網路配置總數：使用Web UI的RV345P和思科企業無線

目標

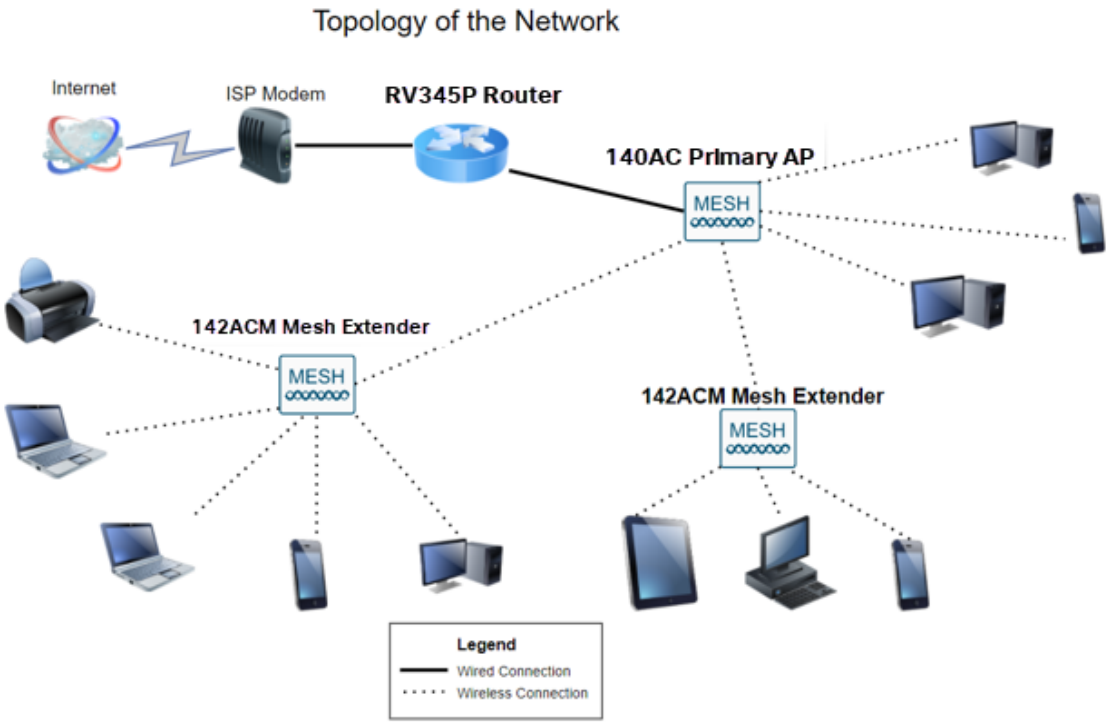
本指南將介紹如何使用RV345P路由器、CBW140AC接入點和兩個CBW142ACM網狀擴展器配置無線網狀網路。

本文使用Web使用者介面(UI)來設定Mesh無線網路。如果您更喜歡使用移動應用程式（建議使用它來實現輕鬆的無線設定），請按一下跳轉到使用移動應用程式的文章。

目錄

- 使用Web UI檢查和更新軟體
- 在Web UI上建立WLAN
- 可選無線配置
    - 使用Web UI建立訪客WLAN（可選）
    - 使用Web UI進行應用程式分析（可選）
    - 使用Web UI進行客戶端分析（可選）

拓撲



簡介

您的所有研究都齊聚一堂，並且已購買您的思科裝置，真令人興奮！在此案例中，我們使用RV345P路由器。此路由器提供乙太網供電(PoE)，允許您將CBW140AC連線到路由器而不是交換機。CBW140AC和CBW142ACM網狀擴展器將用於建立無線網狀網路。

此高級路由器還提供其他功能的選項。

1. 應用控制允許您控制流量。此功能可配置為允許流量但記錄流量、阻止流量並記錄流量，或僅阻止流量。
2. 網路過濾用於防止網路流量流向不安全或不合適的網站。沒有使用此功能的日誌記錄。
3. AnyConnect是思科提供的安全套接字層(SSL)虛擬專用網路(VPN)。VPN允許遠端使用者和站點通過網際網路建立安全隧道連線到公司辦公室或資料中心。

如果要使用這些功能，您需要購買許可證。路由器和許可證均線上註冊，本指南將介紹這些資訊。

如果您不熟悉本文檔中使用的某些術語，或者希望瞭解有關網狀網路的更多詳細資訊，請查閱以下文章：

- Cisco Business：新字詞詞彙表
- 歡迎使用Cisco Business Wireless Mesh Networking
- 思科企業無線網路常見問題(FAQ)

適用裝置 |軟體版本

- RV345P | 1.0.03.21
- CBW140AC | 10.4.1.0
- CBW142ACM | 10.4.1.0（網狀網路至少需要一個網狀延伸器）

必要條件

準備路由器

1. 確保您當前有用於設定的Internet連線。
2. 請聯絡您的網際網路服務提供商(ISP)，瞭解他們在使用RV345P路由器時有何特殊說明。某些ISP提供帶有內建路由器的網關。如果您有一個整合路由器的網關，則可能必須禁用該路由器並將廣域網(WAN)IP地址（網際網路提供商分配給您帳戶的唯一網際網路協定地址）和所有網路流量傳送到您的新路由器。
3. 決定路由器的放置位置。如果可能的話你需要一個開放區域。這可能並不容易，因為您必須將路由器從您的網際網路服務提供商(ISP)連線到寬頻網關（數據機）。

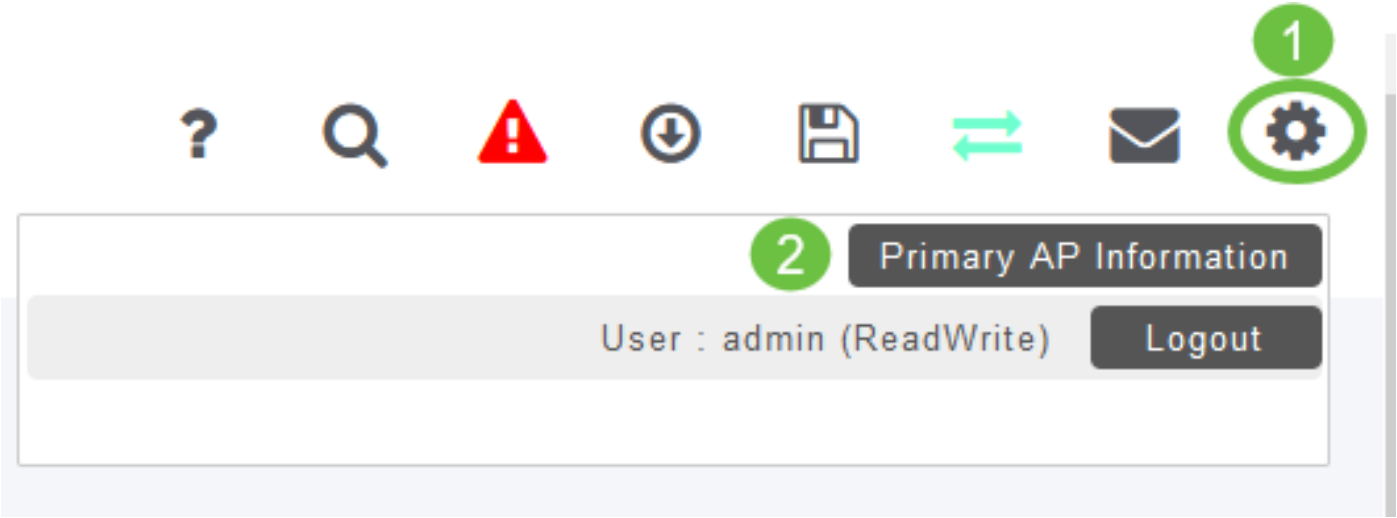
獲取Cisco.com帳戶

現在您擁有了思科裝置，您需要獲得Cisco.com帳戶，有時也稱為思科連線線上標識(CCO ID)。 帳戶不收費。

如果您已經擁有帳戶，可以跳轉到本文的下一部分。

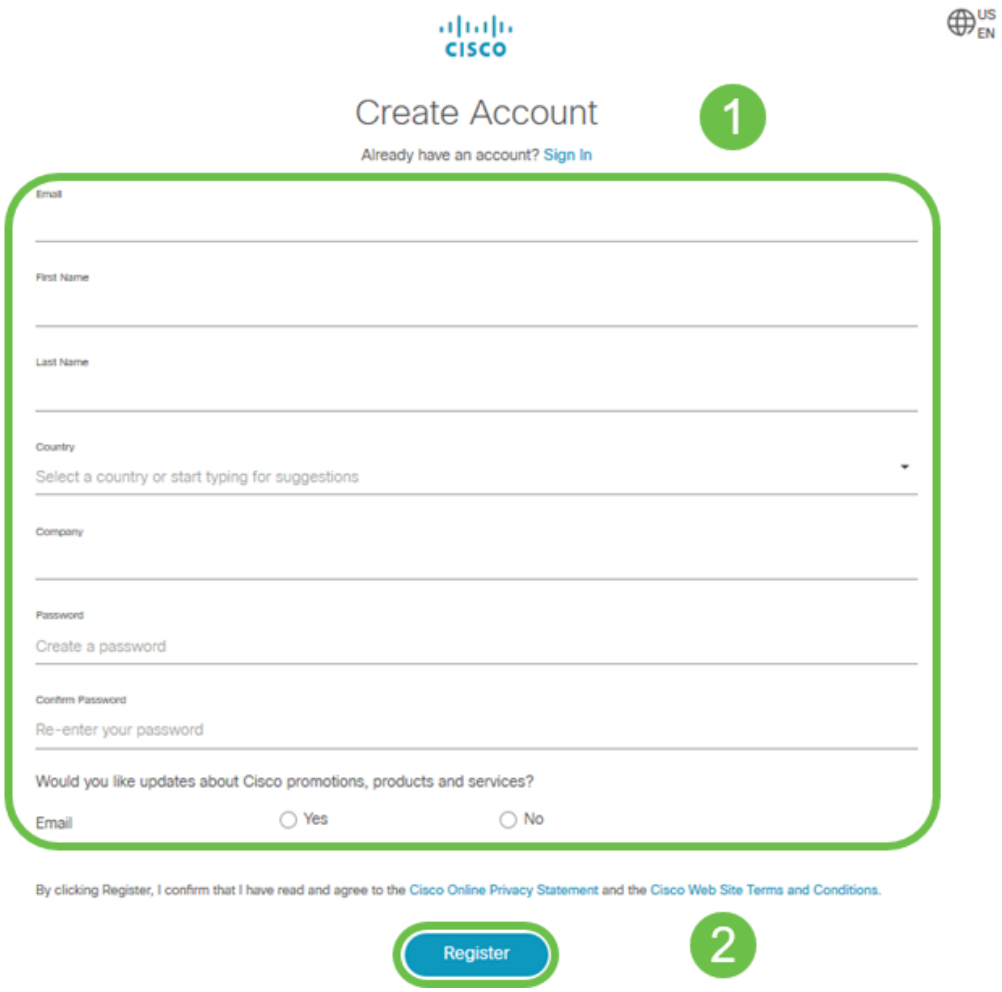
步驟1

前往Cisco.com。按一下**person icon**，然後按一下**Create an account**。



步驟2

輸入建立帳戶所需的詳細資訊，然後按一下**註冊**。按照說明完成註冊過程。



如果有任何問題，請[按一下以跳至Cisco.com帳戶註冊幫助頁面]。

配置RV345P路由器

路由器在網路中至關重要，因為它路由資料包。它使電腦能夠與不在同一網路或子網中的其他電腦通訊。路由器訪問路由表以確定應傳送資料包的位置。路由表列出了目的地址。靜態和動態配置都可以在路由表中列出，以便將資料包傳送到其特定的目的地。

您的RV345P帶有針對許多小型企業進行最佳化的預設設定。但是，您的網路要求或Internet服務提供商(ISP)可能會要求您修改其中一些設定。在聯絡您的ISP瞭解要求後，您可以使用Web使用者介面(UI)進行更改。

準備好了嗎？開始吧！

RV345P開箱即用

步驟1

將乙太網電纜從其中一個RV345P LAN（乙太網）埠連線到電腦上的乙太網埠。如果您的電腦沒有乙太網埠，您將需要介面卡。終端必須與RV345P處於同一有線子網中才能執行初始配置。

步驟2

確保使用RV345P隨附的電源介面卡。使用不同的電源介面卡可能會損壞RV345P或導致USB轉換器故障。電源開關預設開啟。

將電源介面卡連線到RV345P的12VDC埠，但不要將其插上電源。

步驟3

確保數據機已關閉。

步驟4

使用乙太網電纜將電纜或DSL數據機連線到RV345P上的WAN埠。

步驟5

將RV345P介面卡的另一端插入電源插座。這將開啟RV345P的電源。重新插入數據機，以便它也能通電。正確連線電源介面卡且RV345P完成啟動後，前面板上的電源指示燈呈穩定綠色。

設定路由器

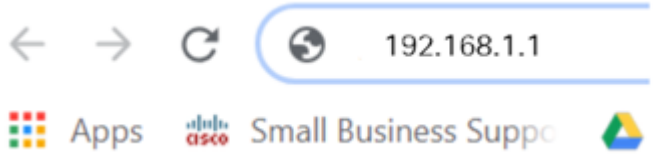
準備工作已完成，現在需要執行一些配置！要啟動Web UI，請執行以下步驟。

步驟1

如果電腦配置為成為動態主機配置協定(DHCP)客戶端，則192.168.1.x範圍內的IP地址將分配給PC。DHCP自動將IP地址、子網掩碼、預設網關和其他設定分配給電腦。必須將電腦設定為參與DHCP過程以獲取地址。這可以通過在電腦上的TCP/IP屬性中選擇自動獲取IP地址來實現。

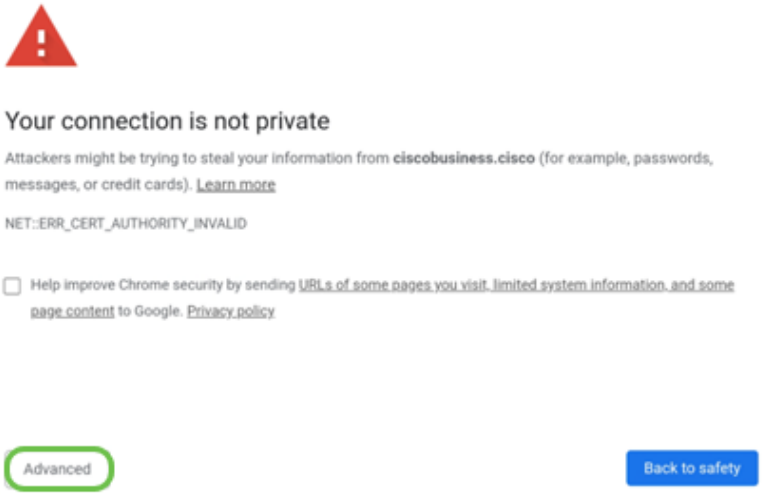
步驟2

開啟Web瀏覽器，例如Safari、Internet Explorer或Firefox。在位址列中，輸入RV345P的預設IP地址192.168.1.1。



步驟3

瀏覽器可能會發出警告，指出該網站不可信。繼續瀏覽網站。如果您未連線，請跳至Internet連線故障排除。

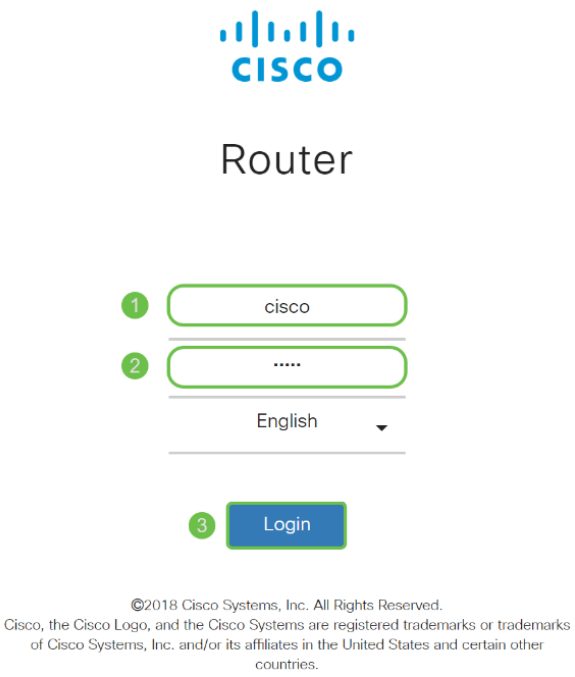


步驟4

登入頁面顯示時，輸入預設使用者名稱*cisco*和預設密碼*cisco*。

按一下「**Login**」。

有關詳細資訊，請按一下How to access the web-based setup page of Cisco RV340 series VPN routers。



步驟5

按一下「**Login**」。系統將顯示*Getting Started*頁面。如果導航窗格未開啟，可以通過按一下選單圖示來打**開它**。

確認連線並登入到路由器後，跳至本文的初始配置部分。

Internet連線故障排除

見鬼，如果您正在閱讀此內容，則可能難以連線到Internet或Web UI。其中一種解決方案應該會有所幫助。

在連線的Windows作業系統上，可以通過開啟命令提示符來測試網路連線。輸入**ping 192.168.1.1**（路由器的預設IP地址）。 如果請求超時，您將無法與路由器通訊。

如果沒有建立連線，您可以檢視本**疑難排解**文章。

還有其它事情要嘗試：

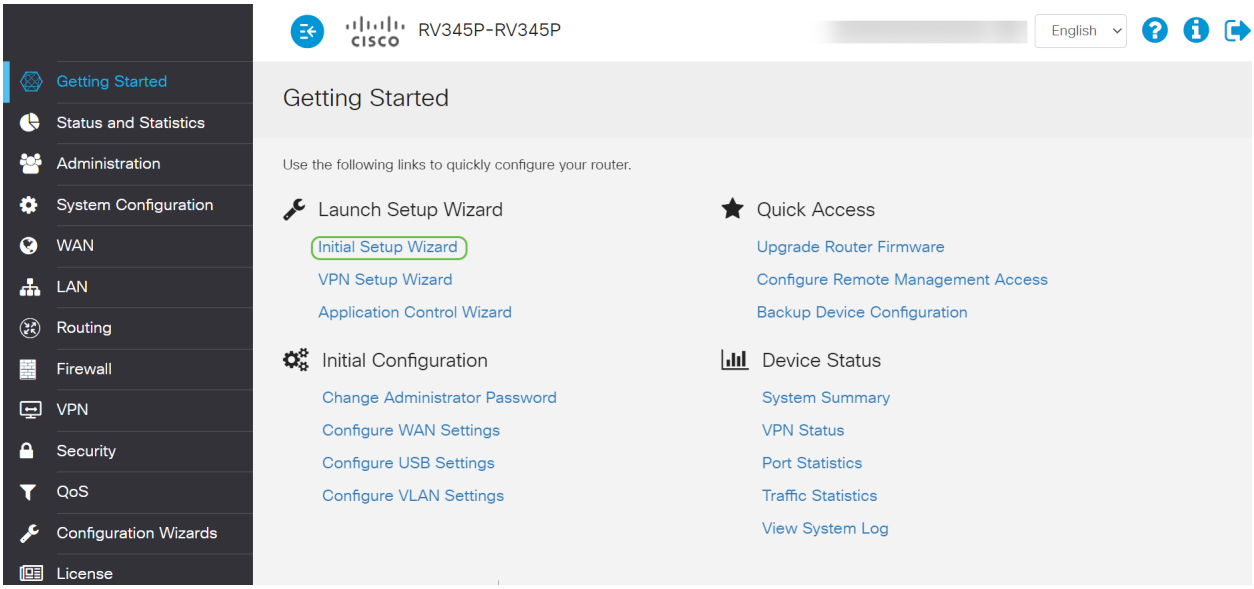
1. 確認您的Web瀏覽器未設定為「離線工作」。
2. 檢查乙太網介面卡的區域網連線設定。PC應通過DHCP獲取IP地址。或者，PC可以擁有一個192.168.1.x範圍內的靜態IP地址，預設網關設定為192.168.1.1（RV345P的預設IP地址）。 要連線，可能需要修改RV345P的網路設定。如果您使用的是Windows 10，請檢視**Windows 10說明以修改網路設定**。
3. 如果現有裝置佔用了192.168.1.1 IP地址，您需要解決此衝突才能使網路正常運行。在本節結尾處對此進行更多說明，或**點選此處直接進行說明**。
4. 通過關閉兩台裝置來重置數據機和RV345P。然後，開啟數據機的電源，使其空閒約2分鐘。然後開啟RV345P的電源。您現在應該會收到WAN IP地址。
5. 如果您有DSL數據機，請讓ISP將DSL數據機置於網橋模式。

初始配置

建議您完成本部分所列*的初始設*置嚮導步驟。您可以隨時更改這些設定。

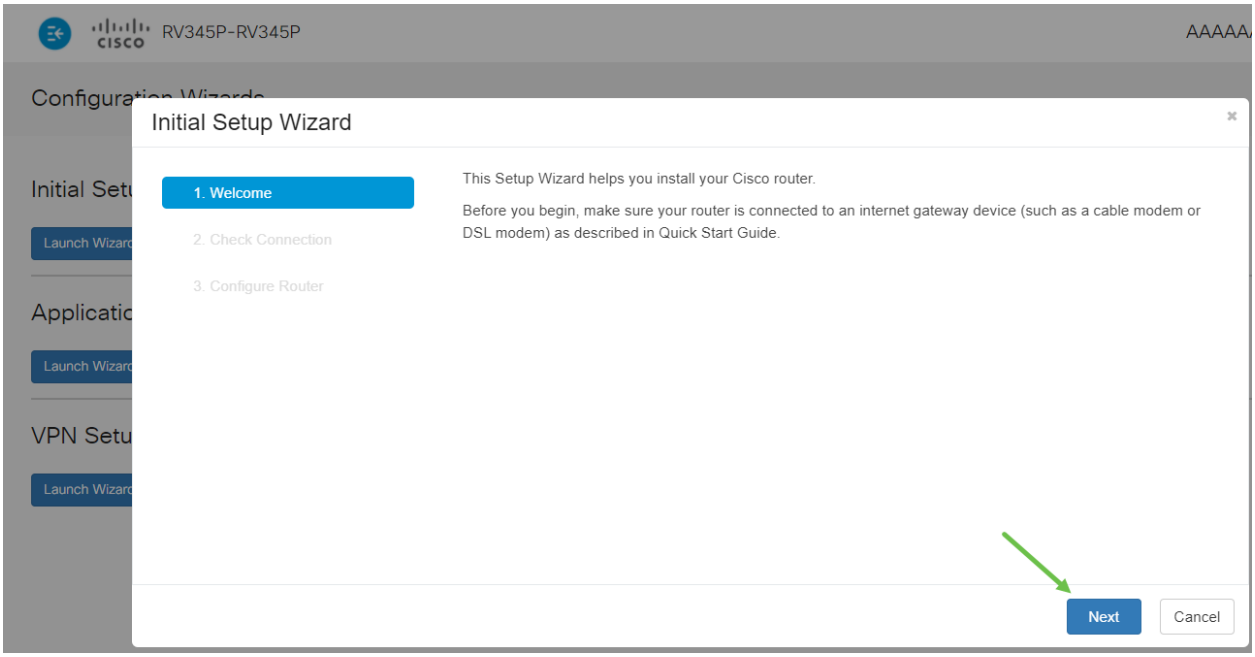
步驟1

在*Getting Started*頁中按一下**Initial Setup Wizard**。



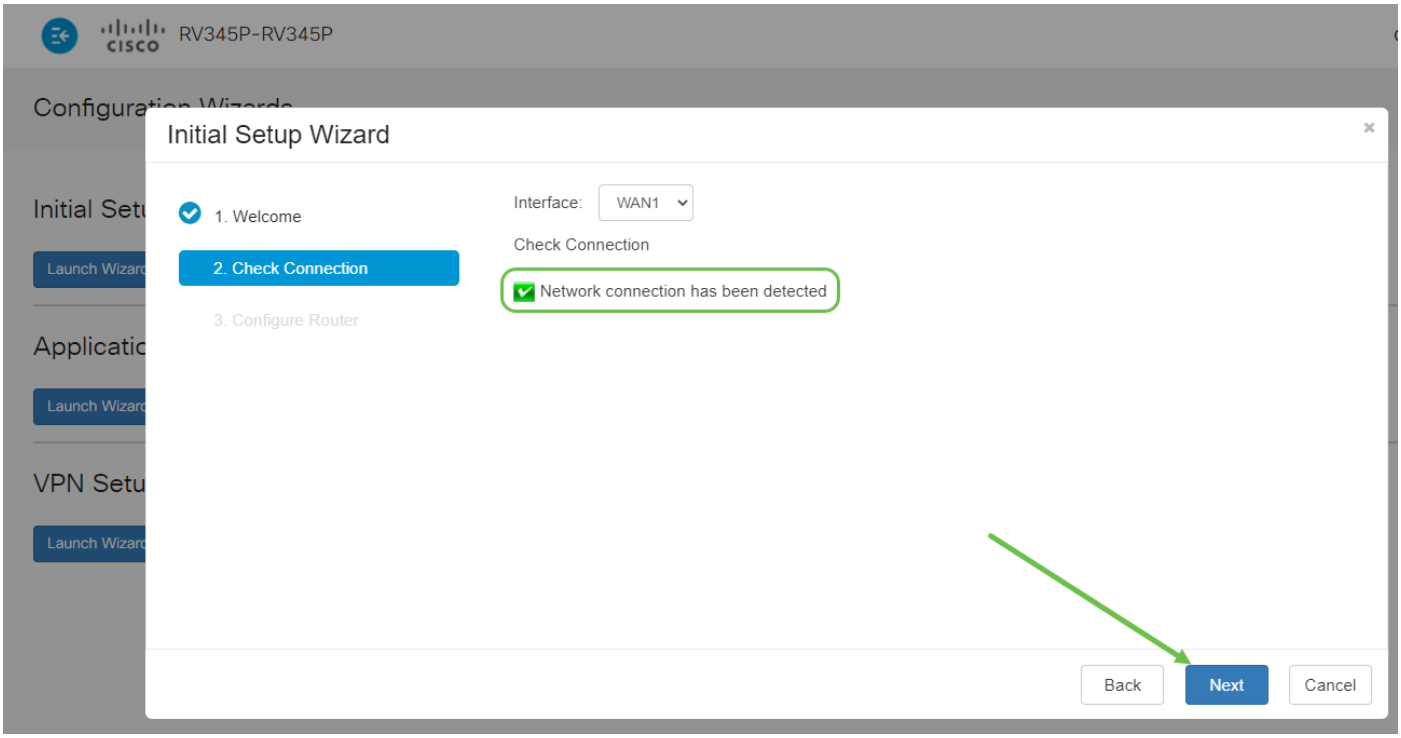
步驟2

此步驟確認電纜已連線。由於您已確認此情況，請按一下**下一步**。



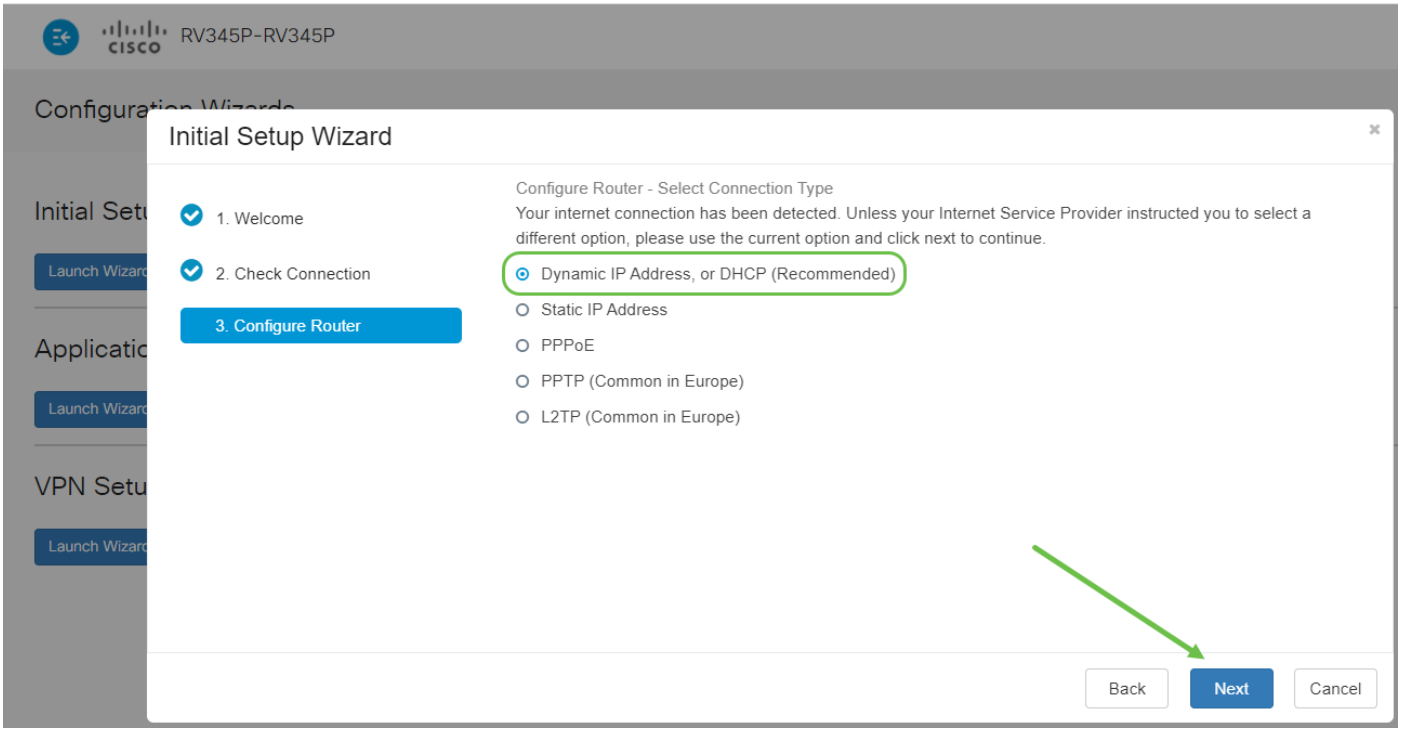
步驟3

此步驟包含確保路由器連線的基本步驟。由於您已確認這一點，請按一下**下一步**。



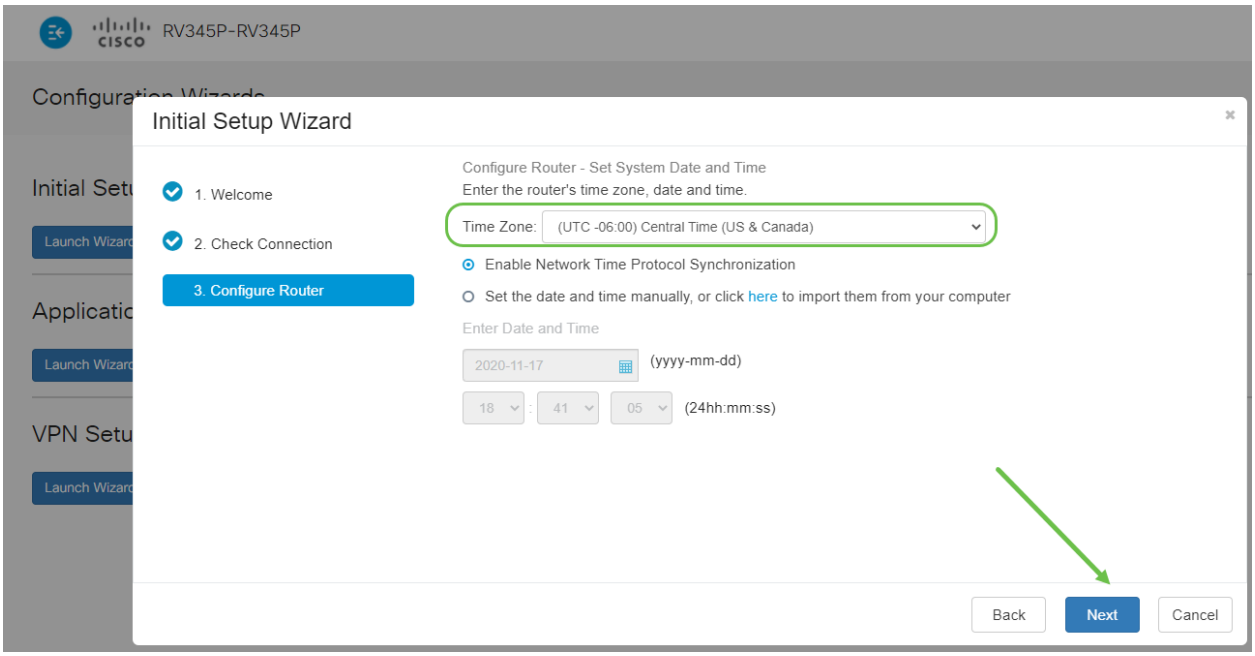
步驟4

下一個螢幕顯示用於為路由器分配IP地址的選項。您需要在此場景中選擇DHCP。按「Next」（下一步）。



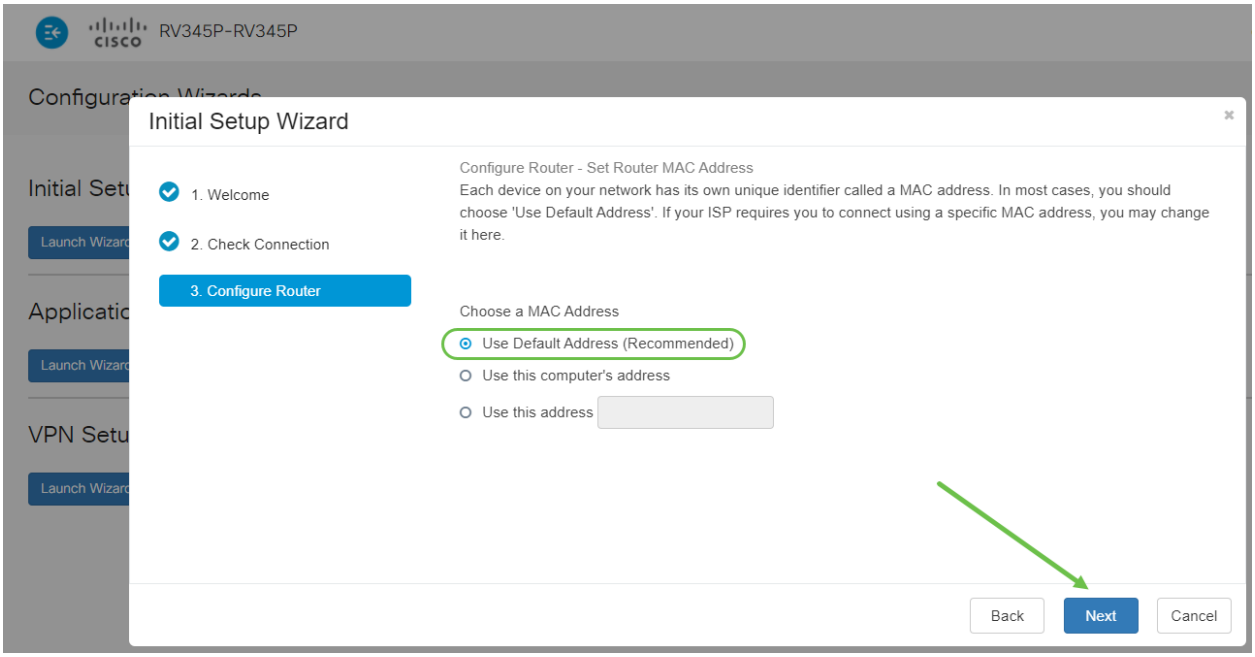
步驟5

系統將提示您設定路由器時間設定。這一點很重要，因為它能夠在檢視日誌或排除事件故障時提供精確性。選擇您的**時區**，然後按一下**下一步**。



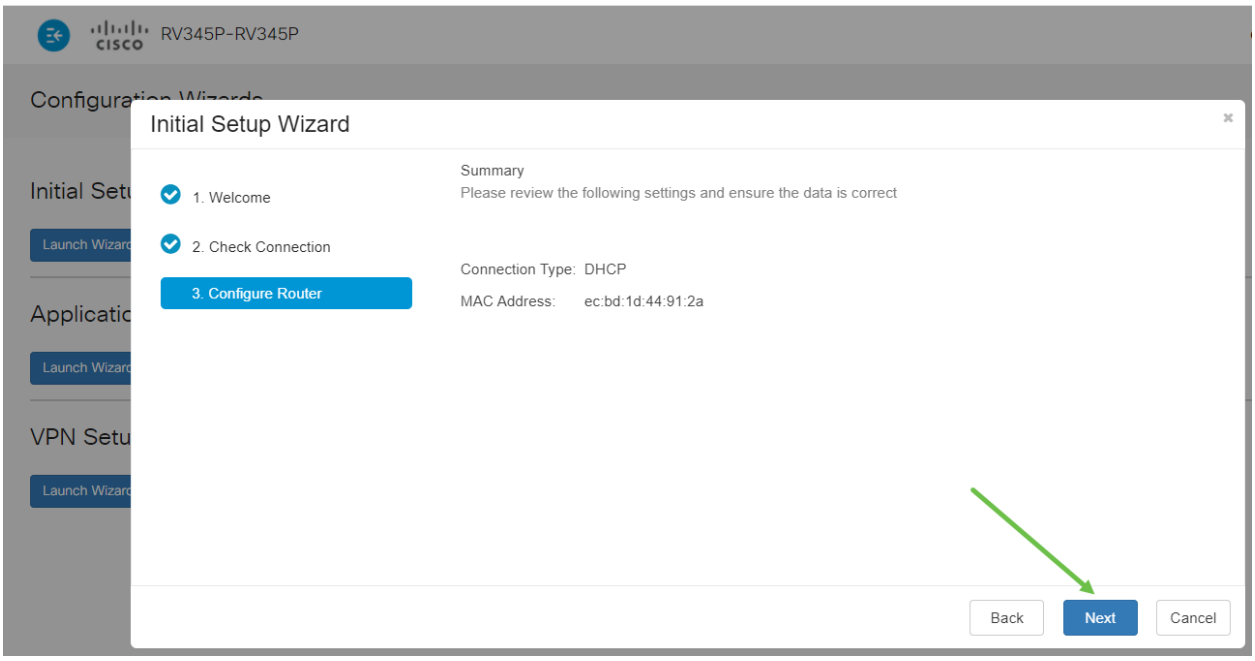
步驟6

您將選擇要分配給裝置的MAC地址。通常，您將使用預設地址。按「Next」（下一步）。



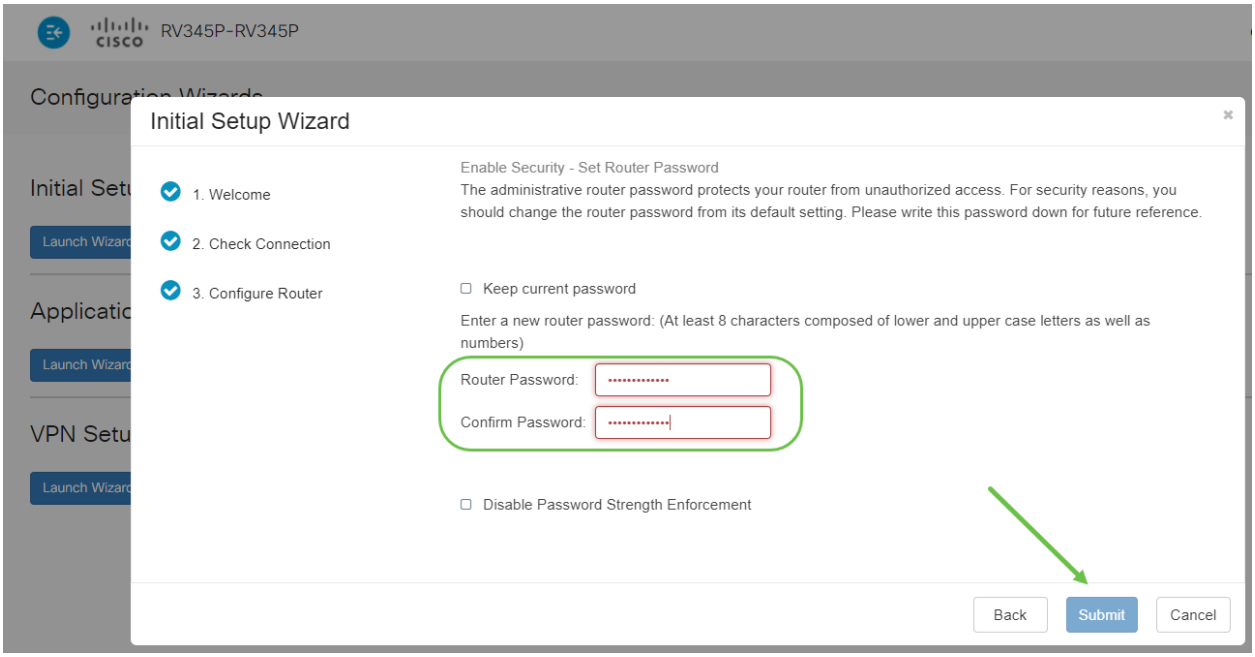
第7步

下一頁是所選選項的摘要。如果滿意，請檢視並按一下**Next**。



步驟8

在下一步中，您將選擇登入路由器時要使用的密碼。密碼的標準是包含至少8個字元（大寫和小寫），並包含數字。請輸入符合強度要求的密**碼**。按「Next」（下一步）。記下您以後登入的密碼。



不建 議您選擇Disable *Password Strength Enforcement*。此選項可讓您選擇簡單到123的密碼，對於惡意攻擊者，該密碼可輕易破解1-2-3。

步驟9

按一下**save圖示**。

如需這些設定的詳細資訊，可以閱讀[在RV34x路由器上配置DHCP WAN設定]。

您的RV345P預設啟用乙太網供電(PoE)，但是您可以對它們進行一些調整。如果您需要自定義設定，請檢視RV345P路由器上的[配置乙太網供電(PoE)設定]。

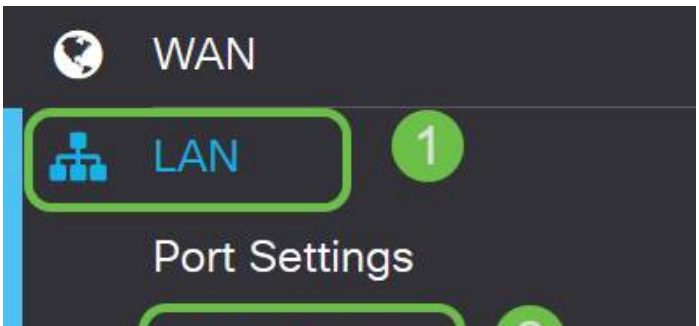
根據需要編輯IP地址（可選）

完成*初始設定嚮導*後，您可以通過編輯VLAN設定來在路由器上設定靜態IP地址。

僅當需要在現有網路中為路由器IP地址分配特定地址時，才需要執行此過程。如果您不需要編輯IP地址，可以轉到本[文的]下一節。

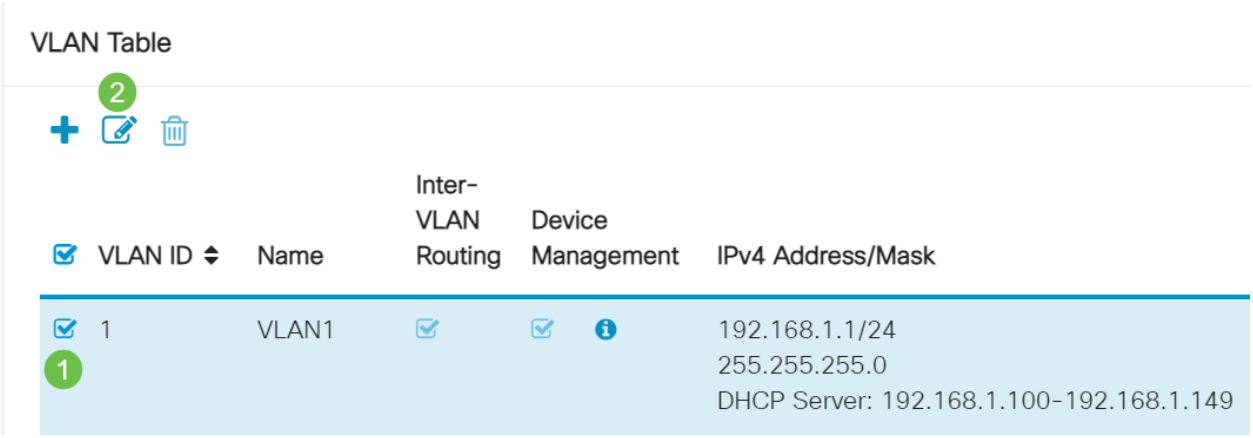
步驟1

在左側選單中，按一下**LAN > VLAN Settings**。



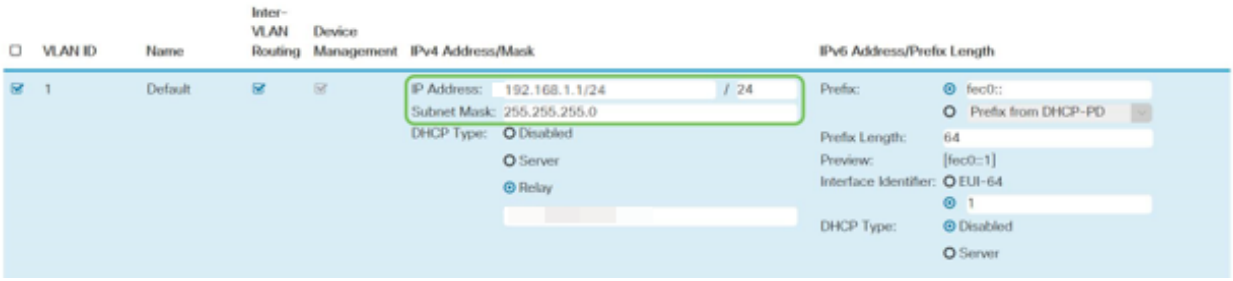
步驟2

選擇包含路由裝置的**VLAN**，然後按一下**edit**圖示。



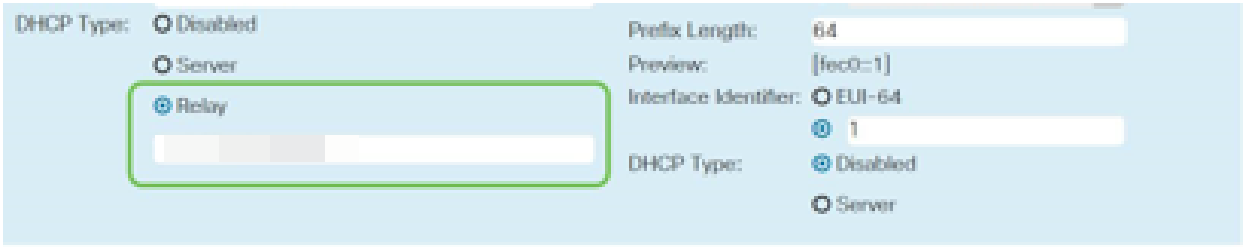
步驟3

輸入所需的**靜態IP地址**，然後按一下右上角的**Apply**。



第4步（可選）

如果您的路由器不是DHCP伺服器/裝置分配IP地址，則可以使用DHCP中繼功能將DHCP請求定向到特定IP地址。IP地址可能是連線到WAN/Internet的路由器。

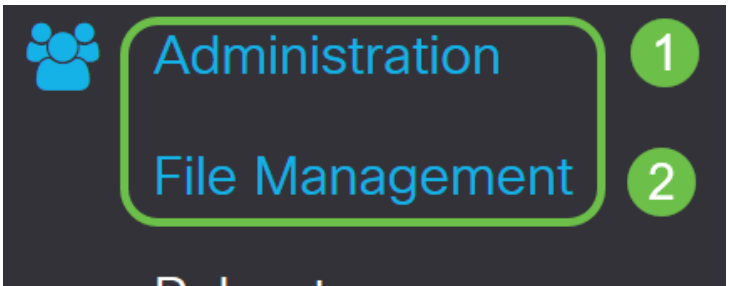


升級韌體（如果需要）

這是重要的一步，不要逃避！

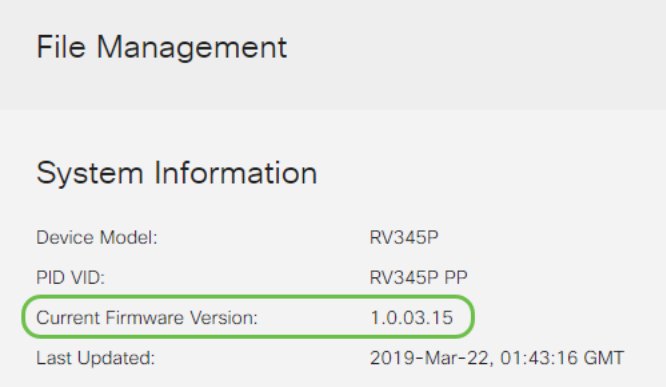
步驟1

選擇**Administration > File Management**。



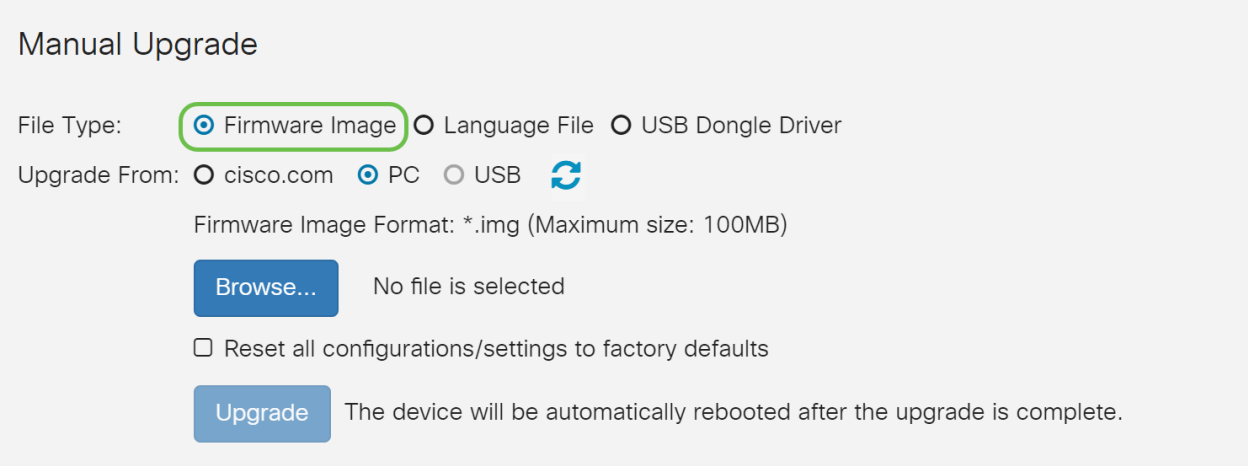
在*System Information*區域中，以下子區域說明以下內容：

- 裝置型號 — 顯示裝置的型號。
- PID VID — 路由器的產品ID和供應商ID。
- Current Firmware Version — 裝置上當前運行的韌體。
- Cisco.com提供的最新版本 — 思科網站提供的最新軟體版本。
- Firmware last updated — 路由器上上次韌體更新的日期和時間。



步驟2

在*Manual Upgrade*部分下，按一下**Firmware Image**單選按鈕*File Type*。



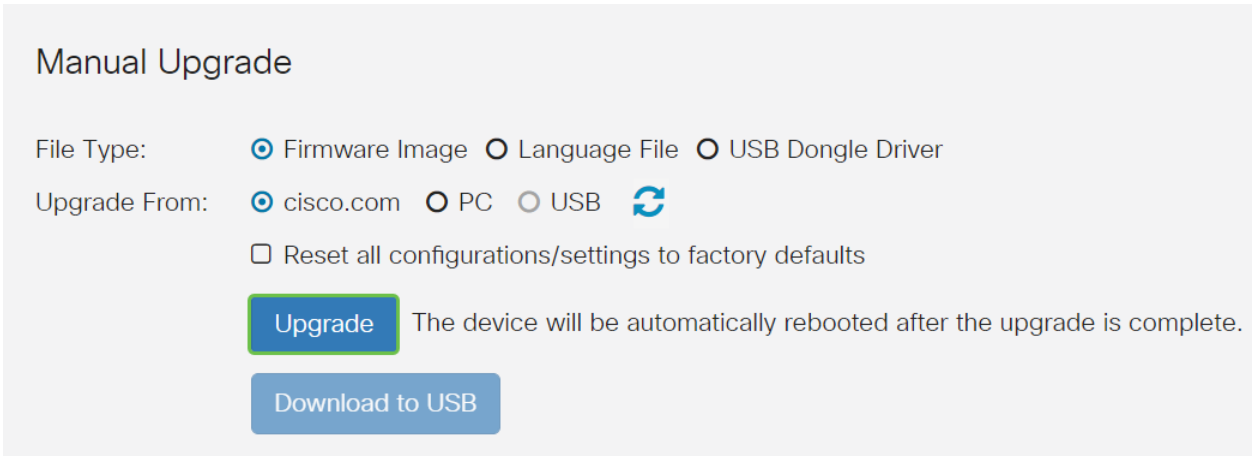
步驟3

在「*Manual Upgrade*」頁面上，按一下單選按鈕選擇*cisco.com*。還有幾個其他選項，但這是最簡單的升級方式。此程式會直接從思科軟體下載網頁安裝最新的升級檔案。

如果您的裝置未連線到Internet或正處於Internet斷開狀態，您將無法從cisco.com進行升級。如果這適用於您，則可以在此處找到替代 選項。

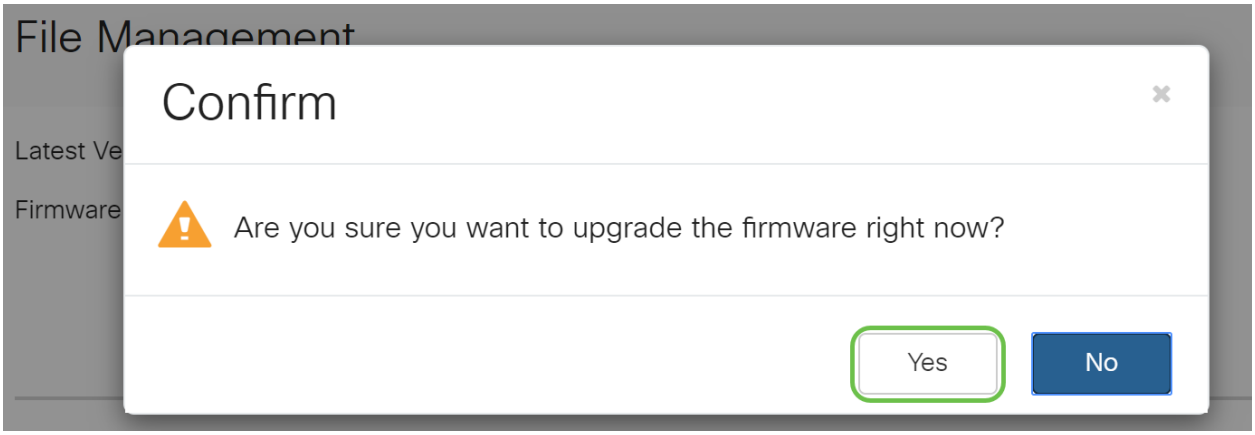
步驟4

按一下「**Upgrade**」。

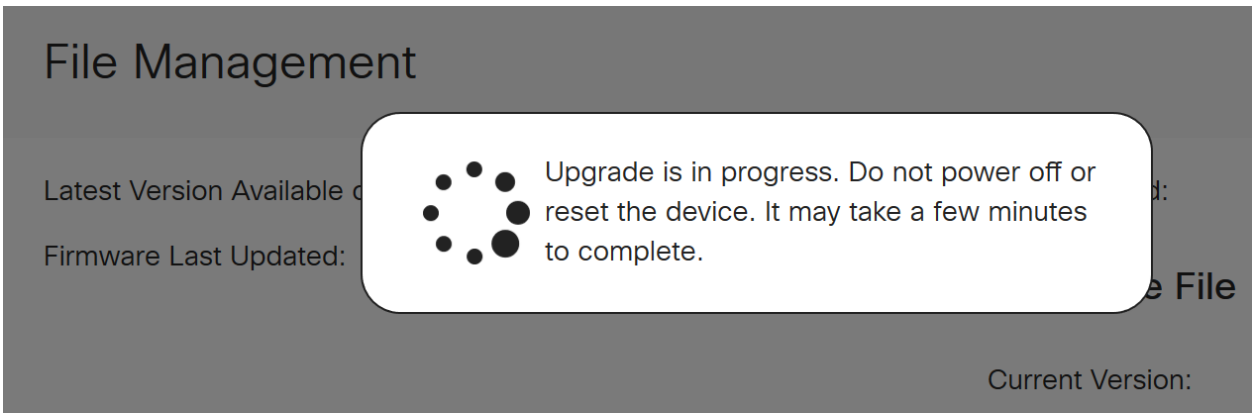


步驟5

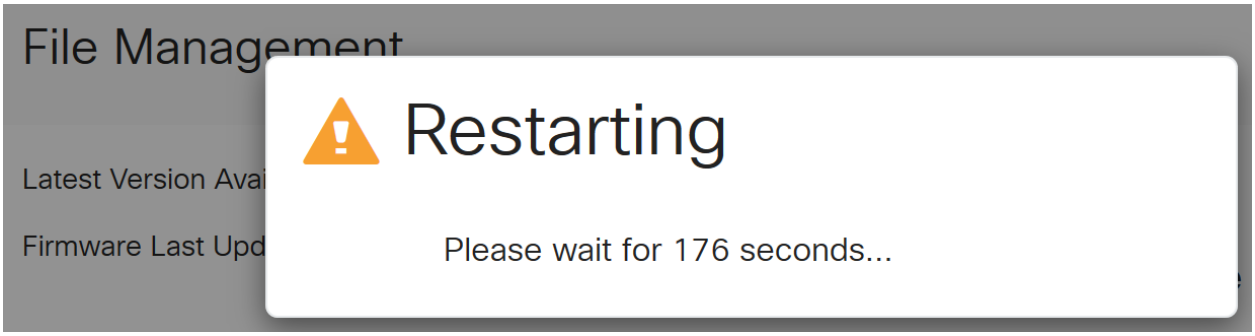
在確認視窗中按一下**Yes**以繼續。



更新過程需要無中斷運行。升級過程中，螢幕上會顯示以下消息。

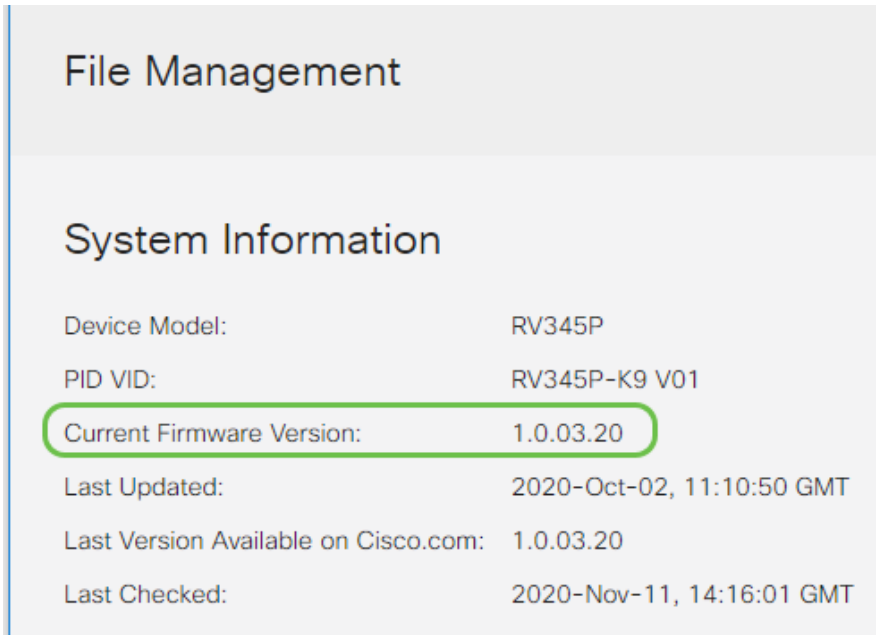


升級完成後，將出現一個通知視窗，通知您路由器將重新啟動，並註明預計完成該過程所需的時間。之後，您將登出。



步驟6

重新登入到基於Web的實用程式以驗證路由器韌體是否已升級，滾動到*系統資訊*。*Current Firmware Version*區域現在應顯示升級後的韌體版本。

