定檔的設定，回應請求並選取要使用的加密和驗證演算法（取得組態請求）。

下方表格顯示 macOS 端點上應用程式和閘道之間加密交換的範例。

表 **10:** 範例：**macOS** 端點的加密交換過程

通訊階段	例如：macOS 端點
1。Client Hello	TLS 1.2 37 個加密套件（ 參考：macOS 端點上的 GlobalProtect 應用程式所支援的 TLS 加密 ）
2.Server Hello	• 當 GlobalProtect 使用 ECDSA 憑證且 TLS 1.2 已獲得接受，SSL 工作階段會使用 ECDSA-AES256-CBC-SHA。 • 當 GlobalProtect 使用 RSA 憑證且 TLS 1.2 已獲得接受，SSL 工作階段會使用 RSA-AES256-CBC-SHA256。
3.選用的用戶端憑證	以 ECDSA 或 RSA，並使用 SHA1、SHA256 或 SHA384 簽署的用戶端憑證。

4.SSL 工作階段	• SSL 工作階段會使用 ECDSA-AES256-CBC-SHA 或 RSA-AES256-CBC-SHA256
	• Get-Config-Request
	  • 加密—AES-256-GCM、AES-128-GCM、AES-128-CBC
	  • 驗證—SHA1 和 OS 類型，偏好的 IP 位址等
	• Get-Config-Response
	  • 用戶端到伺服器、伺服器到用戶端 SPI、加密金鑰和驗證金鑰
	  • 通道類型、連接埠、分割通道模式、IP 和 DNS 等

GlobalProtect 密碼編譯參考

參考：GlobalProtect 應用程式加密功能

GlobalProtect 應用程式使用 OpenSSL library 1.0.1h 建立與 GlobalProtect 入口網站和 GlobalProtect 閘道之間的安全通訊。下表列出每個需要加密功能的 GlobalProtect 應用程式功能，和 GlobalProtect 應用程式使用的加密金鑰：

加密功能	金鑰	使用方式
Winhttp (Windows) 和 NSURL 連線 (macOS) aes256-sha	GlobalProtect 應用程式與 GlobalProtect 入口網站和/或閘道之間交涉的動態金鑰，用於建立 HTTPS 連線。	用於在 GlobalProtect 應用程式與 GlobalProtect 入口網站和 GlobalProtect 閘道之間建立 HTTPS 連線，以進行驗證。
OpenSSL aes256-sha	SSL 交握期間 GlobalProtect 應用程式與 GlobalProtect 閘道之間交涉的動態金鑰。	用於在 GlobalProtect 應用程式與 GlobalProtect 閘道之間建立 SSL 連線，以提交 HIP 報告、交涉 SSL 通道及探索網路。
IPSec 加密與驗證 aes-128-sha1、aes-128-cbc、aes-128-gcm 和 aes-256-gcm	從 GlobalProtect 閘道傳送的工作階段金鑰。	用於在 GlobalProtect 應用程式與 GlobalProtect 閘道之間建立 IPsec 通道。使用您的網路支援的最強演算法（推薦 AES-GCM）。 若要提供資料完整性和驗證保護，aes-128-cbc 加密需要 sha1 驗證演算法。由於 AES-GCM 加密演算法 (aes-128-gcm 和 aes-256-gcm) 提供原生 ESP 整合保護，儘管在設定時需要，這些加密的 sha1 驗證演算法將被忽略。

GlobalProtect 應用程式所支援的 TLS 加密套件

下列各節提供在各種端點作業系統安裝的 GlobalProtect 應用程式所支援的 TLS 加密範例。該清單未涵蓋所有受支援的作業系統。

參考：*macOS* 端點上的 *GlobalProtect* 應用程式所支援的 *TLS* 加密

macOS 端點上的 GlobalProtect 應用程式所支援的 TLS 加密	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384 (0xc024)	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256 (0xc023)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
	TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)
	TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)
	TLS_RSA_WITH_RC4_128_SHA (0x0005)
	TLS_RSA_WITH_RC4_128_MD5 (0x0004)

參考：*Windows 7* 端點上的 *GlobalProtect* 應用程式所支援的 *TLS* 加密

Windows 7 端點上的 GlobalProtect 應用程式所支援的 TLS 加密	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384 (0xc02c)	

Windows 7 端點上的 GlobalProtect 應用程式所支援的 TLS 加密	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384 (0xc024)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256 (0xc023)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