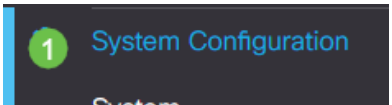


在RV345P系列路由器上配置自動更新

由於更新非常重要，而您是一個繁忙的人，因此從這裡向外配置自動更新很有意義！

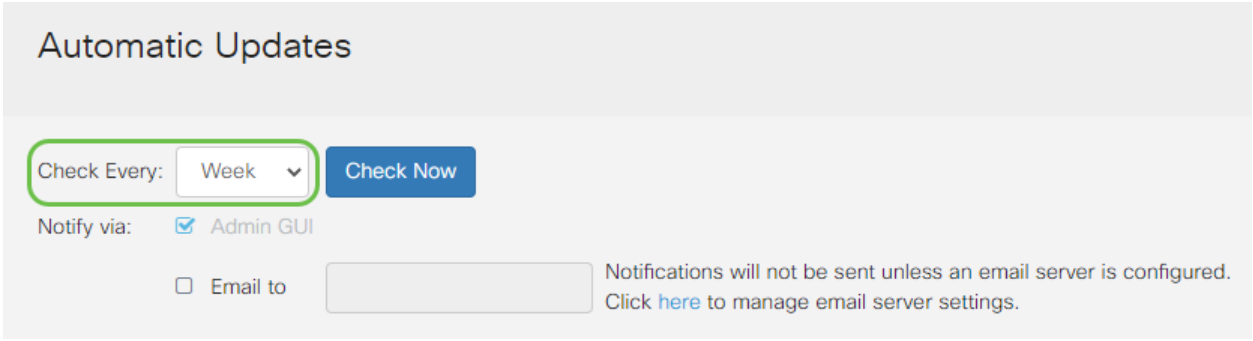
步驟1

登入到基於Web的實用程式，然後選擇**System Configuration > Automatic Updates**。



步驟2

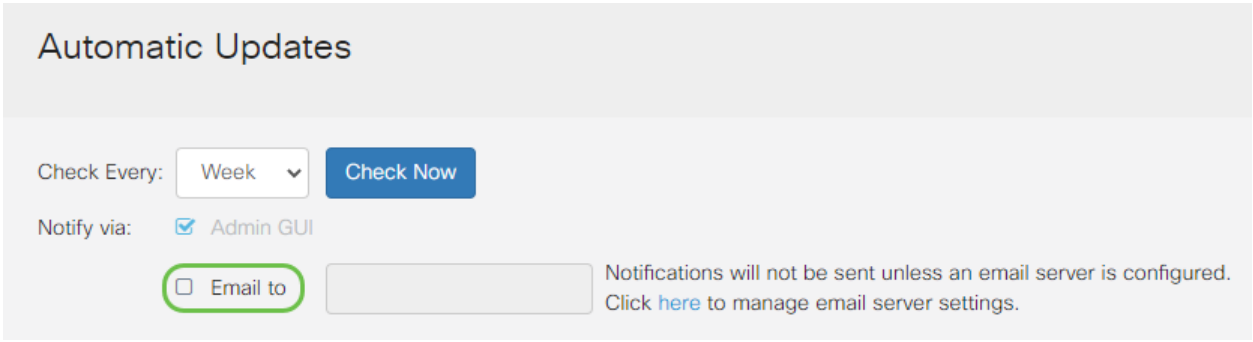
在「*Check Every*」下拉式清單中，選擇路由器應檢查更新的頻率。



步驟3

在*Notify via*區域中，選中**Email to**覈取方塊以通過電子郵件接收更新。*Admin GUI*覈取方塊預設啟用，無法禁用。更新可用後，通知將顯示在基於Web的配置中。

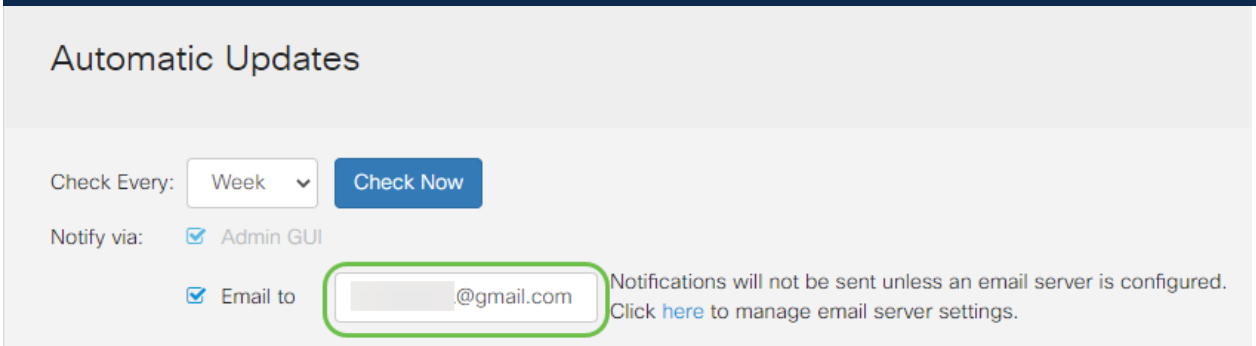
如果要設定電子郵件伺服器設定，請按一下**此處**瞭解方法。



步驟4

在*Email to* address欄位中輸入電*子郵件*地址。

強烈建議使用單獨的電子郵件帳戶，而不是使用個人電子郵件來維護隱私。

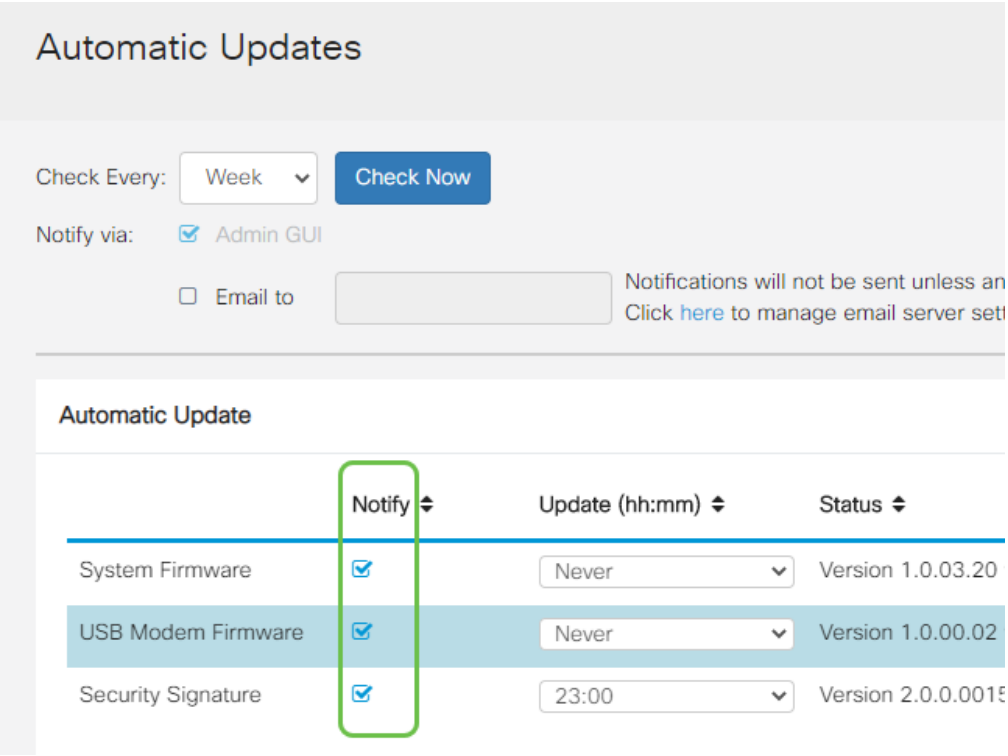


步驟5

在*Automatically Update*區域下，選中要通知的更新型別的**Notify**覈取方塊。選項包括：

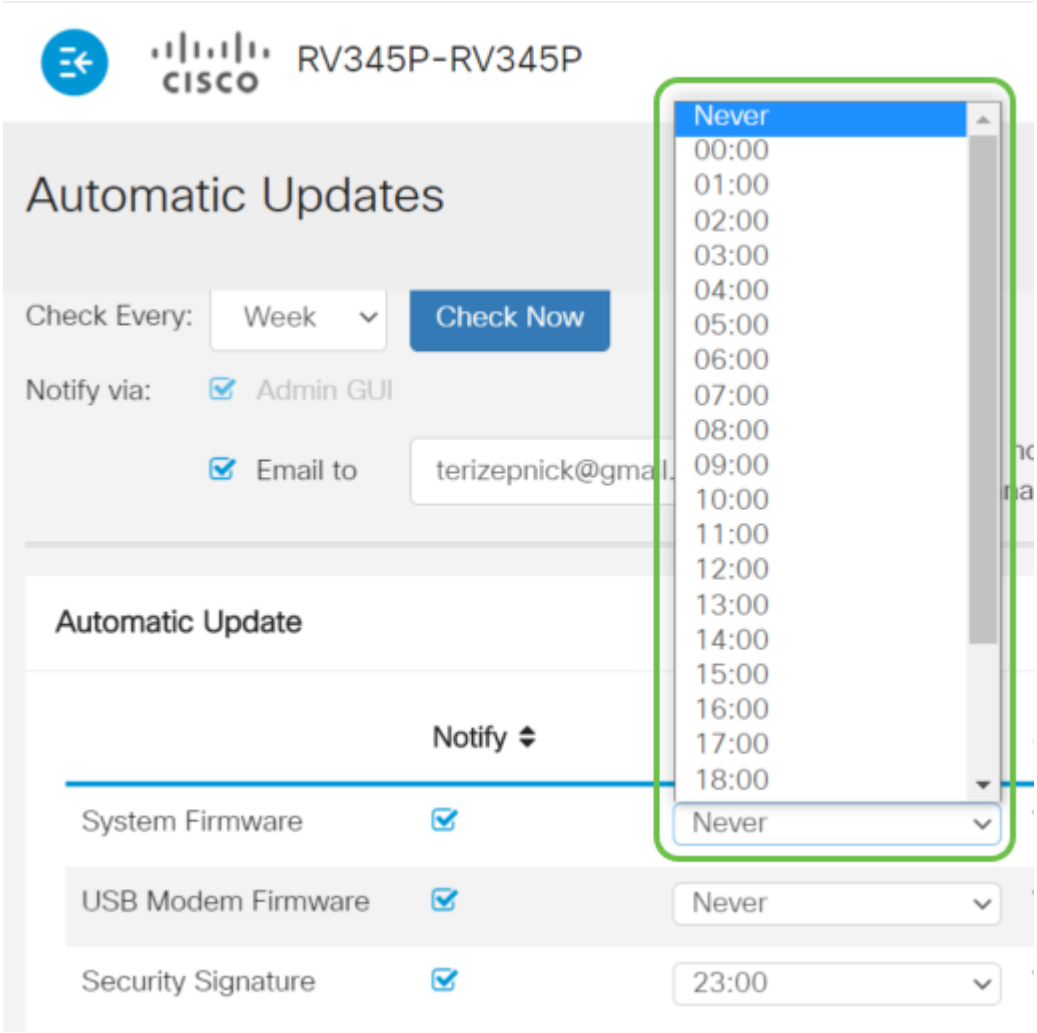
- 系統韌體 — 裝置的主控制程式。

- USB數據機韌體 — USB埠的控制程式或驅動程式。
- 安全簽名 — 這將包含應用程式控制的簽名，以識別應用程式、裝置型別、作業系統等。



步驟6

在「*Automatic Update*」下拉選單中，選擇希望完成自動更新的當天時間。某些選項可能會因您選擇的更新型別而異。安全簽名是進行即時更新的唯一選項。建議您在辦公室關閉時設定時間，以免服務在不方便的時間中斷。



狀態顯示當前運行的韌體版本或安全簽名。

第7步

按一下「Apply」。

步驟8

要永久儲存配置，請轉到「複製/儲存配置」頁，或按一下該頁上方的save圖示。

太棒了，您的路由器基本設定已完成！現在，您可以瞭解一些配置選項。

安全選項

當然，您希望網路安全。有一些簡單的選項，例如使用複雜的密碼，但是如果您想採取步驟來實現更安全的網路，請閱讀本節的安全說明。

RV安全許可證（可選）

此RV安全許可證功能可保護您的網路免受來自網際網路的攻擊：

- 入侵防禦系統(IPS):檢查網路資料包、日誌和/或阻止各種網路攻擊。它可以提高網路可用性、加快補救速度，並提供全面的威脅防護。
- 防病毒：通過掃描應用程式中的各種協定（例如通過路由器的HTTP、FTP、SMTP電子郵件附件、POP3電子郵件附件和IMAP電子郵件附件）來防禦病毒。
- 網路安全：在連線到Internet時提高業務效率和安全性，允許終端裝置和Internet應用程式的網際網路訪問策略來幫助確保效能和安全性。它是基於雲的，包含80多個類別，分類域超過4.5億個。
- 應用程式標識：確定策略並將其分配給Internet應用程式。自動識別出500個獨特的應用程式。
- 客戶端標識：動態識別客戶端並對其進行分類。能夠根據終端裝置類別和作業系統分配策略。

RV安全許可證提供網路過濾。Web篩選功能允許您管理對不合適網站的訪問。它可以遮蔽客戶端的Web訪問請求以確定是允許還是拒絕該網站。

許可的安全功能可免費試用90天。如果要在評估期後繼續使用路由器的高級安全功能，則必須獲取並啟用許可證。

另一個安全選項是Cisco Umbrella。**如果您想跳至Umbrella部分，請按一下此處**。

如果您不需要任何安全許可證，**請按一下以跳轉到本文檔的VPN部分**。

智慧帳戶簡介

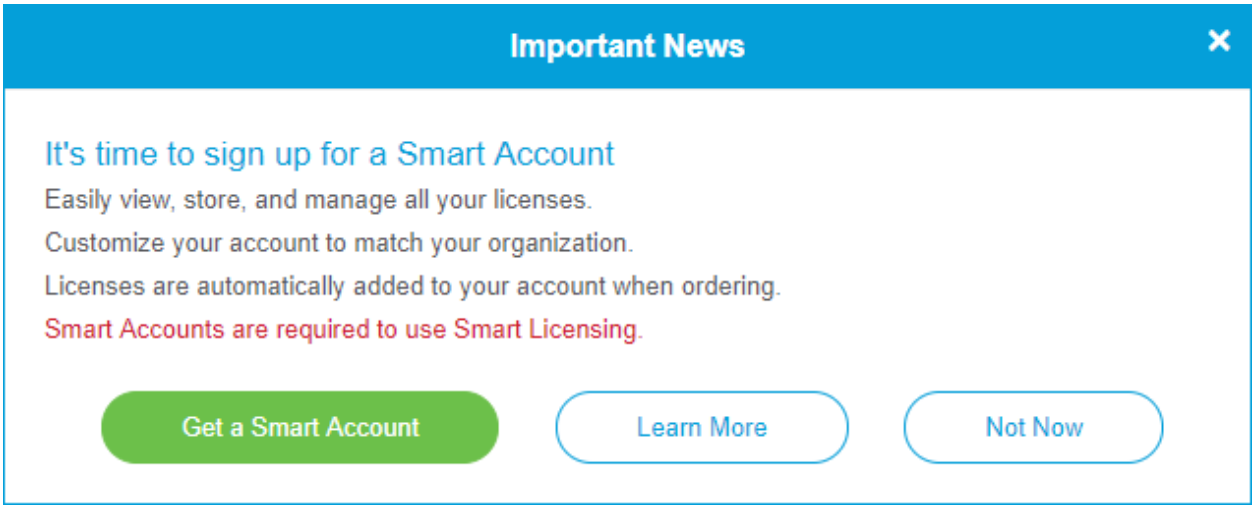
要購買RV安全許可證，您需要一個智慧帳戶。

授權啟用此智慧帳戶即表示您同意授權您代表您的組織建立帳戶、管理產品和服務授權、許可協定以及使用者訪問帳戶。思科合作夥伴不得代表客戶授權建立帳戶。

建立新的智慧帳戶是一個一次性事件，從該點起通過工具向前提供管理。

建立智慧帳戶

當您使用Cisco.com帳戶或CCO ID（您在本文檔開頭建立的帳戶）訪問您的常規思科帳戶時，可能會收到一條建立智慧帳戶的消息。



如果您沒有看到此彈出視窗，可以按一下進入智慧帳戶**建立頁面**。您可能需要使用Cisco.com帳戶憑據登入。

有關請求智慧帳戶涉及的步驟的其他詳細資訊，請點選此處。

請務必記下您的帳戶名以及其他註冊詳細資訊。

快速提示：如果您需要輸入域，但您沒有域，則可以以name@domain.com的形式輸入您的電子郵*件地址*。常見的域包括gmail、yahoo等，具體取決於您的公司或提供商。

在購買RV安全許可證之前，請務必擁有Cisco.com(CCO ID)帳戶和思科智慧帳戶。

購買RV安全許可證

您必須從您的思科總代理商或思科合作夥伴處購買許可證。若要尋找思科合作夥伴，請按一下**此處**。

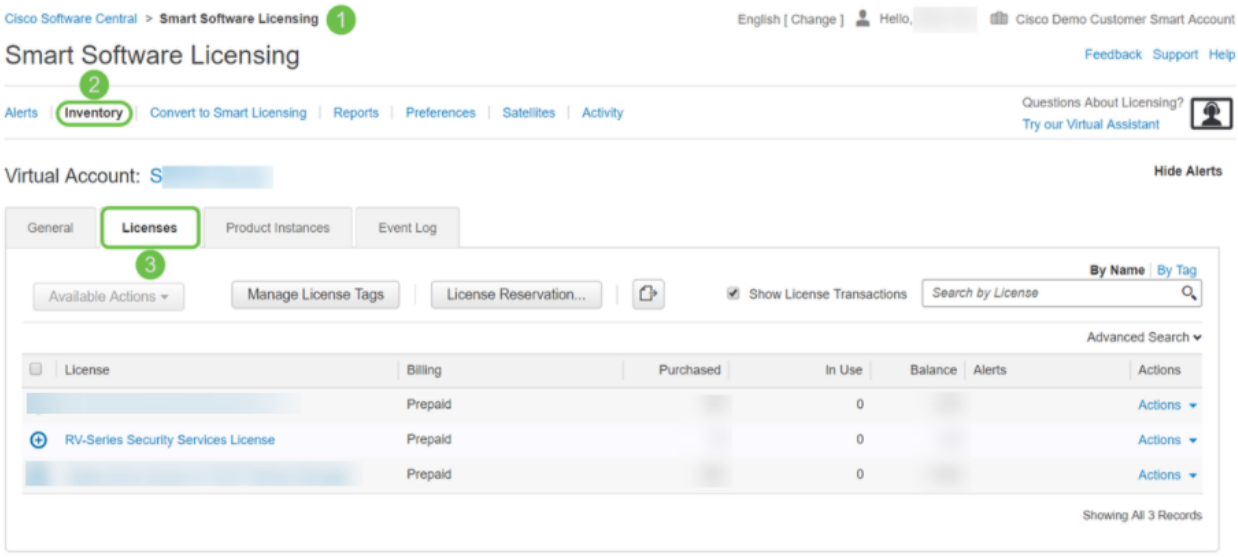
下表顯示了許可證的部件號。

類型	產品ID	說明
RV安全許可證	LS-RV34X-SEC-1YR=	RV安全性：1年：動態Web過濾器、應用可視性、客戶端識別和統計

許可證金鑰不會直接輸入路由器，但會在您訂購許可證後分配給您的思科智慧帳戶。許可證顯示在您的帳戶上所需的時間取決於合作夥伴接受訂單的時間以及經銷商將許可證連結到您的帳戶的時間（通常為24-48小時）。

確認許可證在智慧帳戶中

導航到您的智慧許可證帳戶頁面，然後點選**智慧軟體許可證頁面>清單>許可證**。

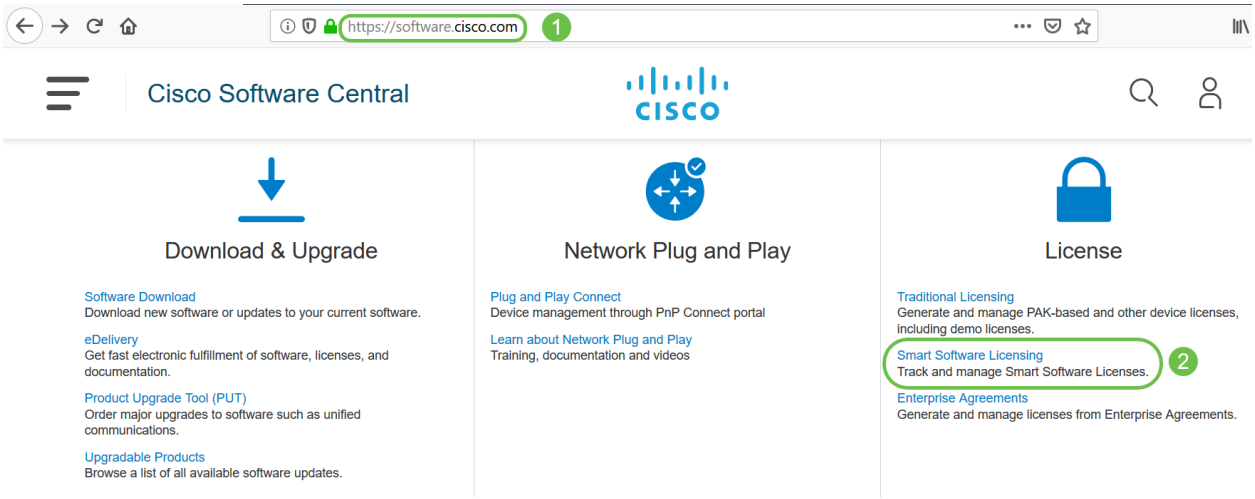


如果您在智慧帳戶中看不到許可證，請聯絡您的思科合作夥伴。

在RV345P系列路由器上配置RV安全許可證

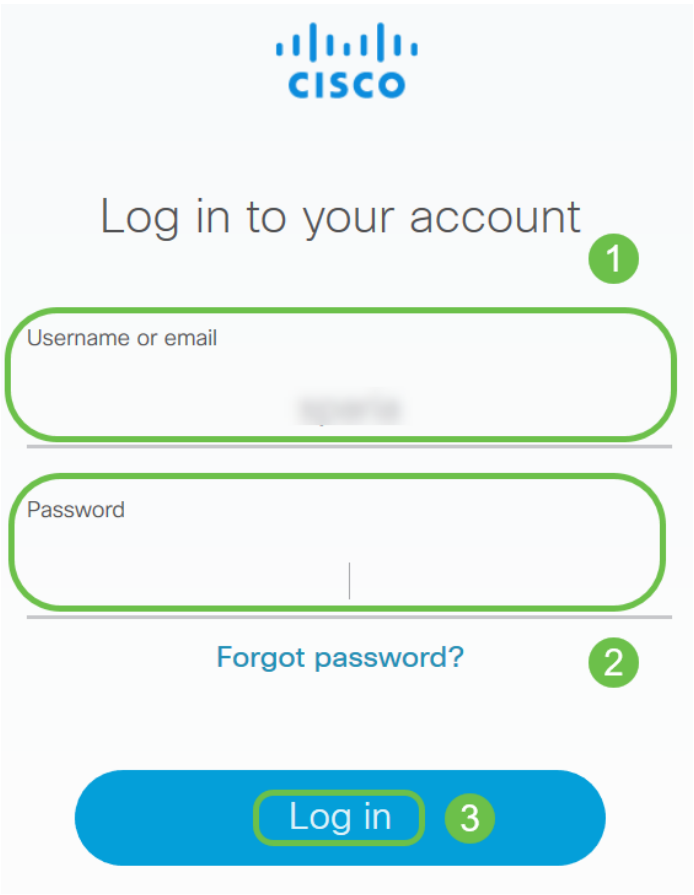
步驟1

存取思科軟體並導覽至**智慧軟體授權**。



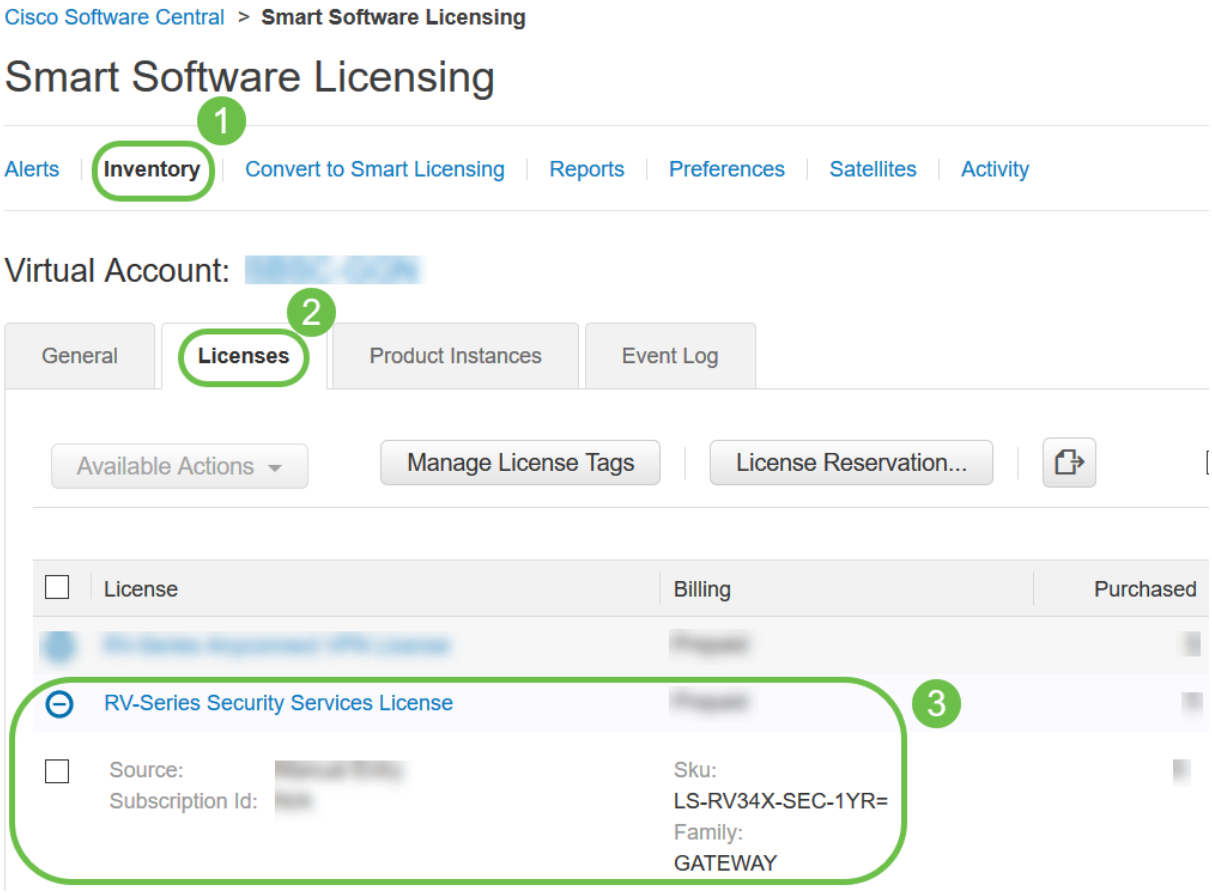
步驟2

輸入您的*使用者名稱*、*電子郵件*和*密碼*以登入您的智慧帳戶。按一下「**Log in**」。



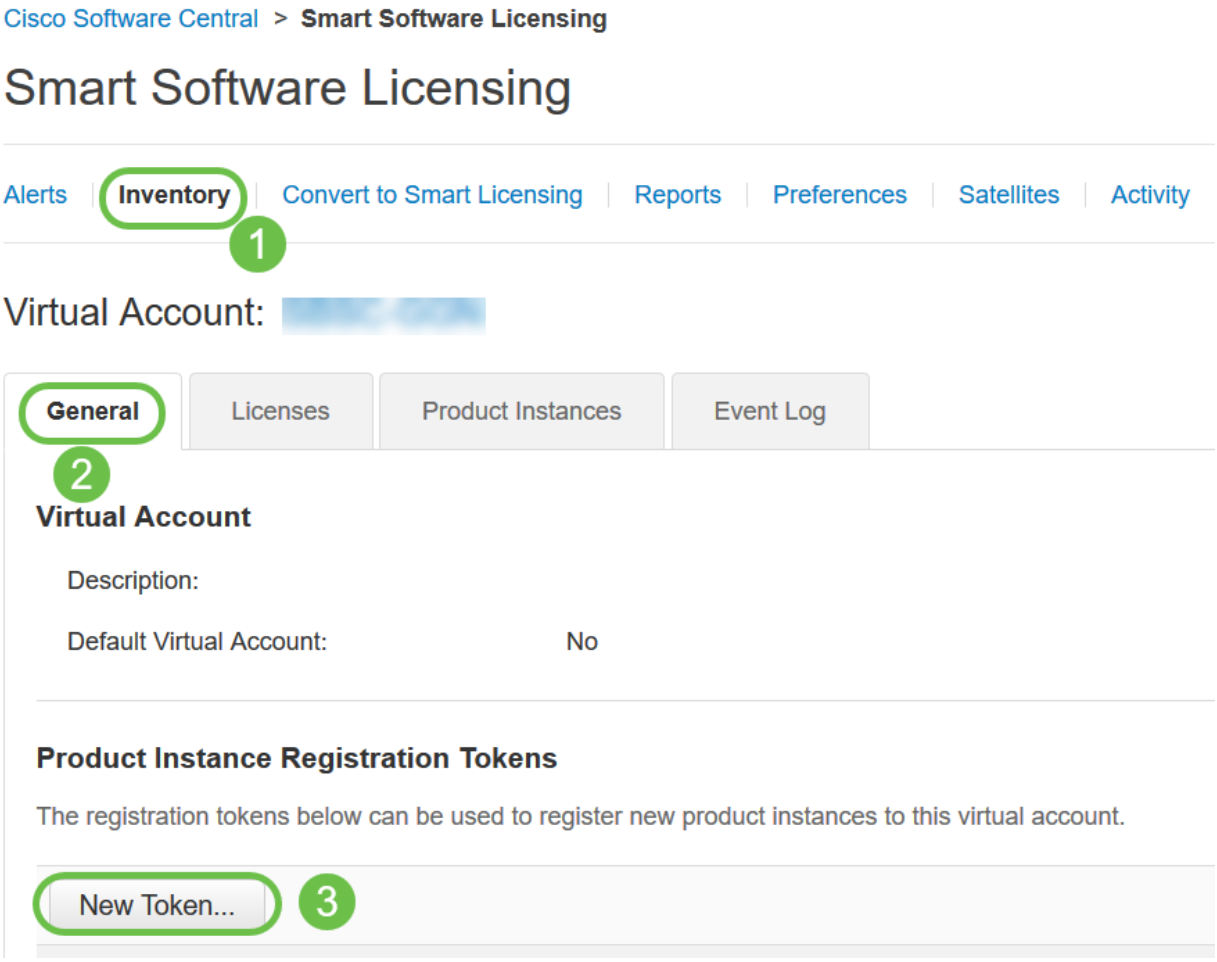
步驟3

導覽至**Inventory > Licenses**，確認*RV-Series Security Services License*已列在智慧帳戶中。如果您沒有看到列出的許可證，請聯絡您的思科合作夥伴。



步驟4

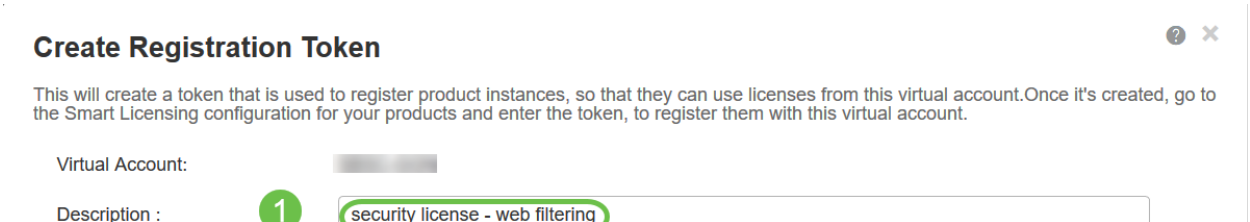
定位至**庫存>常規**。在*Product Instance Registration Tokens*下，按一下**New Token**。



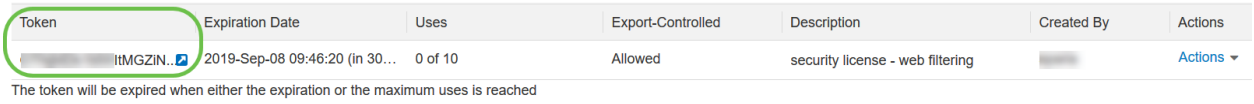
步驟5

將會出現「建立註冊令牌」視窗。*Virtual Account*區域顯示將在其下建立註冊令牌的虛擬帳戶。在「*建立註冊令牌*」頁上，完成以下操作：

- 在Description欄位中，輸入權杖的唯一說明。在本示例中，輸入了安全許可證 — Web過濾。
- 在「失效時間」欄位中，輸入介於1到365天之間的值。思科建議將此欄位的值設為30天；但是，您可以根據需要編輯該值。
- 在Max。使用次數欄位輸入一個值，以定義要使用該標籤的次數。令牌將在達到天數或最大使用次數時過期。
- 選中允許使用此令牌註冊的產品上的匯出控制功能覈取方塊，以啟用虛擬帳戶中產品例項令牌的匯出控制功能。如果您不想允許匯出控制功能可用於此令牌，請取消選中此覈取方塊。僅當符合匯出控制功能時才使用此選項。一些出口控制功能受到美國商務部的限制。取消選中覈取方塊時，對於使用此令牌註冊的產品，這些功能受到限制。任何違法行為都將會受到處罰和行政收費。
- 按一下**Create Token**以生成令牌。

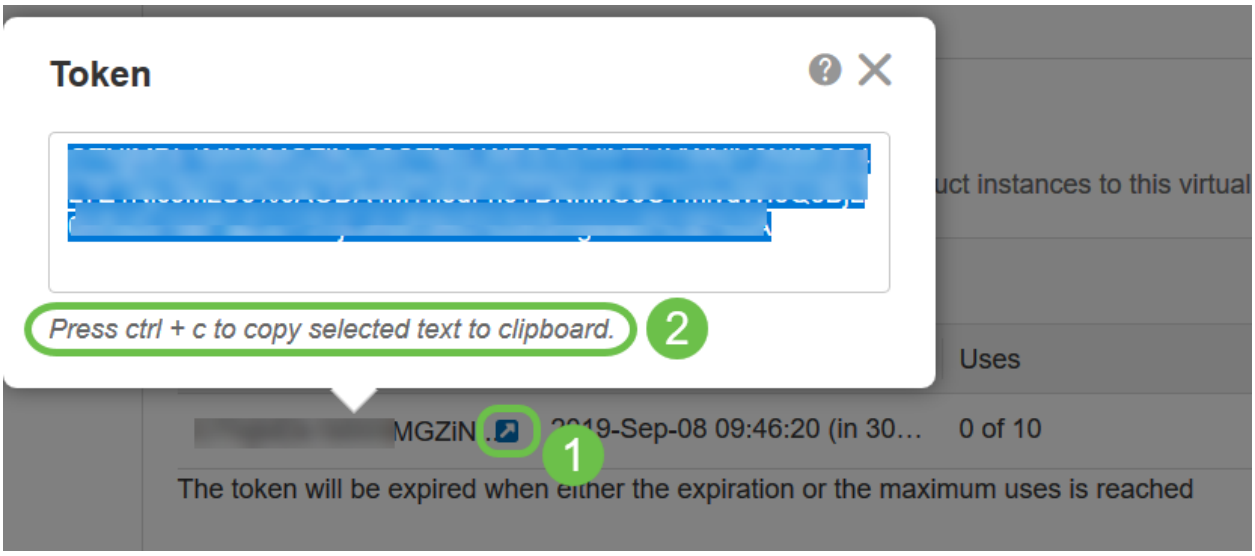


現在，您已成功生成產品例項註冊令牌。



步驟6

按一下*令牌*列中的**箭頭圖示**，將令牌複製到剪貼簿，按鍵盤上的**ctrl + c**。

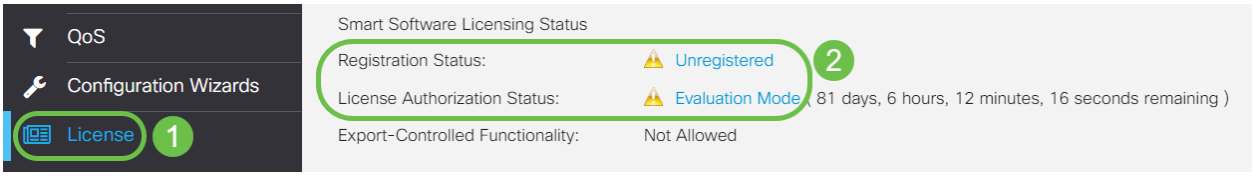


第7步（可選）

按一下**Actions**下拉選單，選擇**Copy**將令牌複製到剪貼簿，或選擇**Download...**下載可從其複製的令牌的文本檔案副本。

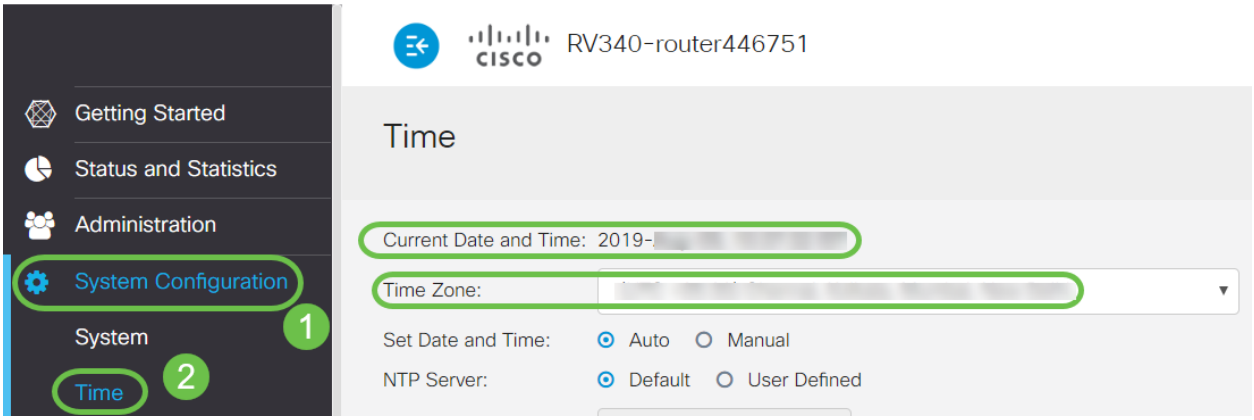
步驟8

導航到License，驗證*Registration Status*是否顯示為*Unregistered*，以及*License Authorization Status*是否顯示為Evaluation Mode。



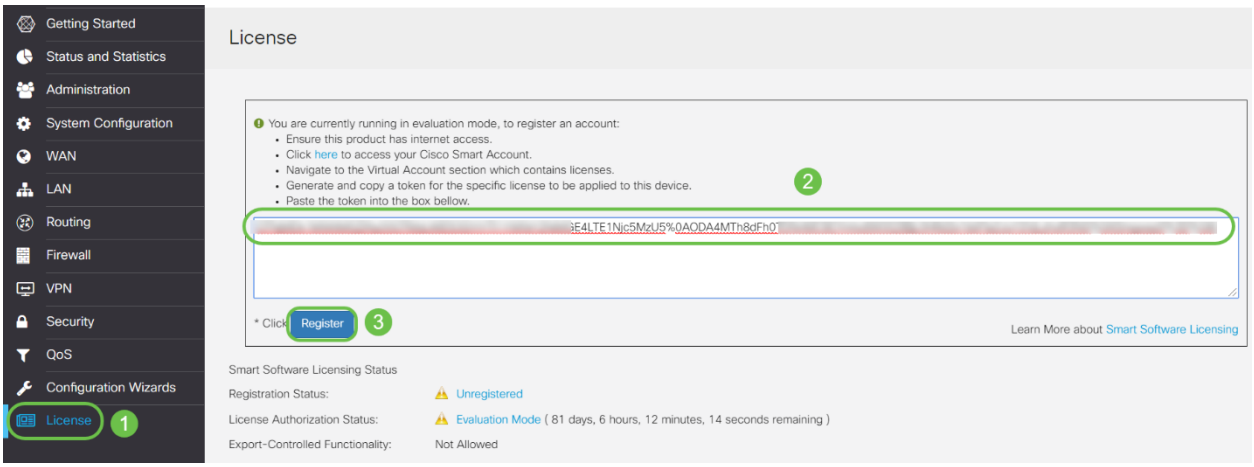
步驟9

導覽至**System Configuration > Time**，然後確認*Current Date and Time*和*Time Zone*是否根據您所在的時區正確反映。



步驟10

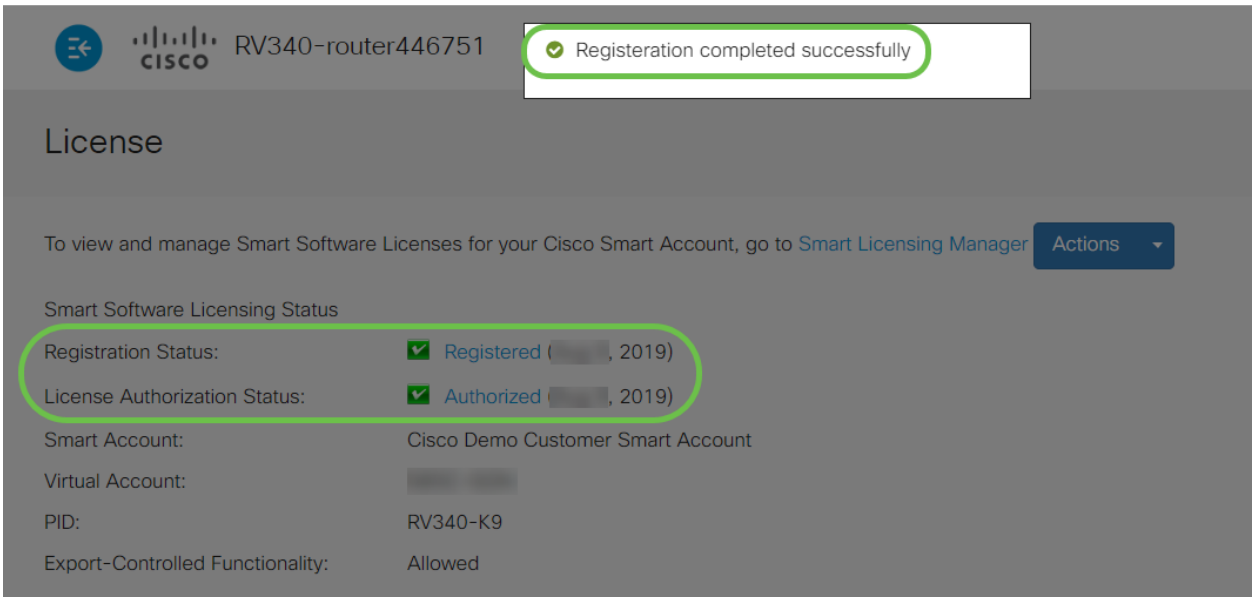
導覽至**License**。通過在鍵盤上選擇**ctrl + v**，將步驟6中複製的標籤貼上到*License*頁籤下的文本框中。按一下「**Register**」。



註冊可能需要幾分鐘時間。當路由器嘗試聯絡許可證伺服器時，請勿離開該頁面。

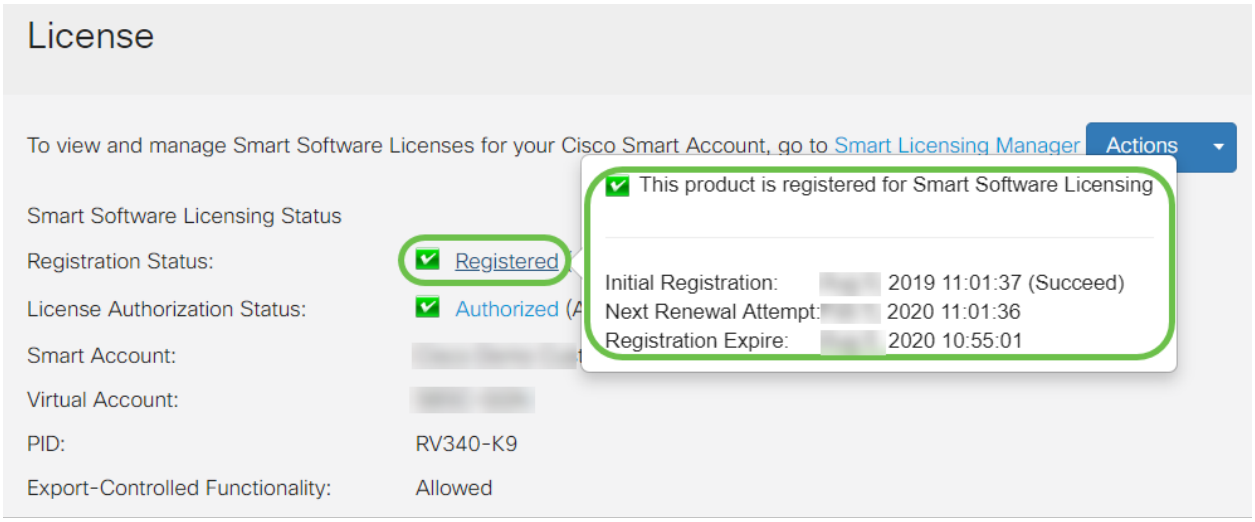
步驟11

您現在應該已經成功註冊並授權使用智慧許可證的RV345P系列路由器。您將在成功完成註冊的螢幕上*收到通知*。此外，您還可以看到*Registration Status*顯示為*Registered*，而*License Authorization Status*顯示為*Authorized*。



第12步（可選）

要檢視許可證的*註冊狀*態的更多詳細資訊，請將指標懸停在*註冊*狀態。將顯示包含以下資訊的對話方塊消息：

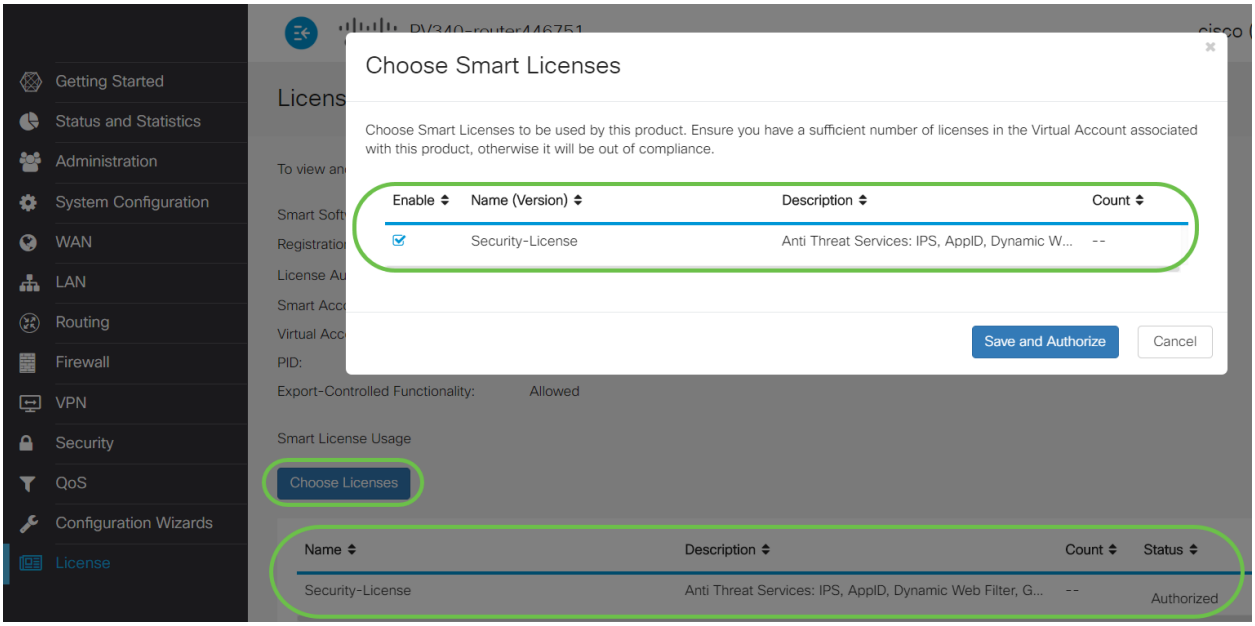


- 初始註冊 — 此區域表示註冊許可證的日期和時間。
- 下一次續訂嘗試 — 此區域表示路由器將嘗試續訂許可證的日期和時間。
- 註冊過期 — 此區域指示註冊到期的日期和時間。

步驟13

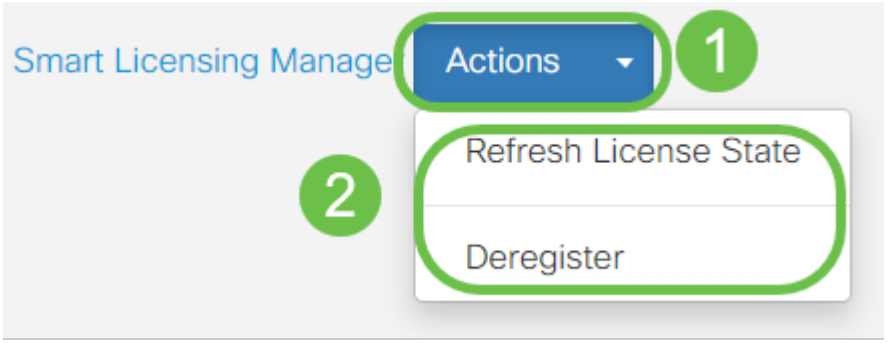
在*License*頁面上，驗證*Security-License*狀態是否顯示*Authorized*。您也可以按一下**Choose License**按鈕驗證*Security-License*是否已啟用。

如果您在此步驟中遇到任何問題，可能需要重新啟動路由器。



第14步（可選）

要刷新許可證狀態或從路由器取消註冊，請按一下*Smart Licensing Manager*操作*下拉選單並選擇操作項。*



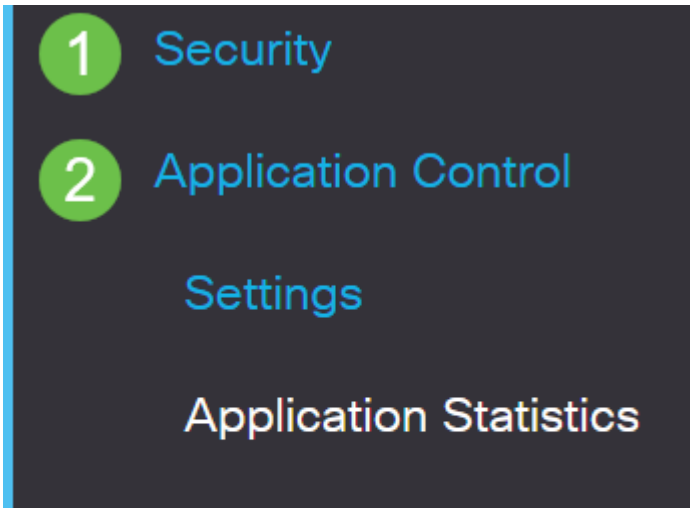
現在路由器上已經有了您的許可證，您需要完成下一部分中的步驟。

RV345P路由器上的網路過濾

啟用後90天可免費使用Web過濾。免費試用版之後，如果您想繼續使用此功能，則需要購買許可證。[按一下可返回該部分。]

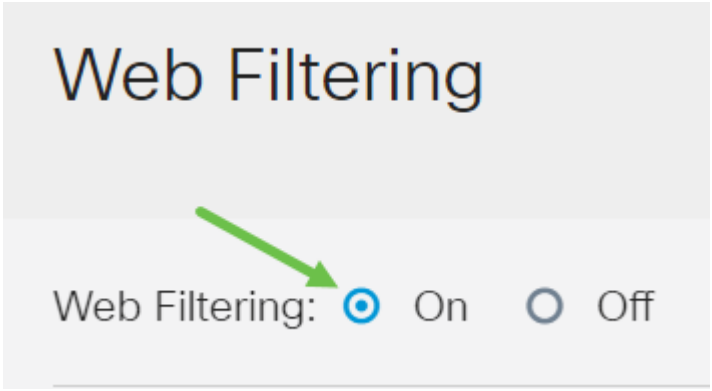
步驟1

登入到基於Web的實用程式，然後選擇**Security > Application Control > Web Filtering**。



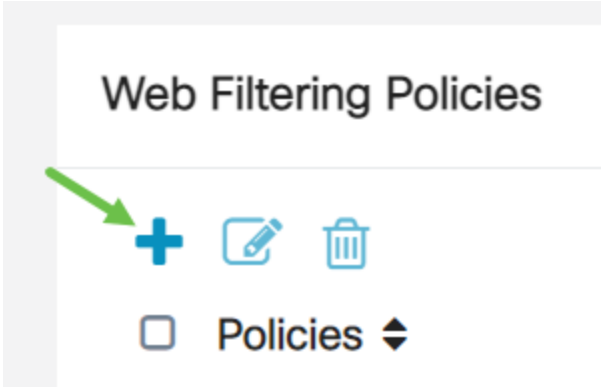
步驟2

選擇On單選按鈕。



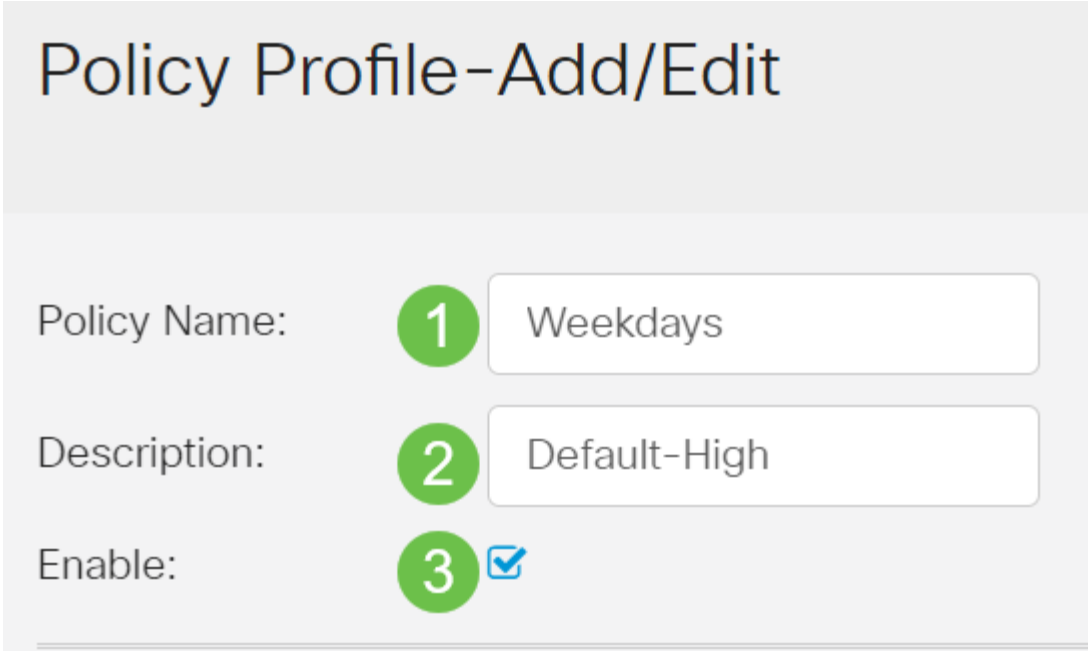
步驟3

按一下add圖示。



步驟4

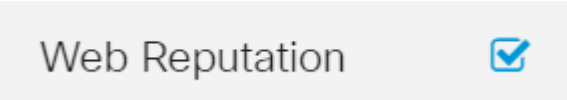
輸入*Policy Name*、*Description*和*Enable*覈取方塊。



如果路由器上啟用了內容過濾，將出現一條通知，通知您已禁用內容過濾，且不能同時啟用這兩個功能。按一下「 **Apply**」以繼續設定。

步驟5

選中Web Reputation覈取方塊以啟用基於Web信譽索引的過濾。

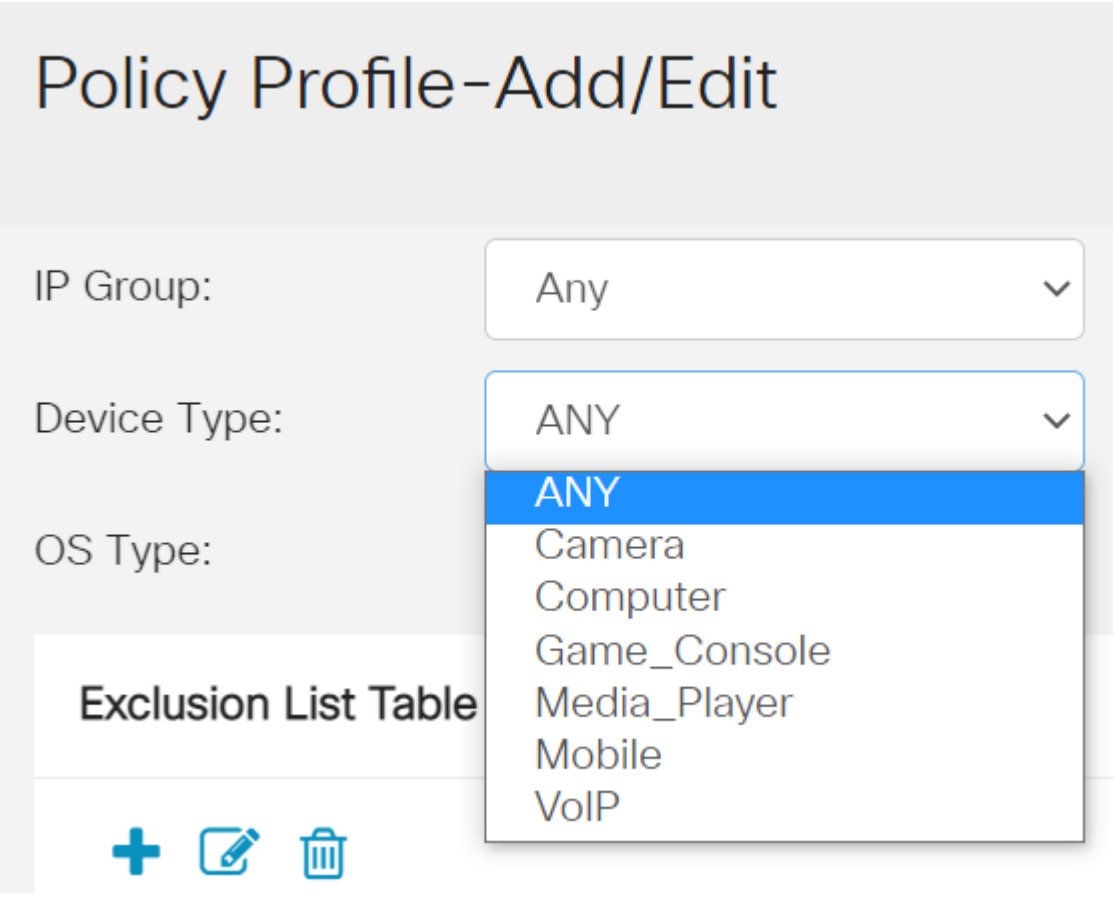


內容將根據網站或URL的惡名基於Web信譽索引進行過濾。如果分數低於40，網站將被阻止。要瞭解有關Web信譽技術的詳細資訊，請按一下 此處瞭解詳細資訊。

步驟6

從*Device Type*下拉選單中，選擇要過濾的資料包的源/目標。一次只能選擇一個選項。選項包括：

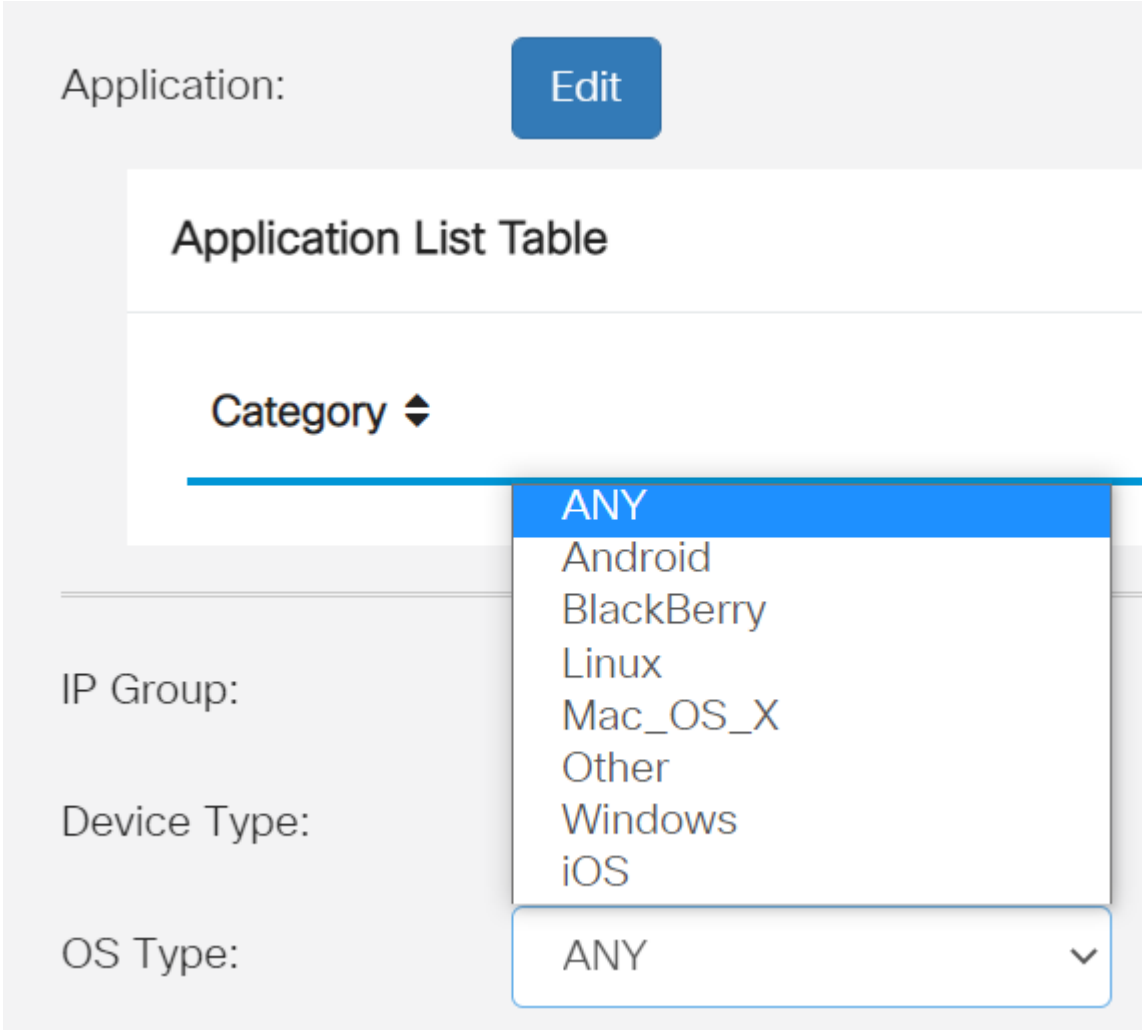
- ANY — 選擇此項可將策略應用於任何裝置。
- 監視器 — 選擇此項可將策略應用於監視器（例如IP安全監視器）。
- 電腦 — 選擇此項可將策略應用於電腦。
- Game_Console — 選擇此項可將策略應用於遊戲控制檯。
- Media_Player — 選擇此項可將策略應用於媒體播放器。
- 移動 — 選擇此項可將策略應用於流動裝置。
- VoIP — 選擇此項可將策略應用於網際網路語音協定裝置。



第7步

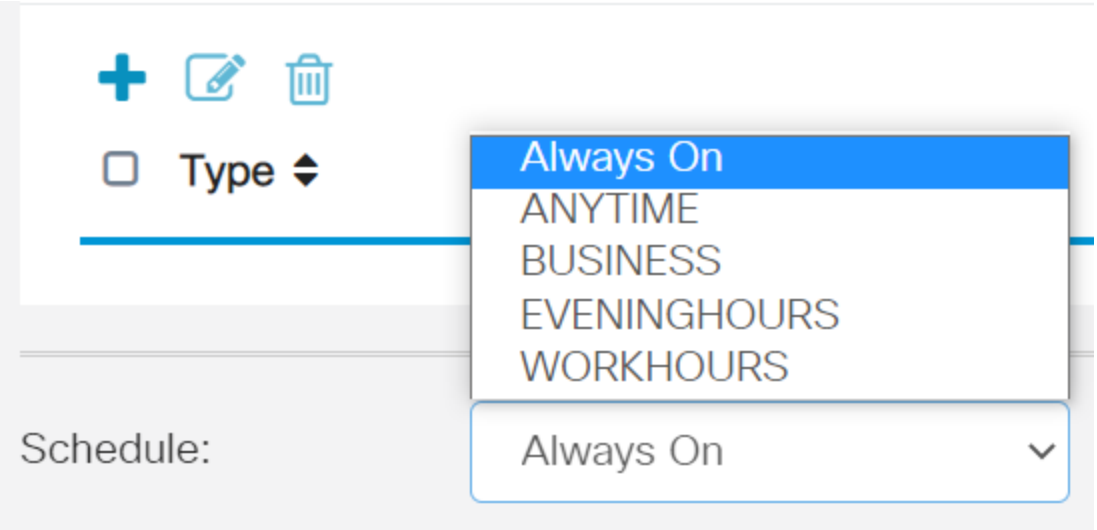
在「*OS Type*」下拉選單中，選擇策略應適用的作業系統(OS)。一次只能選擇一個選項。選項包括：

- ANY — 將策略應用於任何型別的作業系統。這是預設設定。
- Android — 僅將策略應用於Android OS。
- BlackBerry — 僅將策略應用於Blackberry OS。
- Linux — 僅將策略應用於Linux OS。
- Mac_OS_X — 僅將策略應用於Mac OS。
- 其他 — 將策略應用於未列出的作業系統。
- Windows — 將策略應用到Windows作業系統。
- iOS — 僅將策略應用於iOS OS。



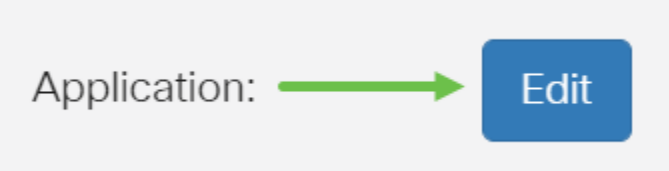
步驟8

向下滾動到*Schedule*部分，然後選擇最符合您需求的選項。



步驟9

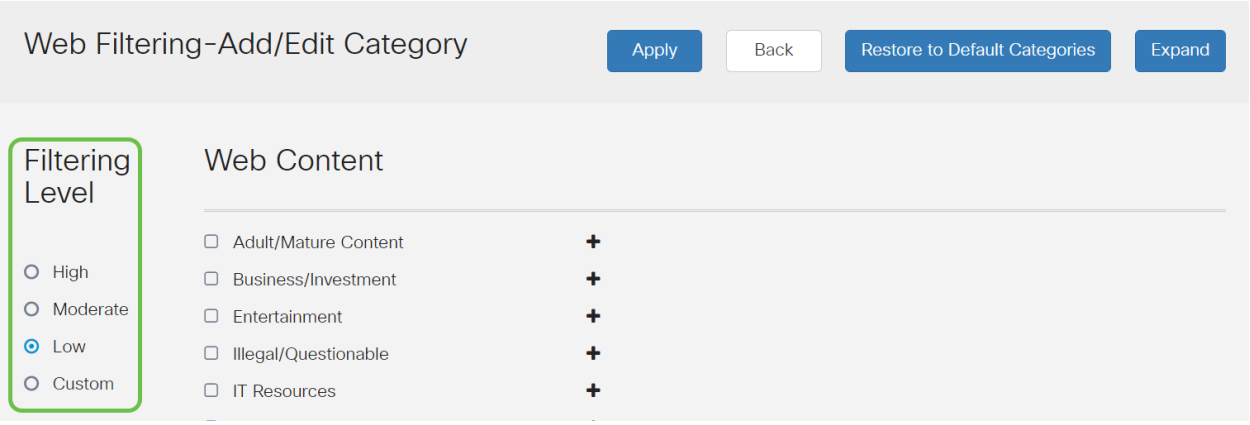
按一下**edit**圖示。



步驟10

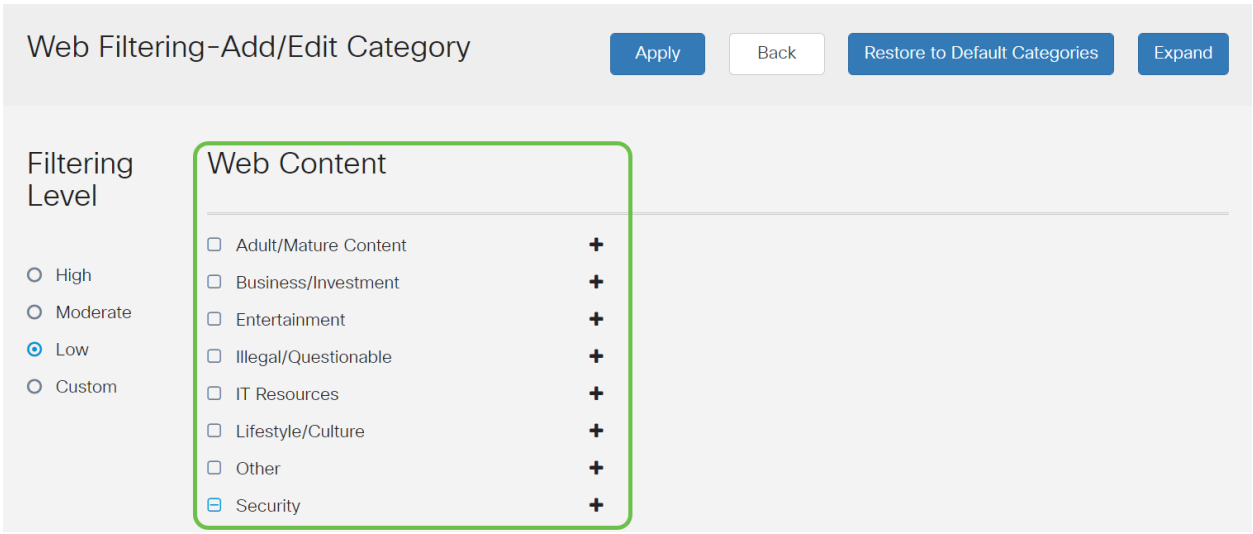
在Filtering Level列中，按一下單選按鈕以快速定義最適合網路策略的過濾範圍。選項包括「高」、「中」、「低」和「自定義」。按一下以下任何過濾級別，瞭解過濾到每個已啟用的Web內容類別的特定預定義子類別。預定義的過濾器不能再更改，將呈灰色顯示。

- **低** — 這是預設選項。此選項啟用安全性。
- **Moderate** — 使用此選項可啟用「成人/成熟內容」、「非法/可疑」和「安全」。
- **高** — 通過此選項啟用成人/成熟內容、業務/投資、非法/可疑、IT資源和安全。
- **自定**義 — 沒有預設值設定為允許使用者定義的篩選器。



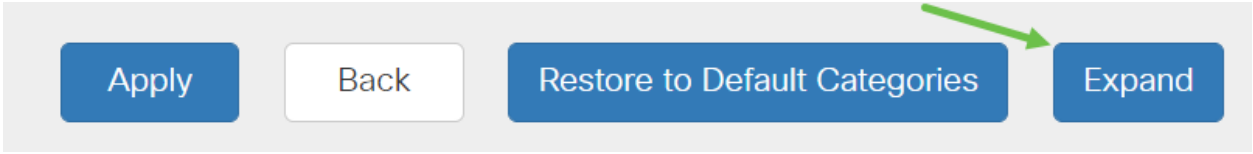
步驟11

輸入要過濾的Web內容。如果您想瞭解某一部分的更多詳細資訊，請按一下**plus**圖示。



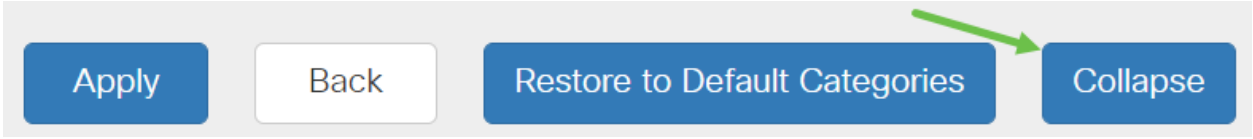
第12步（可選）

要檢視所有Web內容子類別和說明，可以按一下**Expand**按鈕。



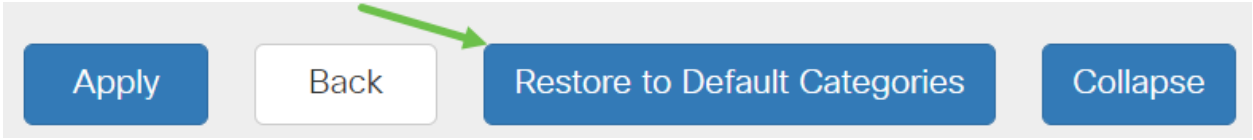
第13步（可選）

按一下**摺疊**可摺疊子類別和說明。



第14步（可選）

要返回到預設類別，請按一下**還原到預設類別**。



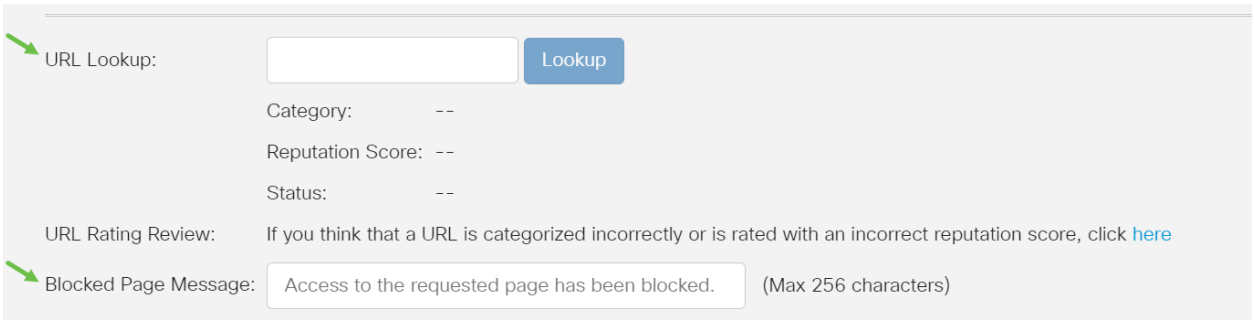
步驟15

按一下**Apply**以儲存配置，並返回「篩選器」頁以繼續設定。

在「應用程式清單表」中，將填充基於所選篩選級別的相應子類別。

第16步（可選）

其他選項包括URL查詢以及顯示請求的頁面被阻止時間的消息。



第17步（可選）

按一下「Apply」。

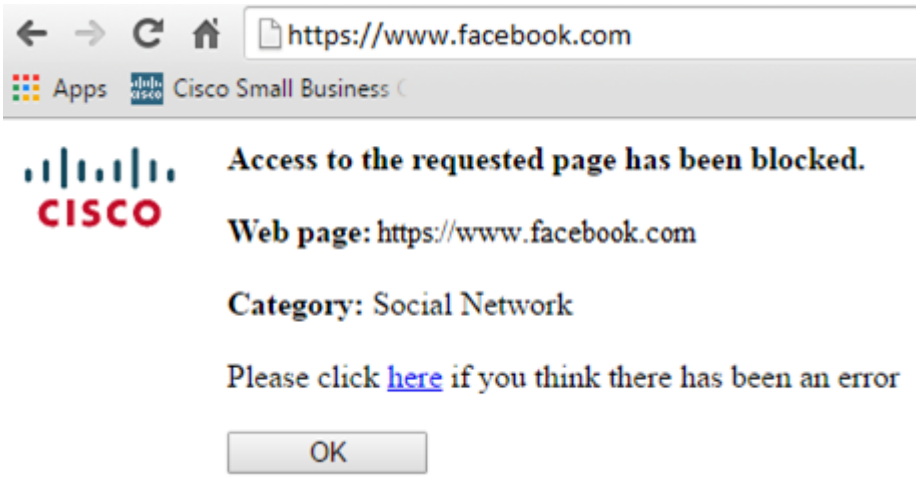
步驟18

要永久儲存配置，請轉到*複製/儲存配置*頁，或按一下該頁上方的**save icon**。

第19步（可選）

要驗證網站或URL是否已被過濾或阻止，請啟動Web瀏覽器或在瀏覽器中開啟一個新頁籤。輸入您已列出阻止或過濾為阻止或拒絕的域名。

在本例中，我們使用www.facebook.com。



您現在應該已經在RV345P路由器上成功配置網路過濾。由於您使用RV安全許可證進行網路過濾，因此您可能不需要使用Umbrella。如果您還需要Umbrella，請按一下此處。如果您有足夠的安全性，請按一下跳至下一節。

疑難排解

如果您購買了許可證，但許可證不會顯示在虛擬帳戶中，則有兩個選項：

1. 聯絡經銷商，請求他們進行轉接。
2. 聯絡我們，我們將與經銷商聯絡。

理想情況下，您也不必這樣做，但是如果您到達這個十字路口，我們樂意為您提供幫助！為了儘可能加快這一過程，您將需要上表中以及下面概述的憑據。

所需資訊	查詢資訊
許可證發票	完成許可證購買後，應通過電子郵件傳送給您。
思科銷售訂單編號	您可能需要返回經銷商才能獲得此服務。
智慧帳戶許可證頁面的螢幕截圖	擷取螢幕截圖可捕獲您螢幕的內容，以便與我們的團隊共用。如果您不熟悉

螢幕截圖

一旦您擁有了一個令牌，或者如果您要進行故障排除，建議您擷取螢幕截圖來捕獲螢幕內容。

鑑於捕獲螢幕截圖所需的步驟不同，請參閱下面的連結以瞭解特定於您的作業系統的連結。

- Windows
- MAC
- iPhone/iPad
- Android

Umbrella RV分支機構許可證（可選）

Umbrella是思科提供的一個簡單但非常有效的雲安全平台。

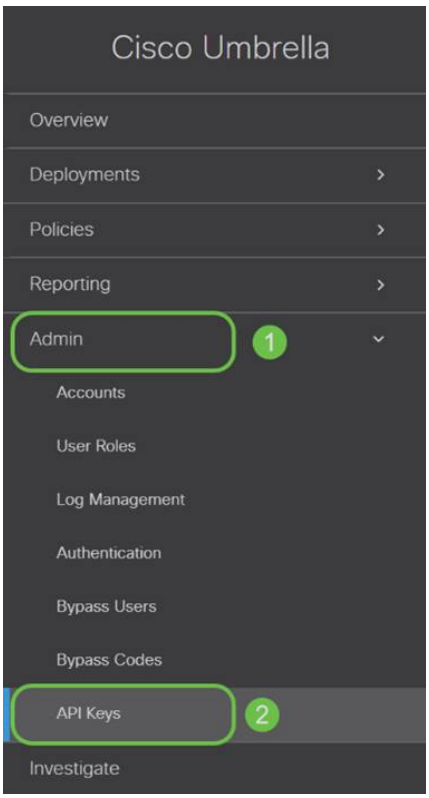
Umbrella在雲中運行並執行許多與安全相關的服務。從緊急威脅到事後調查Umbrella可發現並阻止所有埠和協定上的攻擊。

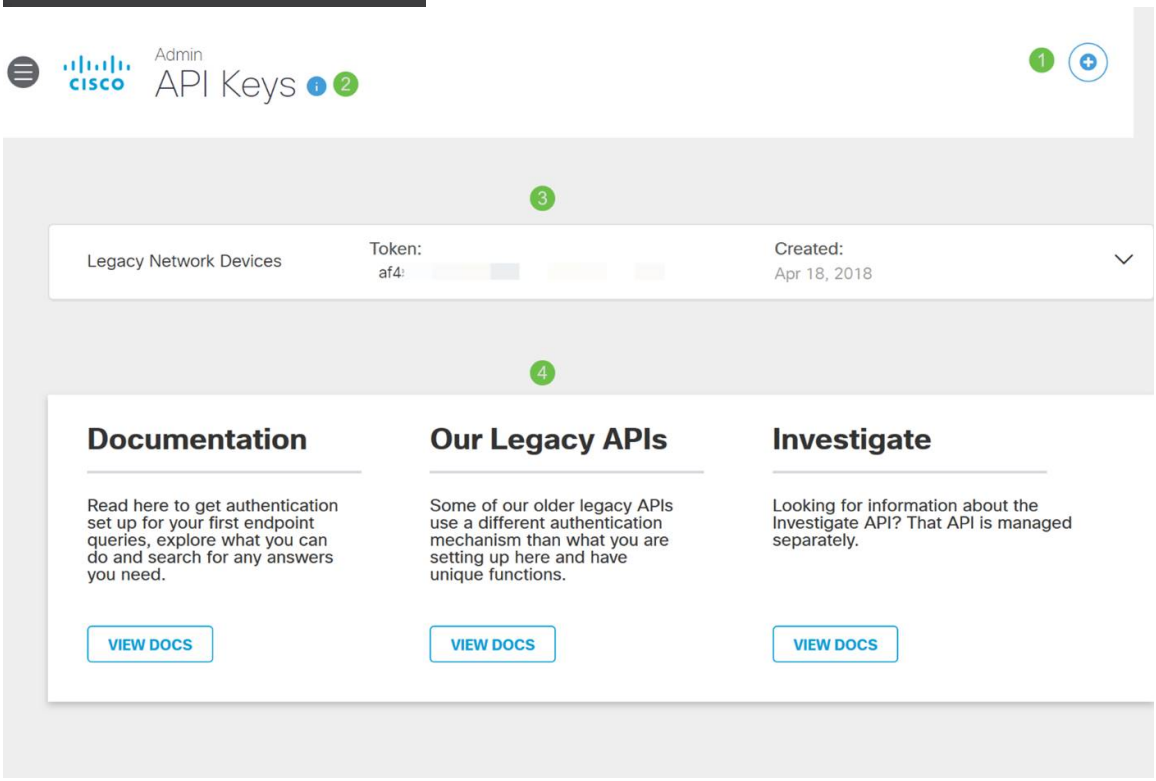
Umbrella使用DNS作為其防禦的主要載體。當使用者在其瀏覽器欄中輸入URL並點選*Enter*時，Umbrella將參與傳輸。該URL會傳遞到Umbrella的DNS解析程式，如果安全警告與域關聯，則請求會被阻止。此遙測資料傳輸和分析在微秒內完成，幾乎不會增加延遲。遙測資料使用日誌和儀器來跟蹤全世界數十億個DNS請求。當這些資料普遍存在時，將其關聯到全球各地便能夠在攻擊開始時快速做出響應。有關詳細資訊，請參閱思科的隱私政策：完整策略，摘要版本。將遙測資料視為源自工具和日誌的資料。

請訪問Cisco Umbrella以瞭解更多資訊並建立一個帳戶。如果遇到任何問題，請查看此處獲取文檔，並查看Umbrella支援選項。

步驟1

登入到您的Umbrella帳戶後，從*Dashboard*螢幕按一下**Admin > API Keys**。



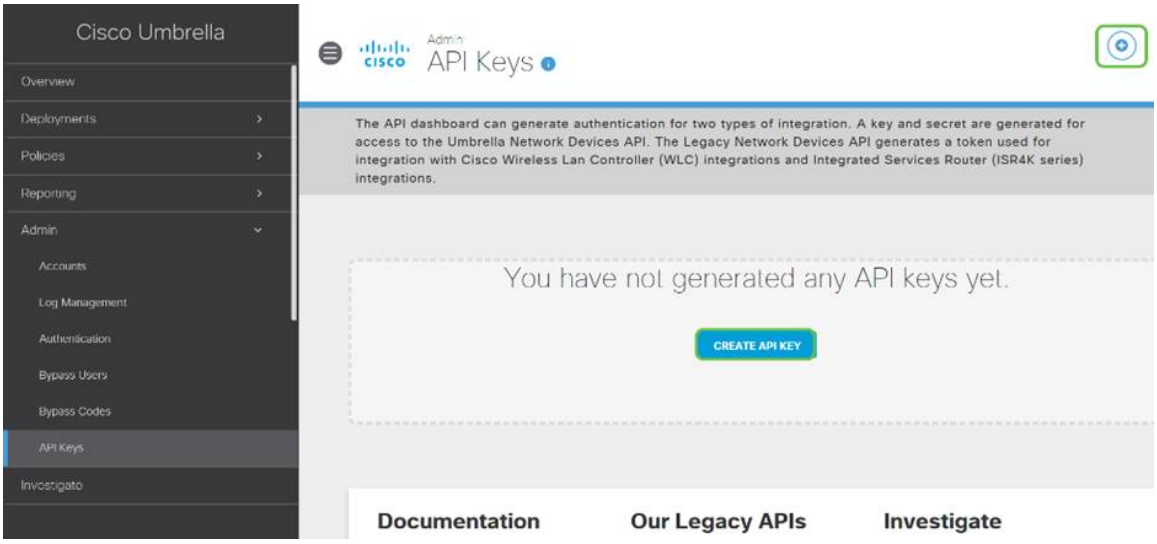


API金鑰螢幕剖析（具有預先存在的API金鑰）

1. 新增API金鑰 — 啟動用於與Umbrella API一起使用的新金鑰的建立。
2. Additional Info — 向下/向上滑動，並提供此螢幕的解釋。
3. Token Well — 包含此帳戶建立的所有金鑰和令牌。（在建立金鑰後填充）
4. 支援文檔 — 指向Umbrella站點上與每個部分中的主題有關的文檔的連結。

步驟2

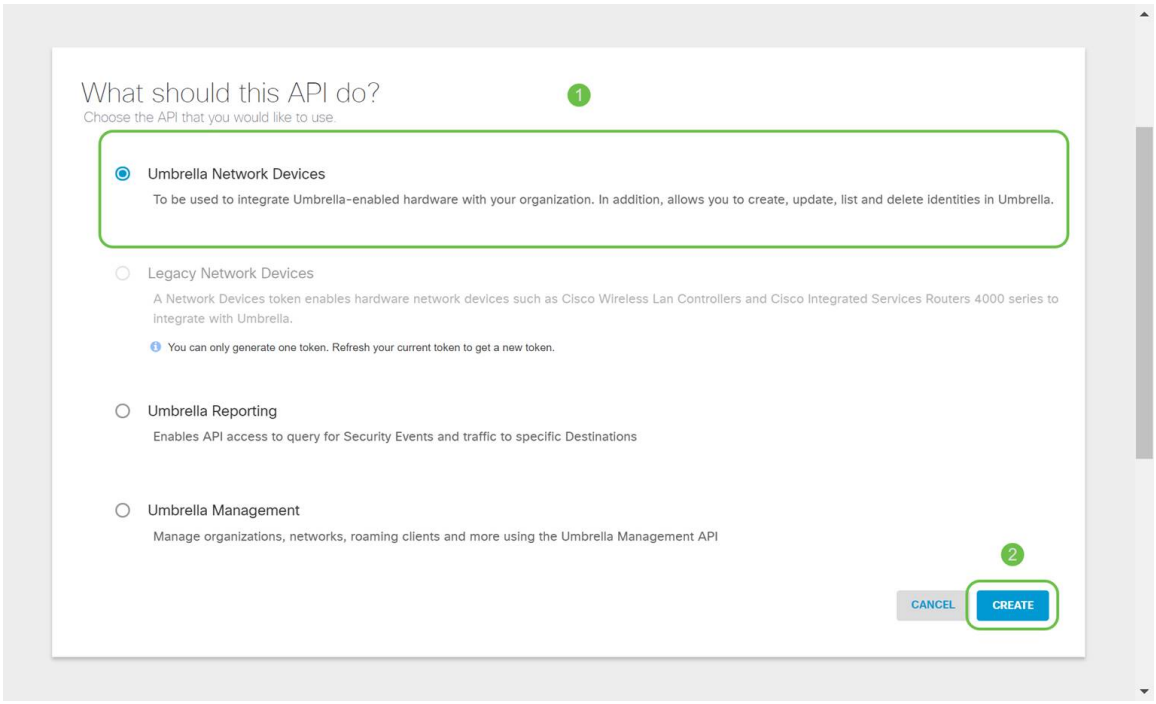
按一下右上角的**Add API Key**按鈕，或按一下**Create API Key**按鈕。兩者功能相同。



上面的螢幕截圖與第一次開啟此選單時看到的類似。

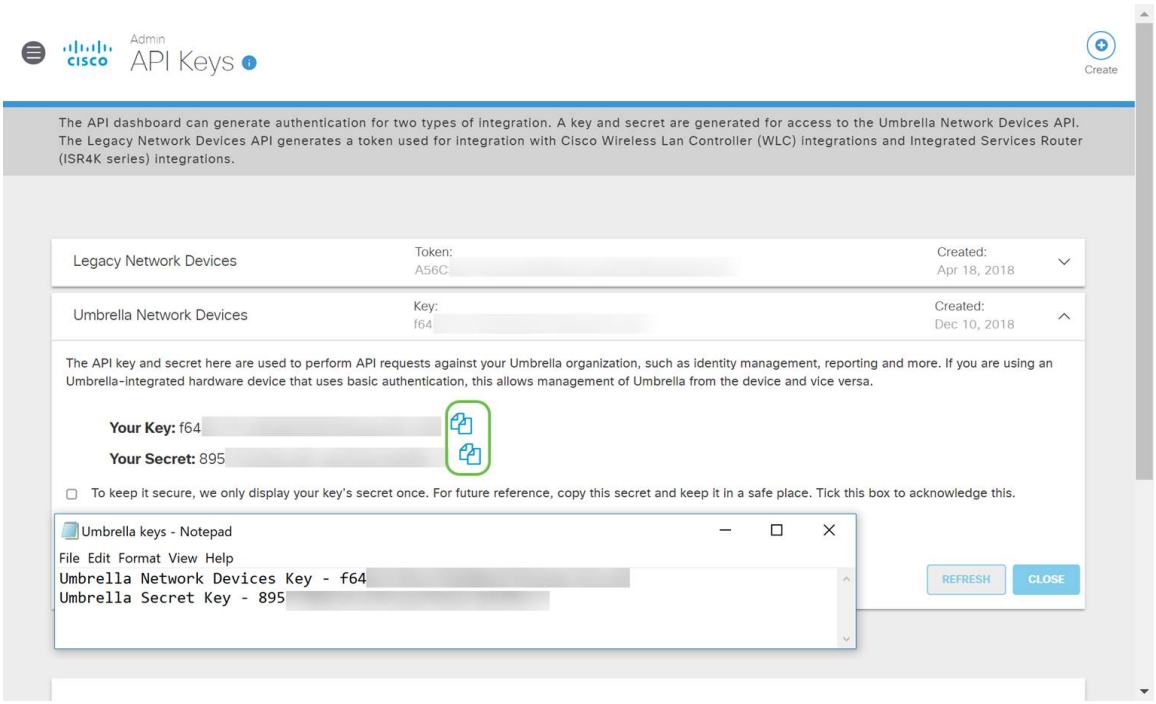
步驟3

選擇**Umbrella Network Devices**，然後按一下**Create**按鈕。



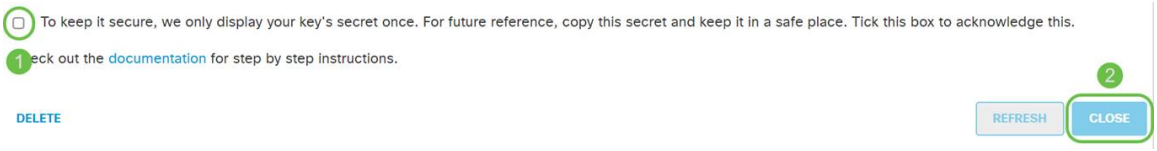
步驟4

開啟文本編輯器（如記事本），然後點選API和API *金鑰右側的*copy icon，彈出通知將確認金鑰被複製到剪貼簿。逐一將您的金鑰和API金鑰貼上到文檔中，並標籤它們以供將來參考。在這種情況下，其標籤為「Umbrella network devices key」。然後將文本檔案儲存到安全位置，以便稍後訪問。



步驟5

將金鑰和金鑰複製到安全位置後，從*Umbrella API螢幕*按一下**覈取方塊**以確認完成臨時檢視金鑰的確認，然後按一下**Close**按鈕。



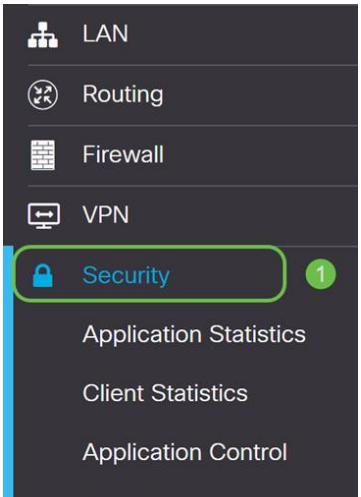
如果丟失或意外刪除了金鑰，則沒有函式或支援號碼可供呼叫以檢索此金鑰。如果丟失，您將需要刪除金鑰並重新授權新API金鑰，用於您要使用Umbrella保護的每台裝置。

在RV345P上配置Umbrella

現在，我們已經在Umbrella內建立了API金鑰，您可以將這些金鑰安裝到您的RV345P上。

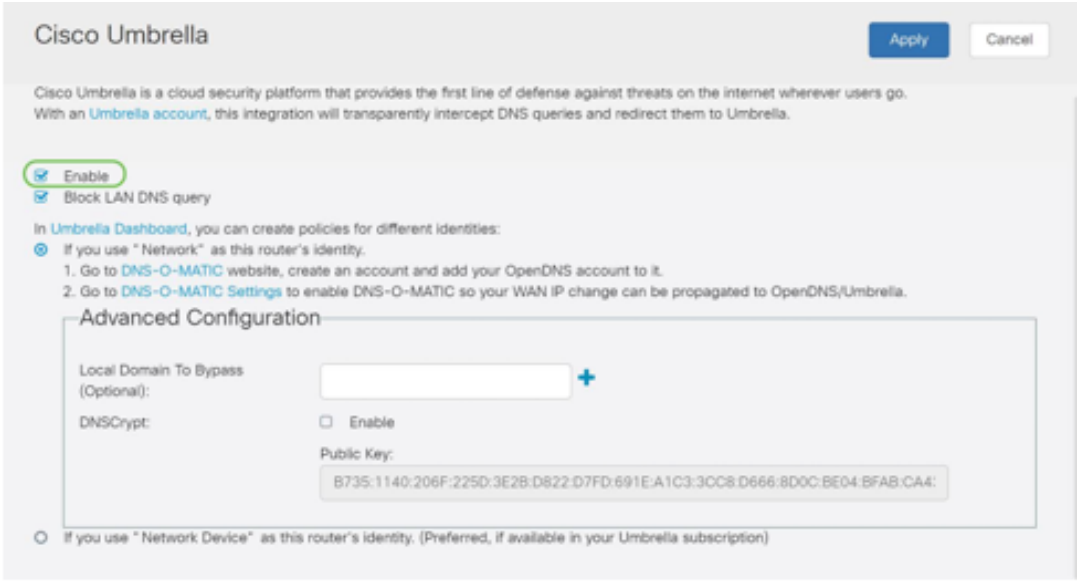
步驟1

登入到RV345P路由器後，按一下邊欄選單中的**Security > Umbrella**。



步驟2

Umbrella API螢幕包含一系列選項，通過按一下**Enable**覈取方塊開始啟用Umbrella。

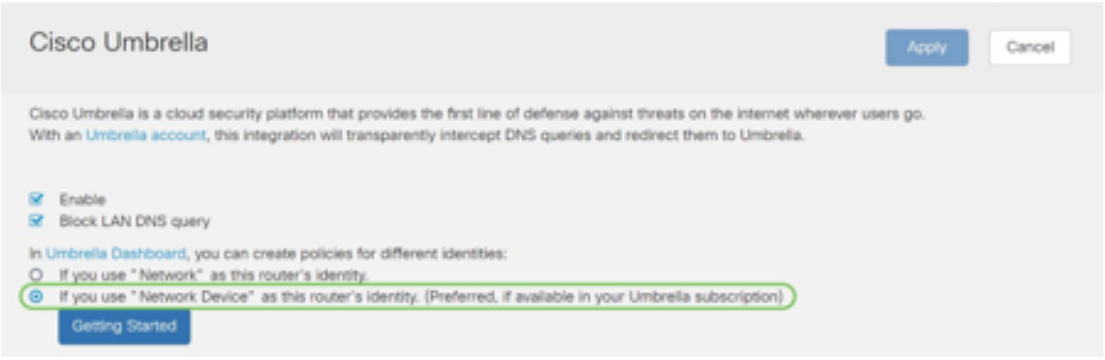


第3步（可選）

預設情況下，選中*Block LAN DNS Queries*框。這一簡潔的功能會自動在您的路由器上建立訪問控制清單，從而阻止DNS流量傳出Internet。此功能強制所有域轉換請求通過RV345P，對大多數使用者來說是一個好主意。

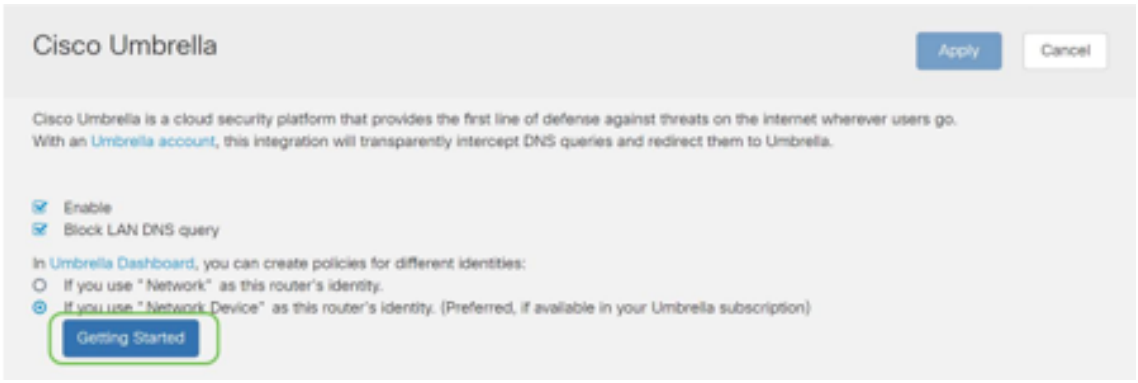
步驟4

下一步有兩種不同的方式。它們都取決於網路的設定。如果您使用DynDNS或NoIP等服務，則保留預設命名方案「Network」。您需要登入這些帳戶，以確保Umbrella在提供保護時與這些服務連線。出於我們的目的，我們依靠「網路裝置」，因此我們點選底部單選按鈕。



步驟5

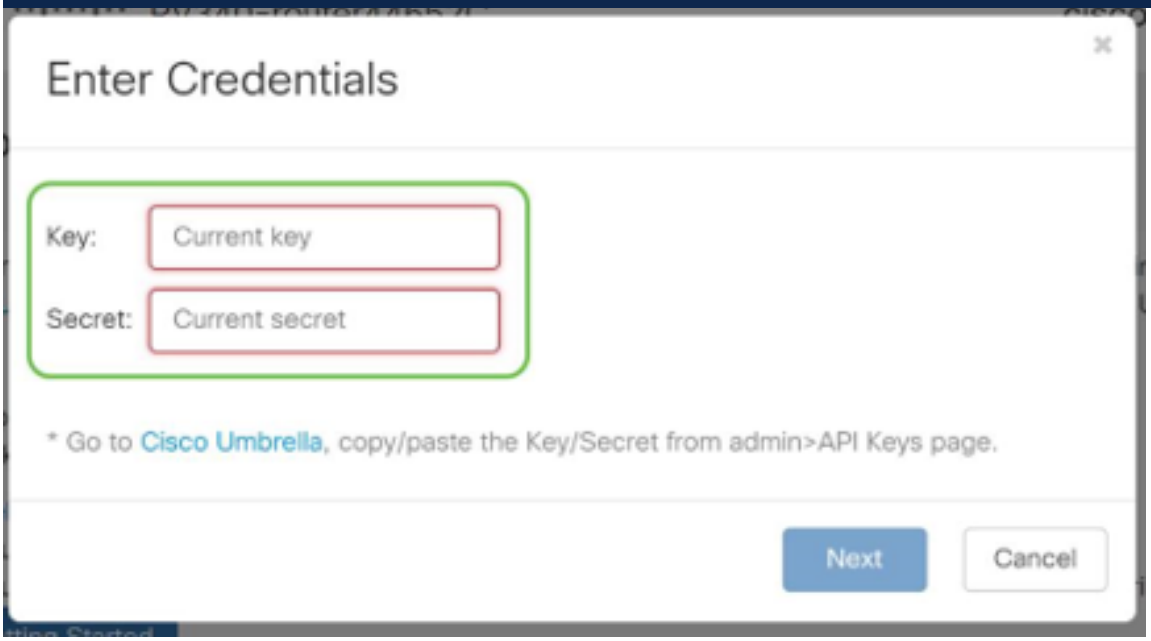
按一下**Getting Started**。



步驟6

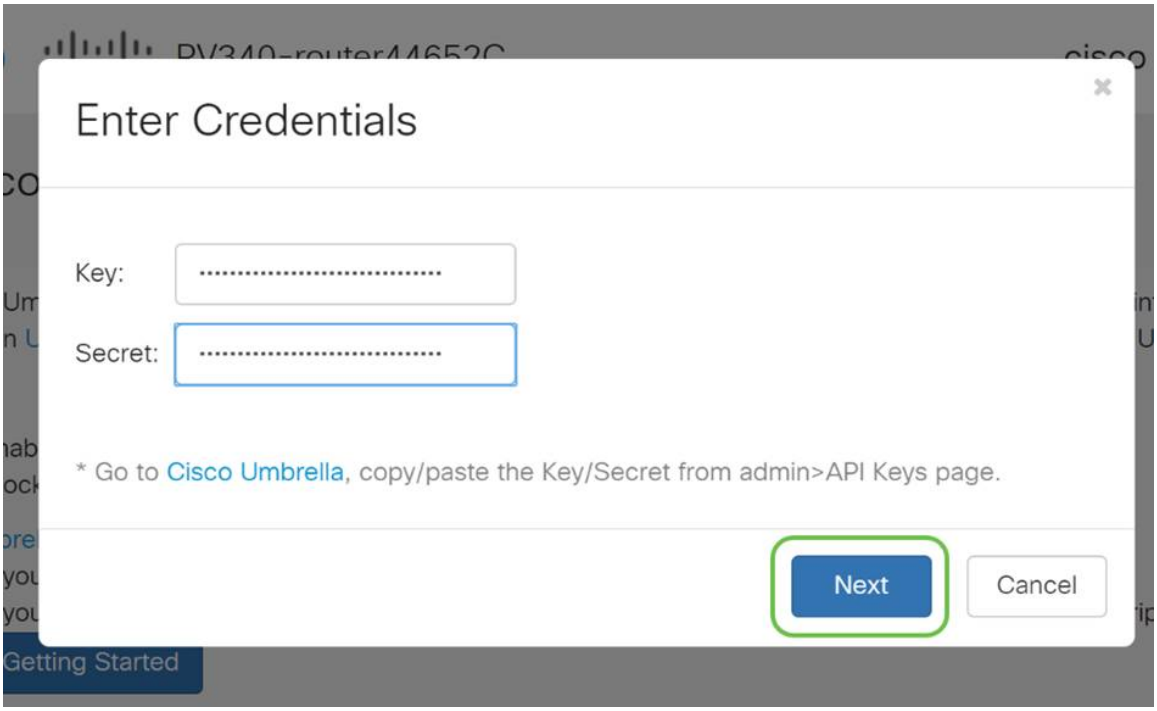
在文本框中輸入**API Key**和**Secret Key**。

說兩遍才知道這很重要！如果丟失或意外刪除了金鑰，則沒有函式或支援號碼可供呼叫以檢索此金鑰。請將其保密並安全。如果丟失，您將需要刪除金鑰並重新授權新API金鑰，用於您要使用Umbrella保護的每台裝置。



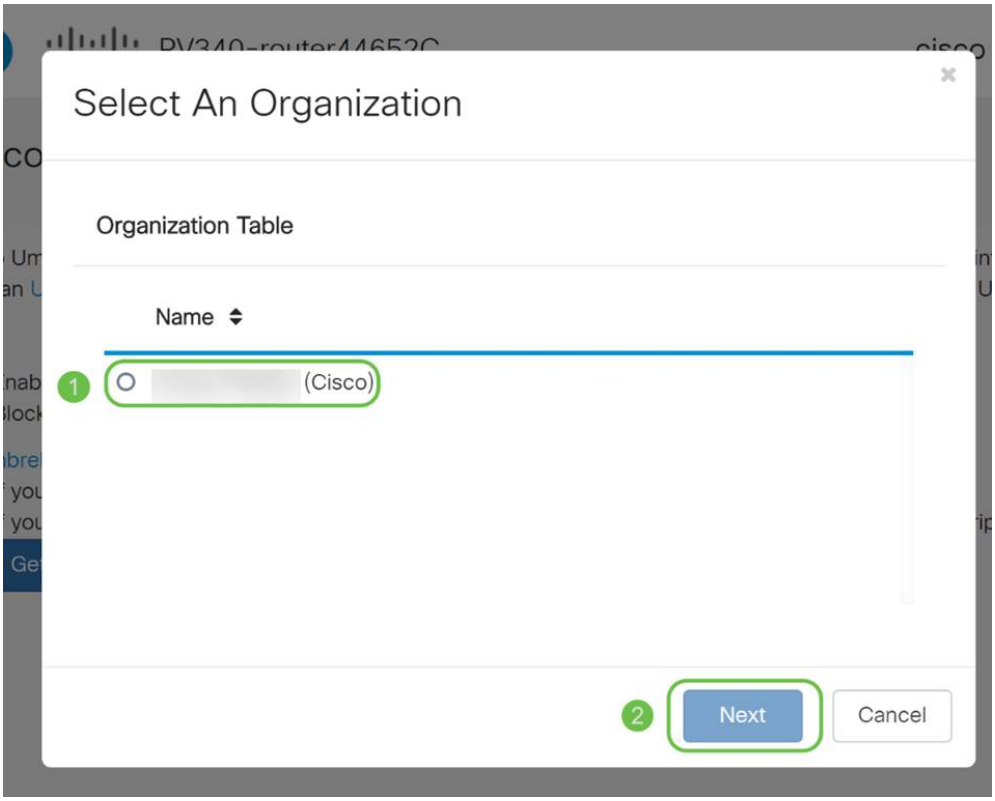
第7步

輸入API和金鑰後，按一下**Next**按鈕。



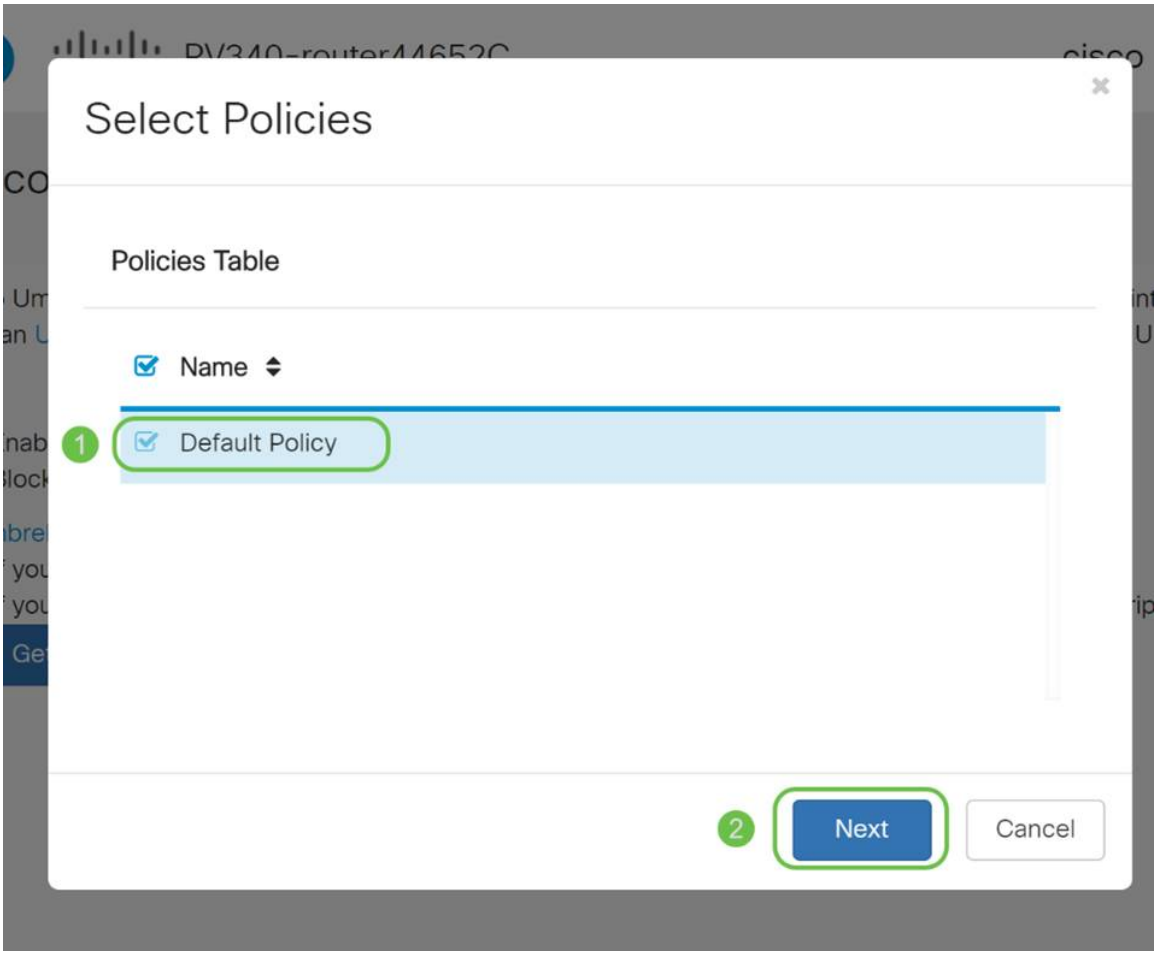
步驟8

在下一個螢幕中，選擇要與路由器關聯的**組織**。按「Next」（下一步）。



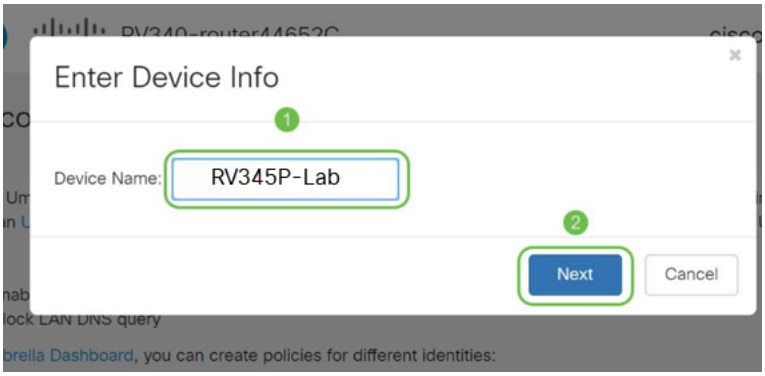
步驟9

選擇要應用於RV345P路由的流量的策略。對於大多數使用者，預設策略將提供足夠的覆蓋範圍。



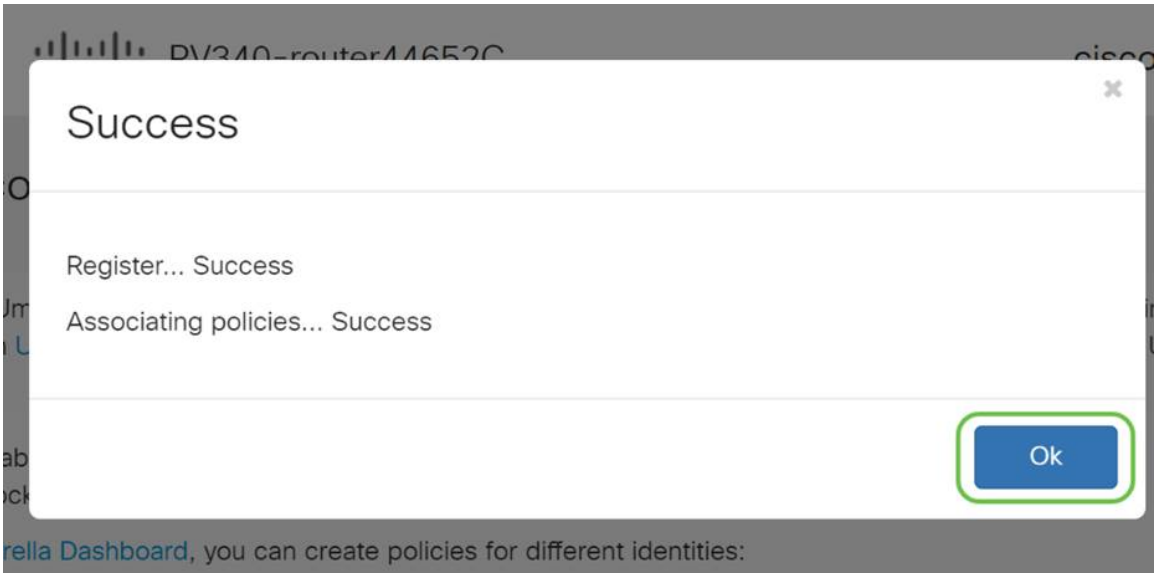
步驟10

為裝置指定名稱，以便可以在Umbrella報告中指定該裝置。在我們的設定中，我們將其命名為*RV345P-Lab*。



步驟11

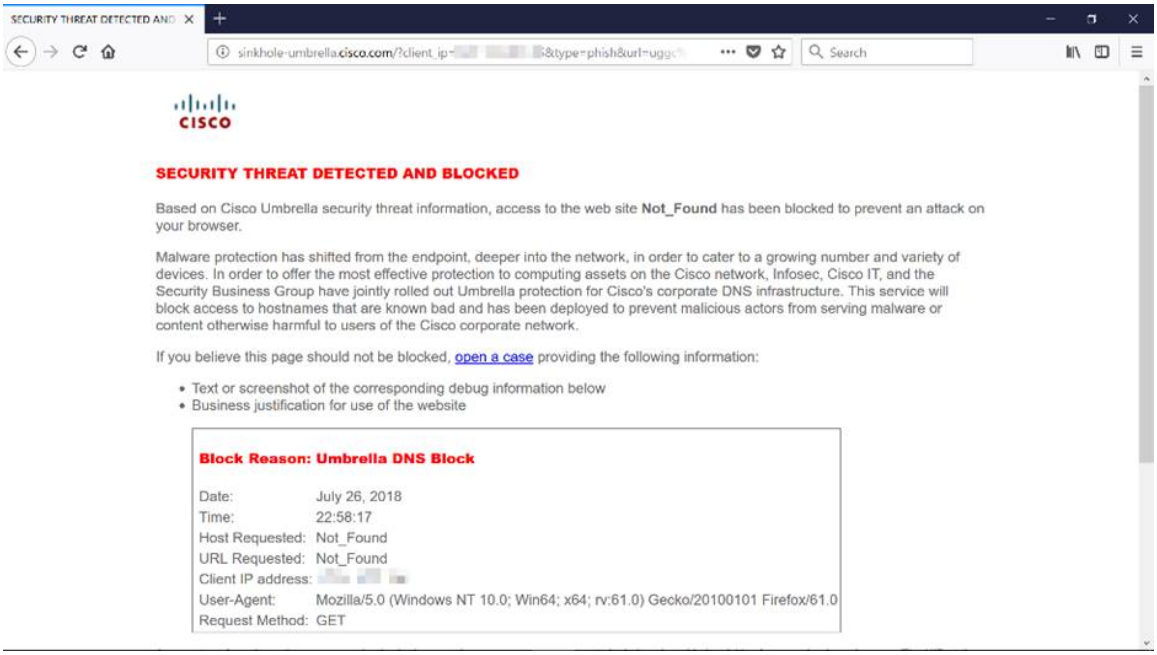
成功關聯後，下一個螢幕將驗證所選設定並提供更新。按一下「OK」（確定）。



確認

祝賀您，您現在受Cisco Umbrella保護。還是你？我們通過一個即時示例進行仔細檢查，確保思科已建立了一個網站，該網站專用於在載入頁面時迅速確定此問題。請按一下此處或在瀏覽器欄中鍵入https://InternetBadGuys.com。