參考：*Android 6.0.1* 端點上的 *GlobalProtect* 應用程式所支援的 *TLS* 加密

適用於 Android 6.0.1 的 GlobalProtect 應用程式支援 20 加密套件。

Android 6.0.1 端點上的 GlobalProtect 應用程式所支援的 TLS 加密	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384 (0xc02c)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_RC4_128_SHA (0x0005)
	TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

參考：*iOS 10.2.1* 端點上的 *GlobalProtect* 應用程式所支援的 *TLS* 加密

適用於 iOS 10.2.1 的 GlobalProtect 應用程式支援 19 加密套件。

iOS 10.2.1 端點上的 GlobalProtect 應用程式所支援的 TLS 加密	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384 (0xc02c)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384 (0xc024)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256 (0xc023)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

參考：在 *Chromebook* 端點上 *GlobalProtect* 應用程式所支援的 *TLS* 加密

適用於 OS 55.0.2883 的 GlobalProtect 應用程式支援 91 加密套件。

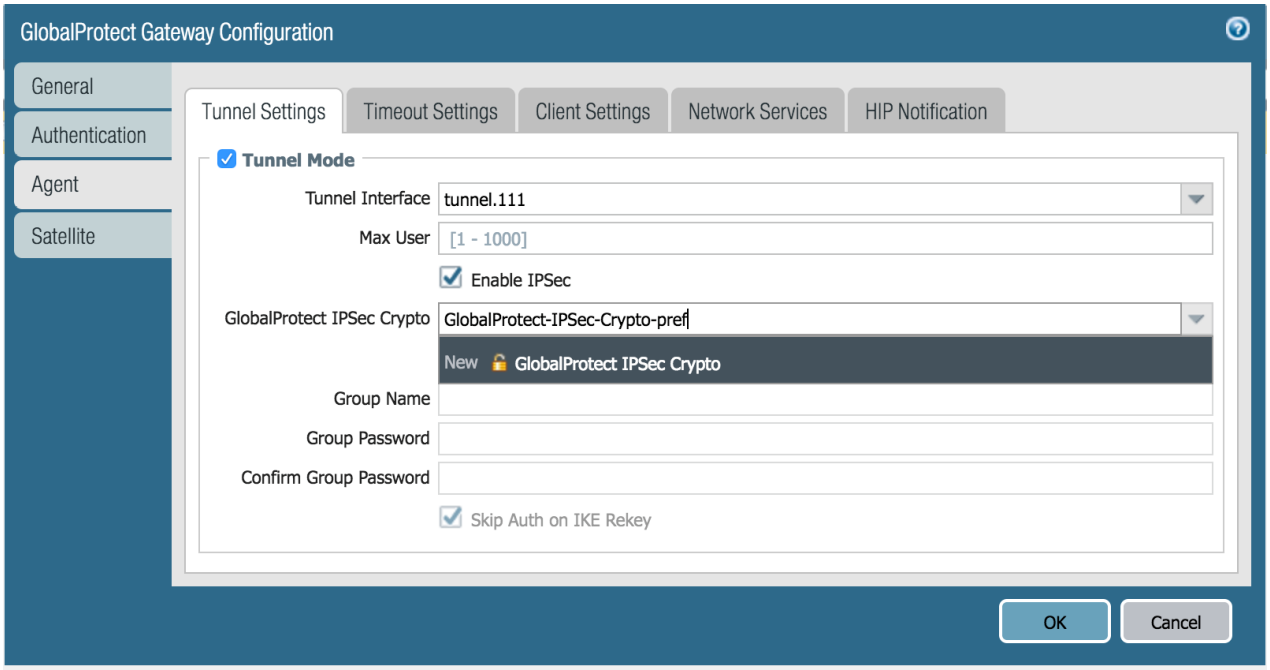
在 Chromebook (Chrome OS 55.0.2883) 上 GlobalProtect 應用程式所支援的 TLS 加密	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0085)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384 (0xc02c)	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384 (0xc024)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
TLS_DH_DSS_WITH_AES_256_GCM_SHA384 (0x00a5)	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)