如果Umbrella配置正確，您會看到一個類似以下的螢幕。



其他安全選項

您是否擔心有人從網路裝置拔下乙太網電纜並連線到該裝置，從而試圖未經授權訪問網路？在這種情況下，必須註冊允許使用主機的IP和MAC地址直接連線到路由器的清單。有關說明，請參閱在RV34x系列路由器上配置IP源保護一文。

VPN選項

虛擬專用網路(VPN)連線允許使用者通過公共或共用網路（例如Internet）來訪問、傳送和從專用網路接收資料，但仍確保與底層網路基礎設施的安全連線，以保護專用網路及

其資源。

VPN隧道建立私有網路，該私有網路可以使用加密和身份驗證安全地傳送資料。企業辦公室大多使用VPN連線，因為即使員工不在辦公室，也允許他們訪問其專用網路既有用又必要。

VPN允許遠端主機像位於同一本地網路一樣工作。該路由器最多支援50條隧道。在路由器配置用於Internet連線後，可以在路由器和終端之間建立VPN連線。VPN客戶端完全依賴於VPN路由器的設定才能建立連線。

如果您不確定哪個VPN最適合您的需求，請檢視**思科業務VPN概述和最佳實踐**。

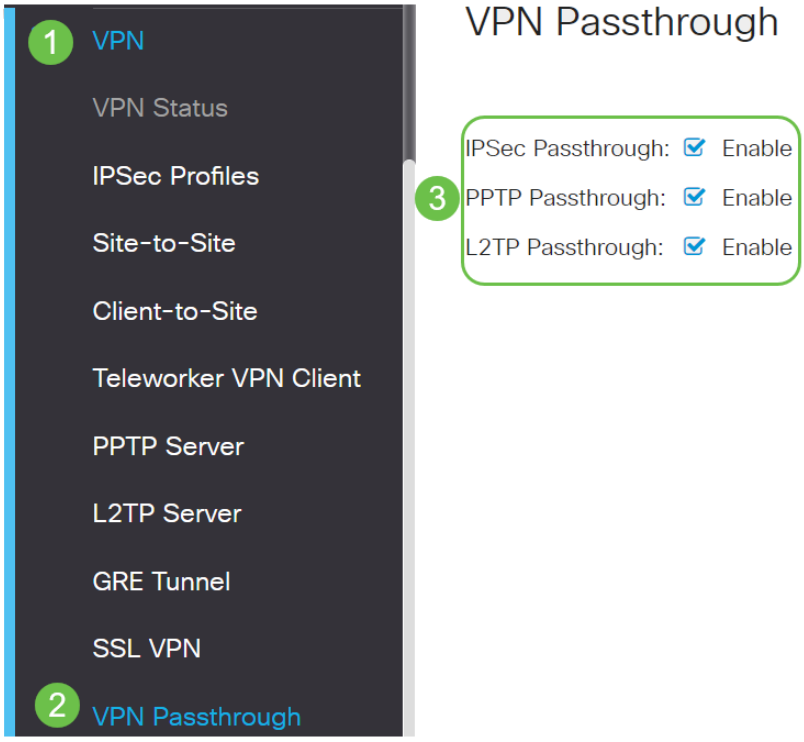
AnyConnect VPN是本配置指南中列出的唯一受思科VPN支援的產品。思科不支援第三方非思科產品，包括GreenBow和Shrew Soft。它們僅用於指導目的。如果您在文章之外需要這些方面的支援，應與第三方聯絡以獲得支援。

如果您不打算設定VPN，可以單**擊跳至下一部分**。

VPN傳輸

一般情況下，當您要支援多個具有相同Internet連線的客戶端時，每台路由器都支援網路地址轉換(NAT)以節省IP地址。但是，點對點通道通訊協定(PPTP)和網際網路通訊協定安全(IPsec)VPN不支援NAT。這就是VPN直通的來源。VPN傳輸是一種功能，允許從連線到此路由器的VPN客戶端生成的VPN流量通過此路由器並連線到VPN終端。VPN直通僅允許PPTP和IPsec VPN通過網際網路（從VPN客戶端啟動），然後到達遠端VPN網關。支援NAT的家庭路由器通常具有此功能。

預設情況下，IPsec、PPTP和L2TP直通已啟用。如果要檢視或調整這些設定，請選擇**VPN > VPN Passthrough**。根據需要檢視或調整。



AnyConnect VPN

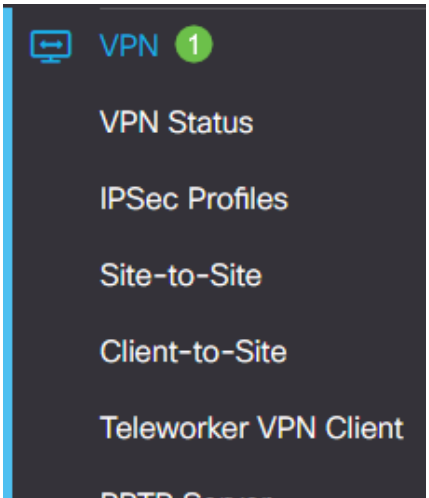
使用Cisco AnyConnect具有以下優點：

1. 安全且持久的連線
2. 持久的安全和策略實施
3. 可以從自適應安全裝置(ASA)或從企業軟體部署系統部署
4. 可定製且可翻譯
5. 易於配置
6. 支援網際網路協定安全(IPsec)和安全套接字層(SSL)
7. 支援Internet金鑰交換版本2.0(IKEv2.0)協定

在RV345P上配置AnyConnect SSL VPN

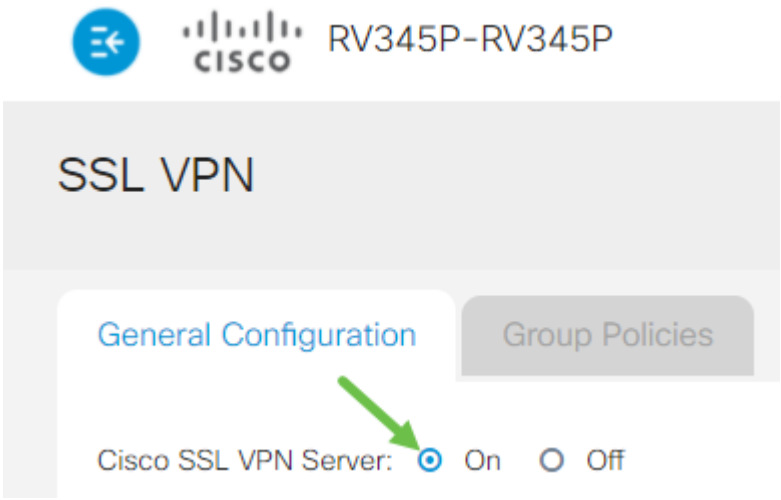
步驟1

訪問路由器基於Web的實用程式並選擇**VPN > SSL VPN**。



步驟2

按一下**On**單選按鈕以啟用Cisco SSL VPN伺服器。



強制網關設定

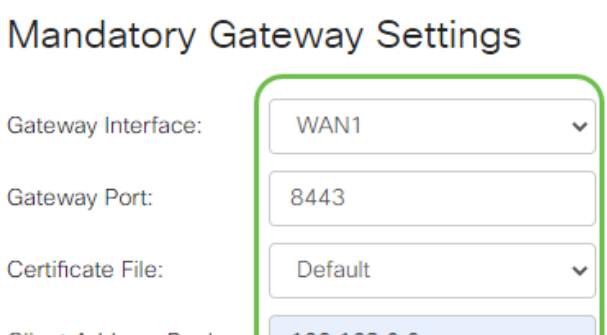
步驟1

必須使用以下配置設定：

1. 從下拉選單中選擇網關介面。此埠將用於通過SSL VPN隧道傳輸流量。選項包括：WAN1、WAN2、USB1、USB2
2. 在Gateway Port欄位中輸入用於SSL VPN網關的埠號，範圍為1到65535。
3. 從下拉選單中選擇Certificate File。此證書對嘗試通過SSL VPN隧道訪問網路資源的使用者進行身份驗證。下拉選單包含預設證書和匯入的證書。
4. 在*Client Address Pool*欄位中輸入客戶端地址池的IP地址。此池將是分配給遠端VPN客戶端的IP地址範圍。

確保IP地址範圍不與本地網路上的任何IP地址重疊。

6. 從下拉選單中選擇客戶端網路掩碼。
7. 在*Client Domain*（客戶端域）欄位中*輸入客戶端*域名。這是應推送到SSL VPN客戶端的域名。
8. 在*Login Banner*欄位中輸入顯示為登入標語的文本。這是每次客戶端登入時顯示的標語。



步驟2

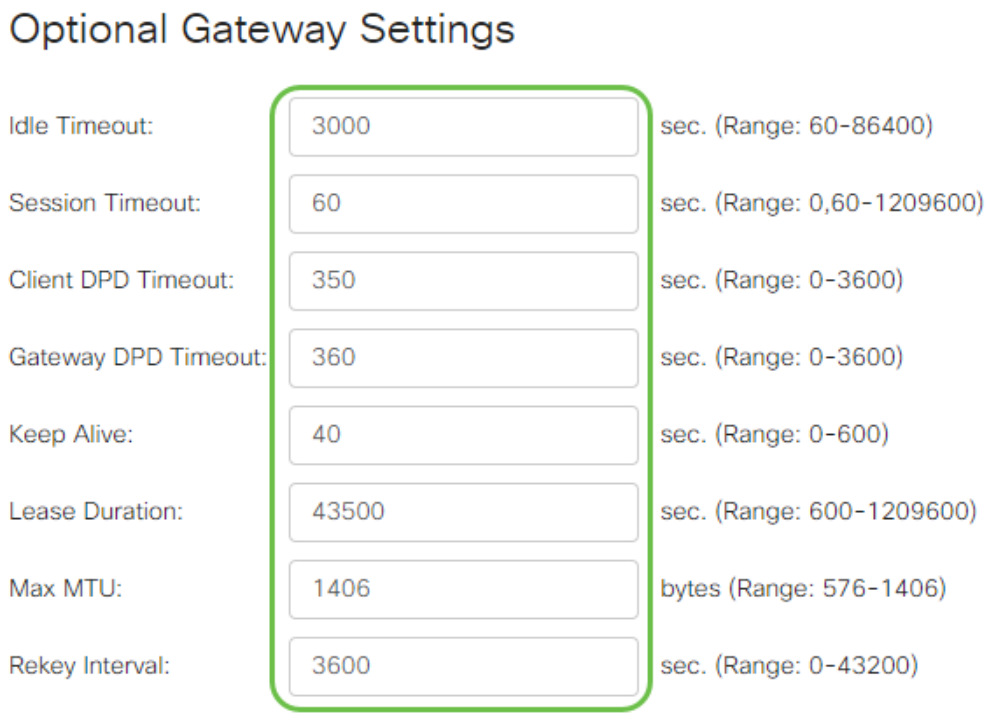
按一下「Apply」。

可選網關設定

步驟1

以下配置設定是可選的：

1. 輸入介於60到86400之間的空閒超時值（以秒為單位）。這是SSL VPN會話可以保持空閒的持續時間。
2. 在*Session Timeout*（會話超時）欄位中輸入一*個以秒為*單位的值。這是傳輸控制通訊協定(TCP)或使用者資料包通訊協定(UDP)作業階段在指定的閒置時間之後逾時的時間。範圍為60到1209600。
3. 在*ClientDPD Timeout*欄位中輸入一個值（以秒為單位），範圍為0到3600。此值指定定期傳送HELLO/ACK消息以檢查VPN隧道的狀態。必須在VPN隧道的兩端啟用此功能。
4. 在*GatewayDPD Timeout*欄位中輸入一個0到3600之間的值（以秒為單位）。此值指定定期傳送HELLO/ACK消息以檢查VPN隧道的狀態。必須在VPN隧道的兩端啟用此功能。
5. 在*Keep Alive*欄位中輸入一個值（以秒為單位），範圍為0到600。此功能可確保您的路由器始終連線到Internet。如果斷開，它將嘗試重新建立VPN連線。
6. 在*Lease Duration*欄位中輸入要連線的隧道的持續時間值（以秒為單位）。範圍為600到1209600。
7. 輸入可通過網路傳送的資料包大小（以位元組為單位）。範圍為576至1406。
8. 在*Rekey Interval*欄位中輸入中繼間隔時間。Rekey功能允許SSL金鑰在會話建立後重新協商。範圍為0到43200。



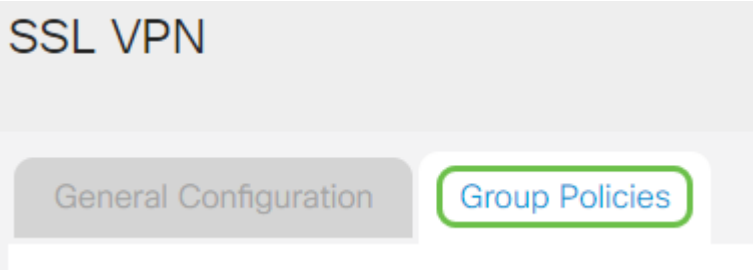
步驟2

按一下「Apply」。

配置組策略

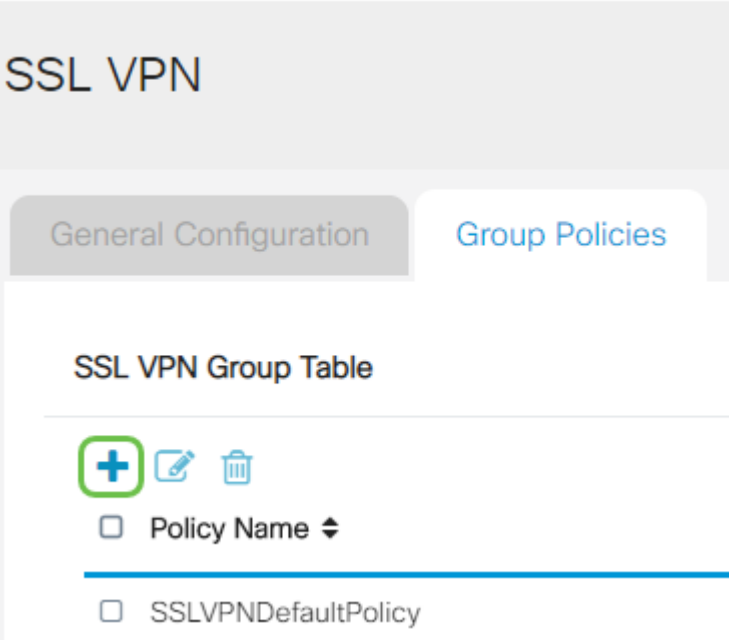
步驟1

按一下**Group Policies**頁籤。



步驟2

點選SSL VPN Group Table下的**add**圖示以新增組策略。

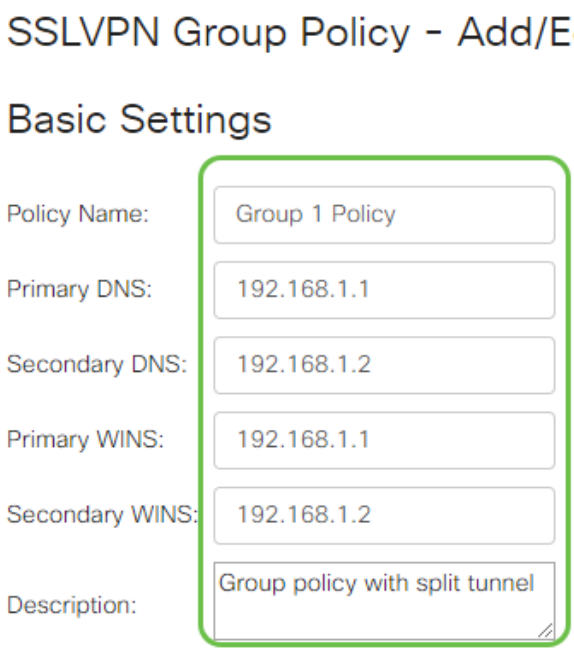


SSL VPN組表將顯示裝置上的組策略清單。您還可以編輯清單中的第一個組策略，該策略名為SSLVPNDefaultPolicy。這是裝置提供的預設策略。

步驟3

1. 在*Policy Name*欄位中輸入您的首選策略名稱。
2. 在提供的欄位中輸入主DNS的IP地址。預設情況下，已提供此IP地址。

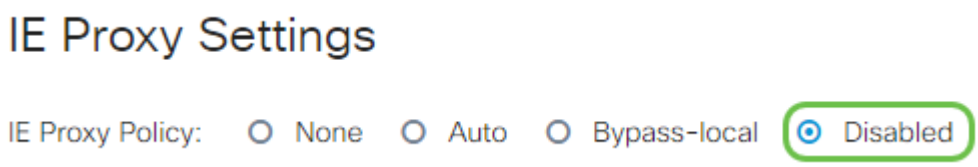
3. *（可選）在提供的欄位中輸入輔助DNS的IP地址。這將在主DNS出現故障時用作備份。*
4. （可選）在提供的欄位中輸入主WINS的IP地址。
5. （可選）在提供的欄位中輸入輔助WINS的IP地址。
6. （可選）在*Description*欄位中輸入策略的說明。



第4步（可選）

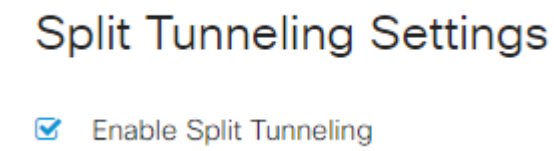
按一下單選按鈕選擇IE代理策略以啟用Microsoft Internet Explorer(MSIE)代理設定來建立VPN隧道。選項包括：

- None — 允許瀏覽器不使用代理設定。
- 自動 — 允許瀏覽器自動檢測代理設定。
- Bypass-local — 允許瀏覽器繞過在遠端使用者上配置的代理設定。
- 已禁用 — 禁用MSIE代理設定。



第5步（可選）

在Split Tunneling Settings區域中，選中**Enable Split Tunneling**覈取方塊，允許以未加密方式將目的地為Internet的流量直接傳送到Internet。全通道會將所有流量傳送到終端裝置，然後將其路由到目的地資源，如此一來，就可以將企業網路從網路存取路徑中移除。

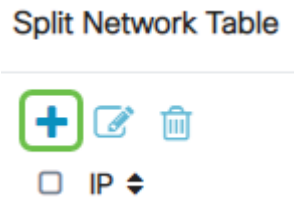


第6步（可選）

按一下單選按鈕，選擇應用分割隧道時是包括還是排除流量。

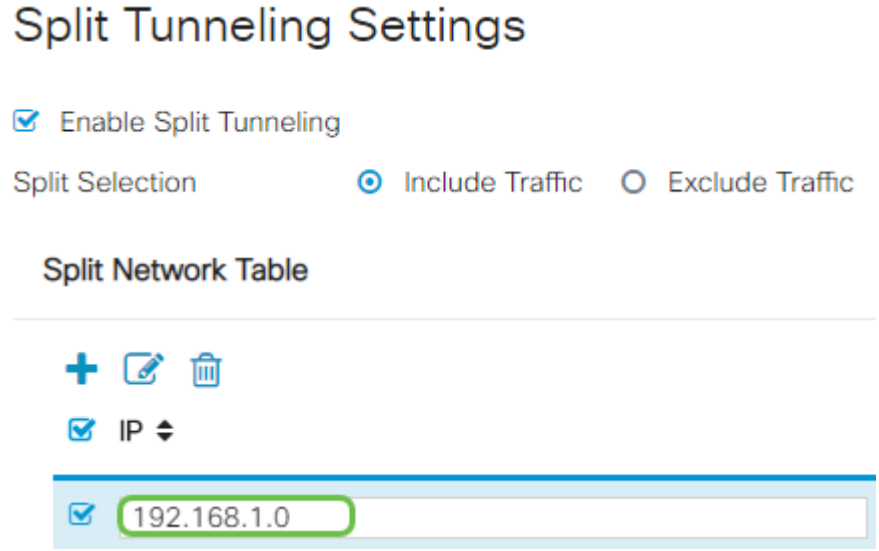
第7步

在Split Network Table中，按一下**add**圖示新增拆分網路例外。



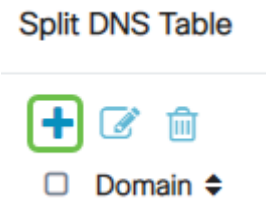
步驟8

在提供的欄位中輸入網路的IP地址。



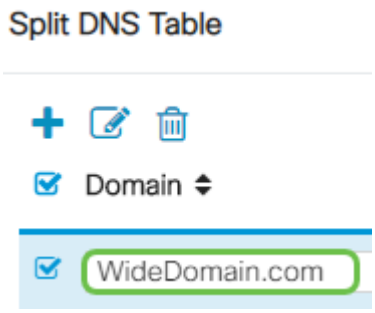
步驟9

在拆分DNS表中，按一下**add**圖示新增拆分DNS例外。



步驟10

在提供的欄位中輸入域名，然後按一下**Apply**。



預設情況下，路由器附帶2個AnyConnect伺服器許可證。這意味著，一旦您擁有AnyConnect客戶端許可證，就可以與任何其他RV340系列路由器同時建立2個VPN隧道。

簡而言之，RV345P路由器不需要許可證，但所有客戶端都需要許可證。AnyConnect客戶端許可證允許案頭和移動客戶端遠端訪問VPN網路。

下一部分詳細介紹如何獲取客戶端許可證。

AnyConnect行動化使用者端

VPN客戶端是在要連線到遠端網路的電腦上安裝並運行的軟體。此客戶端軟體的設定配置必須與VPN伺服器的配置相同，例如IP地址和身份驗證資訊。此驗證資訊包括用於加密資料的使用者名稱和預共用金鑰。根據要連線的網路的物理位置，VPN客戶端也可以是硬體裝置。如果使用VPN連線連線位於不同位置的兩個網路，通常會發生這種情況。

Cisco AnyConnect安全移動客戶端是一種軟體應用程式，用於連線到在各種作業系統和硬體配置上工作的VPN。此軟體應用程式使使用者能夠像直接連線到其網路一樣安全地訪問另一個網路的遠端資源。

在路由器註冊並配置了AnyConnect之後，客戶端可以從您購買的可用許可證池中在路由器上安裝許可證，下一部分將對此進行詳細說明。

購買許可證

您必須從您的思科總代理商或思科合作夥伴處購買許可證。訂購許可證時，您必須以*name@domain.com*的形式提供您的思科智慧帳戶ID或域ID。

如果您沒有思科總代理商或合作夥伴，您可以在此處找到一個。

在撰寫本文時，以下產品SKU可用於購買包含25個捆綁包的額外許可證。請注意，AnyConnect客戶端許可證還有其他選項，如思科AnyConnect訂購指南中所述。但是，列出的產品ID將是完整功能的最低要求。

請注意，首先列出的AnyConnect客戶端許可證產品SKU提供期限為1年的許可證，並且要求至少購買25個許可證。適用於RV340系列路由器的其他產品SKU也具有不同的訂用級別，如下所示：

- LS-AC-PLS-1Y-S1 — 年Cisco AnyConnect Plus客戶端許可證
- LS-AC-PLS-3Y-S1 — 3年Cisco AnyConnect Plus客戶端許可證
- LS-AC-PLS-5Y-S1 — 5年Cisco AnyConnect Plus客戶端許可證
- LS-AC-PLS-P-25-S — 25件裝Cisco AnyConnect Plus永久客戶端許可證
- LS-AC-PLS-P-50-S — 50件裝Cisco AnyConnect Plus永久客戶端許可證

使用者端資訊

當您的使用者端設定以下任一連結時，您應該傳送這些連結：

- Windows:Windows電腦上的AnyConnect
- Mac:在Mac上安裝AnyConnect。
- Ubuntu案頭：在 Ubuntu 桌面上安裝和使用 AnyConnect
- 如果您遇到問題，可以轉至收集資訊以對Cisco AnyConnect安全移動客戶端錯誤進行基本故障排除。

驗證AnyConnect VPN連線

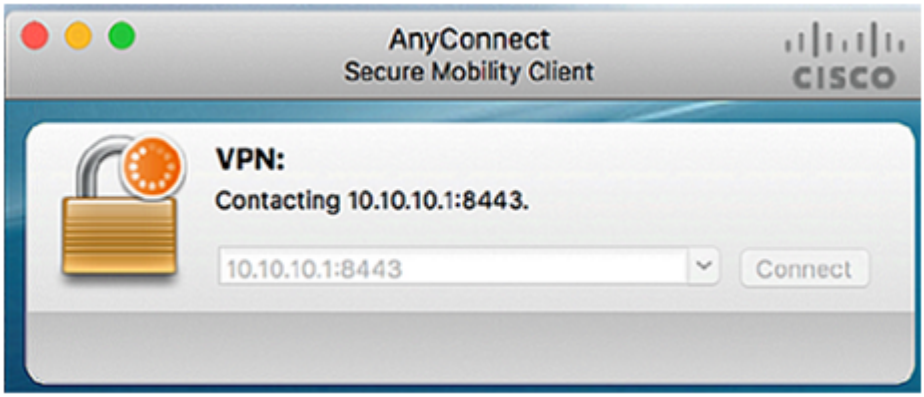
步驟1

按一下**AnyConnect Secure Mobility Client**圖示。

步驟2

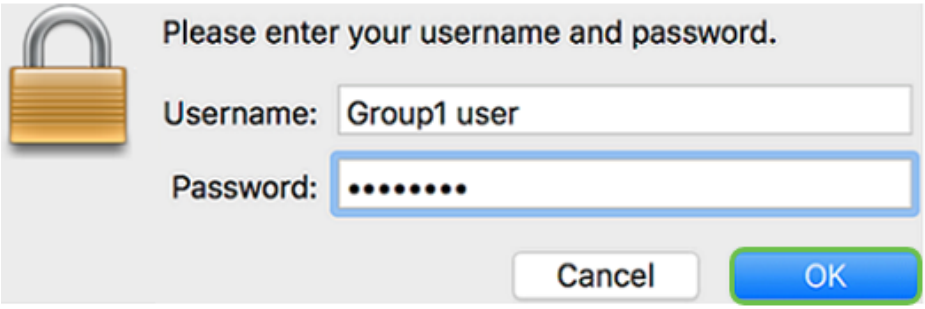
在AnyConnect Secure Mobility Client（AnyConnect安全移動客戶端）視窗中，輸入網關IP地址和網關埠號(用冒號(:)分隔)，然後按一下**Connect**。

軟體現在將顯示它正在聯絡遠端網路。



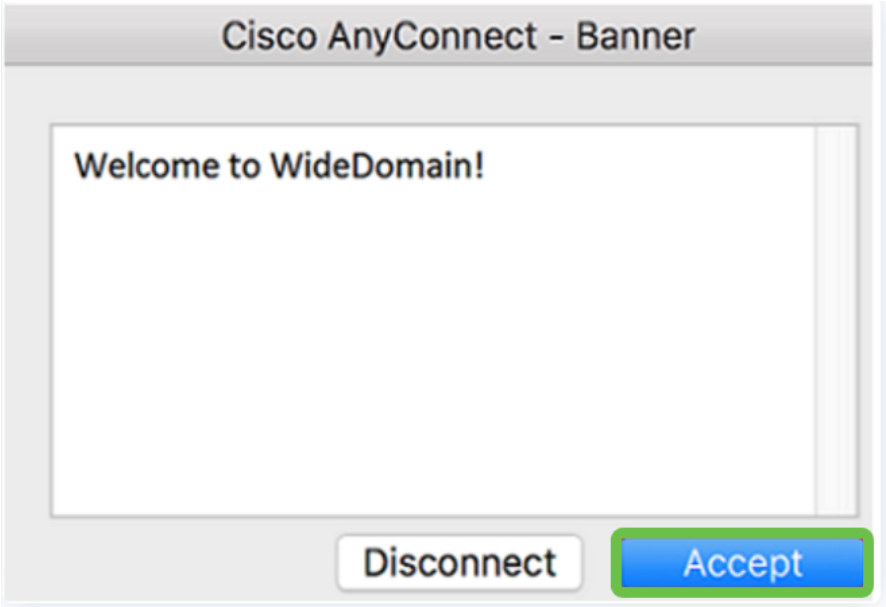
步驟3

在相應的欄位中輸入您的伺服器使用者名稱和密碼，然後按一下**OK**。

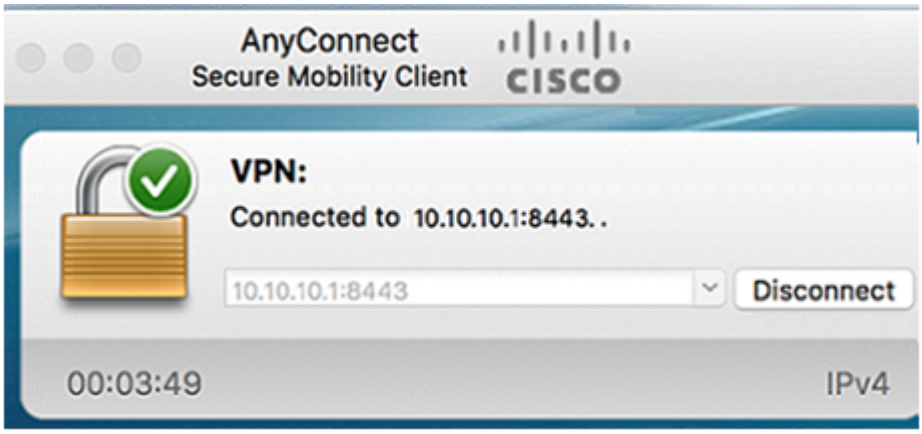


步驟4

一旦建立連線，就會顯示登入橫幅。按一下「**Accept**」。



AnyConnect視窗現在應指示到網路的VPN連線是否成功。



如果您現在使用AnyConnect VPN，可以跳過其他VPN選項並轉到下一節。

精簡型軟VPN

IPsec VPN允許您通過跨網際網路建立加密隧道來安全地獲取遠端資源。RV34X系列路由器充當IPsec VPN伺服器，支援Shrew Soft VPN客戶端。本節將介紹如何配置您的路由器和簡化軟客戶端，以確保與VPN的連線。

思科不支援Shrew Soft。本示例僅用於演示。如果您與Shrew Soft存在問題，請與他們聯絡以獲得支援。

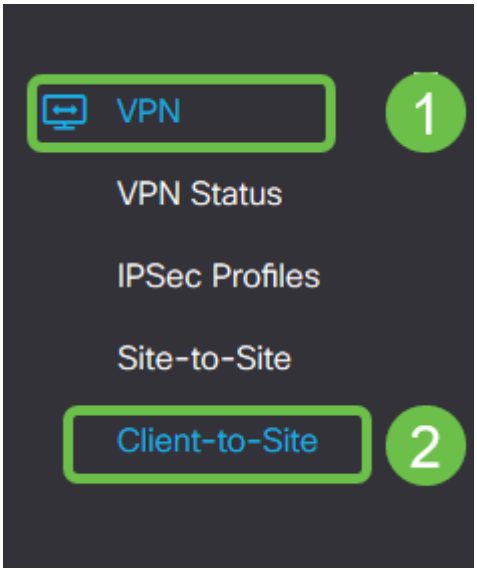
您可以在以下位置下載最新版本的Shrew Soft VPN客戶端軟體：https://www.shrew.net/download/vpn

在RV345P系列路由器上配置Shrew Soft

我們將首先在RV345P上配置**客戶端到站點VPN**。

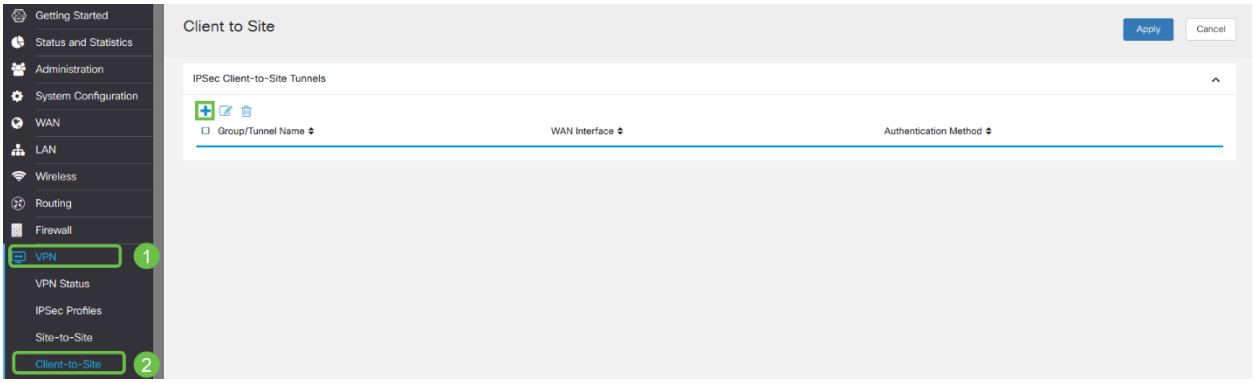
步驟1

導航到**VPN > Client-to-Site**。



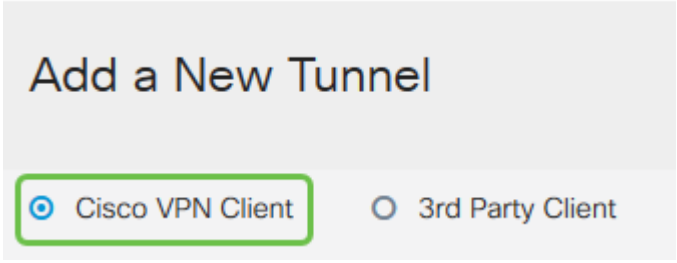
步驟2

新增**客戶端到站點VPN配置檔案**。



步驟3

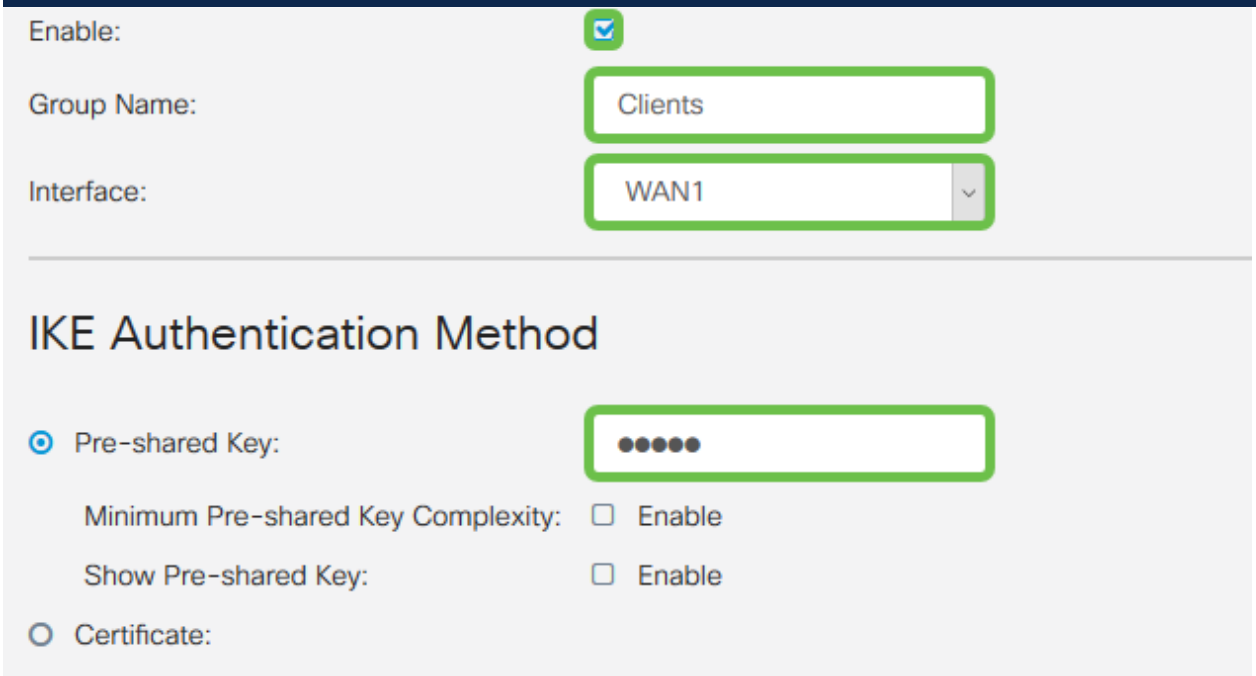
選擇**Cisco VPN Client**選項。



步驟4

選中**Enable**框以啟用VPN客戶端配置檔案。我們還將配置*組名稱*，選擇**WAN介面**，然後輸入**預共用金鑰**。

請記下 *組名*和 *預共用金鑰*，因為它們將在以後配置客戶端時使用。

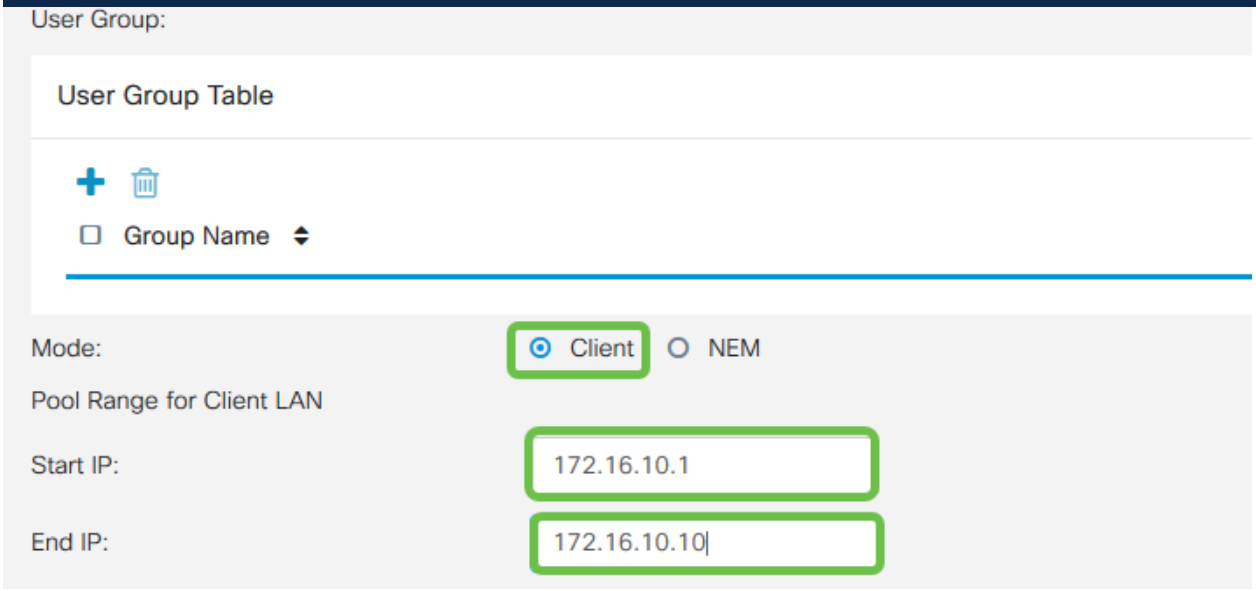


步驟5

暫時將**使用者組表**留空。這是用於路由器上的*使用者組*，但我們尚未對其進行配置。確

保Mode設定為Client。輸入客戶端LAN的池範圍。我們將使用172.16.10.1到172.16.10.10。

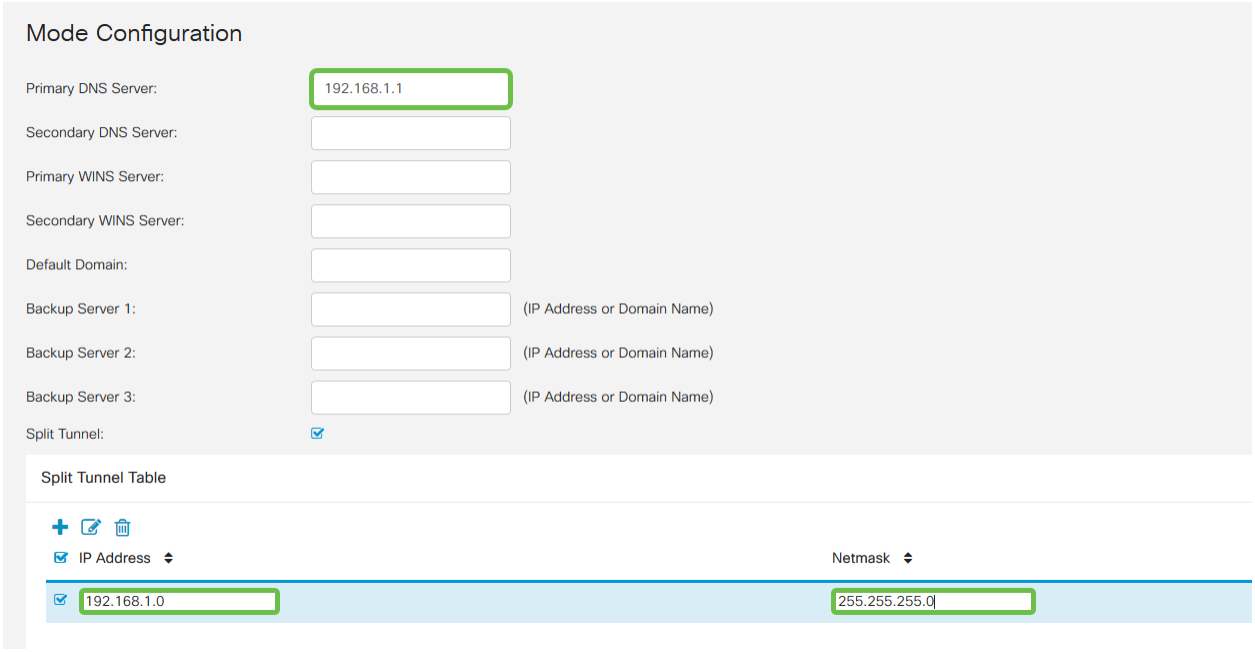
池範圍應使用網路中其它位置未使用的唯一子網。



步驟6

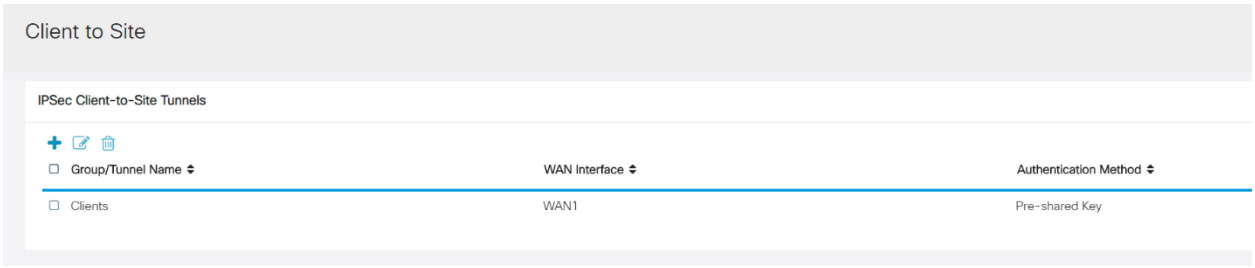
此處我們配置模式**配置**設定。以下是我們將使用的設定：

- **主DNS伺服器**:如果您有內部DNS伺服器或想要使用外部DNS伺服器，可以在此處輸入該伺服器。否則，預設設定為RV345P LAN IP地址。我們將使用示例中的預設值。
- **分割隧道**：選中以啟用分割隧道。這用於指定哪些流量將通過VPN隧道。在我們的示例中，我們將使用拆分隧道。
- **拆分隧道表**：輸入VPN客戶端通過VPN有權訪問的網路。此示例使用RV345P LAN網路。



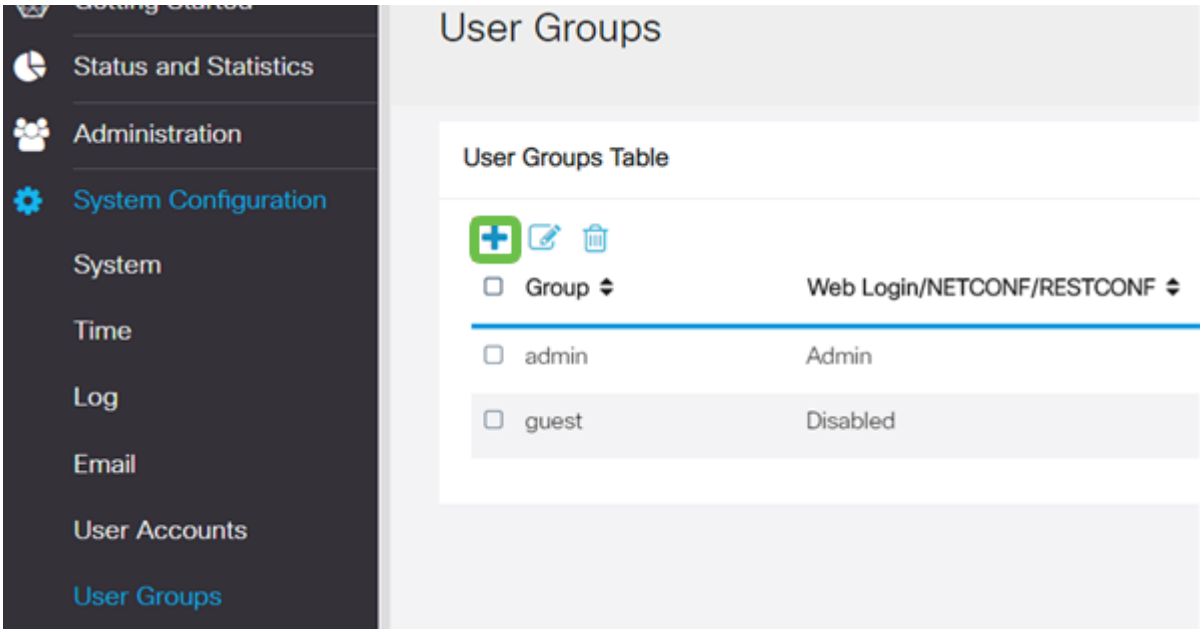
第7步

按一下**Save**後，我們在**IPsec Client-to-Site Groups**清單中可以看到配置檔案。



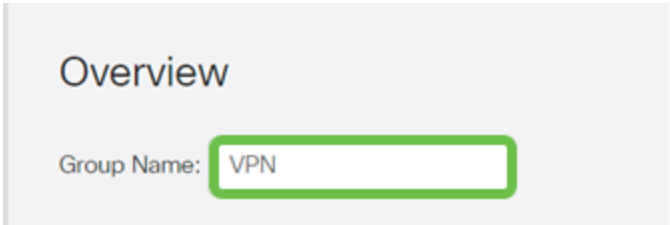
步驟8

配置用**於驗證**VPN客戶端使用者的使用者組。在**System Configuration > User Groups**下，按一下**plus圖示**以新增使用者組。



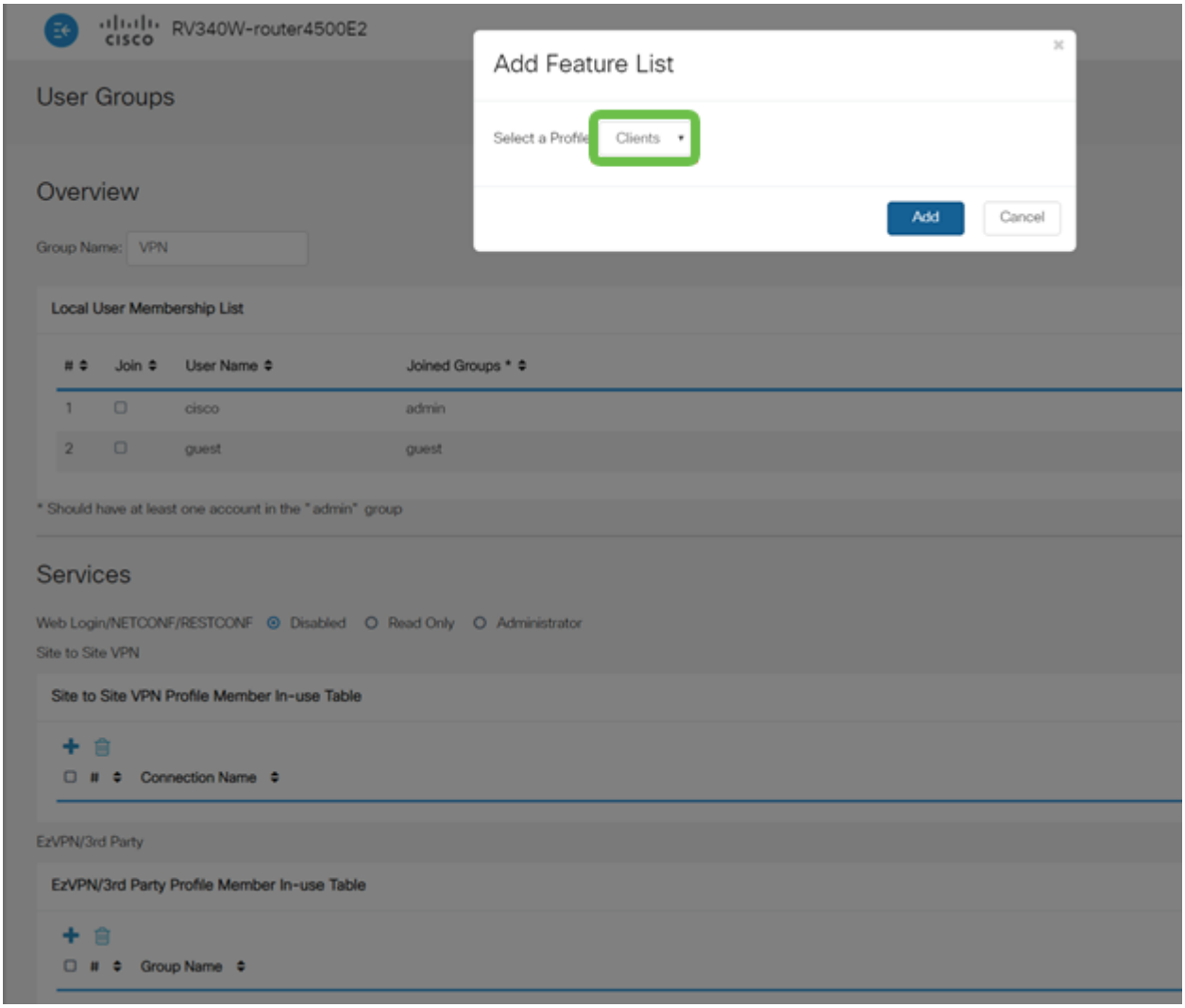
步驟9

輸入組**名稱**。



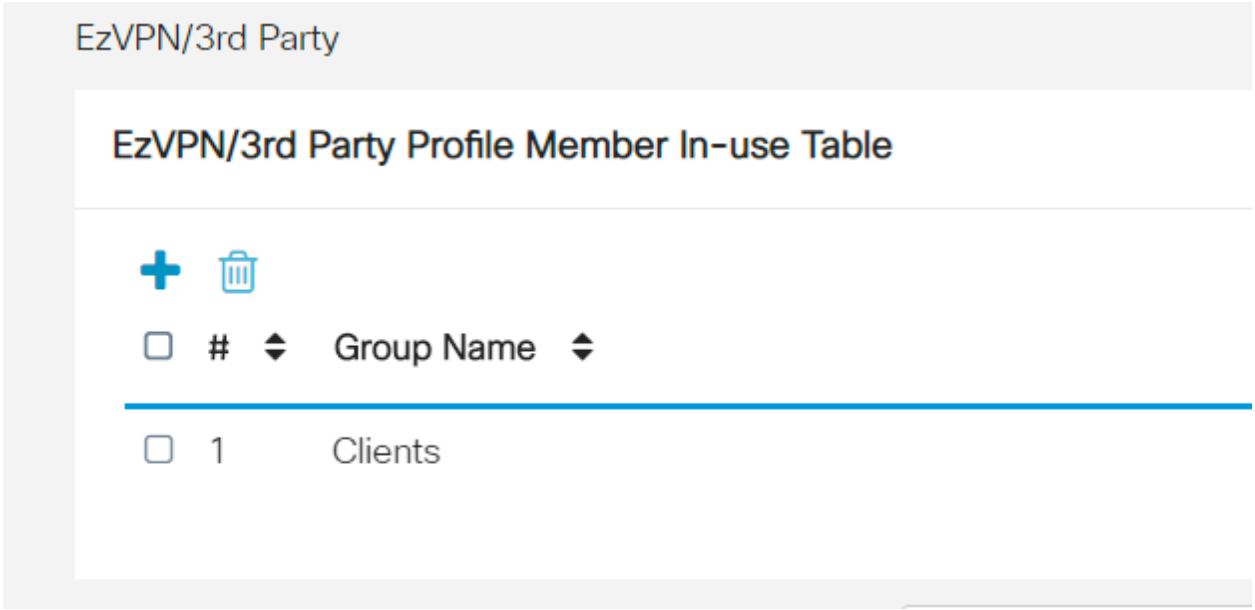
步驟10

在**Services > EzVPN/rd Party**下，按一下**Add**將此使用者組連結到之前配置的**Client-to-Site** Profile。



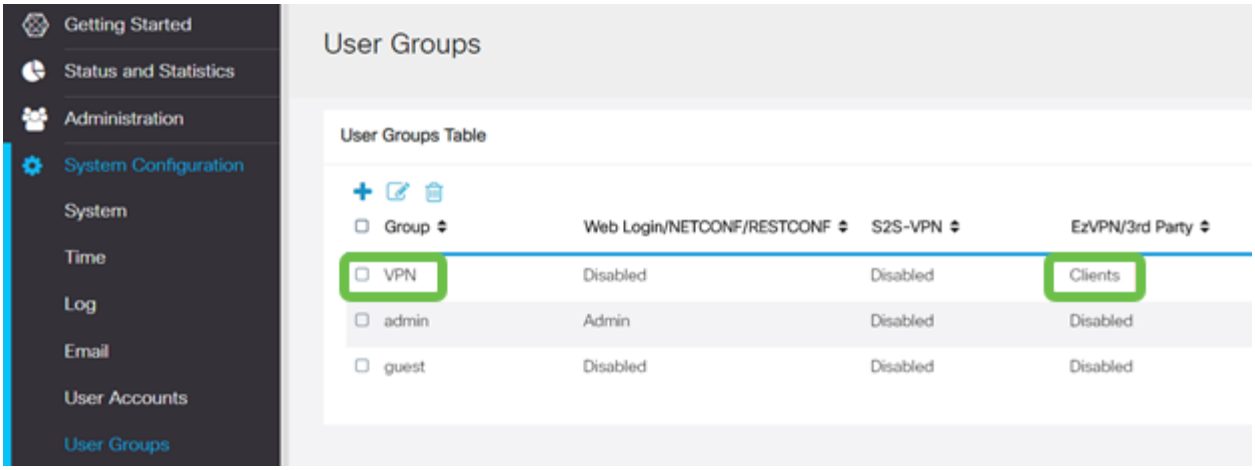
步驟11

現在，您應該會看到**EzVPN/第3方**的清單中的客戶端**到站點組名稱。**



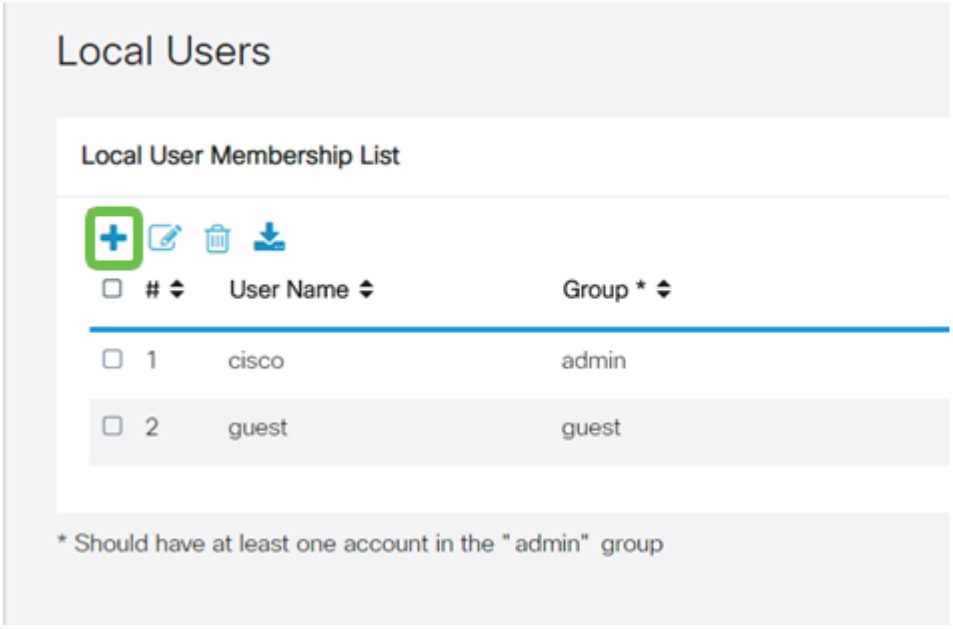
步驟12

Apply User Group配置後，您將在**User Groups**清單中看到它，並且它將顯示新的使用者組將與之前建立的客戶端到站點配置檔案一起使用。



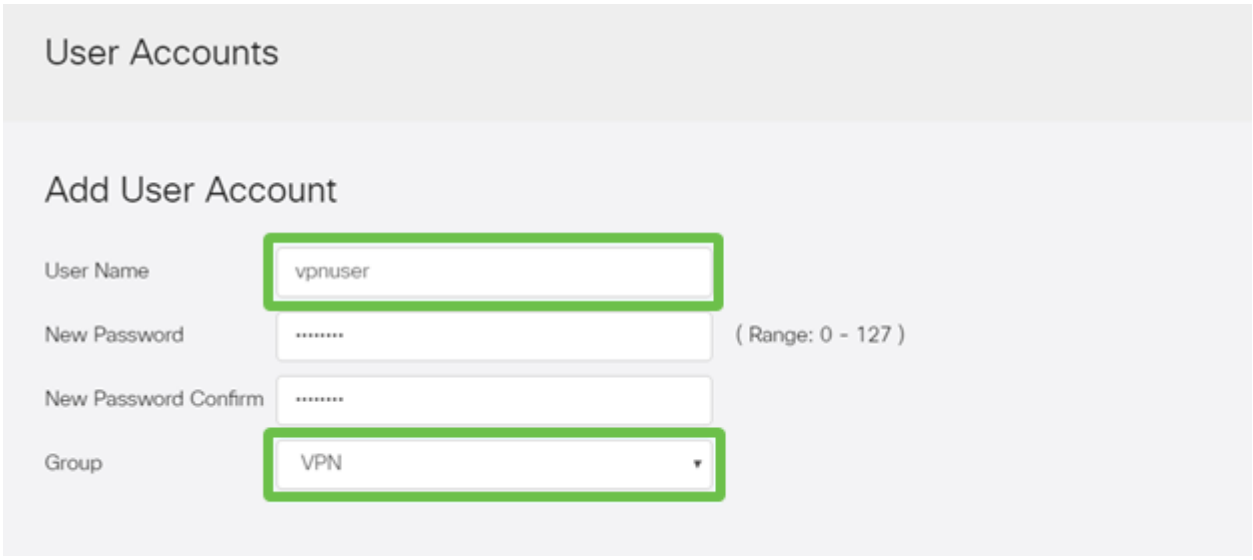
步驟13

在**System Configuration > User Accounts**中配置新使用者。按一下**plus圖示**建立新使用者。



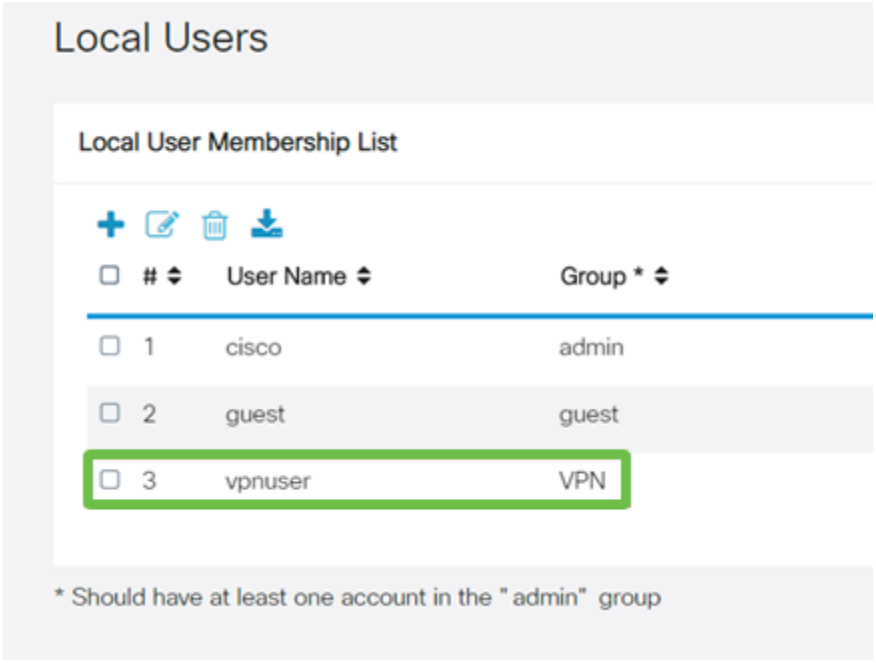
步驟14

輸入新**使用者名稱**和**新密碼**。驗證**Group**已設定為您剛才配置的**新User Group**。完成後按一下**Apply**。



步驟15

新使用者將顯示在**本地使用者**清單中。



這樣即可完成RV345P系列路由器的配置。接下來，您將配置Shrew Soft VPN客戶端。

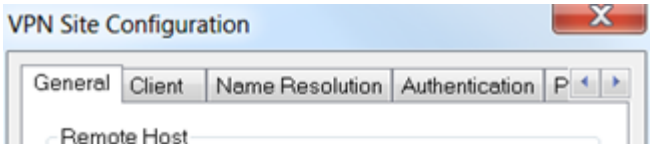
配置Show Soft VPN客戶端

請執行以下步驟。

步驟1

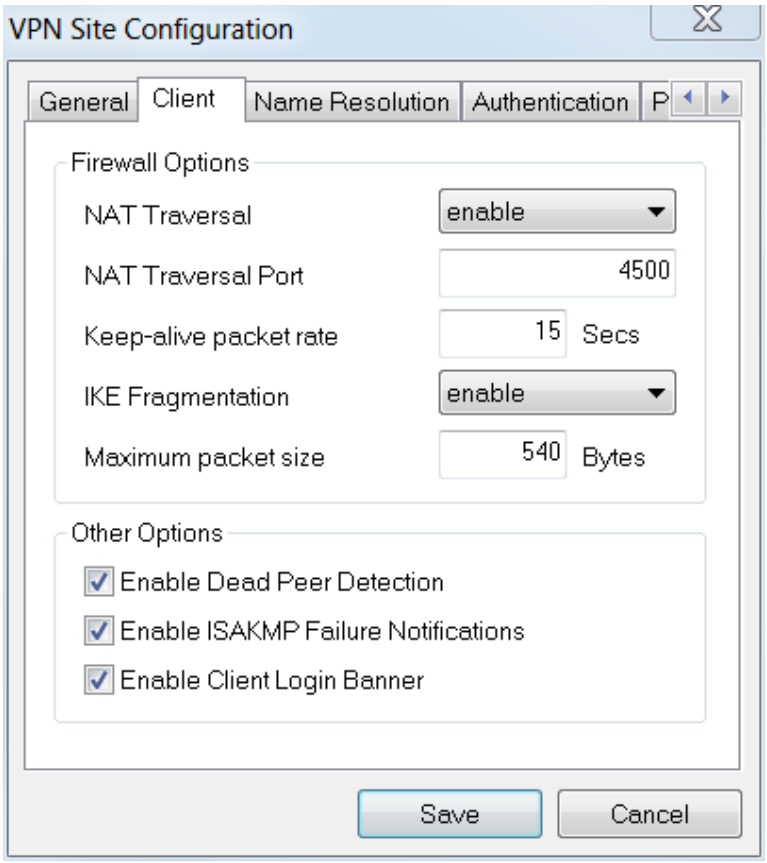
開啟Show Soft *VPN Access Manager*並單擊**Add**以新增配置檔案。在出現的*VPN Site Configuration*視窗中，配置**General**頁籤：

- **主機名或IP地址**:使用WAN IP地址（或RV345P的主機名）
- **自動配置**:選擇ike config pull
- **介面卡模式**:選擇**使用虛擬介面卡和分配的地址**



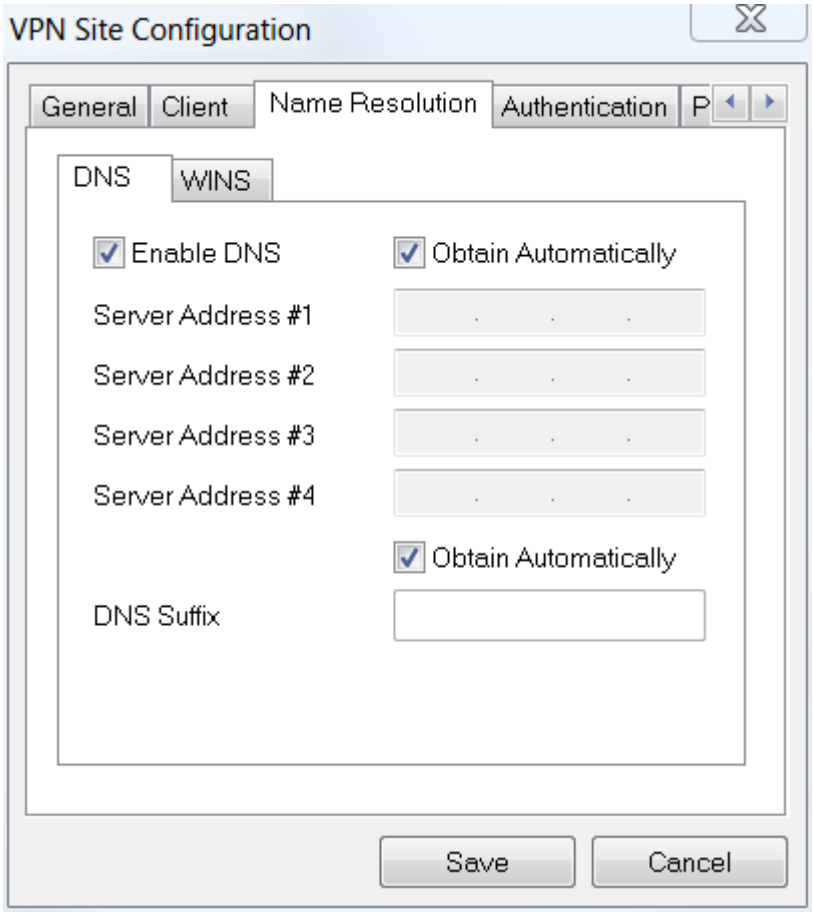
步驟2

配置Client頁籤。在本例中，我們保留了預設設定。



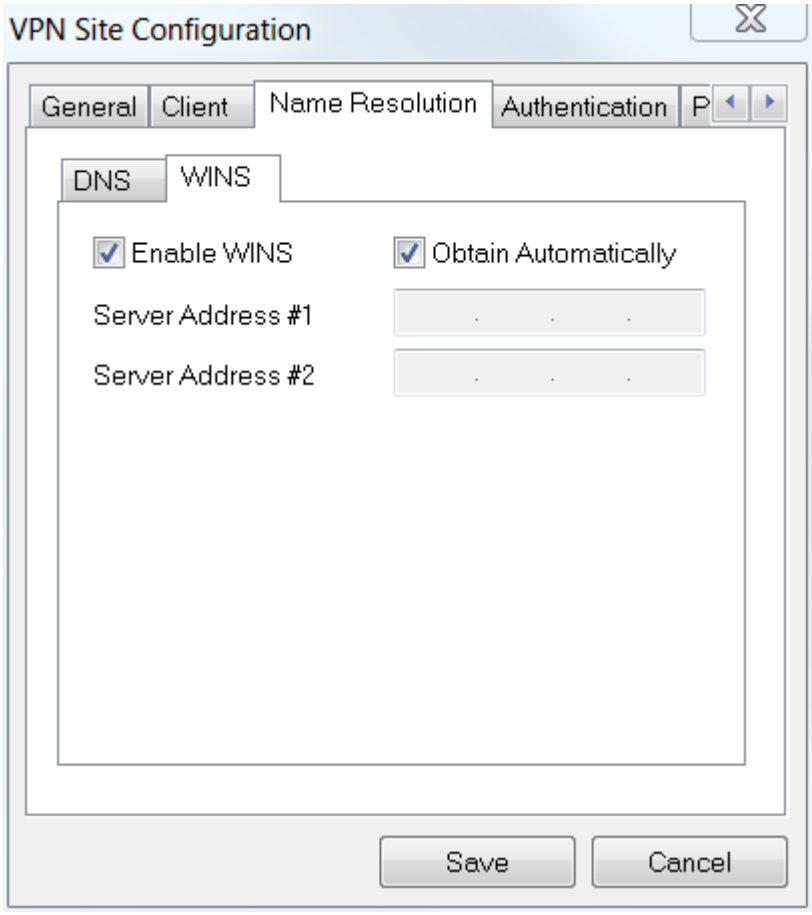
步驟3

在Name Resolution > DNS下，選中Enable DNS框，並選中Obtain Automatically框。



步驟4

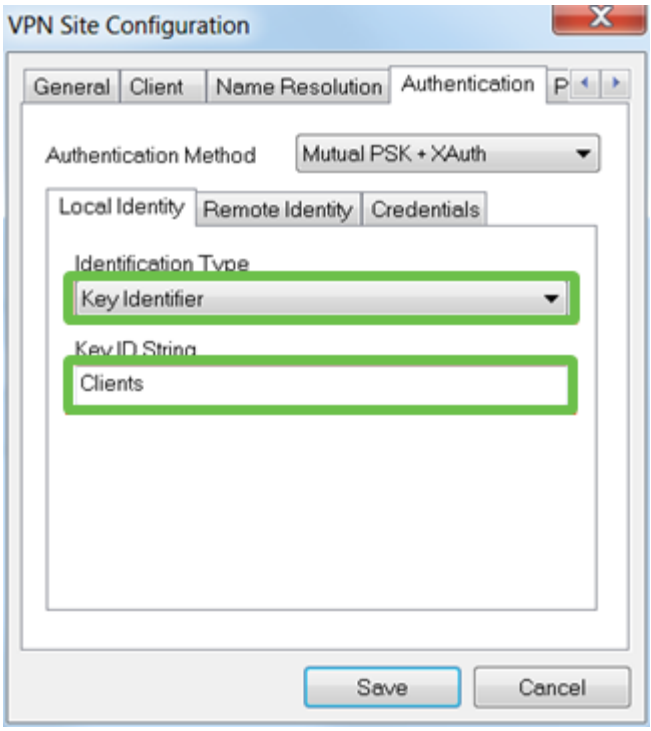
在**Name Resolution > WINS**頁籤下，選中**Enable WINS**覈取方塊，並保留**Obtain Automatically**覈取方塊。



步驟5

按一下**Authentication > Local Identity**。

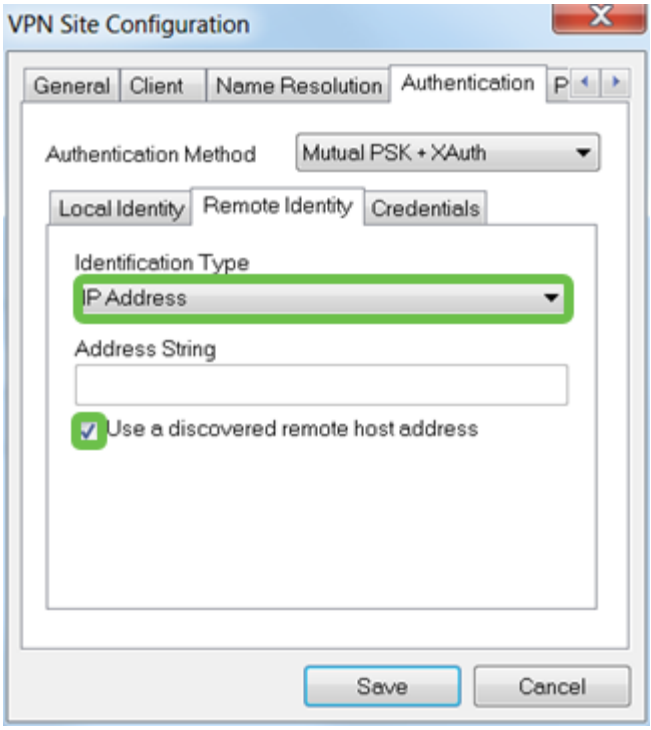
- **標識型別**:選擇**金鑰識別符號**
- **金鑰ID字串**:輸入在RV345P上配置的**Group Name**



步驟6

在**Authentication > Remote Identity**下。在本例中，我們保留了預設設定。

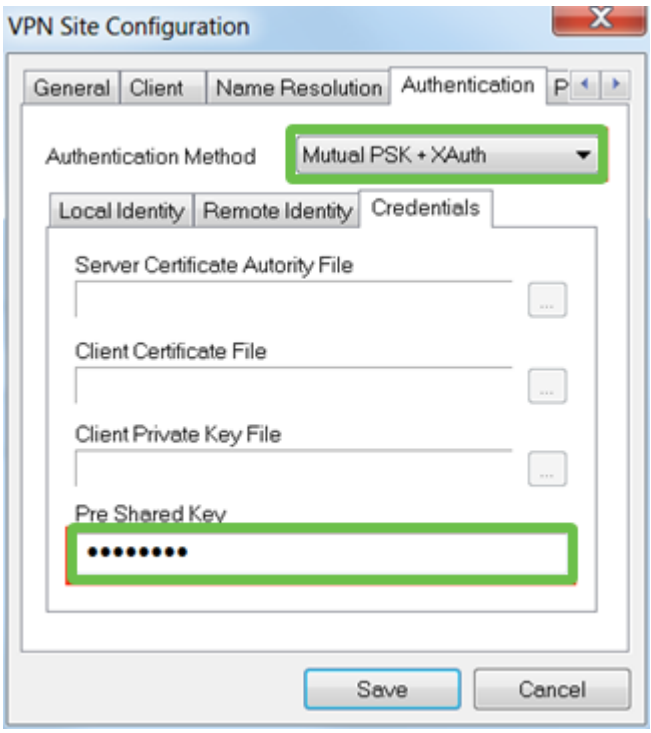
- **標識型別**:IP 位址
- **地址字串**:<blank>
- **使用發現的遠端主機地址**框：已檢查



第7步

在**Authentication > Credentials**下，配置以下內容：

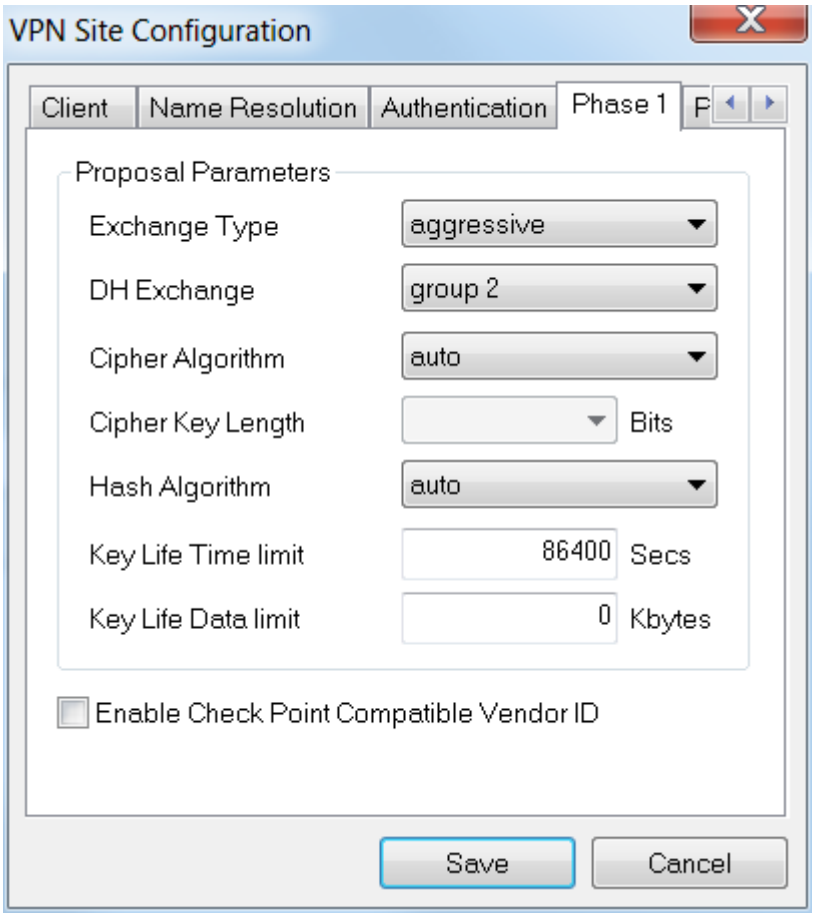
- **身份驗證方**法：選擇**Mutual PSK +擴展驗證**
- **預共用金鑰**:輸入在RV345P客戶端配置檔案中配置的**預共用金鑰**



步驟8

用於**Phase 1**頁籤。在此範例中，保留預設設定：

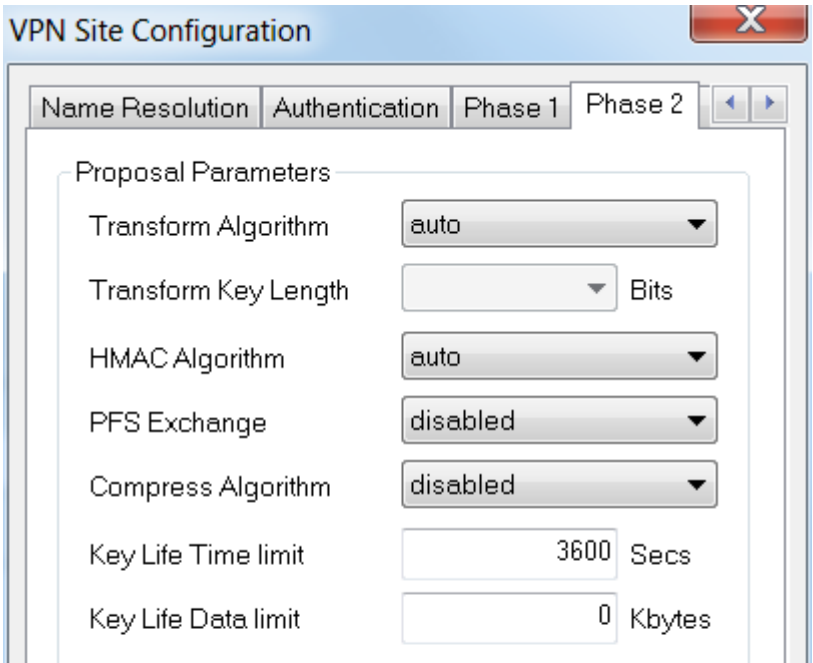
- **Exchange型別：積極性**
- **DH交換：組2**
- **密碼演算法：自動**
- **雜湊演算法：自動**



步驟9

在本例中， **Phase 2**頁籤的預設值保持不變。

- **轉換演算法：自動**
- **HMAC演算法：自動**
- **PFS Exchange：已禁用**
- **壓縮演算法：禁用**

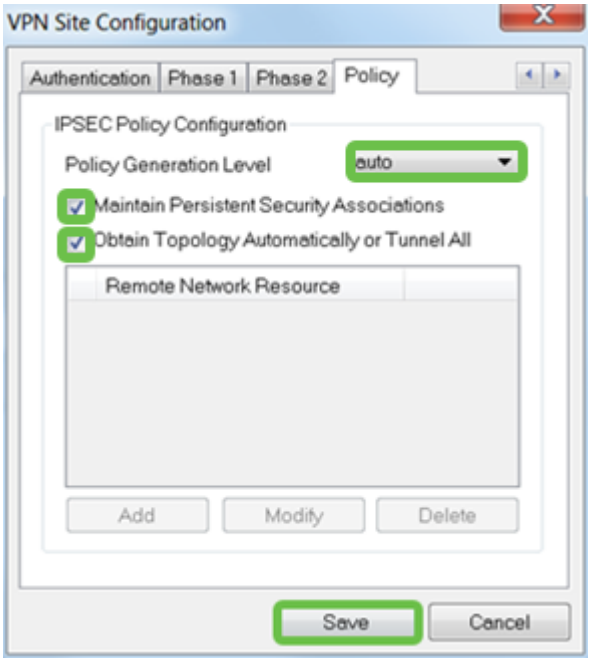


步驟10

在**Policy**頁籤示例中，我們使用以下設定：

- **策略生成級別：自動**
- **維護永續性安全關聯：已選中**
- **自動獲取拓撲或全部建立隧道：選中**

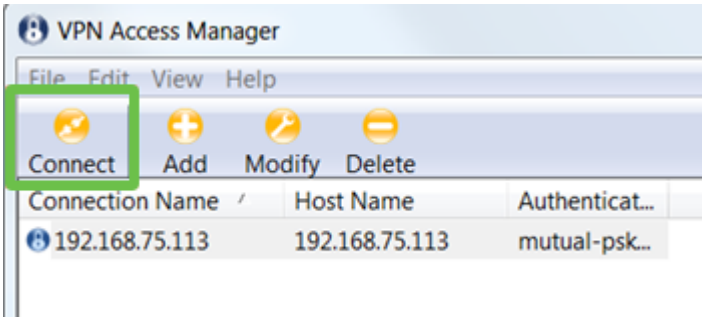
由於我們在RV345P上配置了**Split-Tunneling**，因此不需要在此處進行配置。



完成後，按一下**Save**。

步驟11

現在已準備好測試連線。在*VPN Access Manager*中，突出顯示連線配置檔案，然後按一下**Connect**按鈕。

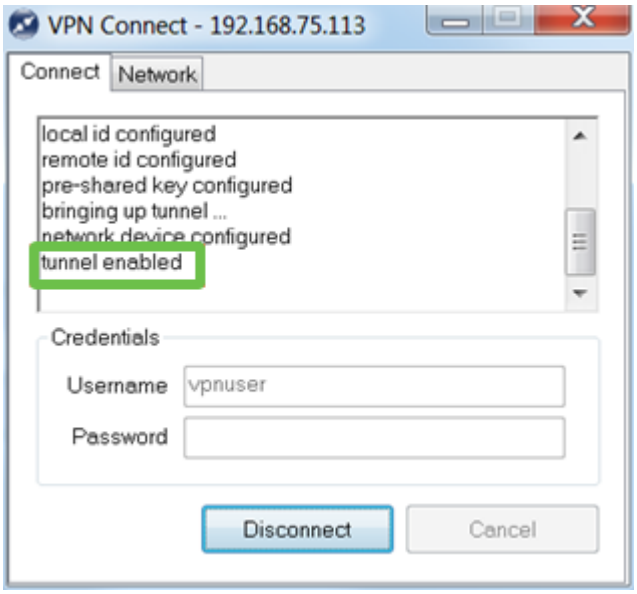


步驟12

在出現的**VPN Connect**視窗中，使用在RV345P上建立的**使用者帳戶**的憑證輸入**Username**和**Password**（步驟13和14）。 完成後，按一下「**Connect**」。

步驟13

驗證通道是否已連線。您應該會看到**通道已啟用**。



在此配置中以Shrew Soft為例。由於Shrew Soft不是思科產品，如果您需要技術協助，請聯絡此第三方。

其他VPN選項

還有其他一些使用VPN的選項。如需詳細資訊，請按一下以下連結：

- 使用GreenBow VPN客戶端連線RV34x系列路由器
- 在RV34x系列路由器上配置Teleworker VPN客戶端
- 在Rv34x系列路由器上配置點對點隧道協定(PPTP)伺服器
- 在RV34x系列路由器上配置網際網路協定安全(IPsec)配置檔案
- 在RV34x路由器上配置L2TP WAN設定
- 在RV34x上配置站點到站點VPN

RV345P路由器的補充配置

配置VLAN（可選）

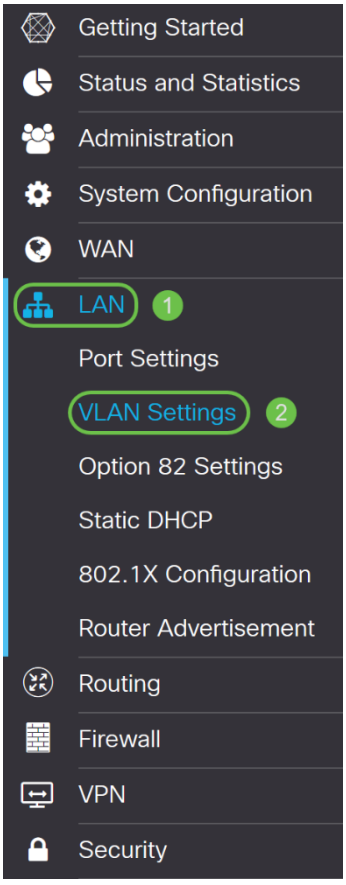
虛擬區域網路(VLAN)允許您以邏輯方式將區域網路(LAN)劃分為不同的廣播網域。在敏感資料可能在網路上廣播的情況下，可以建立VLAN，通過將廣播指定到特定VLAN來增強安全性。VLAN還可用於通過將廣播和組播傳送到不必要目的地的需要降低來提高效能。您可以建立VLAN，但只有將VLAN手動或動態連線到至少一個連線埠時，這才會生效。連線埠必須始終屬於一個或多個VLAN。

您可能希望參閱VLAN最佳實踐和安全提示以獲得其他指導。

如果您不想建立VLAN，可以跳到下一節。

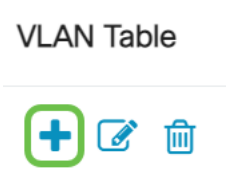
步驟1

導覽至**LAN > VLAN Settings**。



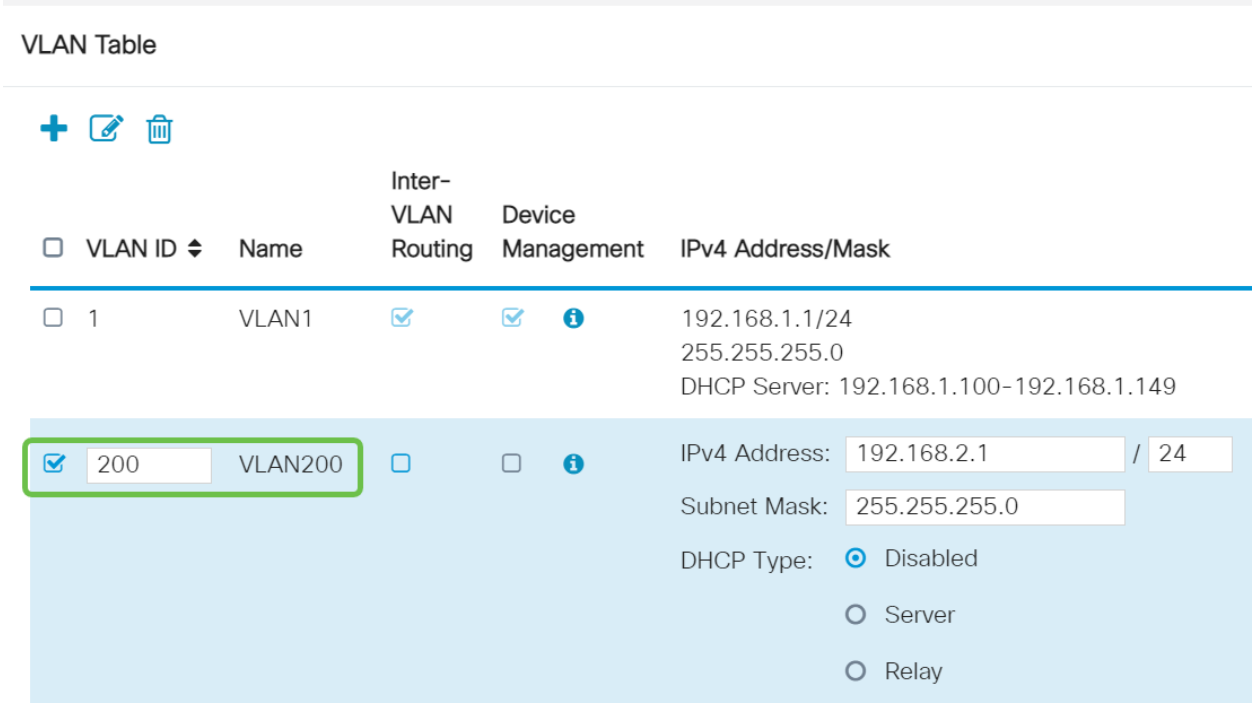
步驟2

按一下**add**圖示建立新的VLAN。



步驟3

輸入要建立的*VLAN ID*和名稱。*VLAN ID*的範圍為1到4093。



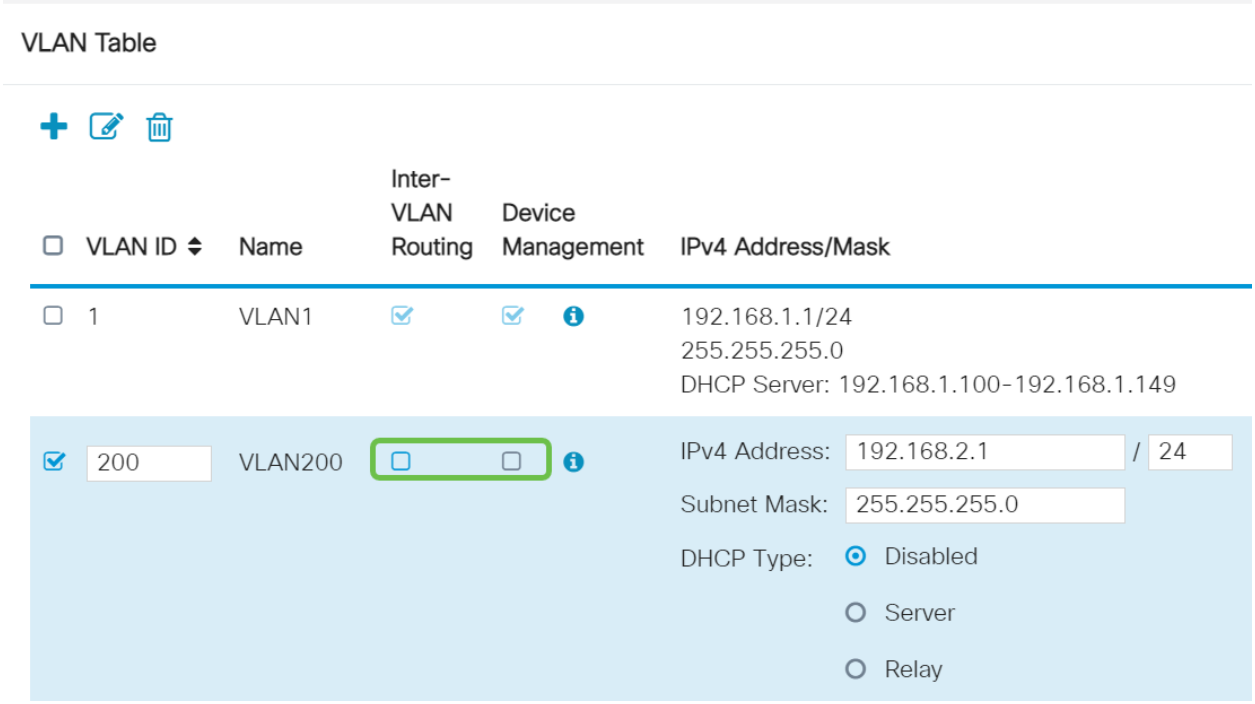
步驟4

如果需要，請取消選中*Inter-VLAN Routing*和*Device Management*的*Enabled*框。VLAN間路由用於將資料包從一個VLAN路由到另一個VLAN。

一般來說，不建議對訪客網路使用這種方法，因為您會想要隔離訪客使用者，因為這會使VLAN安全性降低。有時VLAN可能需要在彼此之間路由。如果是這種情況，請在具有目標ACL限制的RV34x路由器上檢查VLAN間路由，以配置您允許的VLAN之間的特定流量。

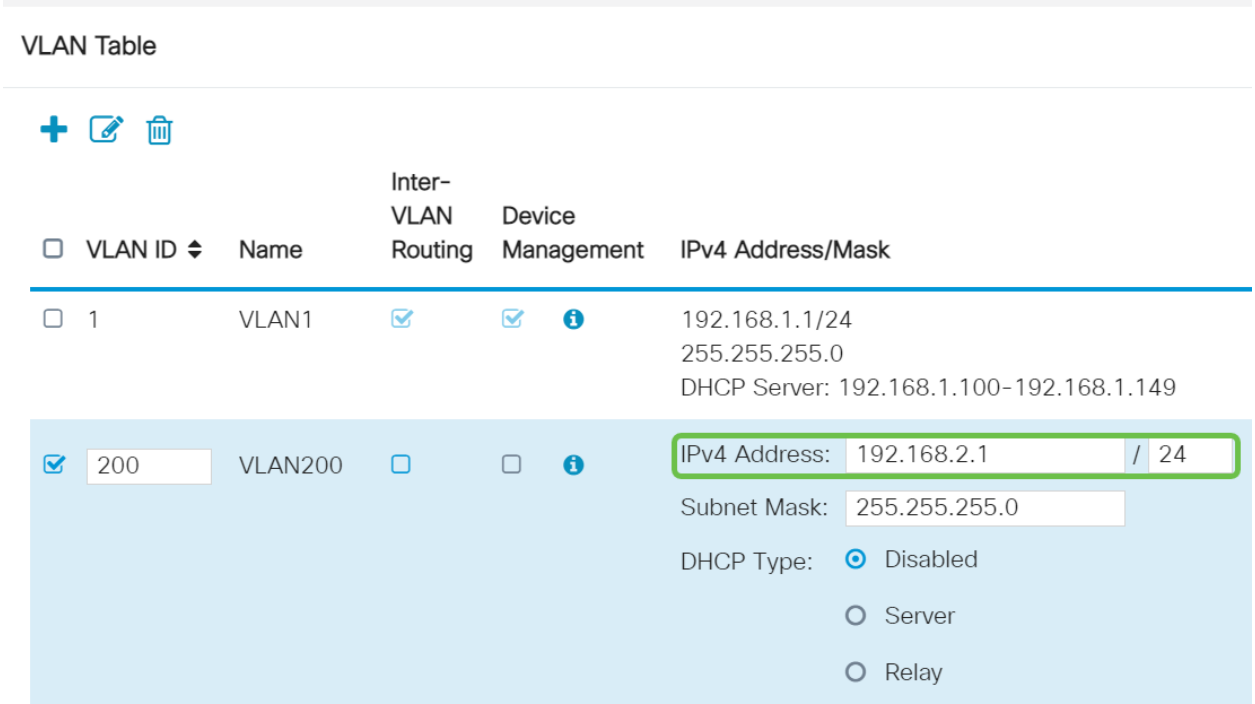
「裝置管理」軟體允許您使用瀏覽器從VLAN登入到RV345P的Web UI並管理RV345P。這也應該在訪客網路上禁用。

在本例中，我們沒有啟用*VLAN間路由*或*裝置管理*來確保VLAN更安全。



步驟5

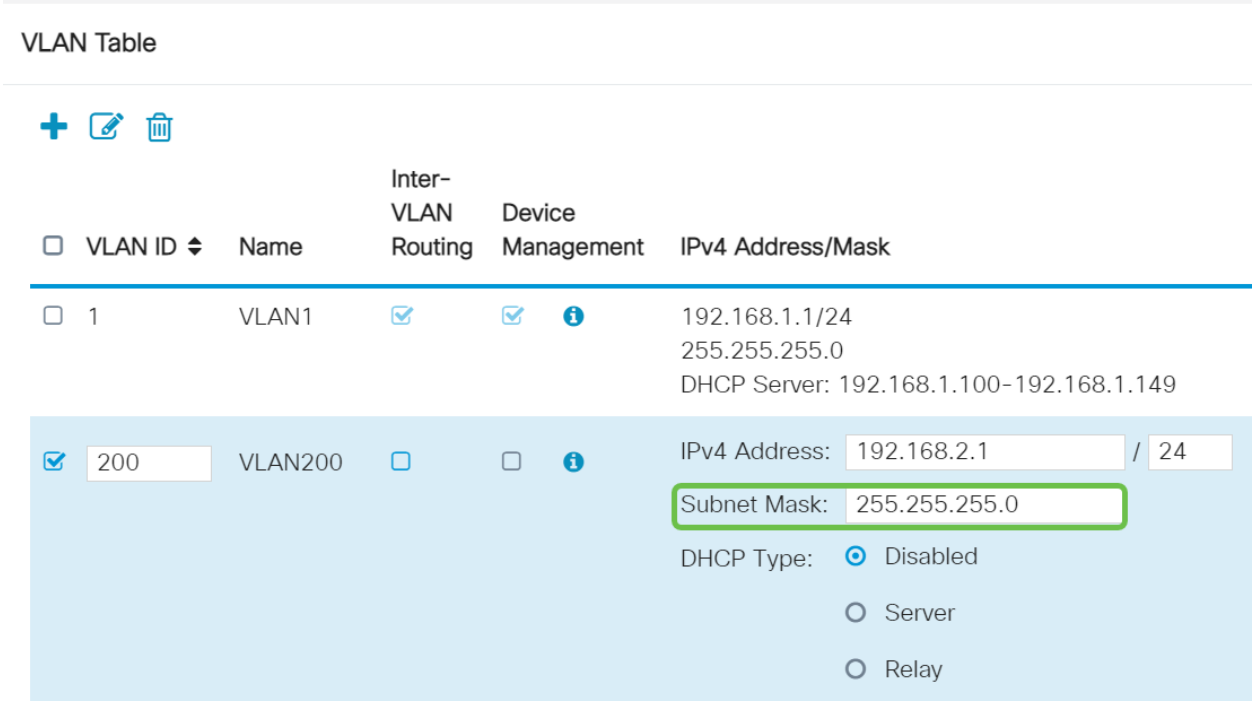
私有IPv4地址將自動填充到*IP Address*欄位中。如果您選擇，可以調整它。在本示例中，子網有192.168.2.100-192.168.2.149可用於DHCP的IP地址。192.168.2.1-192.168.2.99和192.168.2.150-192.168.2.254可用於靜態IP地址。



步驟6

*Subnet Mask*下的子網掩碼將自動填充。如果您進行更改，將自動調整該欄位。

在本演示中，我們將*子網掩碼*保留為**255.255.255.0**或**/24**。



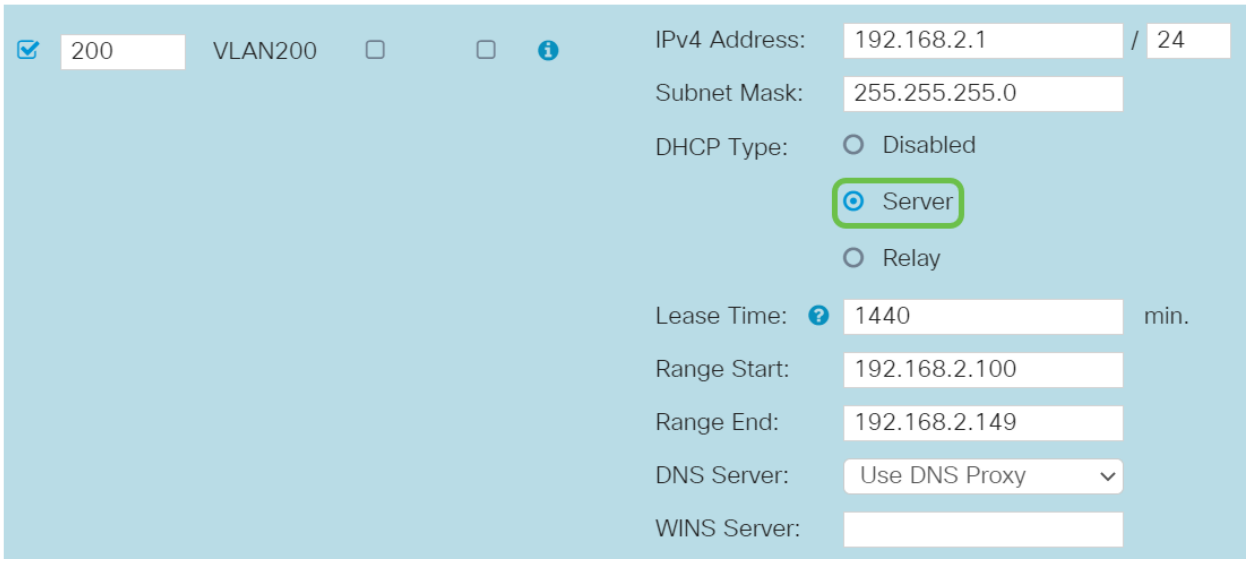
第7步

選擇動*態主機配置協定(DHCP)型別*。以下選項是：

Disabled — 禁用VLAN上的DHCP IPv4伺服器。建議在測試環境中執行此操作。在這種情況下，需要手動配置所有IP地址，並且所有通訊均為內部通訊。

Server — 這是最常用的選項。

- 租用時間 — 輸入時間值5到43,200分鐘。預設值為1440分鐘（等於24小時）。
- Range Start和Range End — 輸入可以動態分配的IP地址的範圍開始和結束。
- DNS Server — 選擇以使用DNS伺服器作為代理，或從下拉選單的ISP中選擇。
- WINS伺服器 — 輸入WINS伺服器名稱。
- DHCP選項：
    - 選項66 — 輸入TFTP伺服器的IP地址。
    - 選項150 — 輸入TFTP伺服器清單的IP地址。
    - 選項67 — 輸入配置檔名。
- 中繼 — 輸入遠端DHCP伺服器IPv4地址以配置DHCP中繼代理。這是一個更高級的配置。



步驟8

按一下「**Apply**」以建立新的VLAN。

為埠分配VLAN（可選）

在RV345P上可以配置16個VLAN，其中一個VLAN用於廣域網(WAN)。不應包含在連線埠上的VLAN應排除。這會將該連線埠上的流量專門保留給使用者特別指定的VLAN/VLAN。這被認為是一種最佳做法。

埠可以設定為接入埠或中繼埠：

- 接入埠 — 分配了一個VLAN。未標籤的幀會被通過。
- 中繼埠 — 可以承載多個VLAN。802.1q。中繼允許本徵VLAN無標籤。您不想要的VLAN應該排除。

一個VLAN分配了自己的埠：

- 視為接入埠。
- 分配給此埠的VLAN應標籤為「未標籤」。
- 對於該埠，所有其他VLAN都應標籤為Excluded。

兩個或多個VLAN共用一個連線埠：

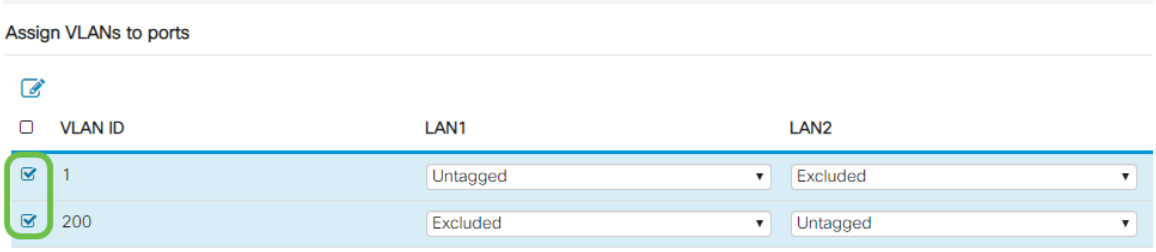
- 被視為中繼埠。
- 其中一個VLAN可以標籤為「未標籤」。
- 屬於Trunk埠的其他VLAN應標籤為Tagged。
- 不屬於中繼埠的VLAN應為該埠標籤為Excluded。

在本示例中，沒有中繼。

步驟1

選擇*要編*輯的VLAN ID。

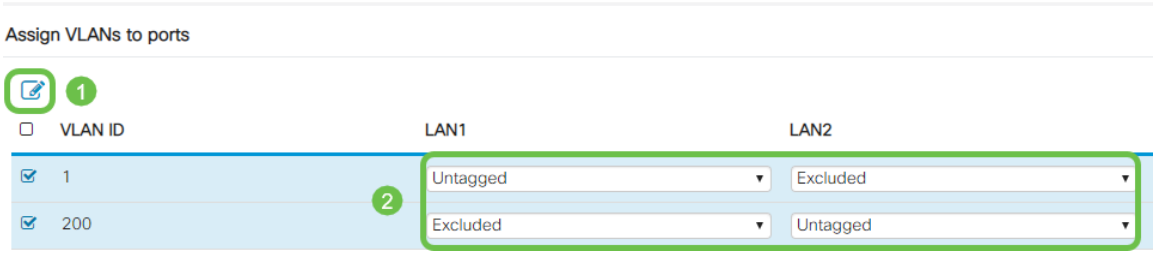
在本範例中，我們選擇了*VLAN 1*和*VLAN 200*。



步驟2

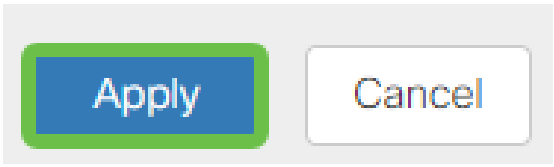
按一下**Edit**將VLAN分配給LAN埠，並將每個設定指定為*Tagged*、*Untagged*或*Excluded*。

在本範例中，在LAN1上，我們將VLAN 1指派為**Untagged**，將VLAN 200指派為**Excluded**。對於LAN2，我們已將VLAN 1分配為**Excluded**，並將VLAN 200分配為**Untagged**。



步驟3

按一下「**Apply**」以儲存組態。



現在，您應該已經成功建立了一個新的VLAN並配置了VLAN到RV345P上的埠。重複該過程以建立其他VLAN。例如，VLAN300是為子網為192.168.3.x的Marketing建立的，VLAN400是為子網為192.168.4.x的Accounting建立的。

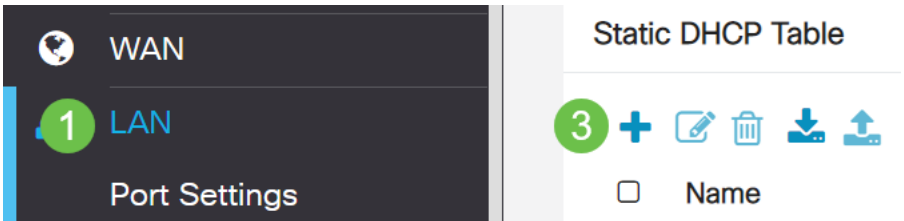
新增靜態IP（可選）

如果希望某個裝置可以訪問其他VLAN，可以為該裝置指定一個靜態本地IP地址並建立訪問規則使其可以訪問。這只會在啟用VLAN間路由時起作用。在其他情況下，靜態IP可能有用。有關設定靜態IP地址的詳細資訊，請檢視**在思科業務硬體上設定靜態IP地址的最佳實踐**。