在 Chromebook (Chrome OS 55.0.2883) 上 GlobalProtect 應用程式所支援的 TLS 加密	
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3) TLS_DH_RSA_WITH_AES_256_GCM_SHA384 (0x00a1) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f) TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b) TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a) TLS_DH_RSA_WITH_AES_256_CBC_SHA256 (0x0069) TLS_DH_DSS_WITH_AES_256_CBC_SHA256 (0x0068) TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039) TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038) TLS_DH_RSA_WITH_AES_256_CBC_SHA (0x0037) TLS_DH_DSS_WITH_AES_256_CBC_SHA (0x0036) TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088) TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0087) TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0086)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) TLS_DH_DSS_WITH_AES_128_GCM_SHA256 (0x00a4) TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00a2) TLS_DH_RSA_WITH_AES_128_GCM_SHA256 (0x00a0) TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067) TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040) TLS_DH_RSA_WITH_AES_128_CBC_SHA256 (0x003f) TLS_DH_DSS_WITH_AES_128_CBC_SHA256 (0x003e) TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033) TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032) TLS_DH_RSA_WITH_AES_128_CBC_SHA (0x0031) TLS_DH_DSS_WITH_AES_128_CBC_SHA (0x0030) TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x009a) TLS_DHE_DSS_WITH_SEED_CBC_SHA (0x0099) TLS_DH_RSA_WITH_SEED_CBC_SHA (0x0098) TLS_DH_DSS_WITH_SEED_CBC_SHA (0x0097)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) TLS_RSA_WITH_SEED_CBC_SHA (0x0096) TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041) TLS_RSA_WITH_IDEA_CBC_SHA (0x0007) TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007) TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c) TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002) TLS_RSA_WITH_RC4_128_SHA (0x0005) TLS_RSA_WITH_RC4_128_MD5 (0x0004) TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)

在 Chromebook (Chrome OS 55.0.2883) 上 GlobalProtect 應用程式所支援的 TLS 加密	
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0044)	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0043)	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA (0x0010)
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0042)	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA (0x000d)
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)	TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)	TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)	TLS_DH_RSA_WITH_DES_CBC_SHA (0x000f)
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)	TLS_DH_DSS_WITH_DES_CBC_SHA (0x000c)
	TLS_RSA_WITH_DES_CBC_SHA (0x0009)
	TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

用來設定 IPsec 通道的加密

GlobalProtect 可以限制和/或設定哪個加密和驗證演算法 GlobalProtect 應用程式可用於 IPsec 通道的優先順序。當您為 GlobalProtect 閘道設定通道時，演算法和偏好設定會在您設定的 **GlobalProtect IPSec Crypto**（**GlobalProtect IPSec** 加密）設定檔中定義（**Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> **<gateway-config>** > **GlobalProtect Gateway Configuration**（**GlobalProtect** 閘道組態）> **Agent**（代理程式）> **Tunnel Settings**（通道設定））。



當 GlobalProtect 應用程式透過 GlobalProtect 閘道設定 SSL 工作階段時，用於此 SSL 工作階段的加密套件，是由在閘道上設定的 SSL/TLS 設定檔和用於閘道憑證的演算法類型所控制。在 SSL 工作階段建立後，GlobalProtect 應用程式會透過 SSL 要求設定來起始 VPN 通道設定。

GlobalProtect 閘道會使用相同的 SSL 工作階段，以應用程式應用來設定 IPsec 通道的加密、驗證演算法、金鑰和 SPI 來回應。

如需更加安全，建議使用 *AES-GCM*。若要提供資料完整性和驗證保護，*aes-128-cbc* 加密需要 *SHA1* 驗證演算法。由於 *AES-GCM* 加密演算法 *(aes-128-gcm* 和 *aes-256-gcm)* 提供原生 *ESP* 整合保護，儘管在設定時需要，這些加密的 *SHA1* 驗證演算法將被忽略。

您在閘道上設定的 **GlobalProtect IPSec Crypto**（**GlobalProtect IPSec** 加密）設定檔，會決定要用來設定 IPsec 通道的加密和驗證演算法。GlobalProtect 閘道會以在設定檔的所列第一個符合的加密演算法回應，該設定檔會與應用程式的提案相符。

接著 GlobalProtect 應用程式會根據來自閘道的回應嘗試設定通道。

SSL API

GlobalProtect 同時使用 OpenSSL 和原生系統 API 來執行 SSL 交握。GlobalProtect 閘道延遲量測（GlobalProtect 用來選取最適合的閘道）、閘道登出與傳送 HIP 檢查訊息與報告傳輸等操作都會透過使用 OpenSSL 程式庫而設定的 SSL 工作階段來執行。閘道預先登入、登入和取得設定等操作都透過使用原生系統 API 而設定的 SSL 工作階段來執行。