如果您不需要新增靜態IP地址，可以轉到本文的下一節。

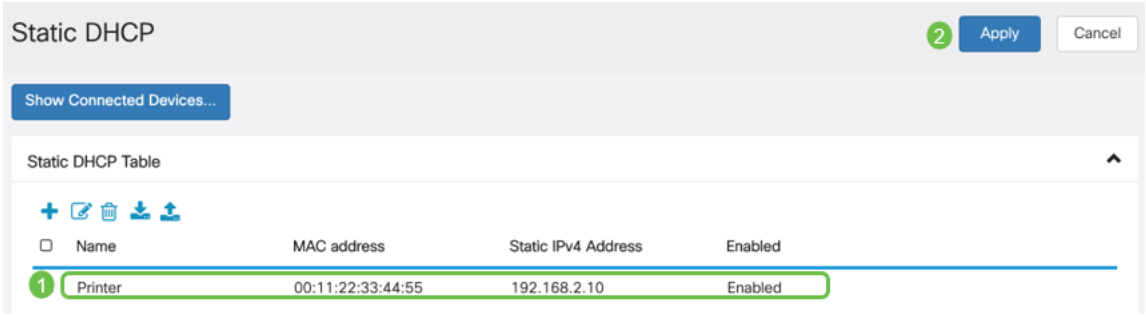
步驟1

導覽至**LAN > Static DHCP**。點選加**號圖示**。



步驟2

為裝置新增**Static DHCP**資訊。在本示例中，裝置是印表機。



管理證書（可選）

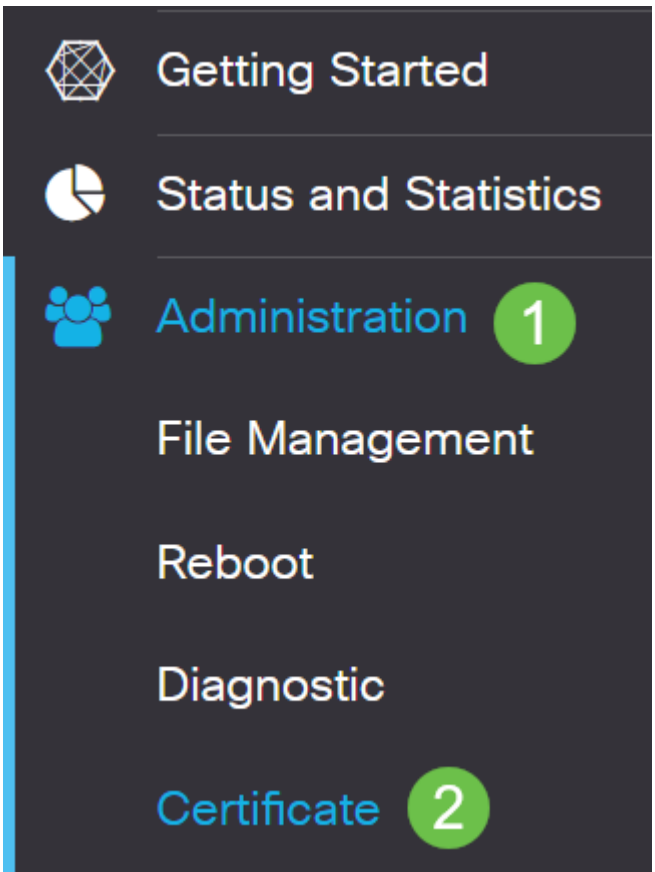
數位證書通過證書的指定主題來證明公共金鑰的所有權。這允許依賴方依賴於由與經認證的公鑰對應的私鑰進行的簽名或斷言。路由器可以生成自簽名證書，即由網路管理員建立的證書。它還可以向證書頒發機構(CA)發出申請數位身份證書的請求。必須擁有來自第三方應用程式的合法證書。

證書頒發機構(CA)用於身份驗證。可以從任意數量的第三方站點購買證書。這是證明您的站點安全的官方方式。實質上，CA是受信任的來源，用於驗證您的企業是否合法以及是否值得信任。根據您的需要，以最低成本獲得證書。您會由CA簽出，他們驗證您的資訊後，會向您頒發證書。此證書可以作為檔案下載到您的電腦上。然後，您可以進入您的路由器（或VPN伺服器）並上傳到那裡。

產生CSR/憑證

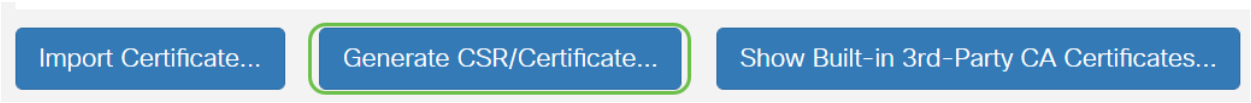
步驟1

登入到路由器的基於Web的實用程式，然後選擇**Administration > Certificate**。



步驟2

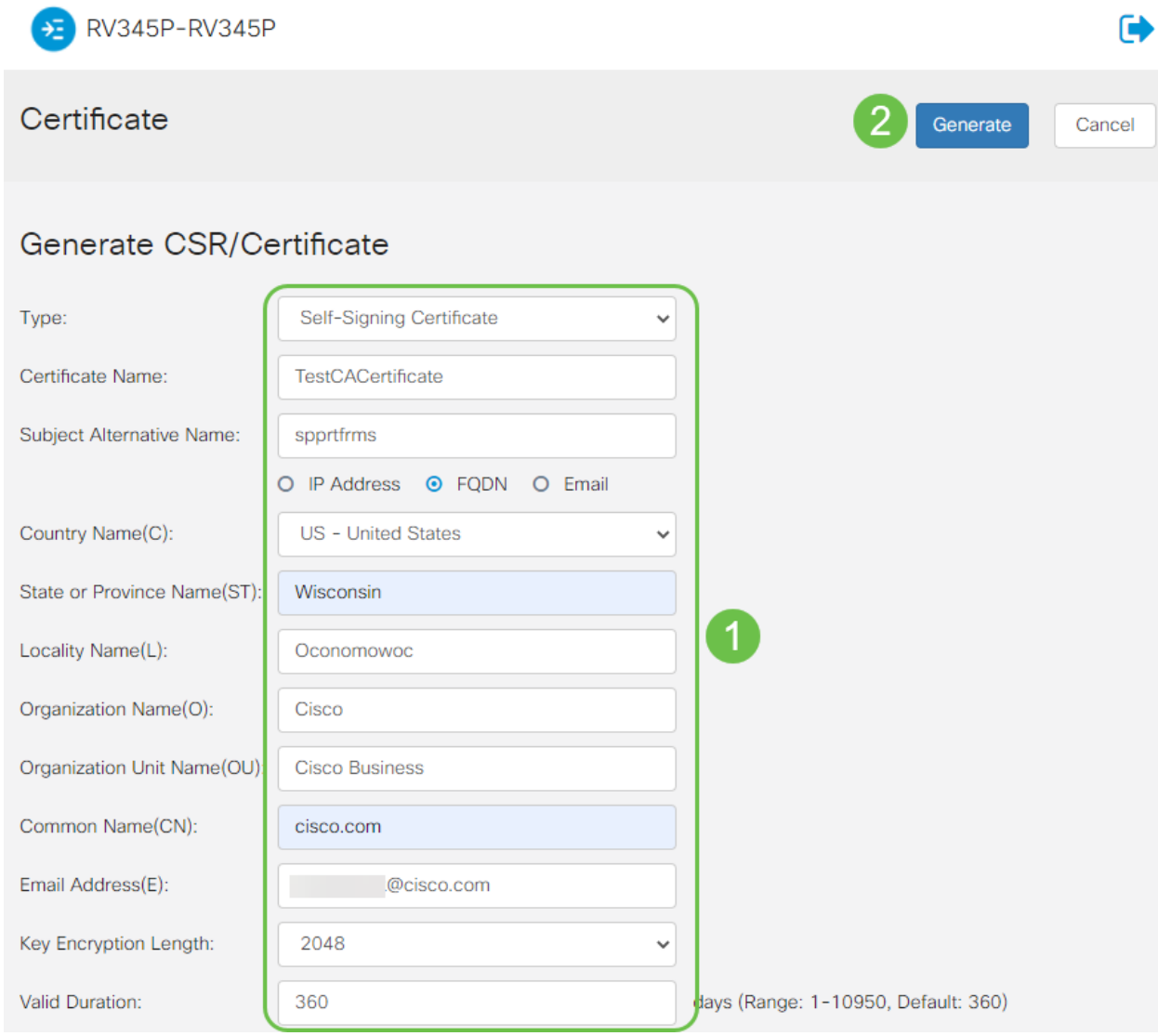
按一下「**Generate CSR/Certificate**」。您將進入「產生CSR/憑證」頁面。



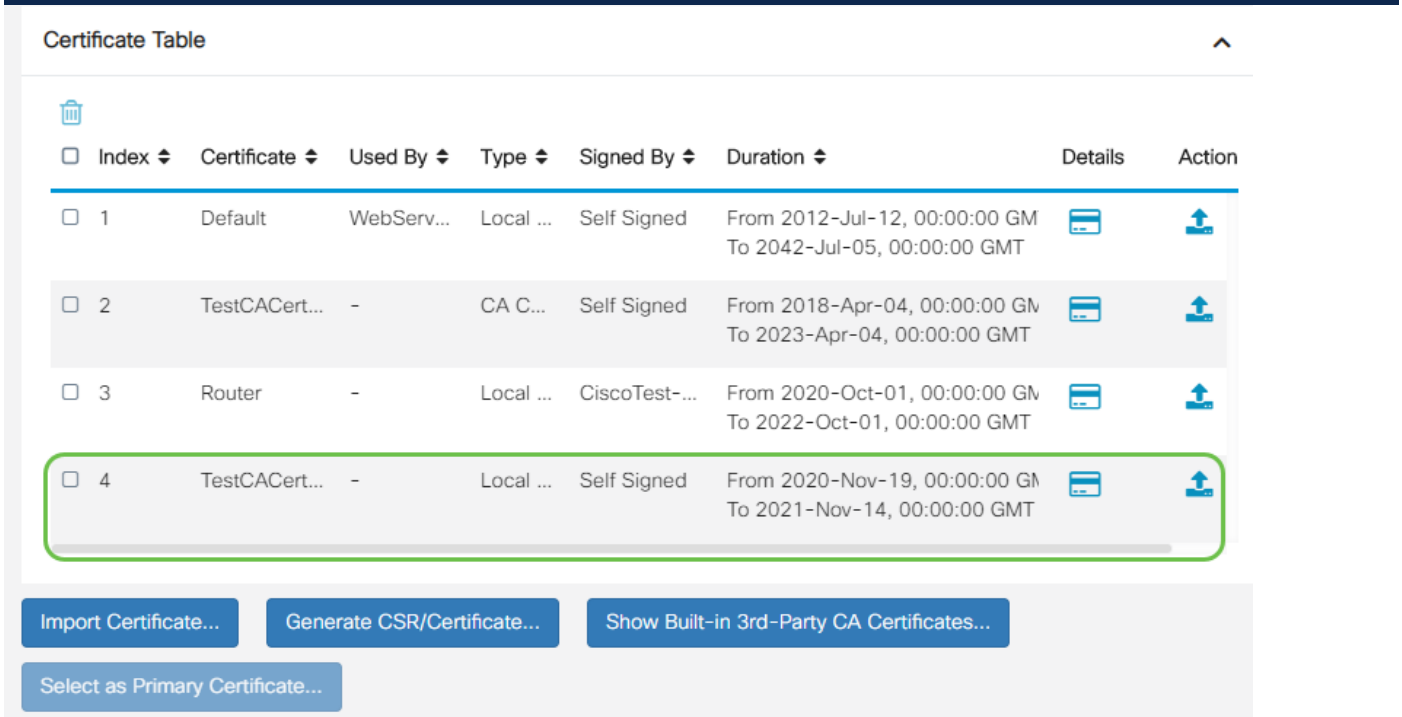
步驟3

在框中填寫以下內容：

- 選擇適當的證書型別
  - 自簽名證書 — 這是由自己的建立者簽名的安全套接字層(SSL)證書。此證書不受信任，因為如果攻擊者以某種方式破壞私鑰，則無法取消此證書。
  - 認證簽名請求 — 這是公鑰基礎設施(PKI)，傳送到證書頒發機構以申請數位身份證書。它比自簽名更安全，因為私鑰是保密的。
- 在Certificate Name欄位中輸入證書名稱以標識請求。此欄位不能為空，也不能包含空格和特殊字元。
- （可選）在Subject Alternative Name區域下，按一下單選按鈕。選項包括：
  - IP地址 — 輸入網際網路協定(IP)地址
  - FQDN — 輸入完全限定域名(FQDN)
  - 電子郵件 — 輸入電子郵件地址
- 在Subject Alternative Name欄位中，輸入FQDN。
- 從Country Name下拉選單中選擇組織合法註冊的國家/地區名稱。
- 在「省（州）」或「省名稱(ST)」欄位中輸入組織所在的州、省、地區或地區的名稱或縮寫。
- 在Locality Name欄位中輸入組織註冊或所在的地點或城市的名稱。
- 輸入企業合法註冊的名稱。如果您以小型企業或獨資企業身份註冊，請在「組織名稱」欄位中輸入證書申請者的名稱。不能使用特殊字元。
- 在「組織單位名稱」欄位中輸入名稱，以區分組織內的各個部門。
- 在公用名欄位中輸入名稱。此名稱必須是您對其使用證書的網站的完全限定域名。
- 輸入希望生成證書的人員的電子郵件地址。
- 從Key Encryption Length下拉選單中，選擇金鑰長度。選項為512、1024和2048。金鑰長度越大，證書就越安全。
- 在「有效持續時間」欄位中，輸入證書有效的天數。預設值為360。
- 按一下「**Generate**」。



生成的證書現在應該顯示在「證書表」中。

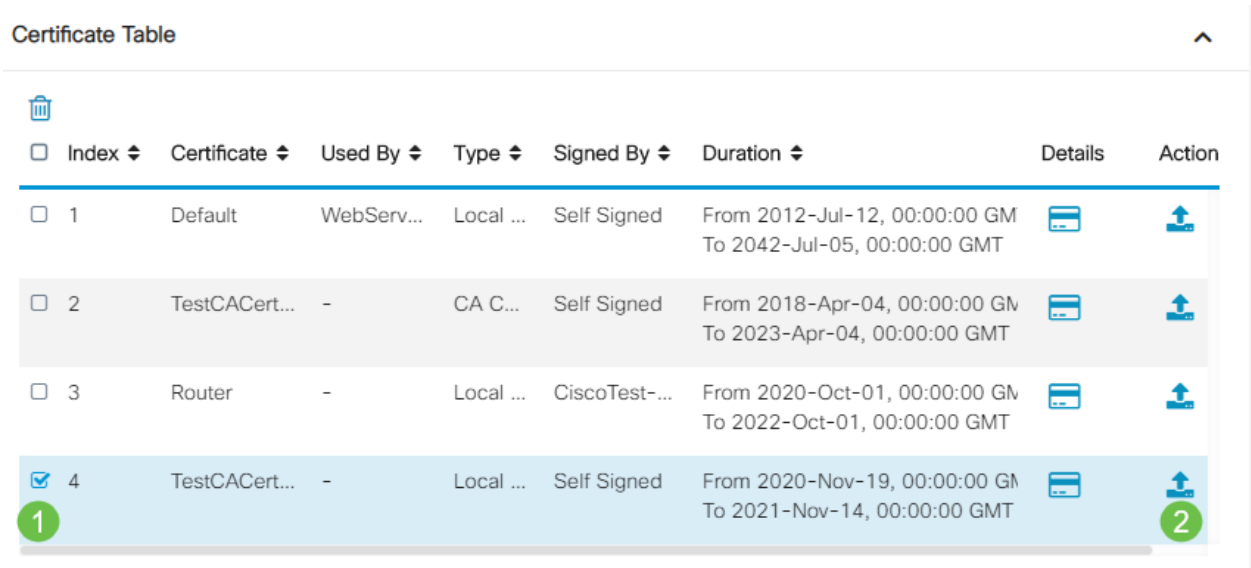


現在，您應該已經在RV345P路由器上成功建立了證書。

匯出證書

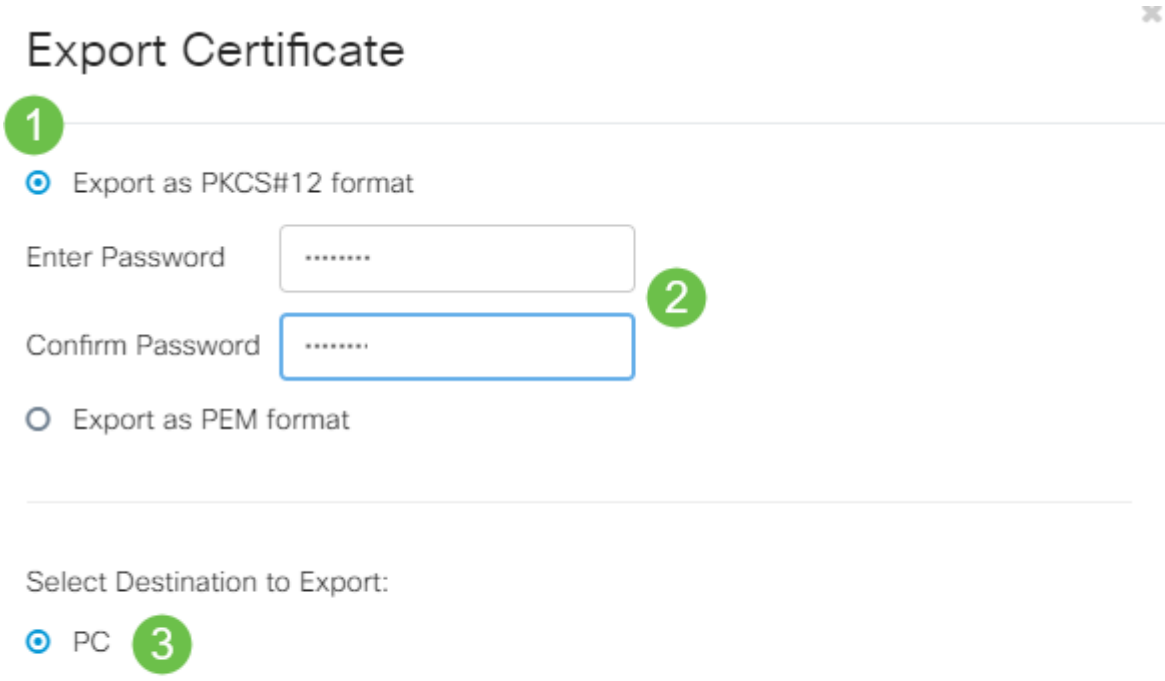
步驟1

在「證書」(Certificate)表格中，選中要匯出的證書的覈取方塊，然後點選**匯出圖示**。



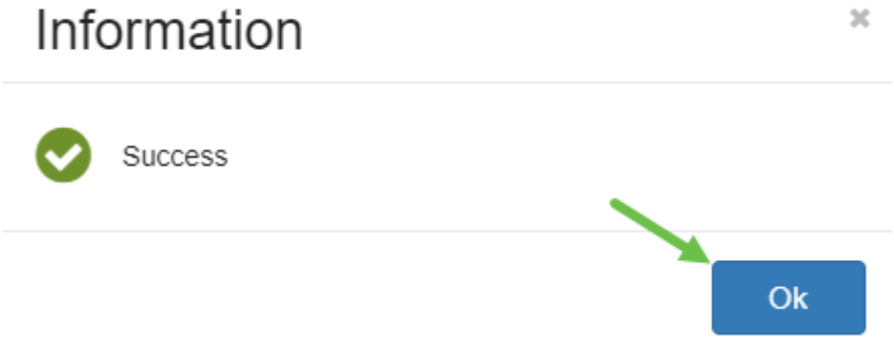
步驟2

- 按一下格式以匯出證書。選項包括：
  - PKCS #12 — 公鑰加密標準(PKCS)#12是以.p12副檔名提供的匯出證書。需要密碼才能加密檔案，以便在匯出、匯入和刪除檔案時對其進行保護。
  - PEM — 隱私增強型郵件(PEM)通常用於Web伺服器，因為它可以使用記事本等簡單文本編輯器輕鬆轉換為可讀資料。
- 如果您選擇PEM，只需按一下**Export**。
- 在「輸入密碼」欄位中輸入密碼以保護要匯出的檔案。
- 在確認密碼欄位中重新輸入密碼。
- 在Select Destination區域，已選擇PC，是目前可用的唯一選項。
- 按一下「**Export**」。



步驟3

「Download（下載）」按鈕下方將顯示一條指示下載成功的消息。檔案將開始在瀏覽器中下載。按一下「OK」（確定）。

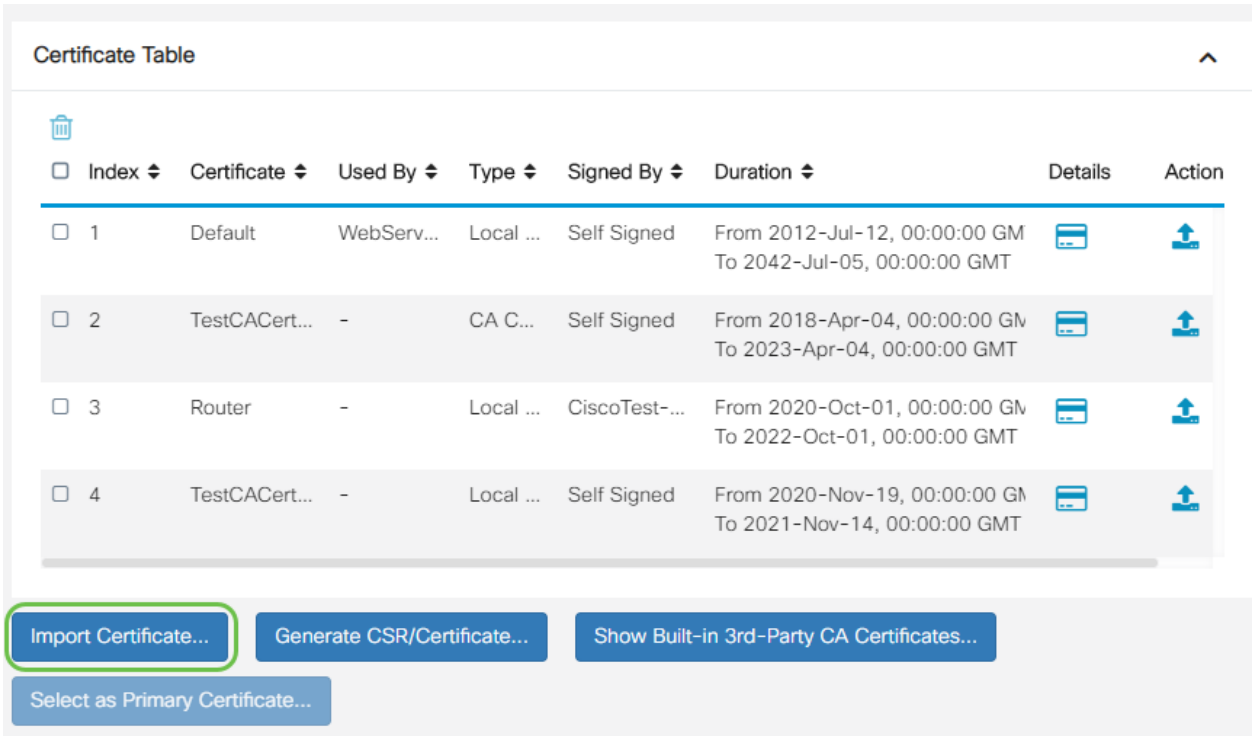


現在，您應該已經在RV345P系列路由器上成功匯出證書。

匯入證書

步驟1

按一下**Import Certificate...**。

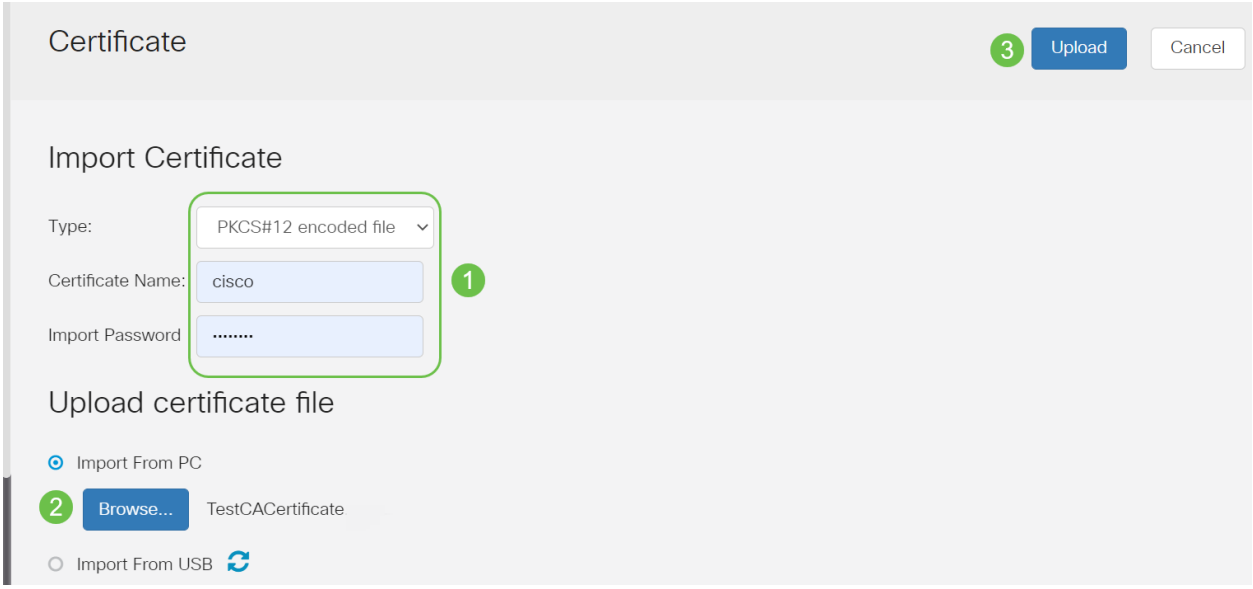


步驟2

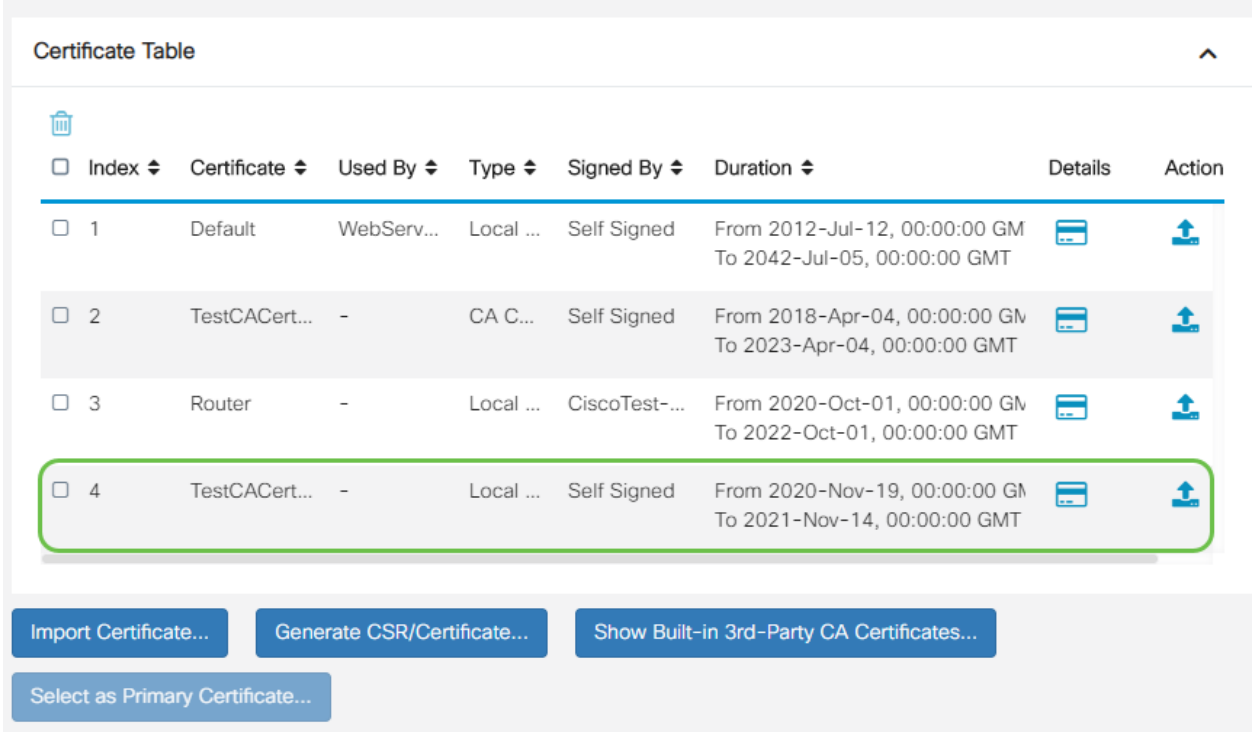
- 從下拉選單中選擇要匯入的證書型別。選項包括：
  - 本地證書 — 路由器上生成的證書。
  - CA證書 — 由受信任的第三方頒發機構認證的證書，該第三方頒發機構已確認證書中包含的資訊是準確的。
  - PKCS #12 Encoded file — 公鑰加密標準(PKCS)#12是儲存伺服器憑證的格式。
- 在Certificate Name欄位中輸入證書的名稱。

- 如果選#12了PKCS，請在Import Password欄位中輸入該檔案的密碼。否則，請跳至步驟3。
- 按一下某個源以匯入證書。選項包括：
    - 從PC匯入
    - 從USB匯入

- 如果路由器未檢測到USB驅動器，則「從USB匯入」選項將呈灰色顯示。
- 如果您選擇「從USB匯入」，並且路由器無法識別您的USB，請按一下「刷新」。
- 按一下「選擇檔案」按鈕並選擇適當的檔案。
- 按一下「**Upload**」。



成功後，您將自動進入主「證書」頁面。證書表將填充最近匯入的證書。



現在，您應該已經成功地在RV345P路由器上匯入了證書。

使用轉換器和RV345P系列路由器配置行動網路（可選）

您可能希望使用加密狗和RV345P路由器配置備份行動網路。如果是這種情況，您應該閱讀使用轉換器和RV34x系列路由器配置行動網路。

祝賀您，您已完成了RV345P路由器的配置！您現在將配置您的思科企業無線裝置。

配置CBW140AC

CBW140AC開箱即用

首先將乙太網電纜從CBW140AC上的PoE埠插入RV345P上的PoE埠。RV345P上的前4個埠可以提供PoE，因此可以使用其中任何一個埠。

檢查指示燈的狀態。該接入點將需要大約10分鐘的啟動時間。LED將以多個模式閃爍綠燈，在再次變為綠色之前，會快速交替顯示綠色、紅色和琥珀色。LED的顏色強度和色調在單位之間可能有小的變化。當LED指示燈呈綠色閃爍時，請繼續執行下一步。

主AP上的PoE乙太網上行鏈路埠只能用於提供到LAN的上行鏈路，而不能連線到任何其他支援主或網狀擴展器裝置。

如果您的接入點不是新的、開箱即用的，請確保將其重置為出廠預設設定，以使*Cisco Business-Setup* SSID顯示在您的Wi-Fi選項中。如需相關協助，請檢視How to Reboot and Reset to Factory Default Settings on RV345x Routers。

在Web UI上設定140AC主無線接入點

您可以使用移動應用程式或Web UI設定接入點。本文使用Web UI進行設定，提供了更多配置選項，但稍微複雜一些。如果您想在下一節中使用移動應用程式，請按一下訪問移動應用程式說明。

如果在連線時出現問題，請參閱本文的無線故障排除提示部分。

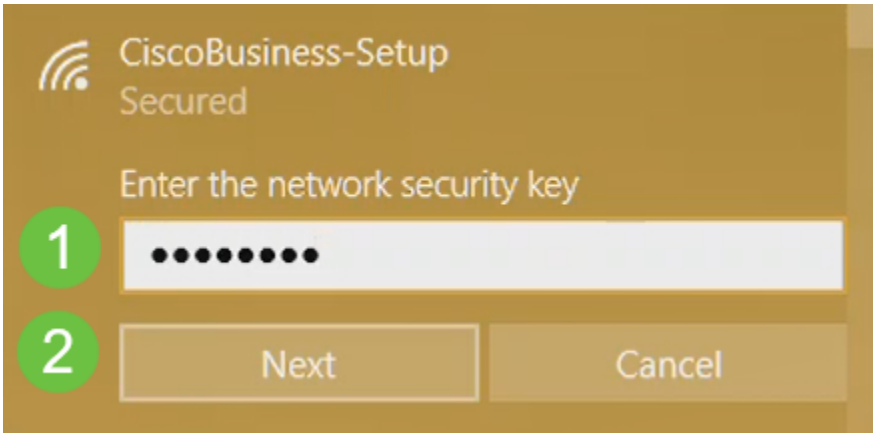
步驟1

在您的PC上，按一下**Wi-Fi**圖示並選擇*CiscoBusiness-Setup*無線網路。按一下連線。

如果您的接入點不是新的、開箱即用的，請確保將其重置為出廠預設設定，以使*Cisco Business-Setup* SSID顯示在您的Wi-Fi選項中。

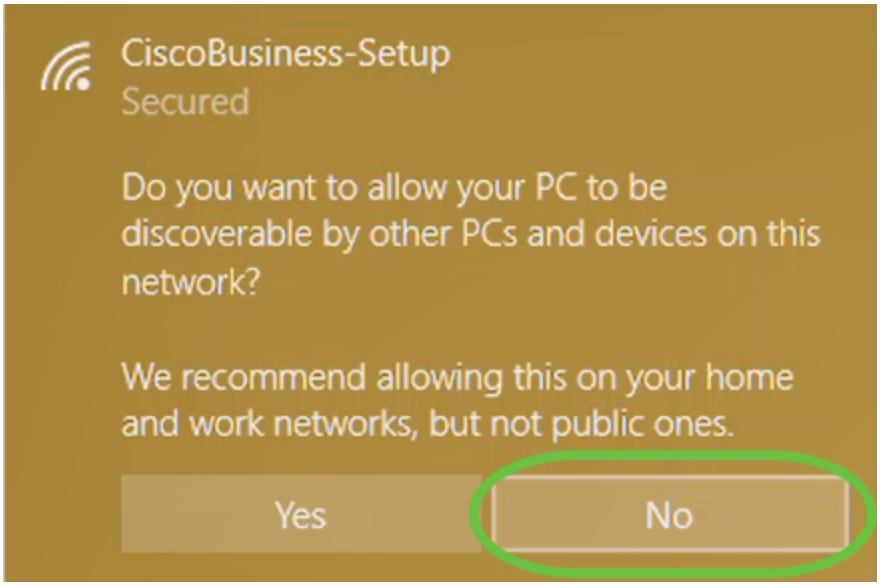
步驟2

輸入密碼短語**cisco123**，然後按一下**Next**。



步驟3

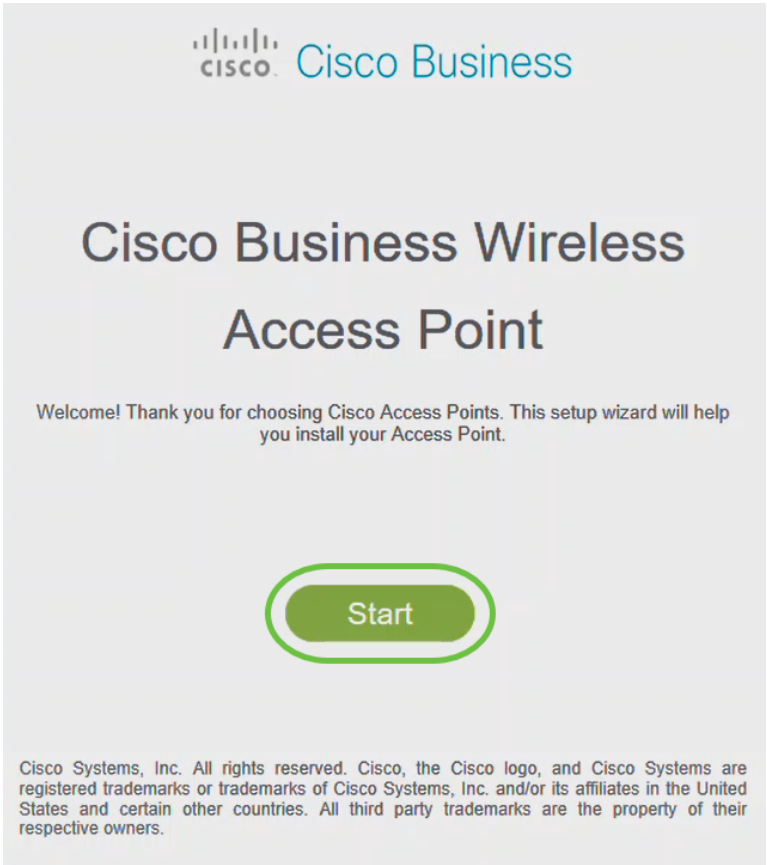
您將看到以下螢幕。由於您一次只能配置一台裝置，請按一下**No**。



只能將一個裝置連線到*CiscoBusiness-Setup* SSID。如果有第二台裝置嘗試連線，它將無法連線。如果您無法連線到SSID並已驗證密碼，則可能是其他裝置建立了連線。重新啟動AP並重試。

步驟4

連線後，Web瀏覽器應自動重定向至CBW AP安裝嚮導。否則，請開啟Web瀏覽器，如Internet Explorer、Firefox、Chrome或Safari。在位址列中，鍵入**http://ciscobusiness.cisco**，然後按**Enter**。在網頁上按一下**Start**。



如果您沒有看到該網頁，請等待幾分鐘，或者重新載入該頁面。完成此初始設定後，您將使

用https://ciscobusiness.cisco登入。如果您的Web瀏覽器使用 *http://*自動填充，則需手動輸入 *https://*來獲取訪問許可權。

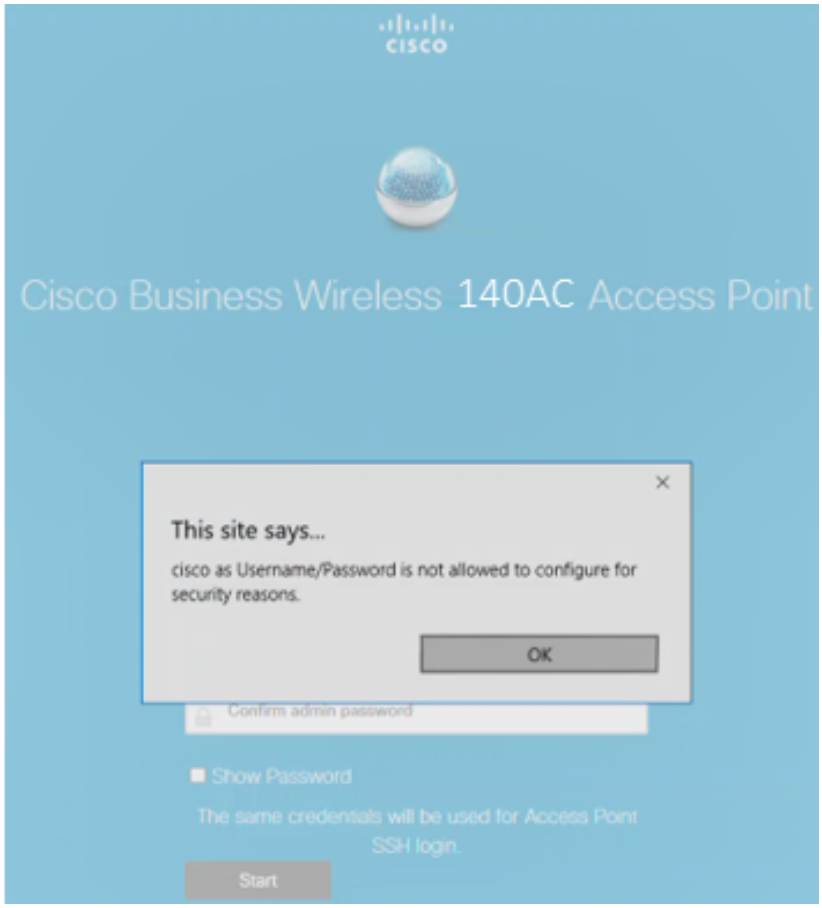
步驟5

通過輸入*以下內容*建立管理員帳戶：

- 管理員使用者名稱（最多24個字元）
- 管理員密碼
- 確認管理員密碼

您可以通過選中*顯示密碼*旁邊的覈取方塊來選擇顯示密碼。按一下「**Start**」。

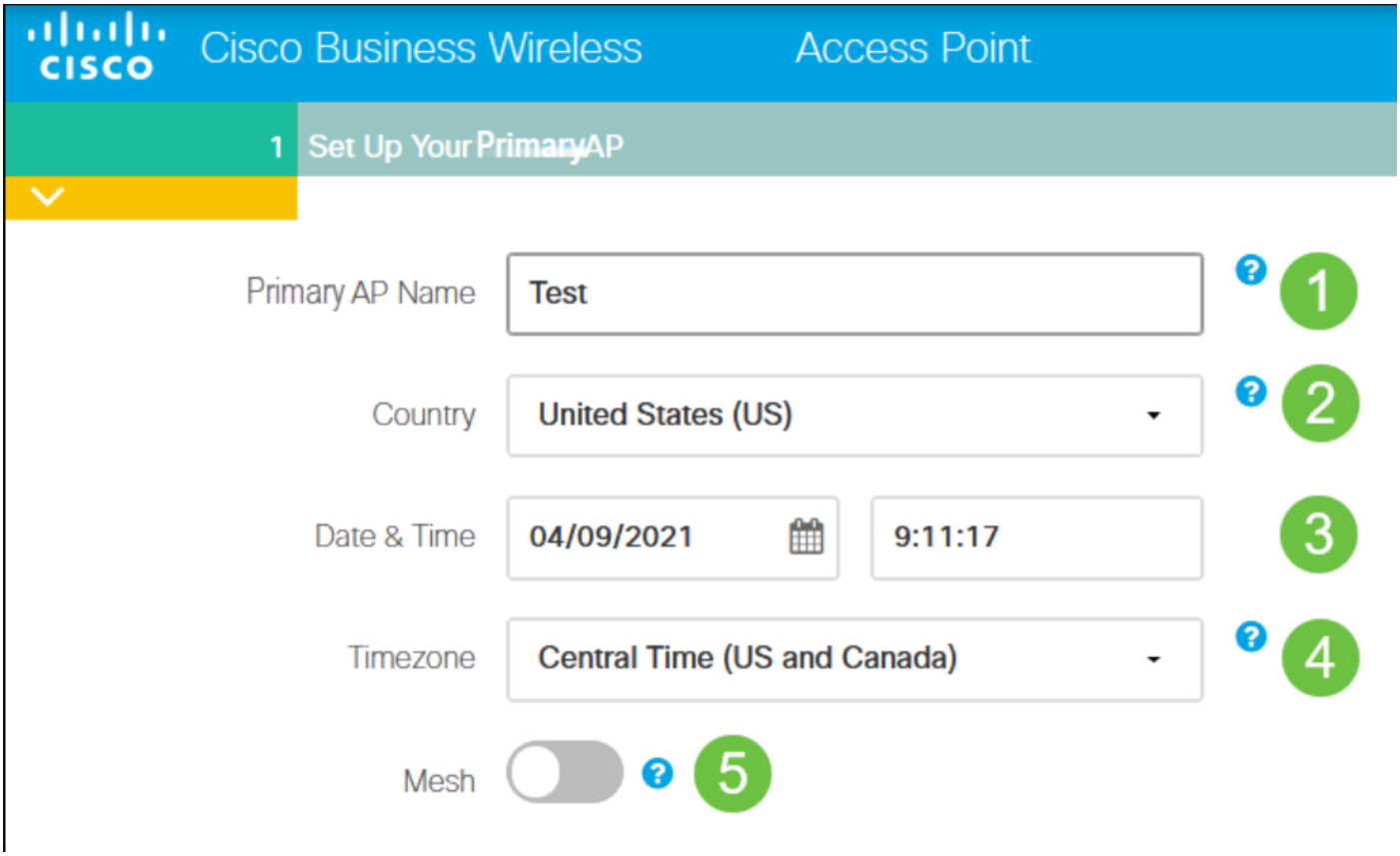
請勿在使用者名稱或密碼欄位中使用*cisco*或其變體。如果這樣做，您將收到如下所示的錯誤消息。



步驟6

*通過輸入以下內容*來設定主AP:

- 主AP名稱
- 國家/地區
- 日期和時間
- 時區
- 網狀



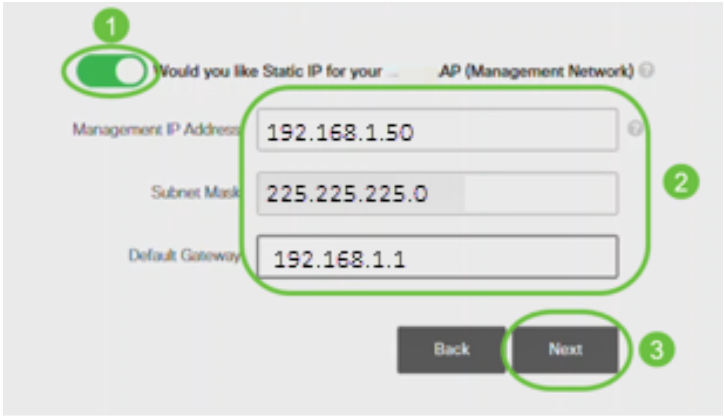
*只有*在計畫建立網狀網路時，才應啟用網格。預設情況下，該選項處於禁用狀態。

第7步

（可選）您可以為CBW140*AC啟用靜*態IP以用於管理目的。否則，該介面將從DHCP伺服器獲取IP地址。要配置靜態IP，請輸入以下內容：

- 管理IP地址
- 子網路遮罩
- 預設閘道

按「Next」（下一步）。



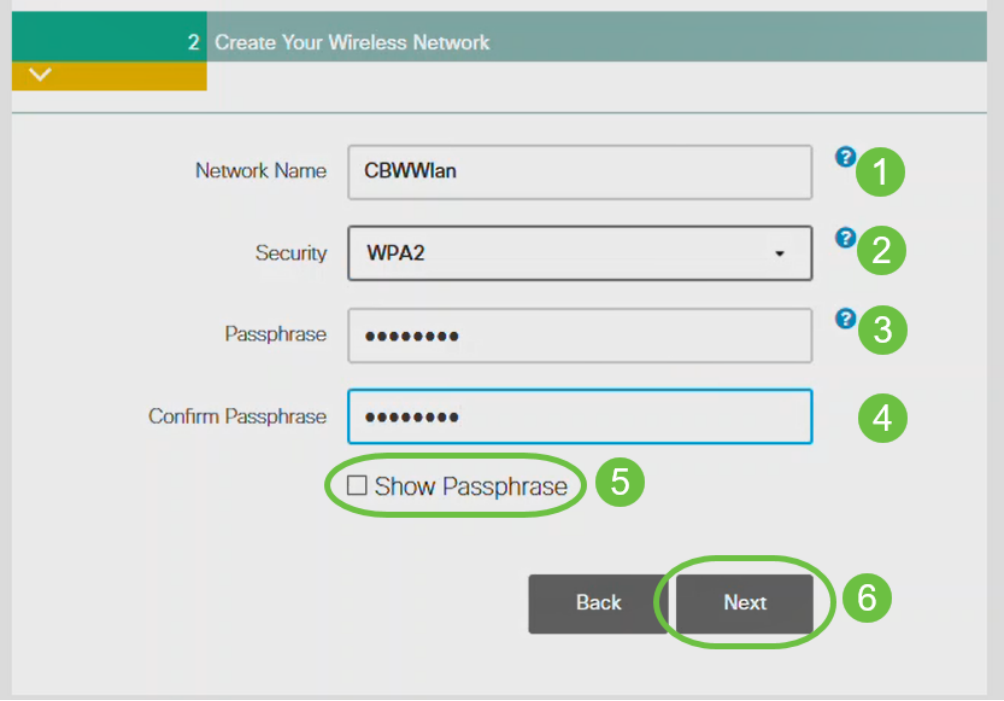
預設情況下，此選項處於禁用狀態。

步驟8

通過輸入以下內容建立您的無線網路：

- 網路名稱
- 選擇安全性
- 密碼短語
- 確認密碼短語
- （可選）勾選覈取方塊以顯示密碼短語。

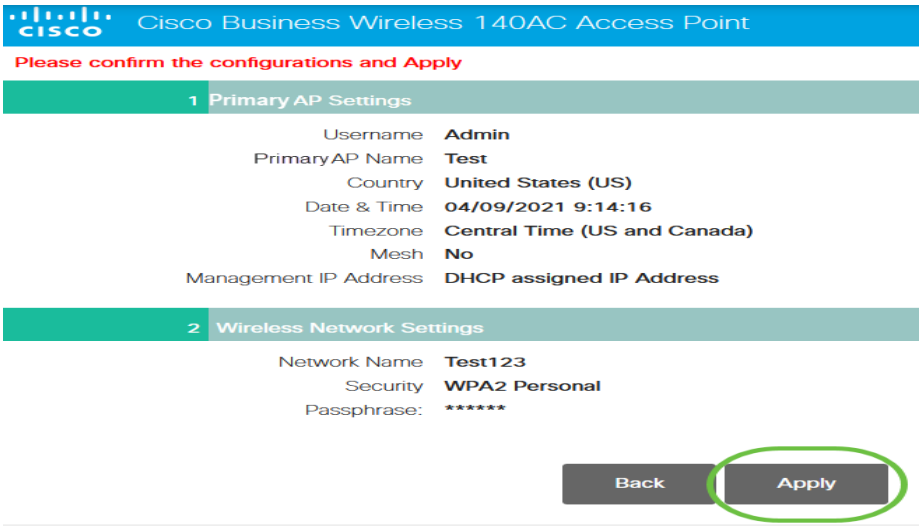
按「Next」（下一步）。



Wi-Fi保護訪問(WPA)第2版(WPA2)是Wi-Fi安全的當前標準。

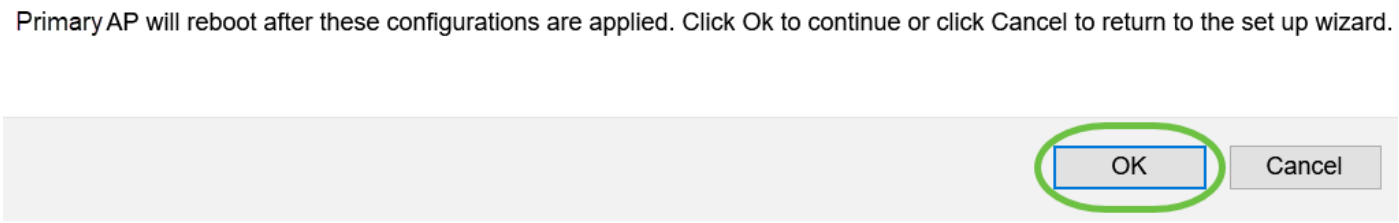
步驟9

確認設定並按一下**Apply**。

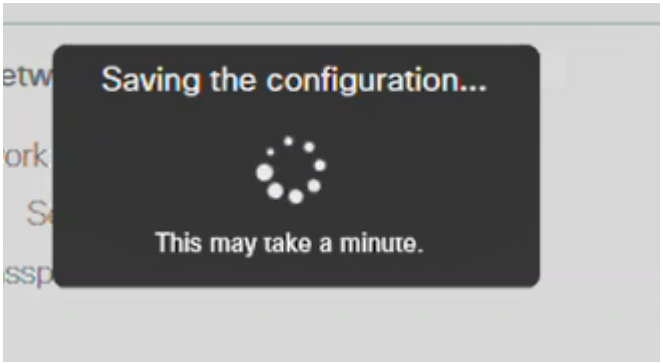


步驟10

按一下「**OK**」以應用設定。



儲存配置並重新啟動系統時，您將看到以下螢幕。這可能需要10分鐘。

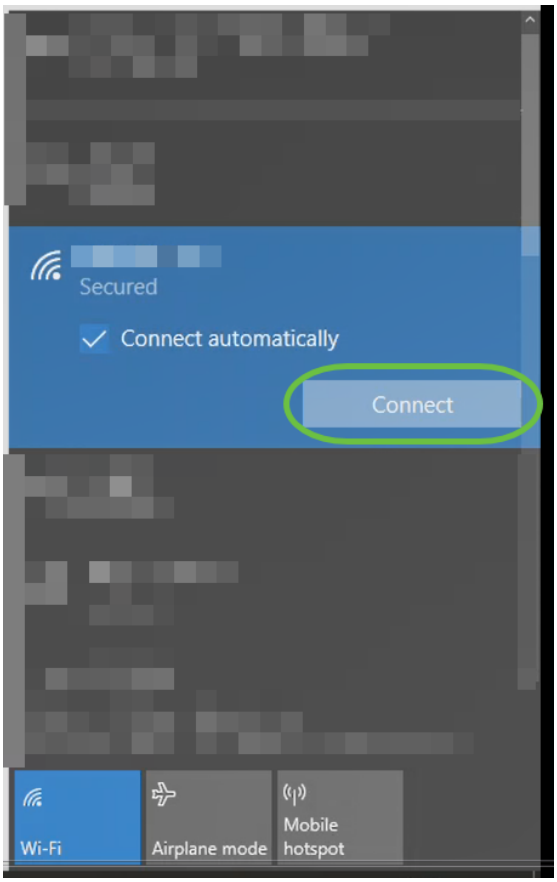


在重新引導期間，接入點中的LED將經歷多種顏色模式。當LED呈綠色閃爍時，繼續下一步。如果LED沒有通過紅色閃爍模式，則表示您的網路中沒有DHCP伺服器。確保AP連線到交換機或具有DHCP伺服器的路由器。

步驟11

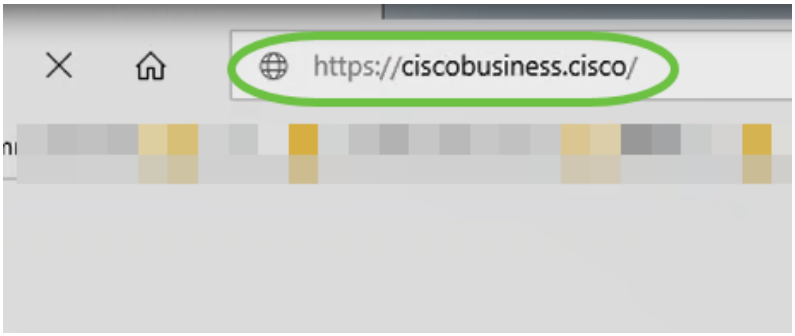
轉到PC上的無線選項，並選擇您配置的網路。按一下「**Connect**」。

CiscoBusiness-Setup SSID將在重新啟動後消失。



步驟12

開啟Web瀏覽器並鍵入*https:///[CBW AP的IP地址]*。或者，您也可以在位址列中鍵入*https://ciscobusiness.cisco*，然後按Enter鍵。



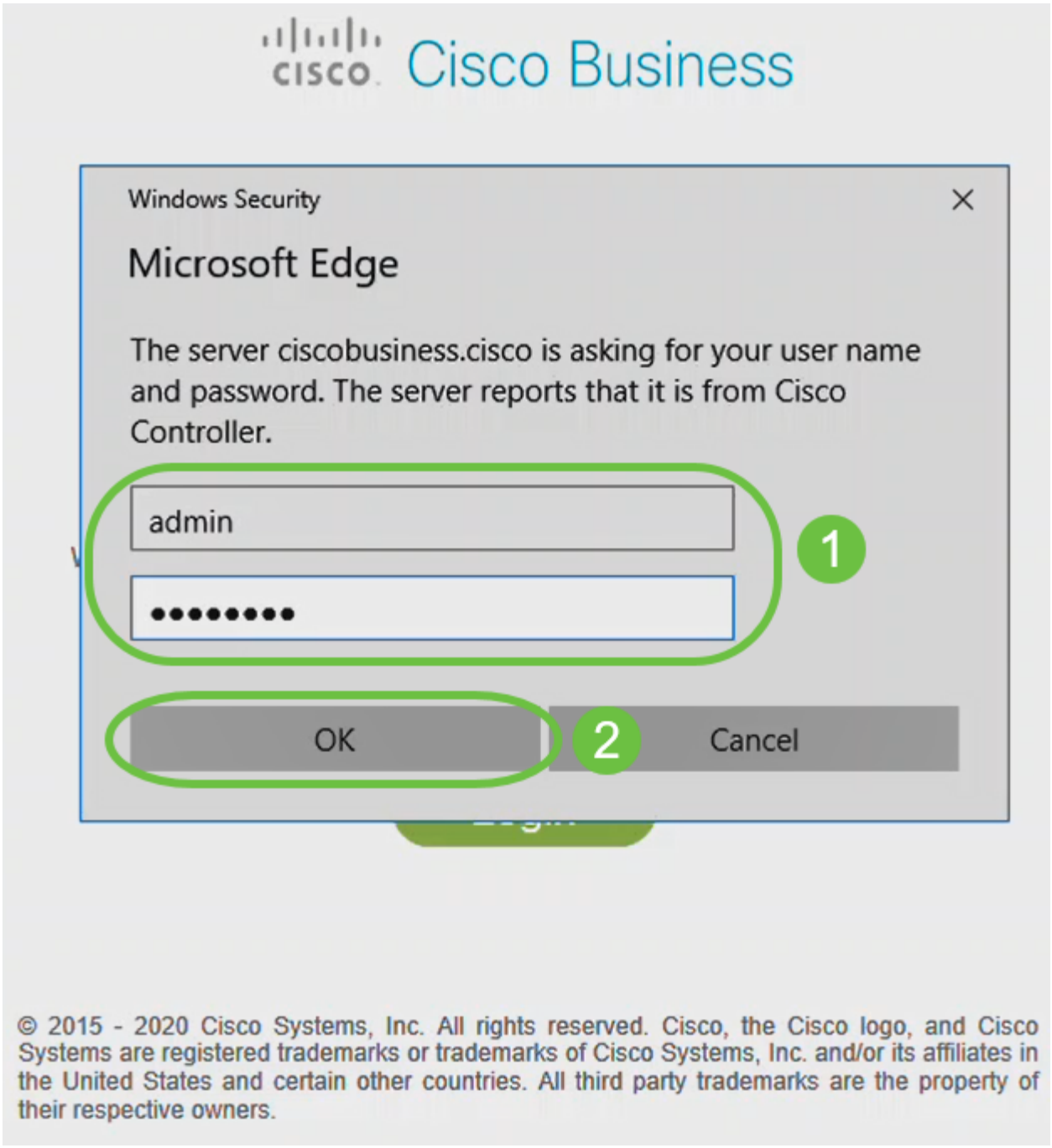
請確保在此步驟中輸入 *https*而不是 *http*。

步驟13

按一下「**Login**」。

步驟14

使用已配置的憑據登入。按一下「OK」（確定）。



步驟15

您將能夠訪問AP的Web UI頁面。

無線故障排除提示

如果您有任何問題，請檢視以下提示：

- 確保選擇了正確的服務集識別符號(SSID)。這是您為無線網路建立的名稱。
- 斷開移動應用或筆記型電腦上的任何VPN。您甚至可能連線到您的移動服務提供商使用的、您甚至可能不知道的VPN。例如，Android(Pixel 3)手機使用Google Fi作為服務提供商，它有一個內建VPN，無需通知即可自動連線。要查詢主AP，需要禁用此選項。
- 使用https://<主AP的IP地址>登入到主AP。
- 進行初始設定後，無論您是登入*ciscobusiness.cisco*，還是在Web瀏覽器中輸入IP地址，請確保使用https:// is。根據您的設定，您的電腦可能已自動填充了http:// since，這是您首次登入時所用的名稱。
- 要幫助解決在使用AP期間與訪問Web UI或瀏覽器問題相關的問題，請在Web瀏覽器（本例中為Firefox）中按一下「Open（開啟）」選單，轉到「Help（幫助）」>「Troubleshooting Information（故障排除資訊）」，然後按一下「Refresh Firefox（刷新Firefox）」。

使用Web UI配置CBW142ACM網狀擴展器

您處於設定此網路的基本階段，只需新增網狀擴展器即可！

步驟1

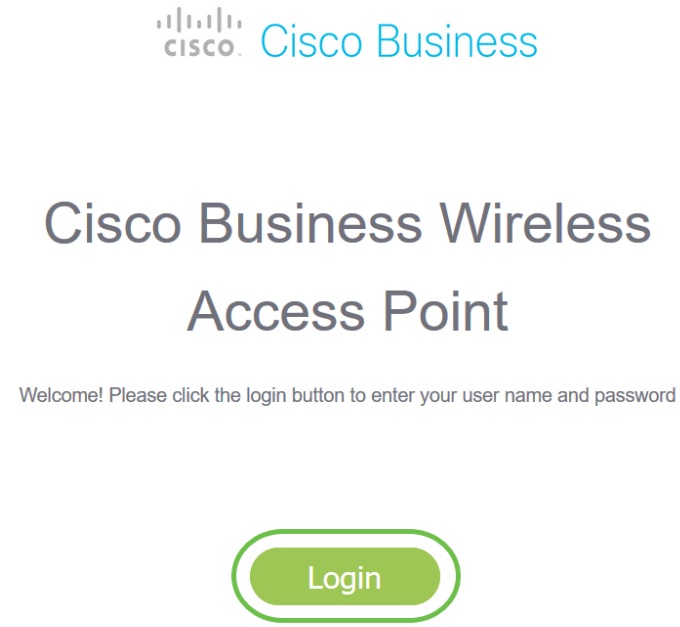
將兩個網格延伸器插入到所選位置的牆中。記下每個網狀擴展器的MAC地址。

步驟2

等待大約10分鐘，以便網狀擴展器啟動。

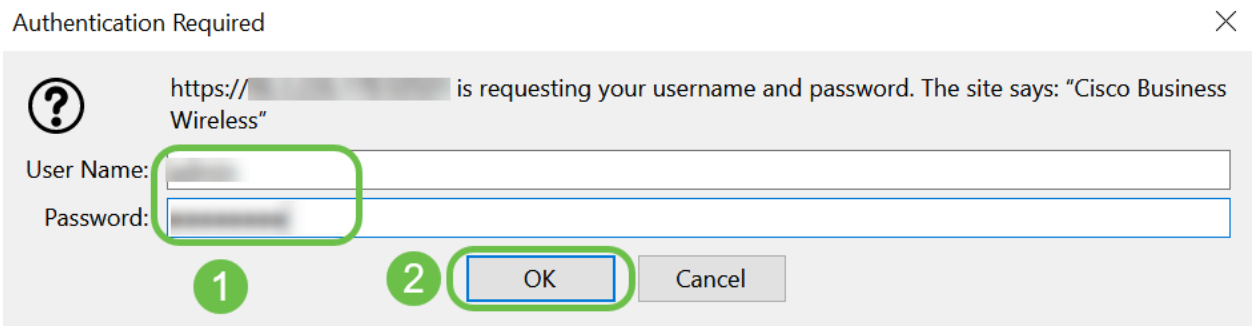
步驟3

在Web瀏覽器中輸入主要接入點(AP)IP地址。按一下**Login**以訪問主AP。



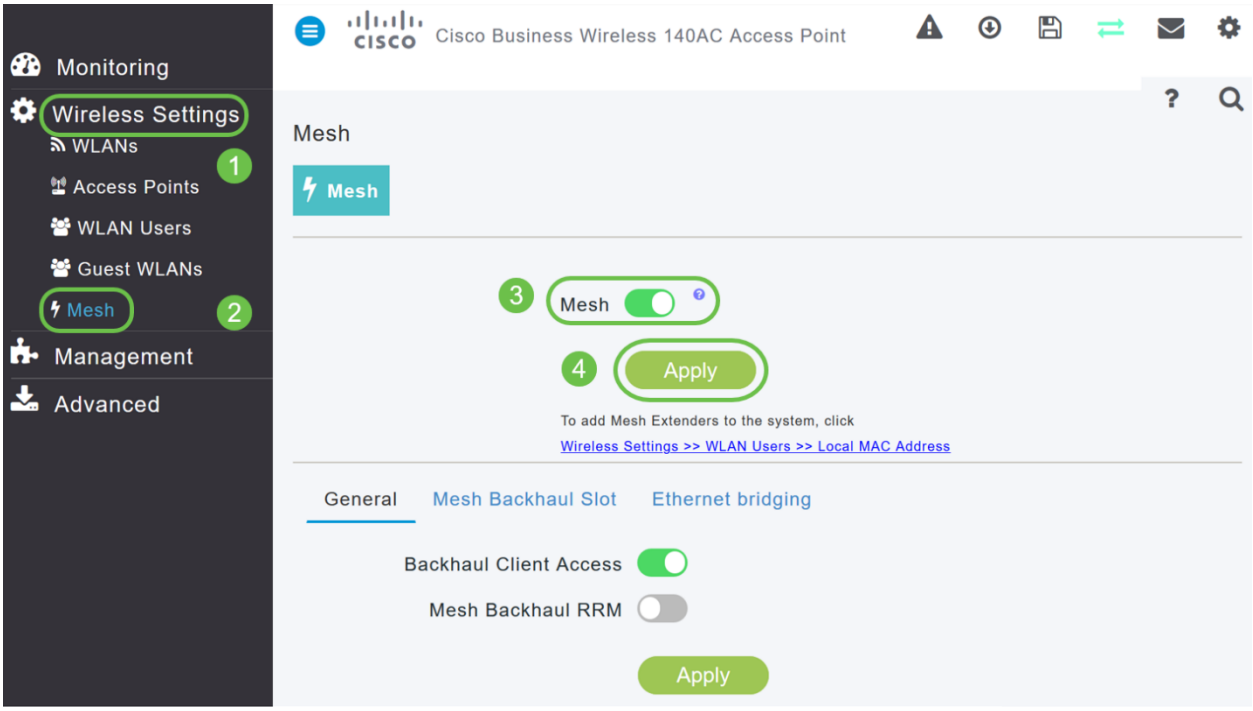
步驟4

輸入您的*使用者名稱*和*密碼*憑據以訪問主AP。按一下「OK」（確定）。



步驟5

導覽至**Wireless Settings > Mesh**。確保*Mesh*已啟用。按一下「Apply」。

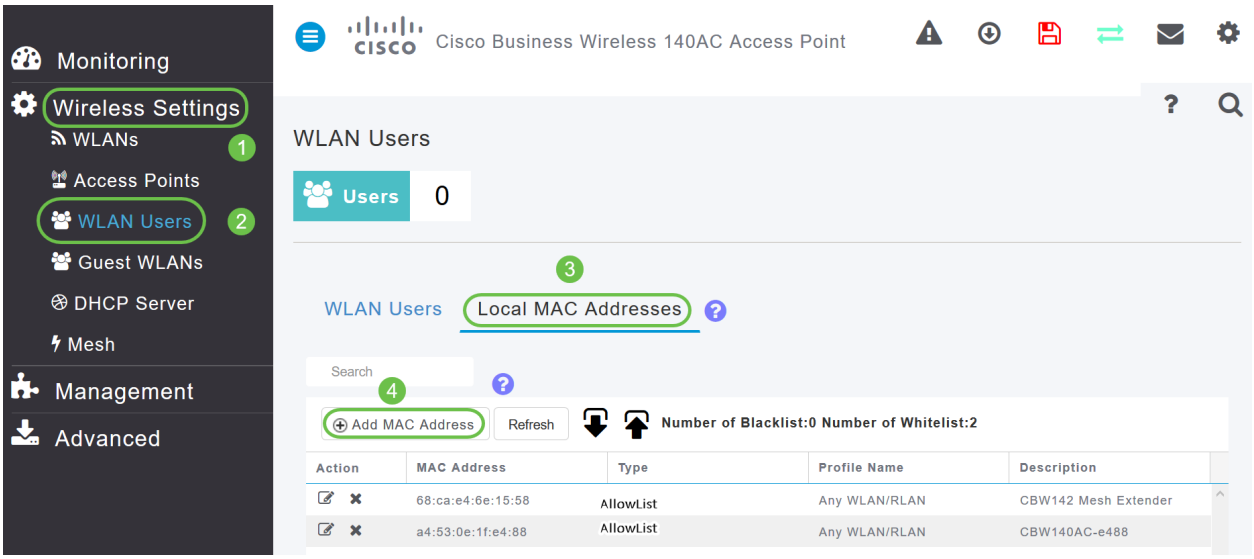


步驟6

如果Mesh尚未啟用，WAP可能需要重新引導。系統將顯示一個彈出視窗，用於重新引導。確認。這大約需要10分鐘。在重新啟動期間，LED會以多種模式閃爍綠燈，在再次變為綠色之前，會快速切換為綠色、紅色和琥珀色。LED的顏色強度和色調在單位之間可能有小的變化。

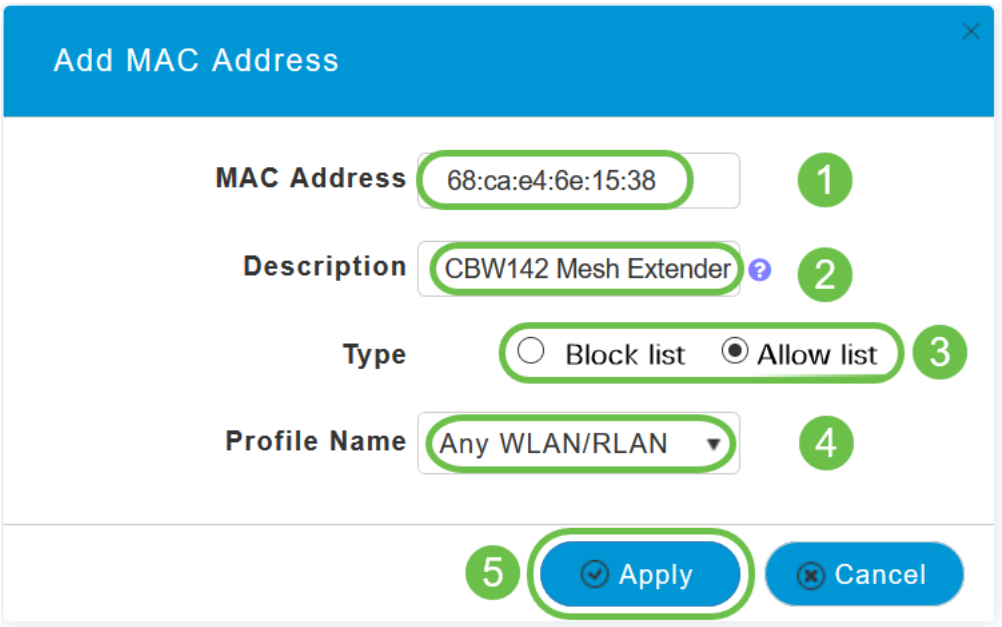
第7步

導覽至**Wireless Settings > WLAN Users > Local MAC Addresses**。按一下「**Add MAC Address**」。



步驟8

輸入網狀擴展器的MAC地址和說明。選擇*Type* as Allow清單。從下拉選單中選擇*Profile Name*。按一下「Apply」。



步驟9

按螢幕右上窗格中的**save icon**，確保儲存所有配置。

對每個網狀擴展器重複上述步驟。

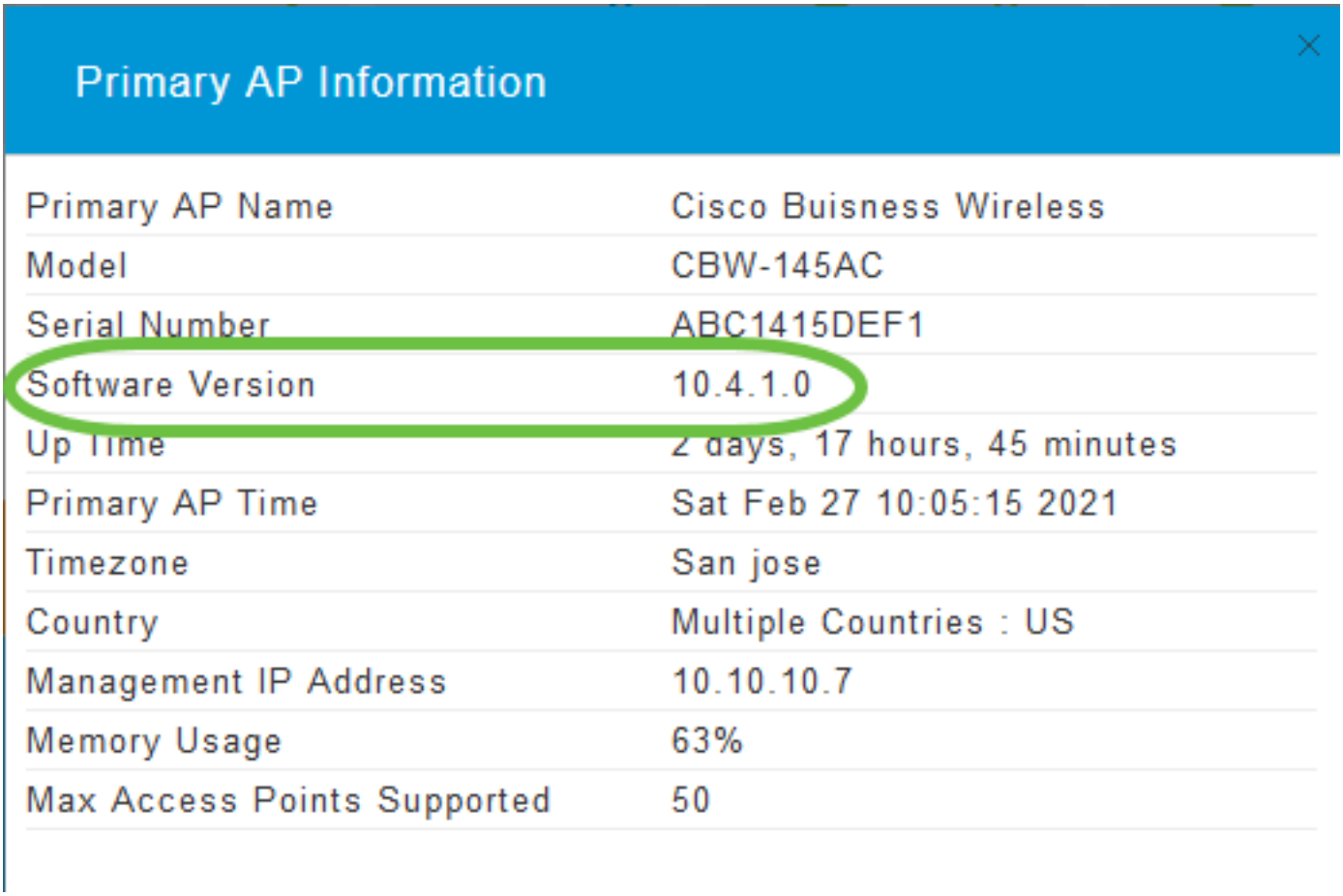
使用Web UI檢查和更新軟體

不要跳過這一重要步驟！更新軟體的方法有很多，但建議您在使用Web UI時最輕鬆執行下面列出的步驟。

要檢視和更新主AP的當前軟體版本，請執行以下步驟。

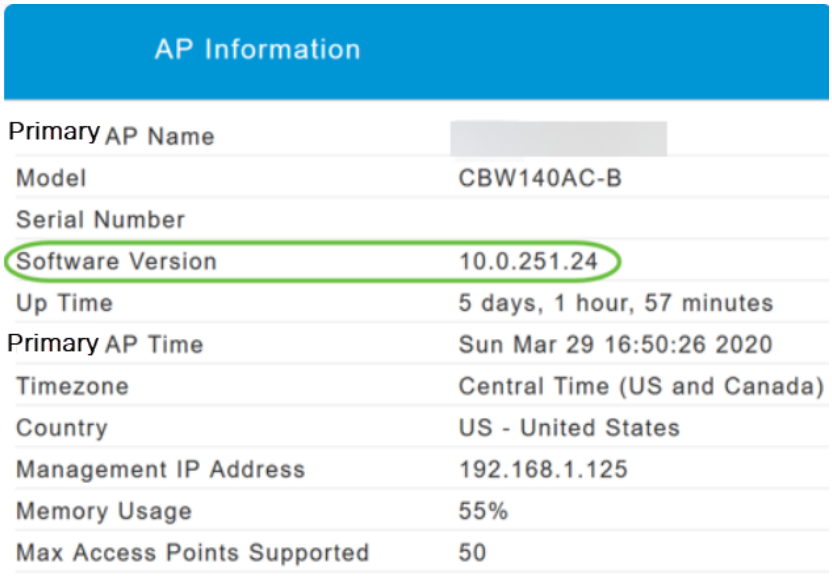
步驟1

按一下Web介面右上角的**gear**圖示，然後按一下**Primary AP Information**。



步驟2

比較運行的版本與最新的軟體版本。如果您知道是否需要更新軟體，請關閉該視窗。

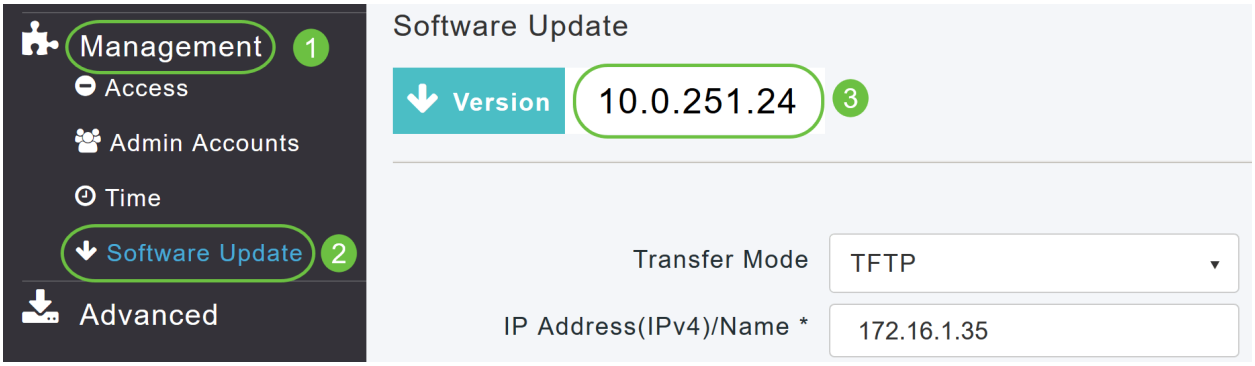


如果您運行的是最新版本的軟體，則可以跳至建立WLANs部分。

步驟3

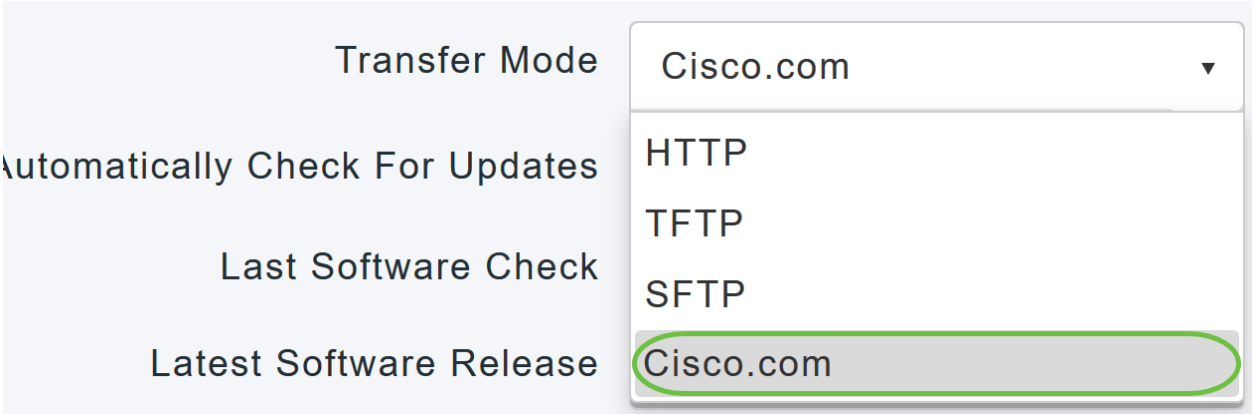
從選單中選擇**管理>軟體更新**。

將顯示「*Software Update*」視窗，其中當前軟體版本號列在頂部。



您可以更新CBW AP軟體，並且不會刪除主AP上的當前配置。

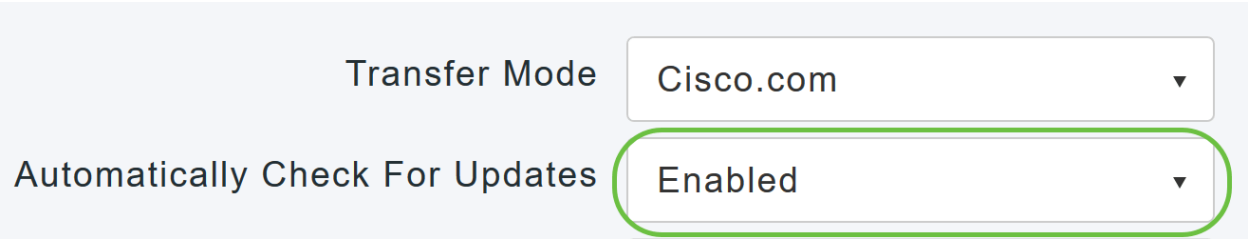
在「*Transfer Mode*」下拉式清單中選擇「**Cisco.com**」。



步驟4

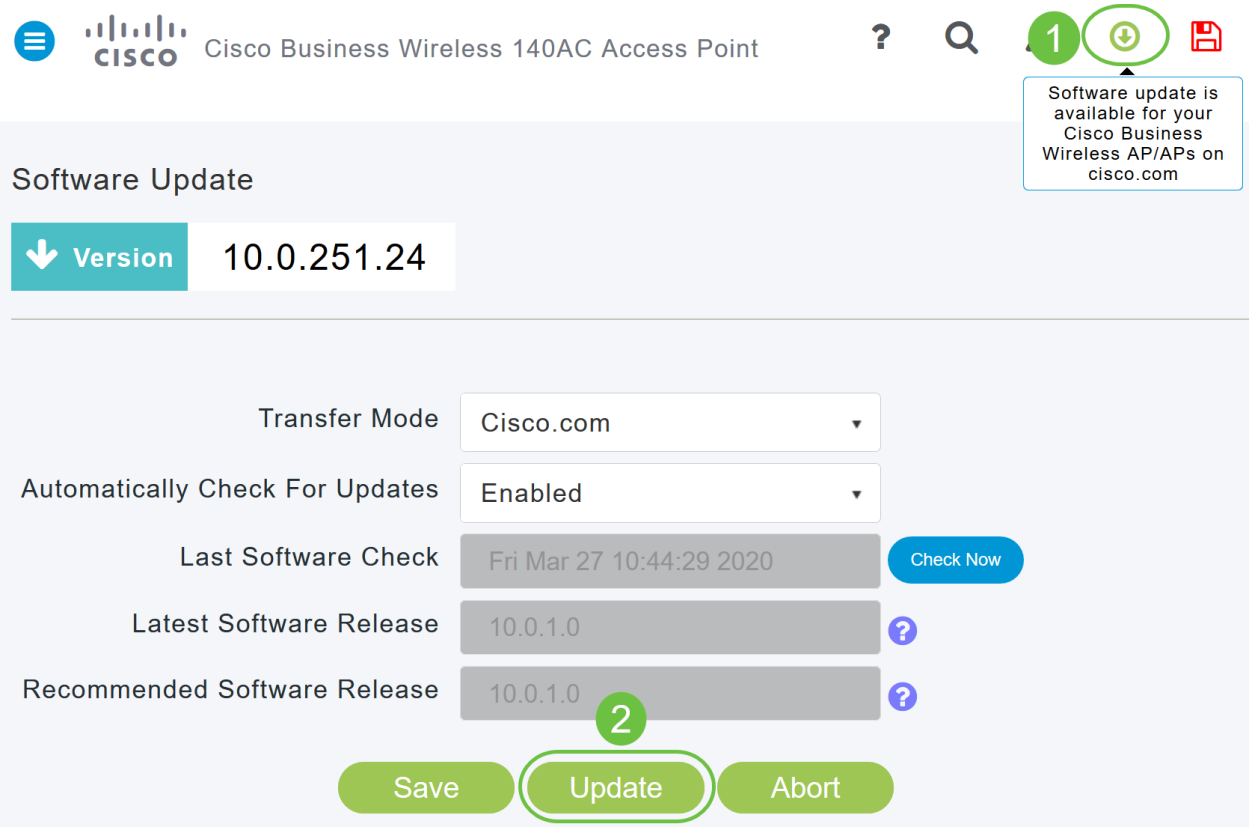
要將主AP設定為自動檢查軟體更新，請在*自動檢查更新*下拉選單中選擇**Enabled**。預設

情況下啟用。



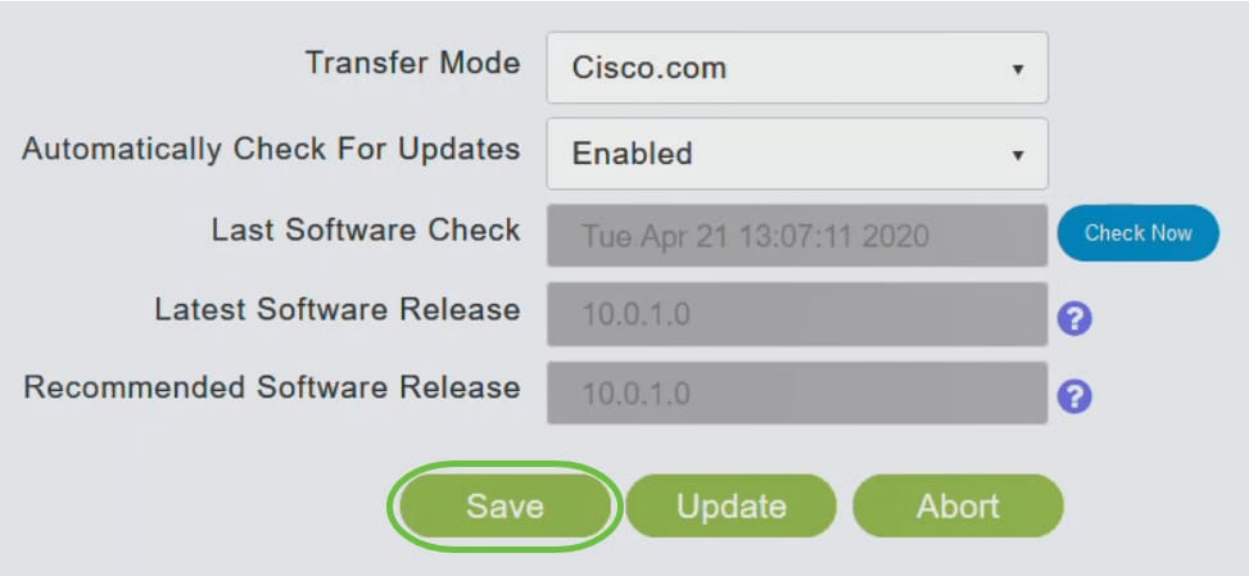
完成軟體檢查後，如果Cisco.com上提供了更新的最新或推薦的軟體更新，則：

- Web UI右上角的**Software Update Alert**圖示將為綠色（或灰色）。 按一下該圖示將進入軟體更新頁面。
- *Software Update*頁面底部的Update按鈕已啟用。

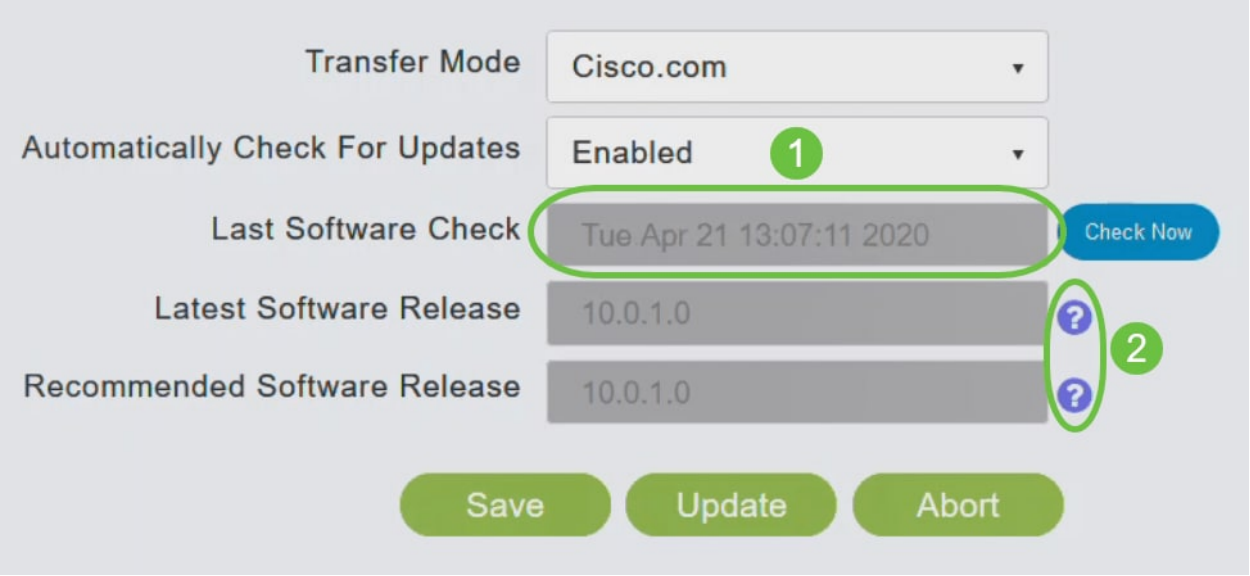


步驟5

按一下「**Save**」。這會儲存在*傳輸模式*和*自動檢查更新*中所做的條目或更改。

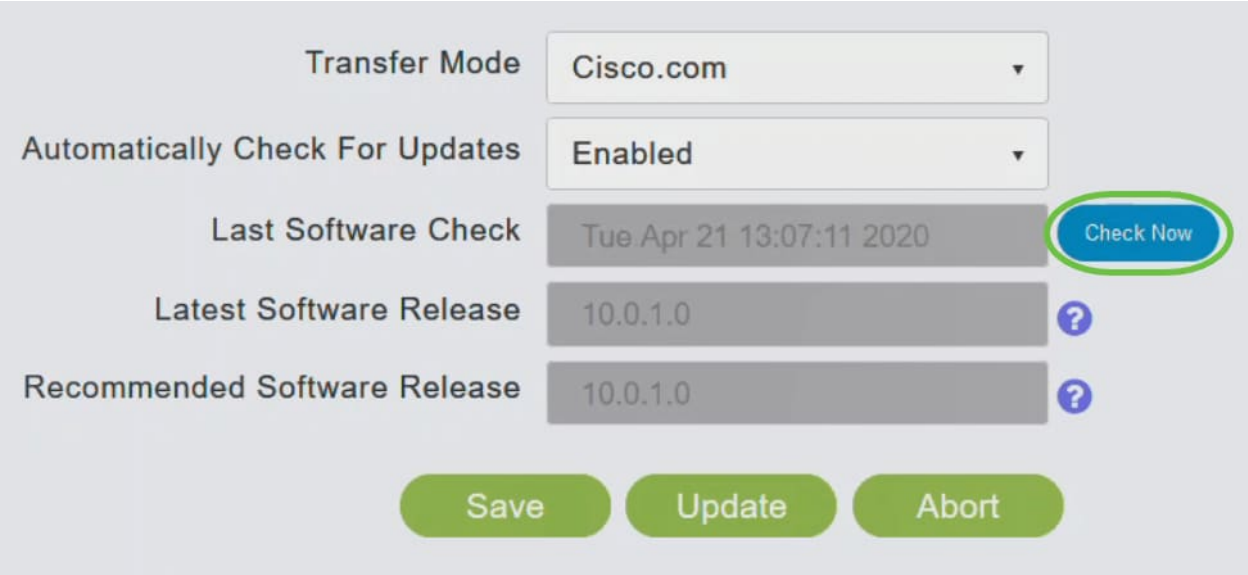


*Last Software Check*欄位顯示上次自動或手動軟體檢查的時間戳。您可以通過按一下其旁邊的問號圖示**來檢視顯**示的版本註釋。



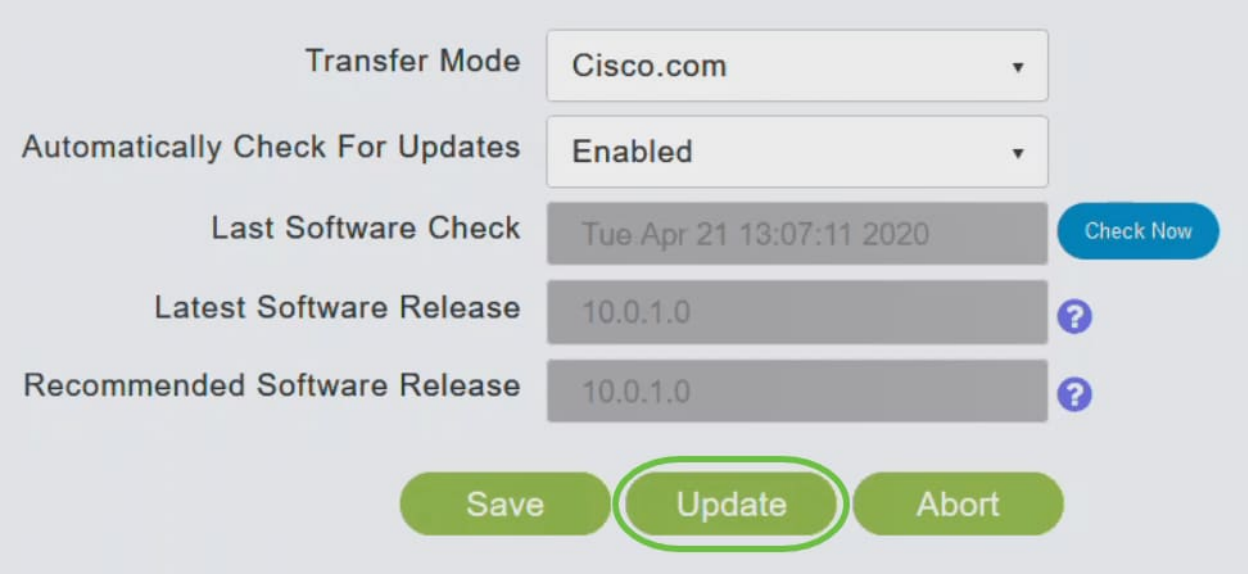
步驟6

您可以隨時按一下*Check Now*手動運行軟體檢查。



第7步

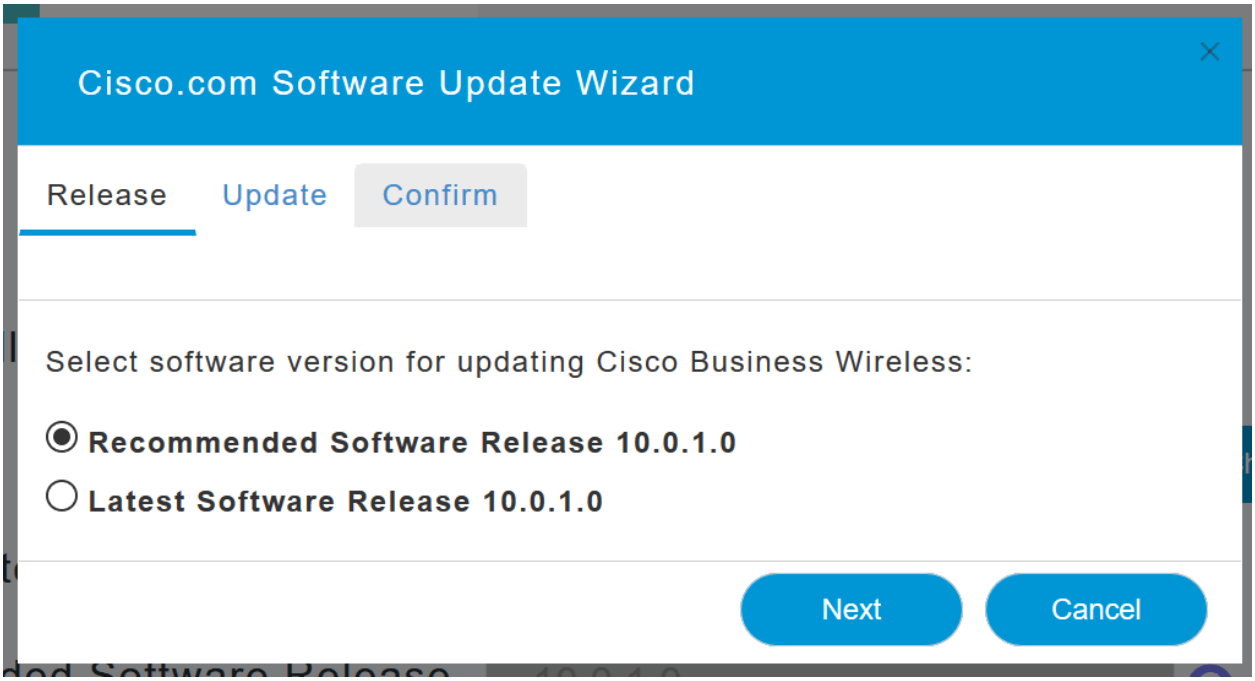
要繼續軟體更新，請按一下**更新**。



出現「*Software Update Wizard*」。該嚮導會按順序引導您完成以下三個頁籤：

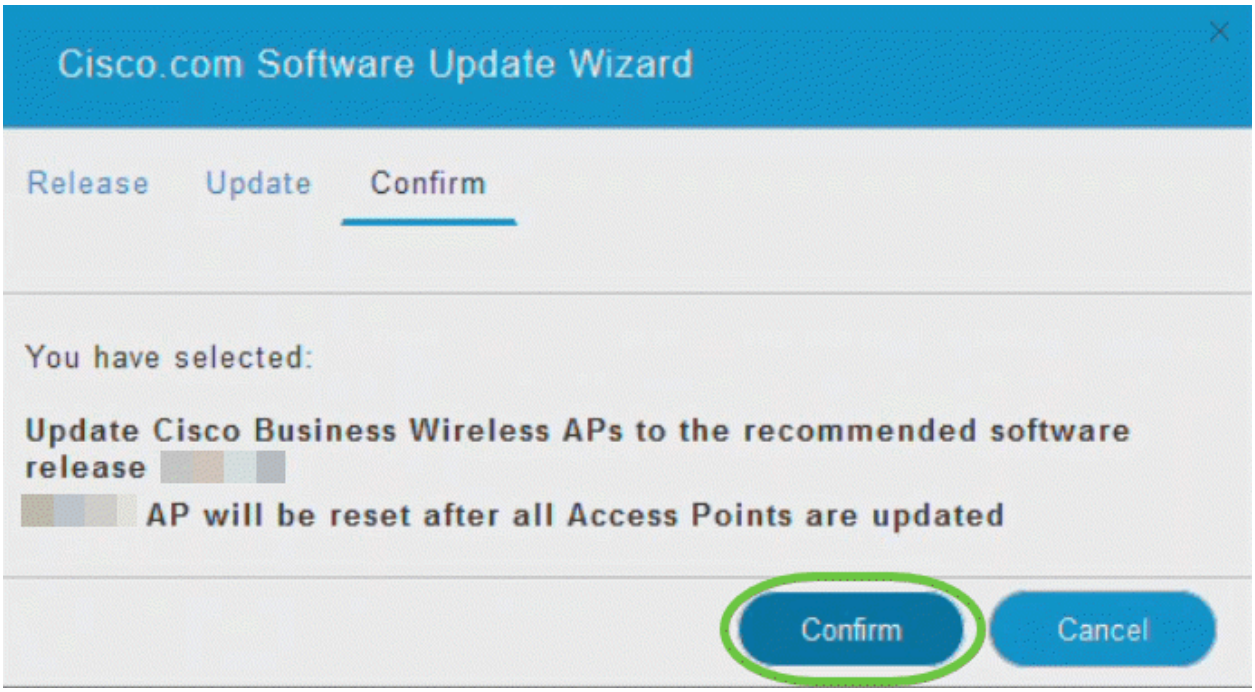
- Release（版本）頁籤 — 指定是要更新到推薦的軟體版本還是最新軟體版本。
- Update頁籤 — 指定應重置AP的時間。您可以選擇立即完成，也可以安排以後完成。要將主AP設定為在映像預下載完成後自動重新啟動，請選中Auto Restart覈取方塊。
- 確認頁籤 — 確認您的選擇。

按照嚮導中的說明操作。在按一下*Confirm*之前，您可以隨時返回到任何頁籤。



步驟8

按一下「**Confirm**」。

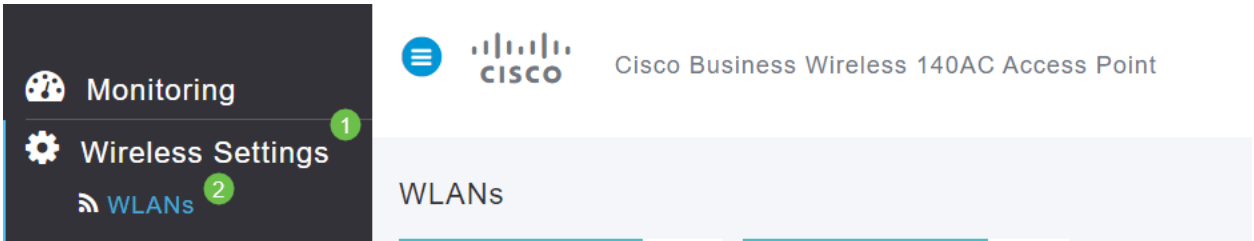


在Web UI上建立WLAN

本節允許您建立無線區域網路(WLAN)。

步驟1

導覽至**Wireless Settings > WLANs**可建立WLAN。然後選擇**Add new WLAN/RLAN**。



步驟2

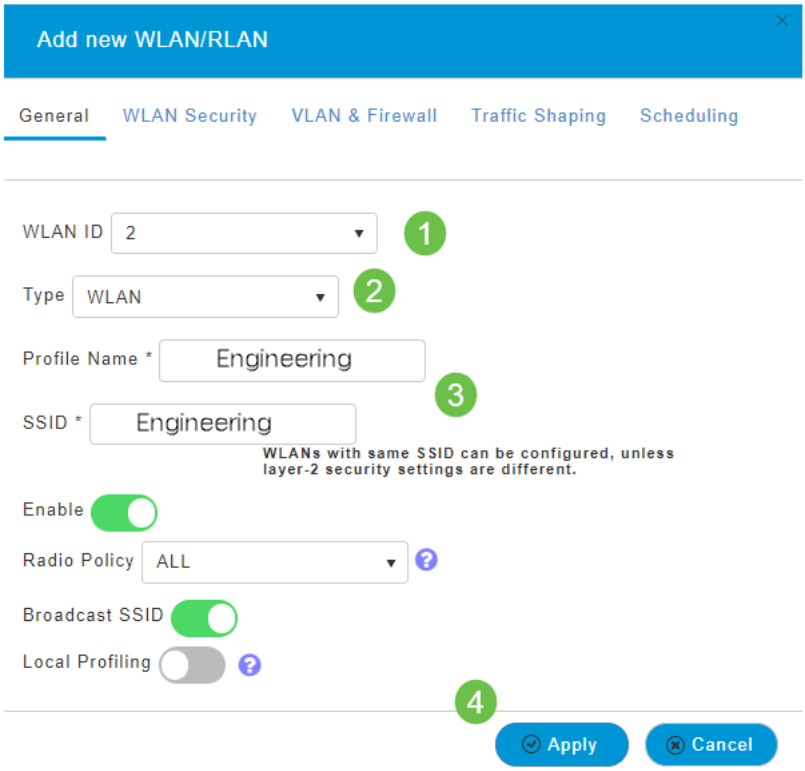
在*General*索引標籤下，輸入以下資訊：

- WLAN ID — 為WLAN選擇一個數字
- 型別 — 選擇**WLAN**
- Profile Name — 輸入名稱后，SSID將自動填充相同的名稱。名稱必須唯一，且不能超過31個字元。

在此示例中，以下欄位保留為預設值，但會列出解釋，以防您要以不同方式配置它們。

- SSID — 配置檔名稱也用作SSID。如果您願意，可以更改它。名稱必須唯一，且不能超過31個字元。
- Enable — 應保持啟用狀態以使WLAN正常運作。
- Radio Policy（無線電策略） — 通常您想將此選項保留為**All**，以便2.4GHz和5GHz客戶端可以訪問網路。
- 廣播SSID — 通常您希望發現SSID，以便將其保留為啟用。
- Local Profiling — 您只希望啟用此選項以檢視客戶端上運行的作業系統或檢視使用者名稱。

按一下「Apply」。



步驟3

您將進入*WLAN Security*頁籤。

在本示例中，以下選項保留為預設值：

- 訪客網路、強制網路助理和MAC過濾被禁用。有關設定訪客網路的詳細資訊將在下一節

中詳述。
- WPA2 Personal - Wi-Fi Protected Access 2 with Pre-shared Key(PSK)Passphrase Format - ASCII。此選項表示使用預共用金鑰(PSK)的Wi-Fi保護訪問2。

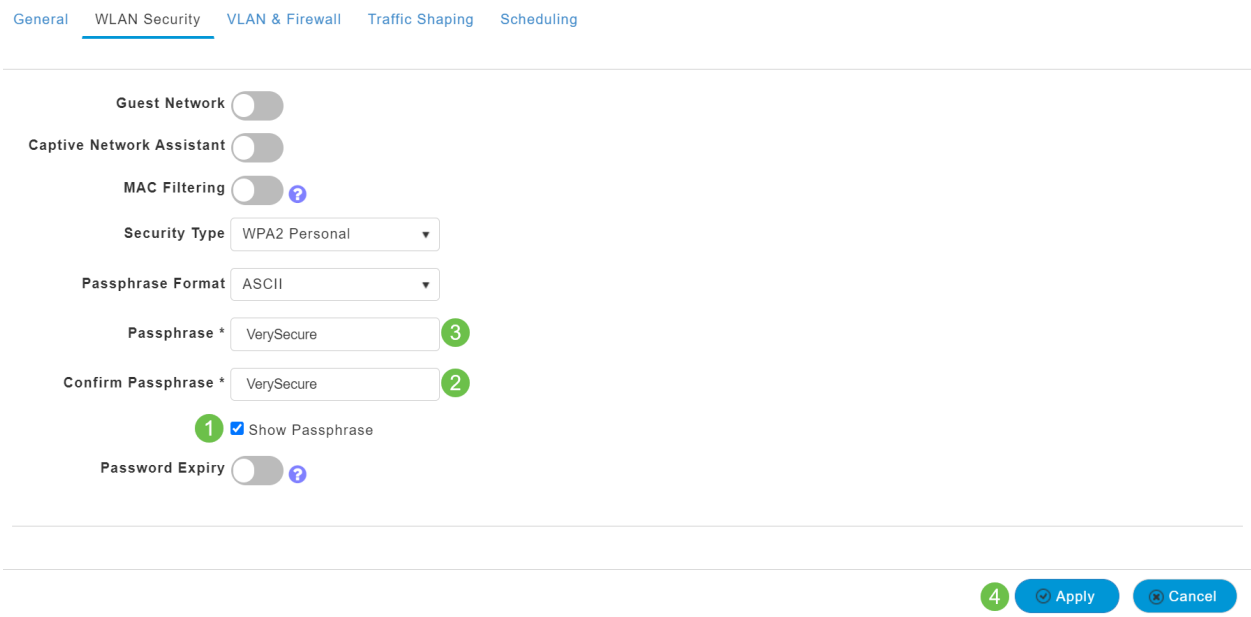
WPA2 Personal是使用PSK身份驗證來保護網路的方法。PSK在主AP、WLAN安全策略下和客戶端上分別配置。WPA2 Personal不依賴於網路上的身份驗證伺服器。

- 密碼格式- **ASCII保留為預設值。**

在此方案中輸入了以下欄位：

- 顯示密碼短語 — 按一下覈取方塊可檢視您輸入的密碼短語。
- 密碼短語 — 輸入密碼短語的名稱（密碼）。
- 確認密碼再次輸入密碼進行確認。

按一下「Apply」。這將自動啟用新的WLAN。

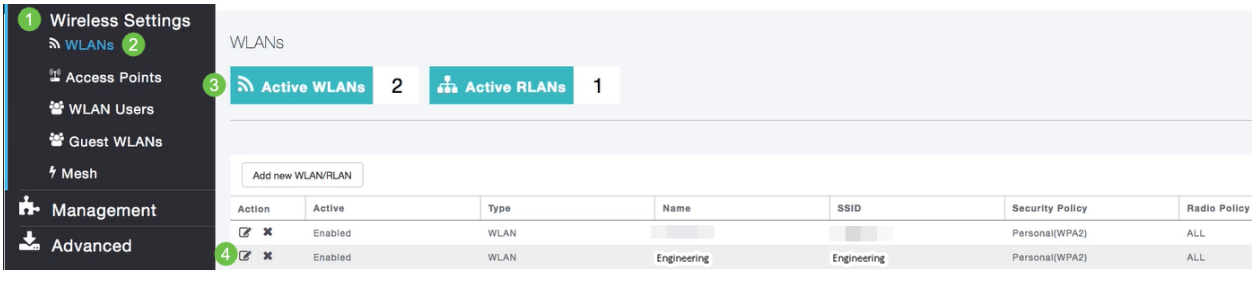


步驟4

請務必按一下Web UI螢幕右上角面板上的**save**圖示來儲存配置。

步驟5

要檢視您建立的WLAN，請選擇**Wireless Settings > WLANs**。您會看到活動WLAN數提高至2，並顯示新的WLAN。



對您要建立的其他WLAN重複這些步驟。

可選無線配置

現在，您已設定所有基本配置，並已準備好進行滾動。您有一些選擇，因此您可以跳轉到以下任何部分：

- 使用Web UI建立訪客WLAN（可選）
- 應用程式分析（可選）
- 客戶端分析（可選）
- 我準備結束此工作並開始使用我的網路！

使用Web UI建立訪客WLAN（可選）

訪客WLAN允許訪客訪問您的思科企業無線網路。

步驟1

登入到主AP的Web UI。開啟Web瀏覽器並輸入www.https://ciscobusiness.cisco。在繼續操作之前，可能會收到警告。輸入您的憑據。您也可以通過輸入主AP的IP地址來訪問它。

步驟2

導覽至**Wireless Settings > WLANs**可建立無線區域網路(WLAN)。然後選擇**Add new WLAN/RLAN**。

步驟3

在*General*索引標籤下，輸入以下資訊：

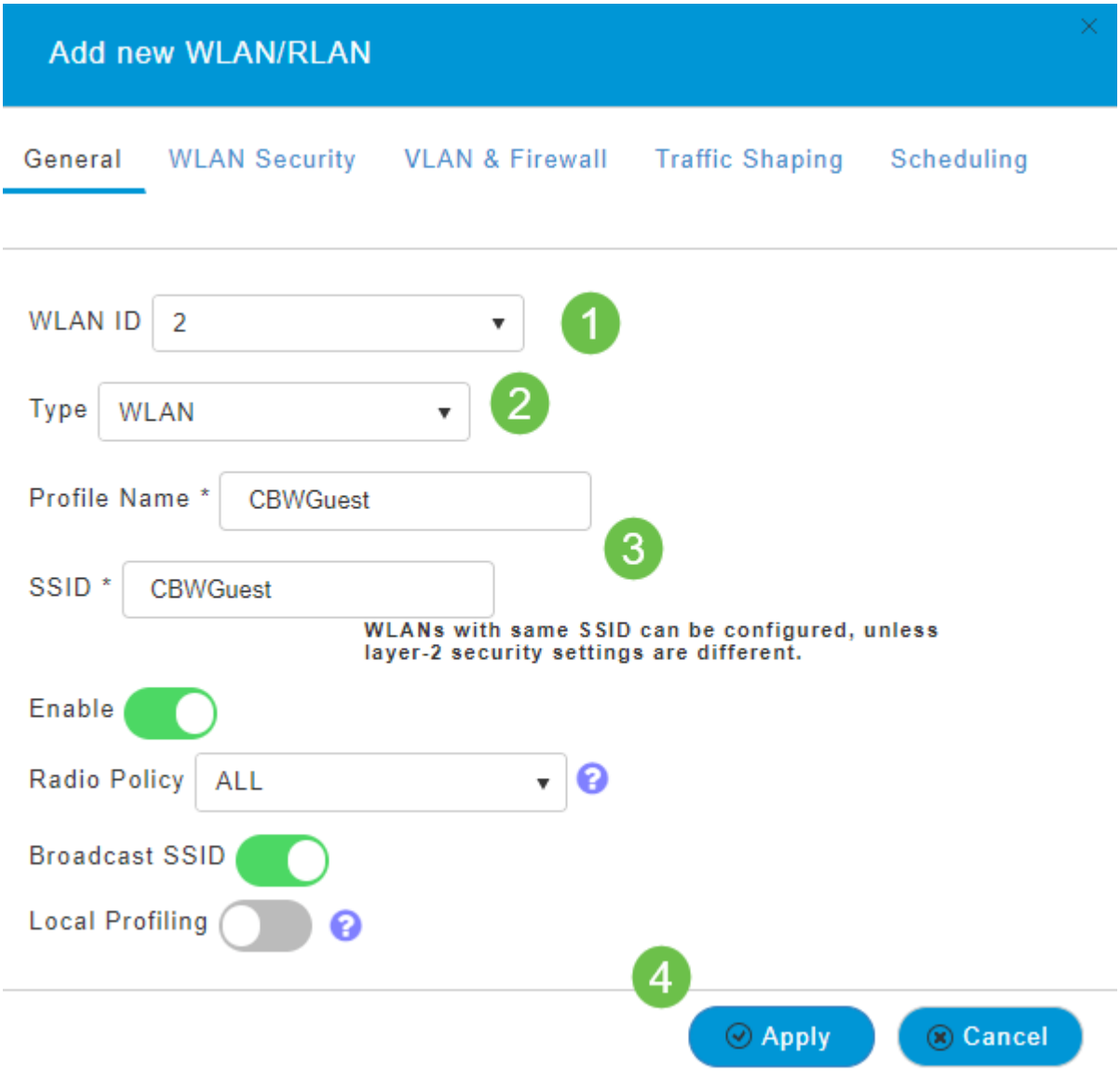
WLAN ID — 為WLAN選擇一個數字

Type — 選擇**WLAN**
Profile Name — 輸入名稱后，SSID將自動填充相同的名稱。名稱必須唯一，且不能超過31個字元。

在此示例中，以下欄位保留為預設值，但會列出解釋，以防您要以不同方式配置它們。

SSID — 配置檔名稱也用作SSID。如果您願意，可以更改它。名稱必須唯一，且不能超過31個字元。
Enable — 應保持啟用狀態以使WLAN正常運作。
Radio Policy — 通常您想將此選項保留為**All**，*以便2.4 GHz和5 GHz客戶端可以訪問網路*。
廣播SSID — 通常您希望發現SSID，以便將其保留為啟用。
Local Profiling — 您只希望啟用此選項以檢視客戶端上運行的作業系統或檢視使用者名稱。

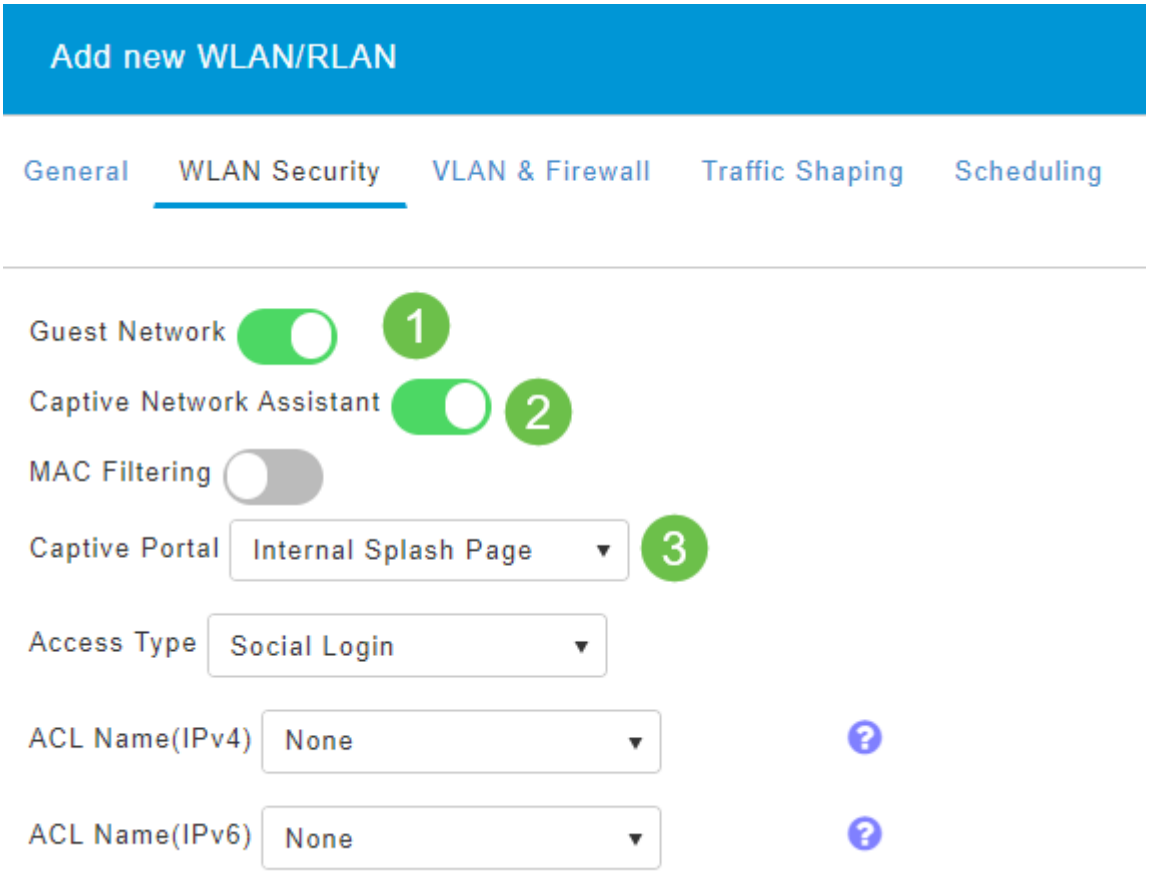
按一下「Apply」。



步驟4

您將進入*WLAN Security*頁籤。在此示例中，選擇了以下選項。

- 訪客網路 — 啟用
- Captive Network Assistant — 如果使用Mac或IOS，您可能要啟用它。此功能通過在連線到無線網路時傳送Web請求來檢測強制網路門戶的存在。該請求被定向到iPhone型號的統一資源定位器(URL)，如果收到響應，則假設網際網路訪問可用，無需進一步的互動。如果沒有收到響應，則假設強制網路門戶阻止網際網路訪問，並且蘋果的強制網路助手(CNA)自動啟動偽瀏覽器，以請求在受控視窗中登入門戶。重定向到身份服務引擎(ISE)強制網路門戶時，CNA可能會中斷。主AP阻止該偽瀏覽器彈出。
- 強制網路門戶 — 僅當啟用訪客網路選項時，此欄位才可見。這用於指定可用於身份驗證的Web門戶的型別。選擇Internal Splash Page使用預設的Cisco Web門戶身份驗證。如果您使用網路外部的Web伺服器進行強制網路門戶身份驗證，請選擇External Splash Page。此外，在「站點URL」欄位中指定伺服器的URL。



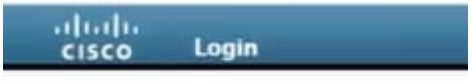
在此範例中，將建立已啟用社交登入存取型別的訪客WLAN。使用者連線到此訪客WLAN後，系統會將其重新導向到思科預設登入頁面，您可以在此找到Google和Facebook的登入按鈕。使用者可以使用其Google或Facebook帳戶登入以訪問Internet。

步驟5

在此頁籤上，從下拉選單中選擇*Access Type*。在本示例中，選擇了*Social Login*。這是允許訪客使用其Google或Facebook憑證進行身份驗證和訪問網路的選項。

訪問型別*的其他選*項包括：

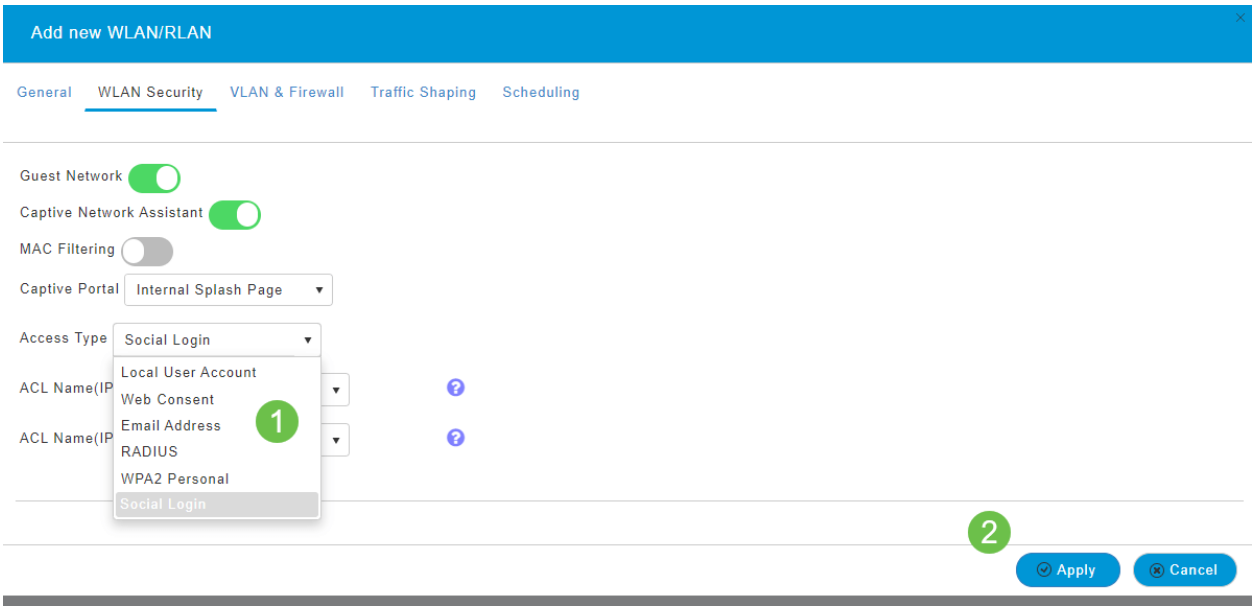
本地使用者帳戶 — 預設選項。選擇此選項可使用您在**Wireless Settings > WLAN Users**下為此WLAN的訪客使用者指定的使用者名稱和密碼對訪客進行身份驗證。以下是預設內部啟動顯示頁面的範例。



您可以導覽至**Wireless Settings > Guest WLANs**來自定義此專案。您可以在此處輸入*頁面標題*和*頁面訊息*。按一下「Apply」。按一下「**Preview**」。

Web Consent — 允許訪客在接受顯示的條款和條件時訪問WLAN。訪客使用者無需輸入使用者名稱和密碼即可存取WLAN。
*電子郵件*地址 — 訪客使用者需要輸入其電子郵件地址才能訪問網路。
RADIUS -將此選項與外部驗證伺服器配合使用。
WPA2個人 — 使用預共用金鑰(PSK)的Wi-Fi保護訪問2

按一下「Apply」。



步驟6

請務必按一下Web UI螢幕右上角面板上的**save**圖示來儲存配置。

現在，您已在CBW網路上建立了可用的訪客網路。客人將欣賞便利設施。

使用Web UI進行應用程式分析（可選）

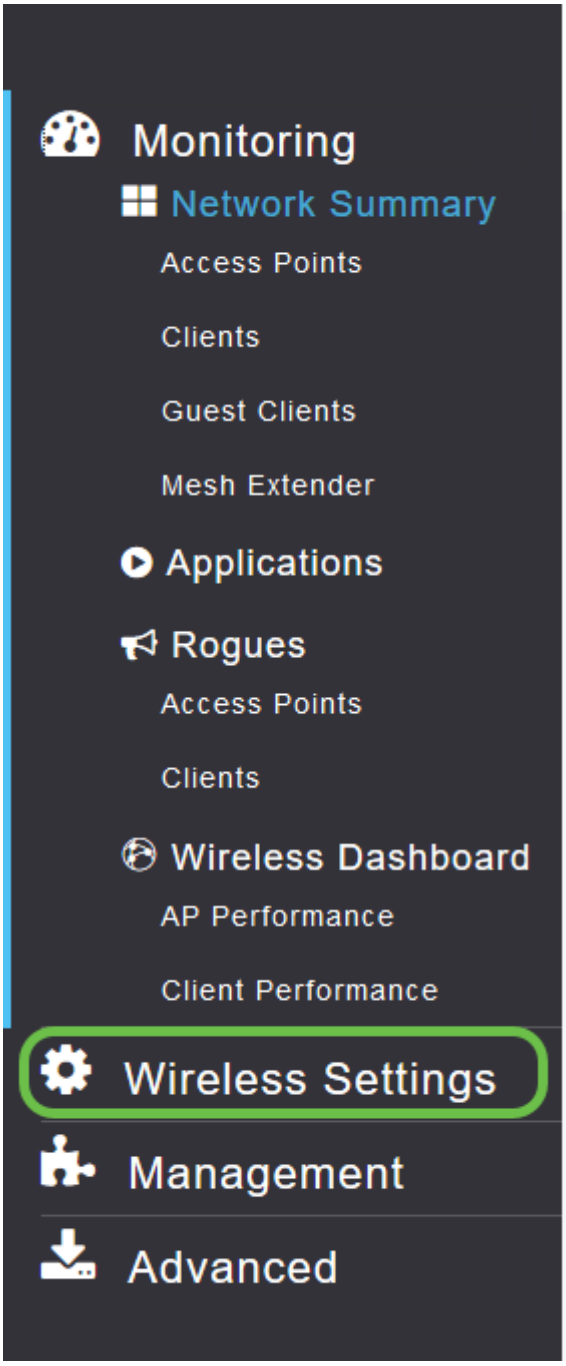
分析功能是實現制定組織策略功能的子集。它允許您匹配流量型別並確定其優先順序。就像規則決定如何對流量進行排名或丟棄流量一樣。Cisco Business Mesh Wireless系統具有客戶端和應用剖析功能。使用者訪問網路的行為始於許多資訊交換，其中資訊是流量的型別。策略會中斷流量來指導路徑，非常類似於流程圖。其他型別的策略功能包括 — 訪客接入、訪問控制清單和QoS。

步驟1

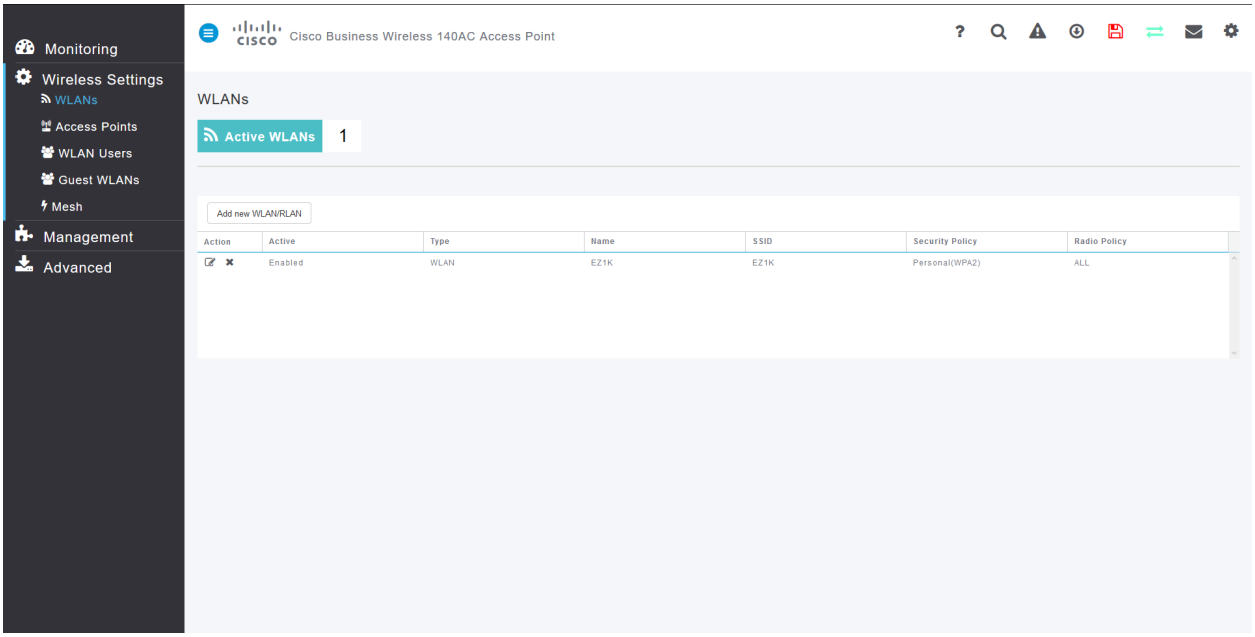
如果未看到左側選單欄，請導航到螢幕左側的選單。

步驟2

預設情況下，在登入到裝置時，會載入「監視」選單。您需要按一下「**Wireless Settings**」。

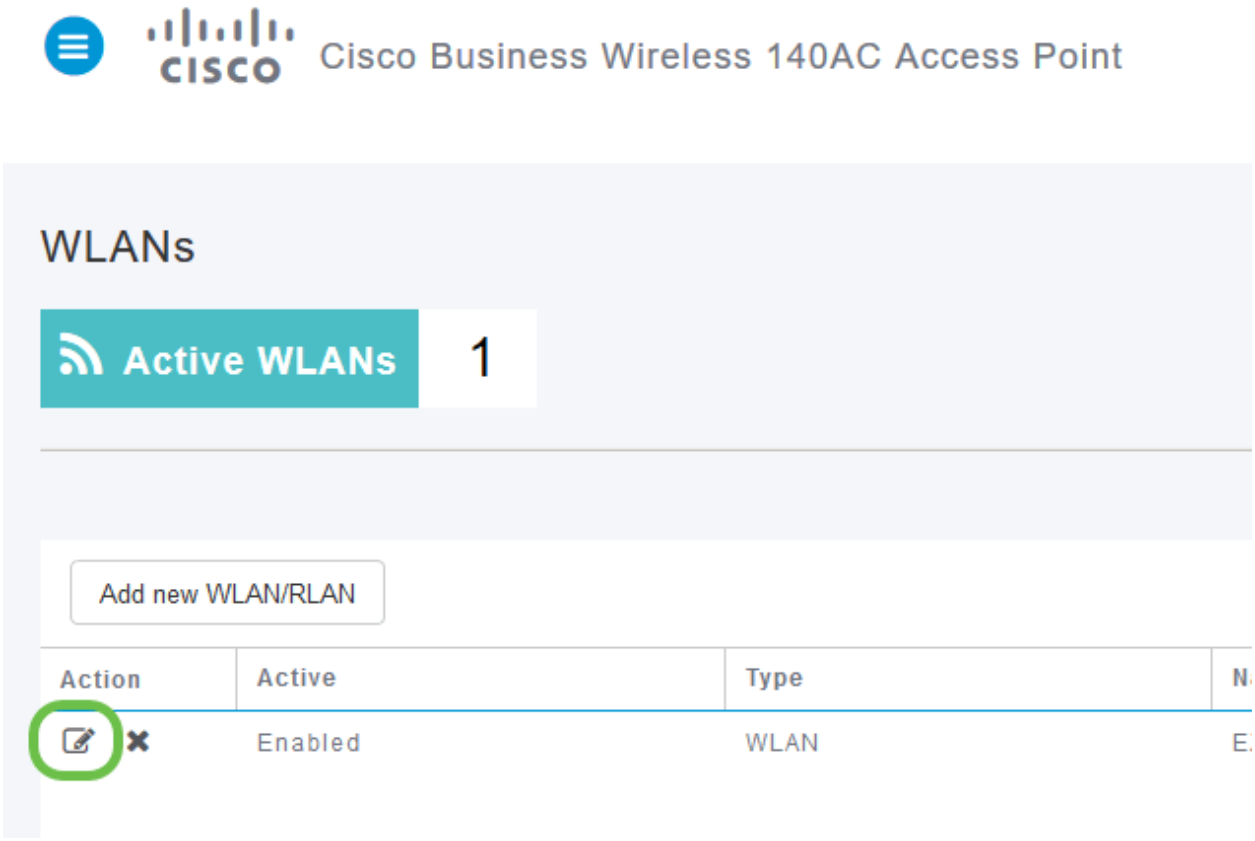


下圖與按一下「Wireless Settings（無線設定）」連結時看到的類似。

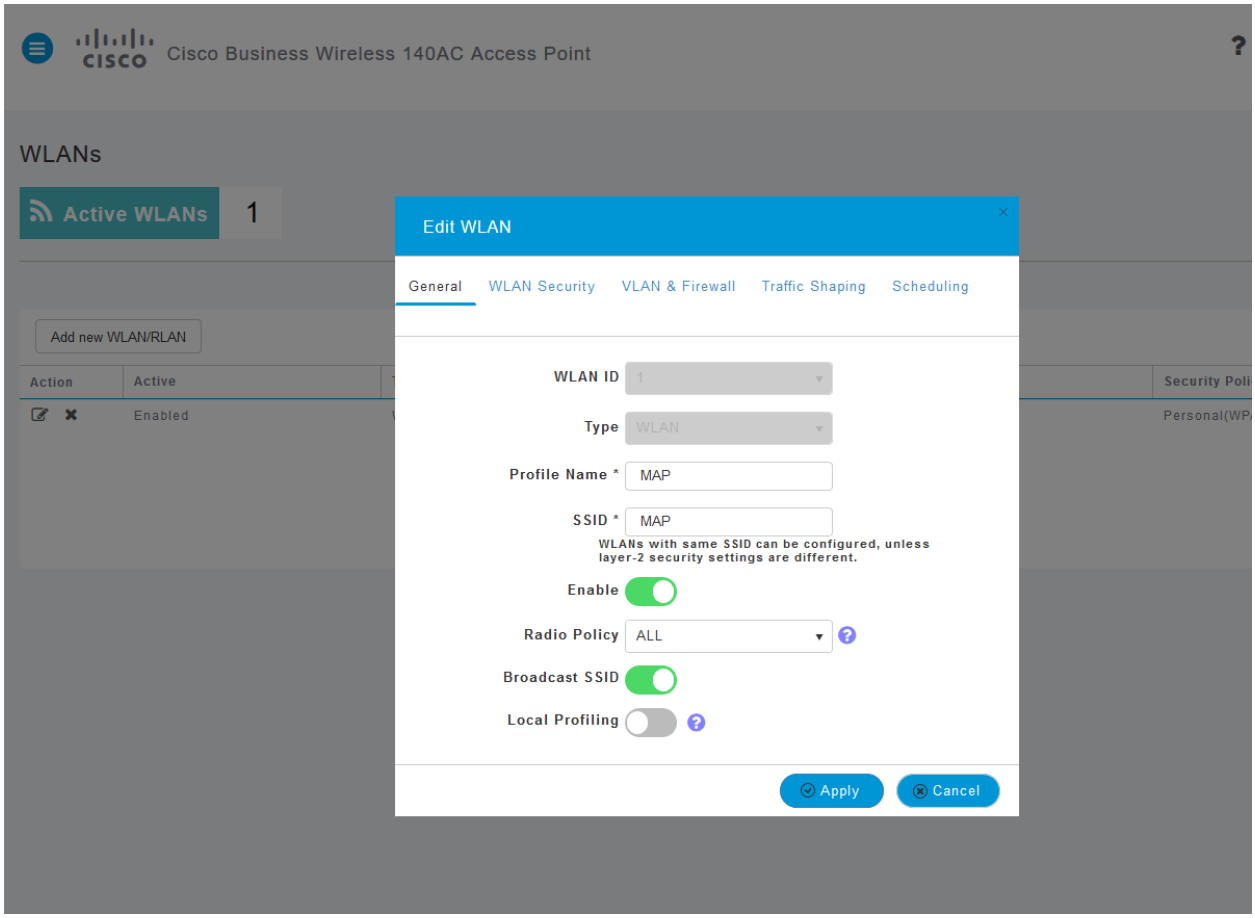


步驟3

按一下要啟用應用的Wireless Local Area Network左側的**edit**圖示。

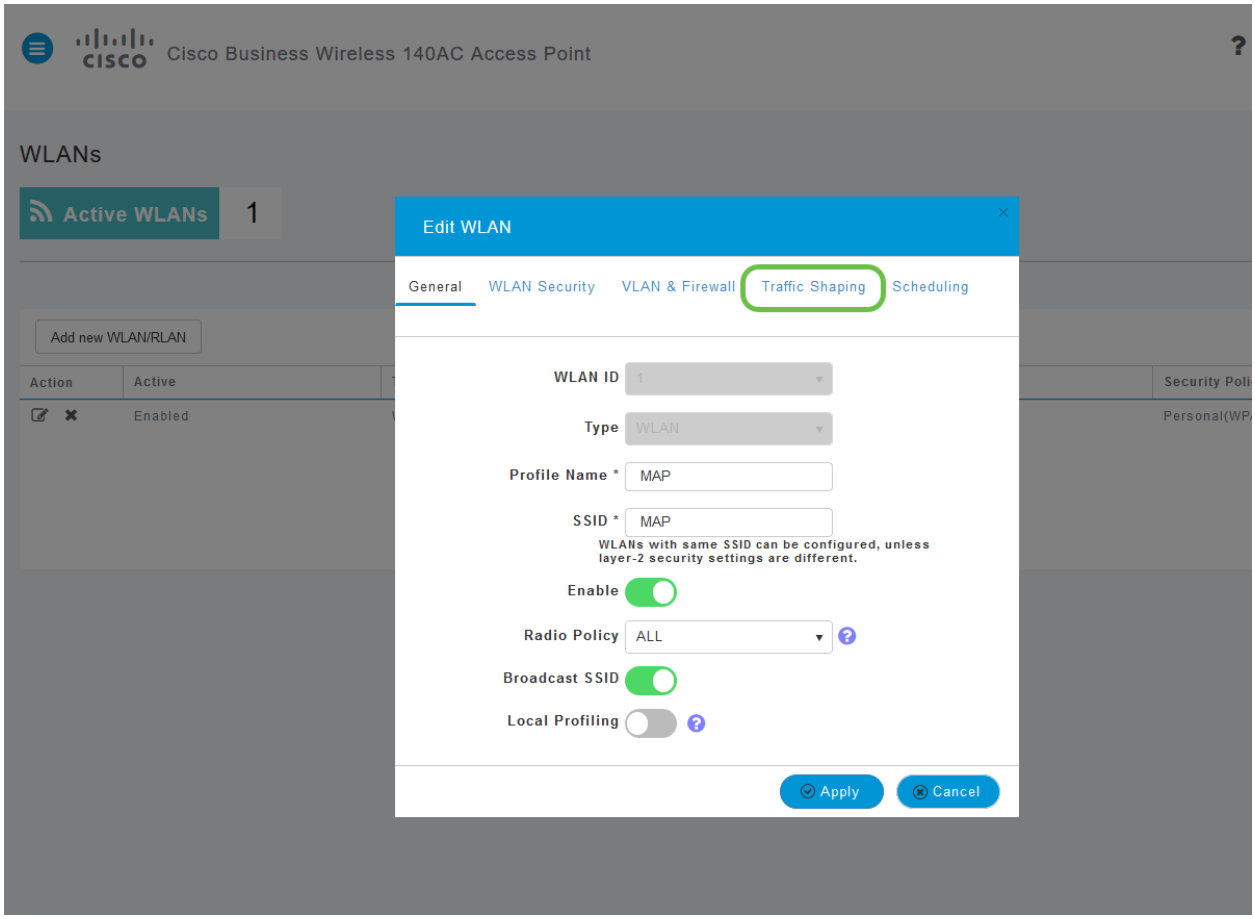


由於您最近新增了WLAN，因此您的*Edit WLAN*頁面可能如下圖所示：

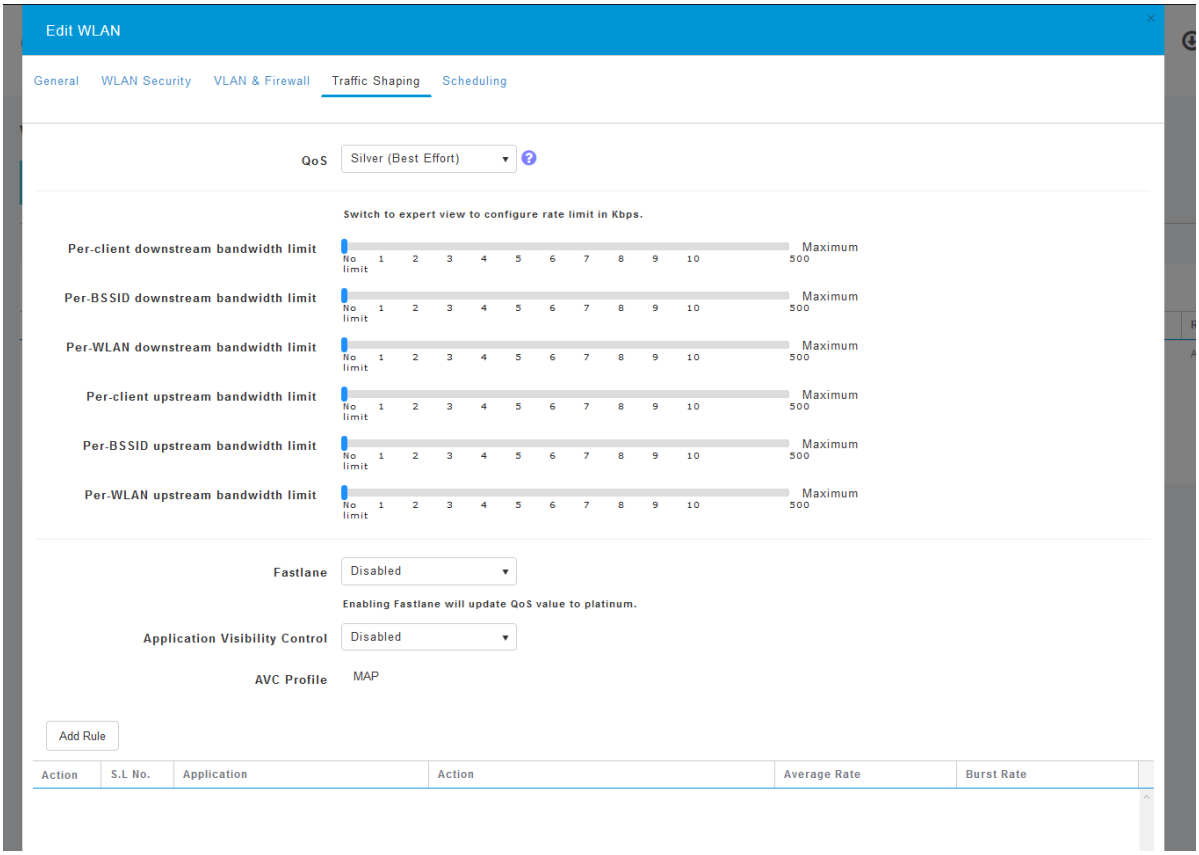


步驟4

按一下導航至**Traffic Shaping**頁籤。

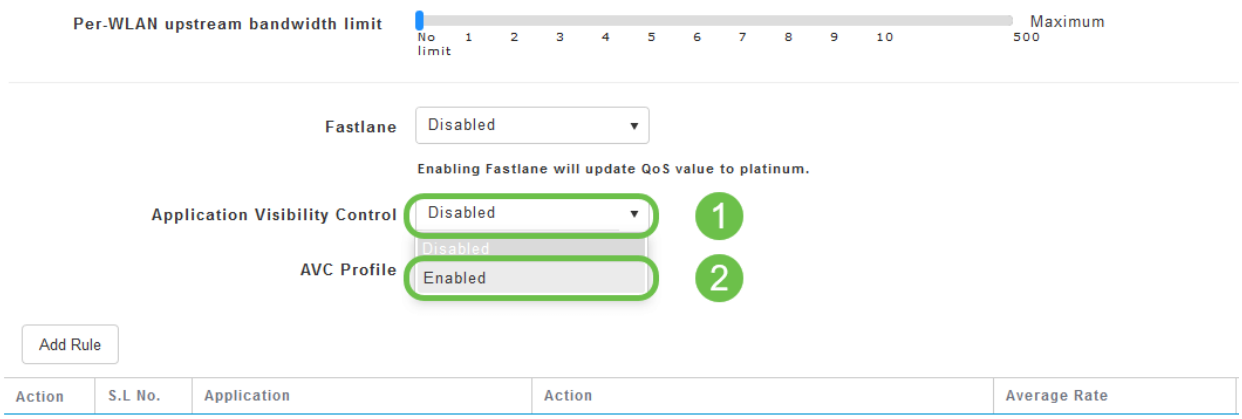


螢幕可能顯示如下：



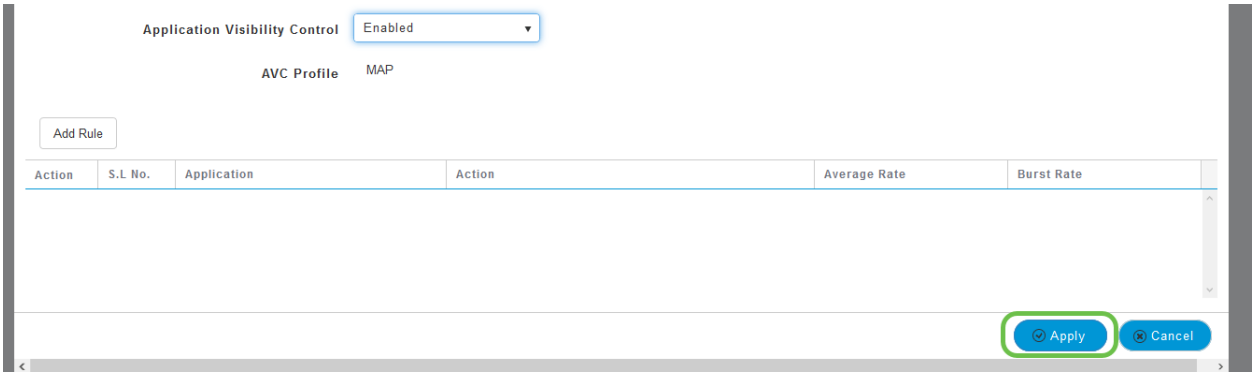
步驟5

在頁面底部，您可以找到應用*可視性控制*功能。預設情況下禁用此選項。按一下下拉選單並選擇**啟用**。



步驟6

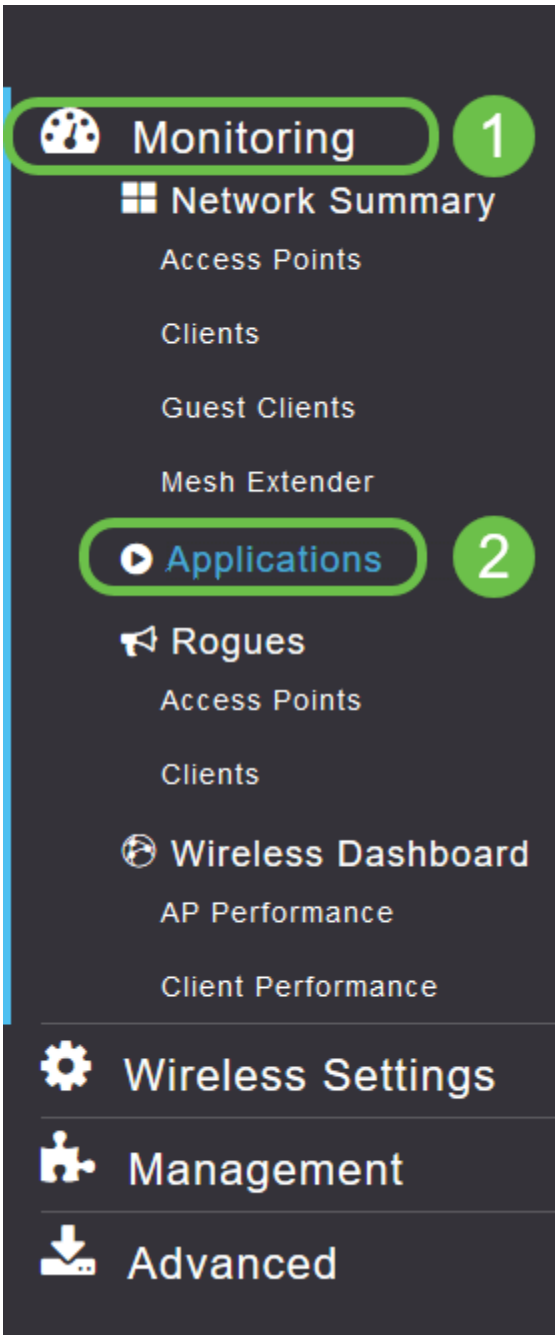
按一下**Apply**按鈕。



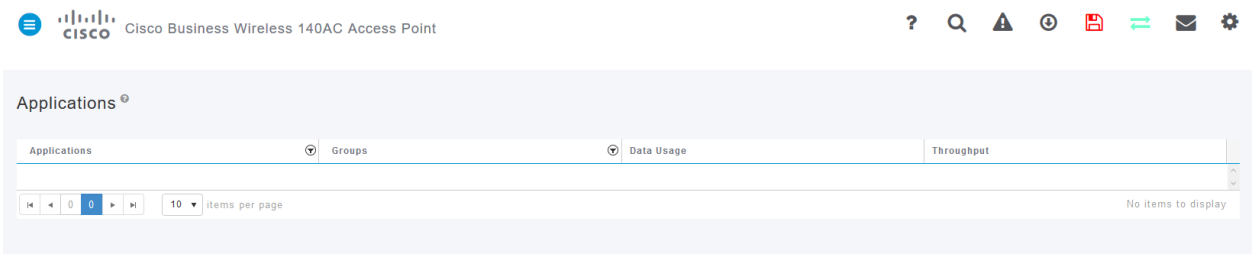
必須啟用此設定，否則功能將無法運行。

第7步

按一下取消按鈕關閉WLAN子選單。然後按一下左側選單欄上的**Monitoring**選單。一旦您能夠訪問，按一下**Applications**選單項。



如果您沒有到任何來源的流量，您的頁面將為空白，如下所示。



此頁將顯示以下資訊：

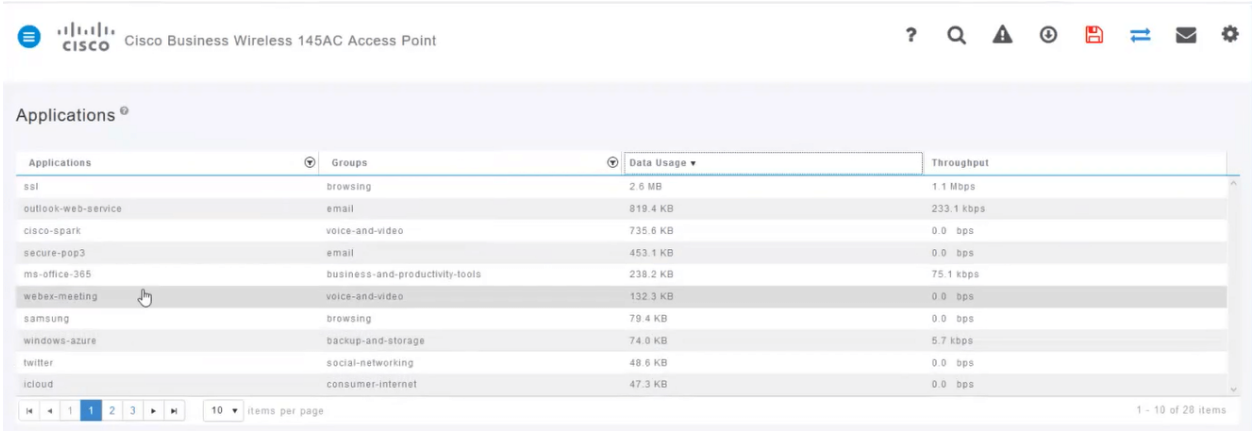
- 應用程式 — 包括許多不同型別
- Groups — 指示應用程式組的型別，以便更輕鬆地排序
- Data Usage — 此服務整體使用的資料量
- 吞吐量 — 應用程式使用的頻寬量

您可以按一下各個頁籤，按照從大到小的順序進行排序，這有助於確定網路資源的最大使用者。

此功能對於在粒度級別上管理您的WLAN資源非常強大。下面是一些比較常見的組和應用程式型別。您的清單可能包括更多內容，包括以下組和示例：

- 瀏覽
  - 例如：客戶端特定的，SSL
- 電子郵件
  - 例如：Outlook、Secure-pop3
- 語音和影片
  - 例如：WebEx、Cisco Spark、
- 業務和工作效率工具
  - 例如：Microsoft Office 365、
- 備份和儲存
  - 例如：Windows-Azure，
- 消費者 — 網際網路
  - iCloud、Google Drive
- 社交網路
  - 例如：推特、臉書
- 軟體更新
  - 例如：Google-Play、IOS
- 即時消息
  - 例如：環遊、消息

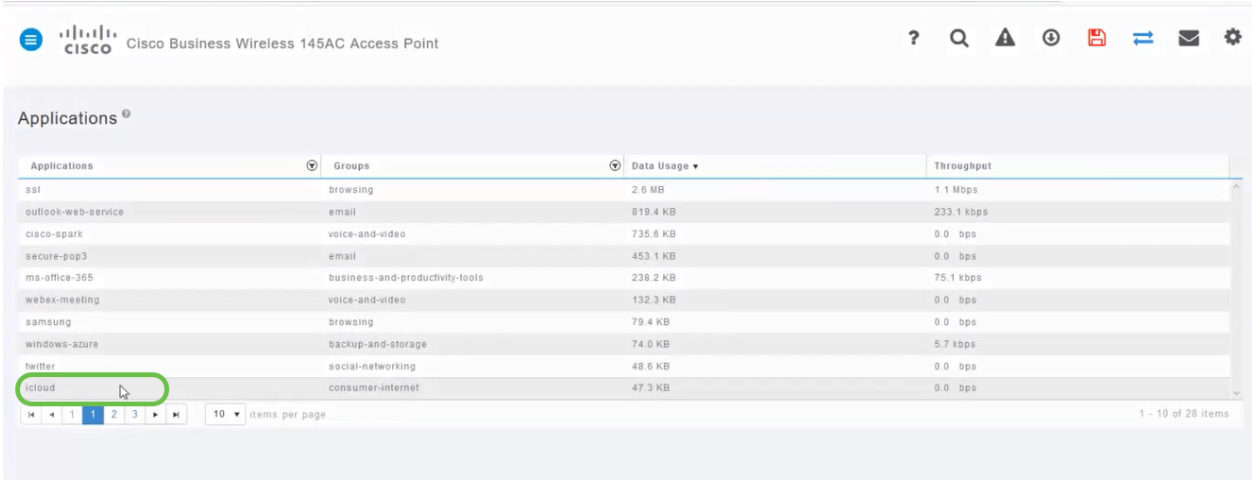
此處顯示的是填充頁面時的頁面外觀。



每個表標題都可以按一下進行排序，這對於資料使用和*吞吐量*字段尤*其*有用。

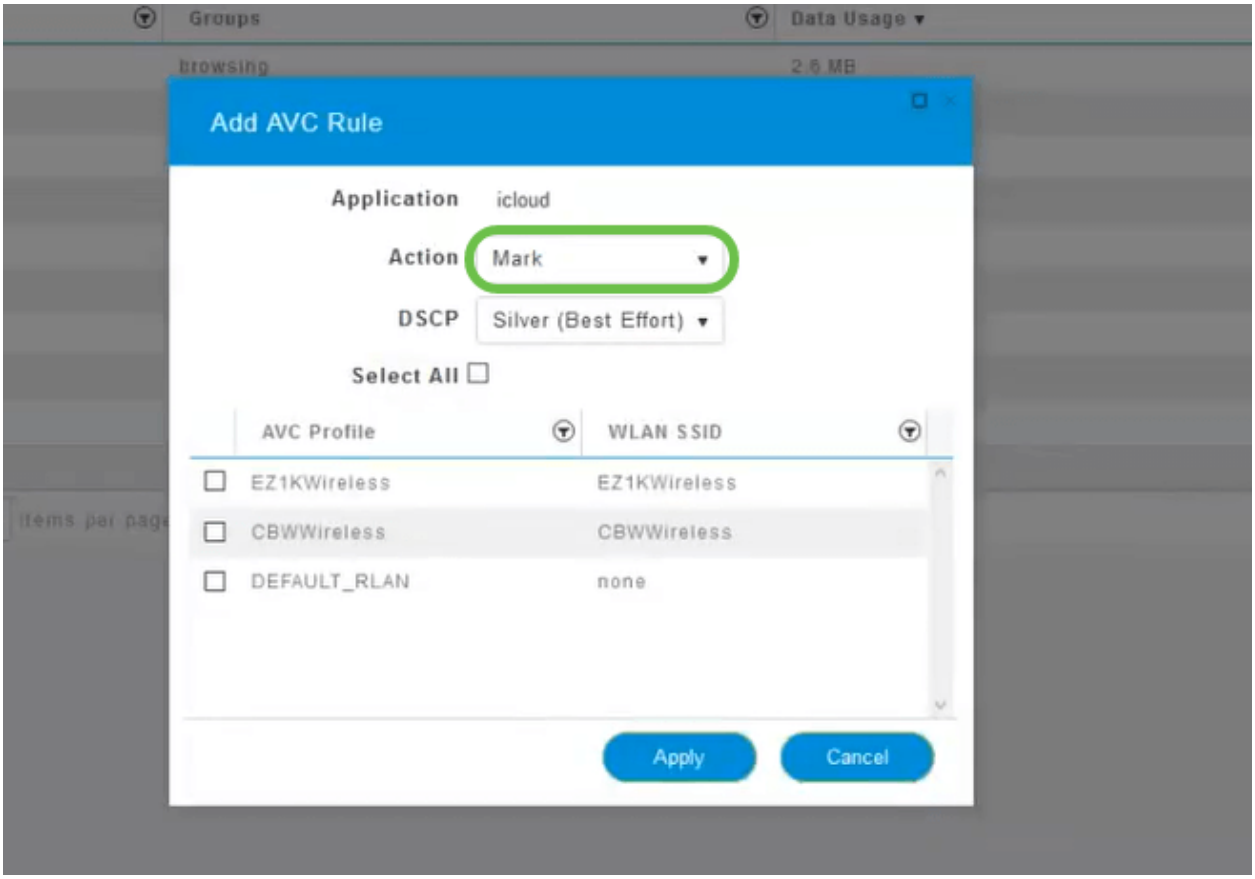
步驟8

點選要管理的流量型別的行。



步驟9

按一下**Action**下拉框以選擇如何處理該流量型別。



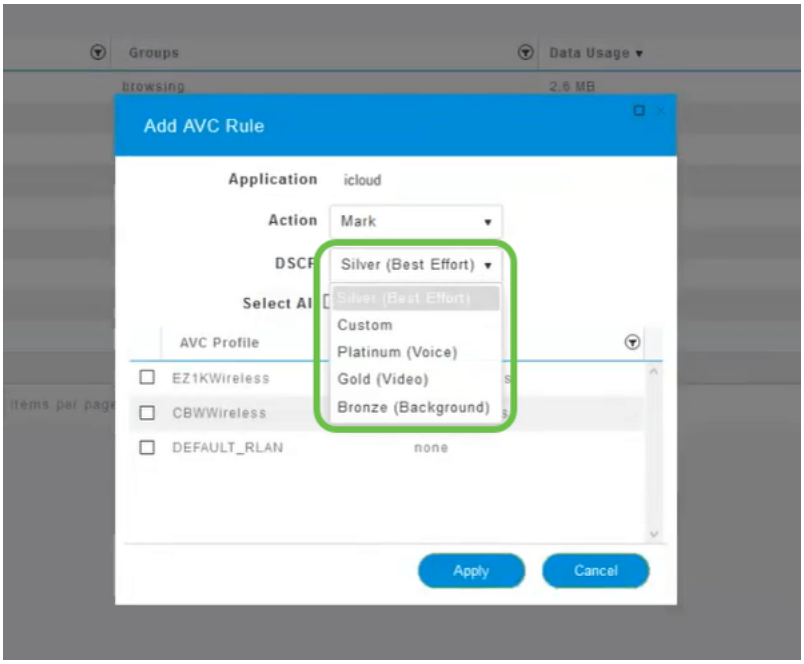
在本例中，我們將在*Mark*中保留此選項。

對流量採取的操作

- 標籤 — 將流量型別置於差分服務代碼點(DSCP)3層之一中 — 控制該應用型別可用的資源數量
- Drop — 除丟棄流量外不執行任何操作
- 速率限制 — 用於設定平均速率、突發速率(Kbps)

步驟10

按一下**DSCP**欄位中的下拉框可從以下選項中進行選擇。



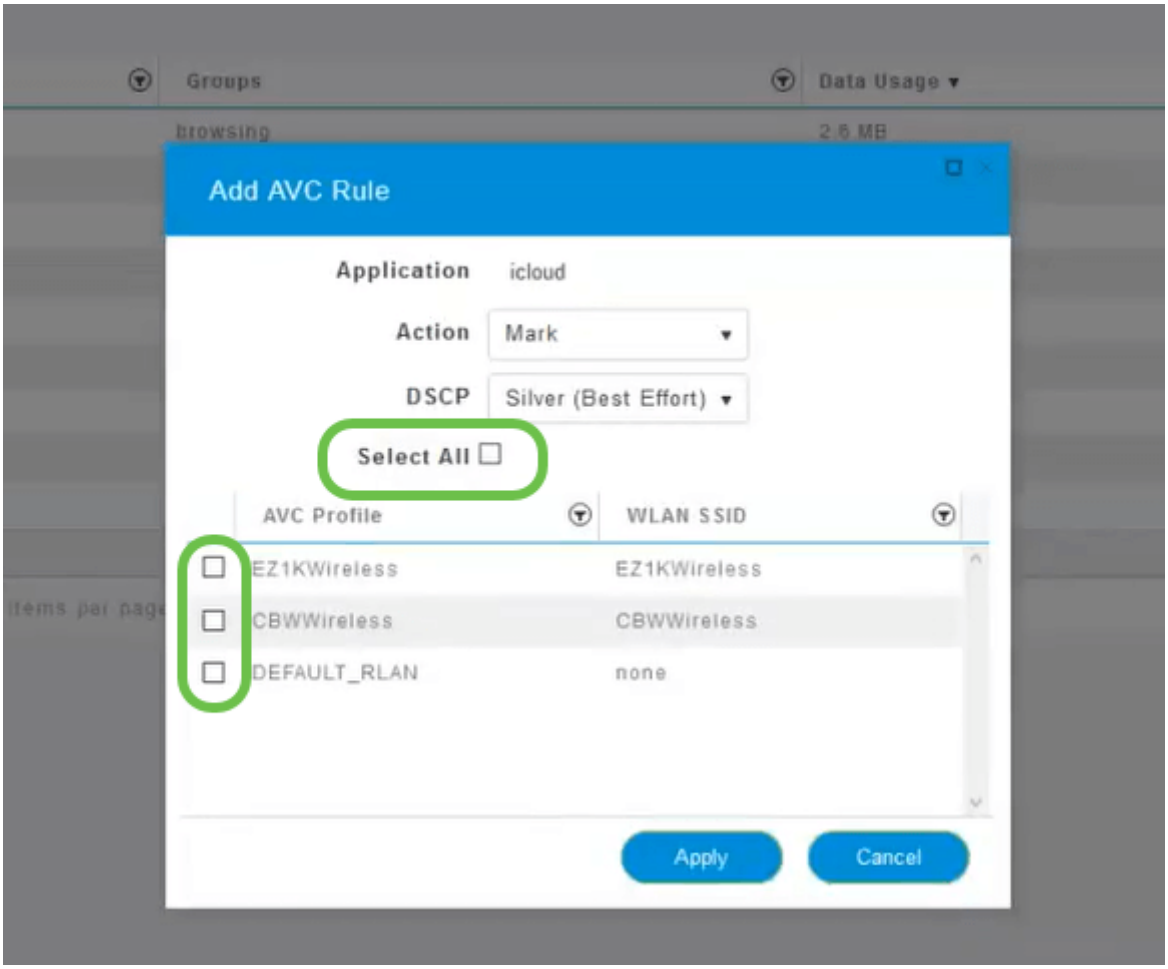
以下是待標籤流量的DSCP選項。這些選項從更少的資源演變為可用於您正在編輯的流量型別的更多資源。

- 銅牌（背景）— 更少
- 銀牌（盡最大努力）
- 金牌（影片）
- 白金（語音）更多
- 自定義 — 使用者設定

根據Web慣例，流量已向SSL瀏覽遷移，這會阻止您在資料包從您的網路移動到WAN時檢視其內部內容。因此，大部分網路流量將使用SSL。將SSL流量設定為較低優先順序可能會影響您的瀏覽體驗。

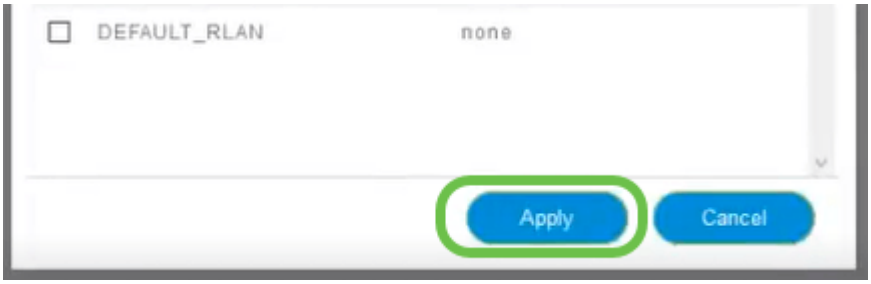
步驟11

現在，請選擇您希望此策略運行的單個SSID或按一下**Select All**。



步驟12

現在，按一下**Apply**開始此策略。



可以適用的兩個案例：

- 訪客/使用者流傳輸大量流量，防止任務關鍵型流量通過。您可以提高Voice的優先順序，降低Netflix流量的優先順序以改善情況。
- 在辦公時間內下載的大型軟體更新可以取消優先順序或限制費率。

你成功了！應用程式分析是一個非常強大的工具，也可以通過啟用客戶端分析來進一步啟用，如下一節所述。

使用Web UI進行客戶端分析（可選）

連線到網路後，裝置會交換客戶端分析資訊。預設情況下，*客戶端分析*處於禁用狀態。這些資訊可能包括：

- 主機名 — 或裝置的名稱
- 作業系統 — 裝置的核心軟體
- 作業系統版本 — 適用軟體的小版本

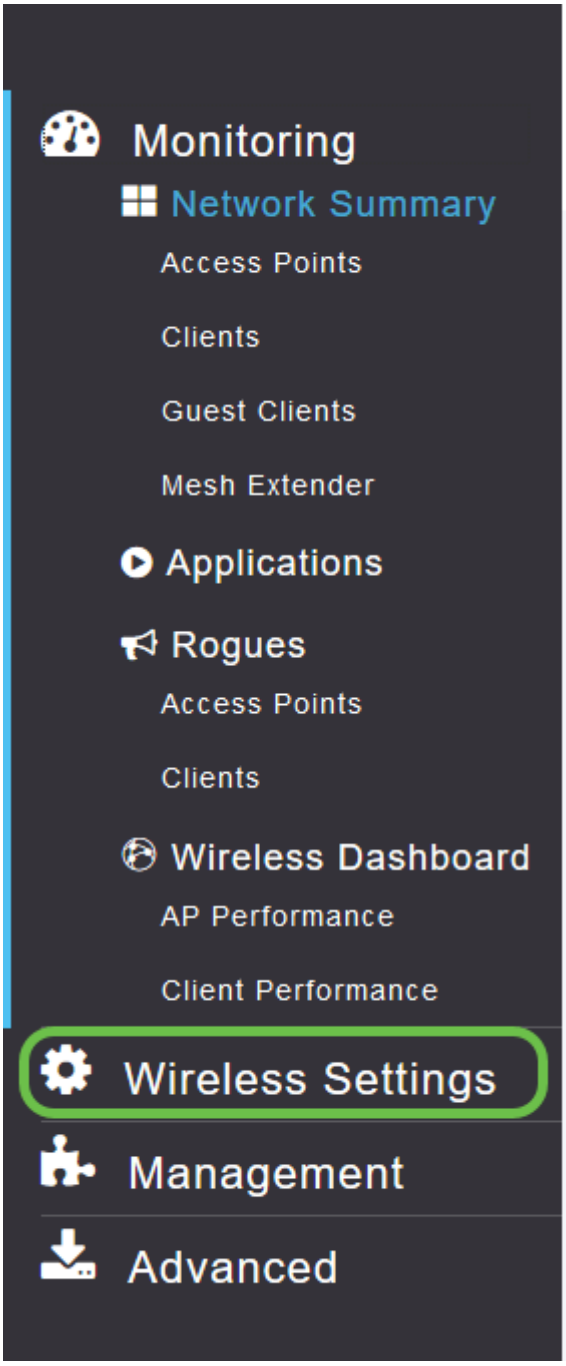
有關這些客戶端的統計資訊包括使用的資料量和吞吐量。

跟蹤客戶端配置檔案可更好地控制無線區域網。或者可以將其用作其他功能的函式。例如使用不傳輸您的業務的關鍵任務資料的應用限制裝置型別。

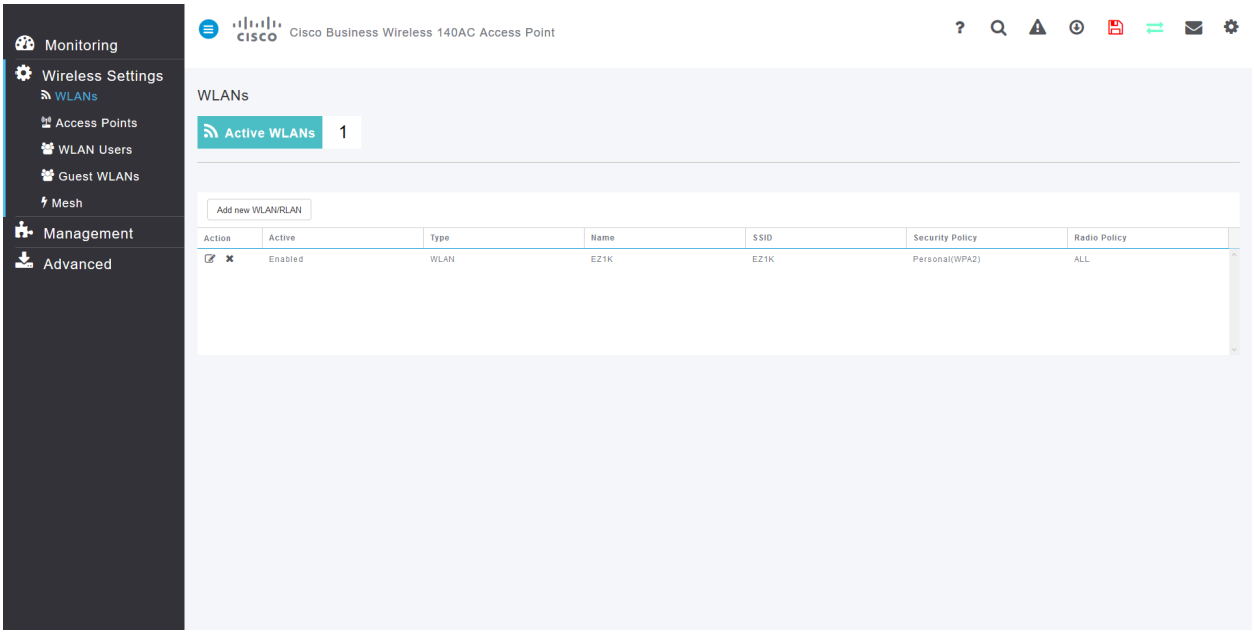
啟用後，您網路的客戶端詳細資訊可在Web UI的「Monitoring（監控）」部分找到。

步驟1

按一下「**Wireless Settings**」。

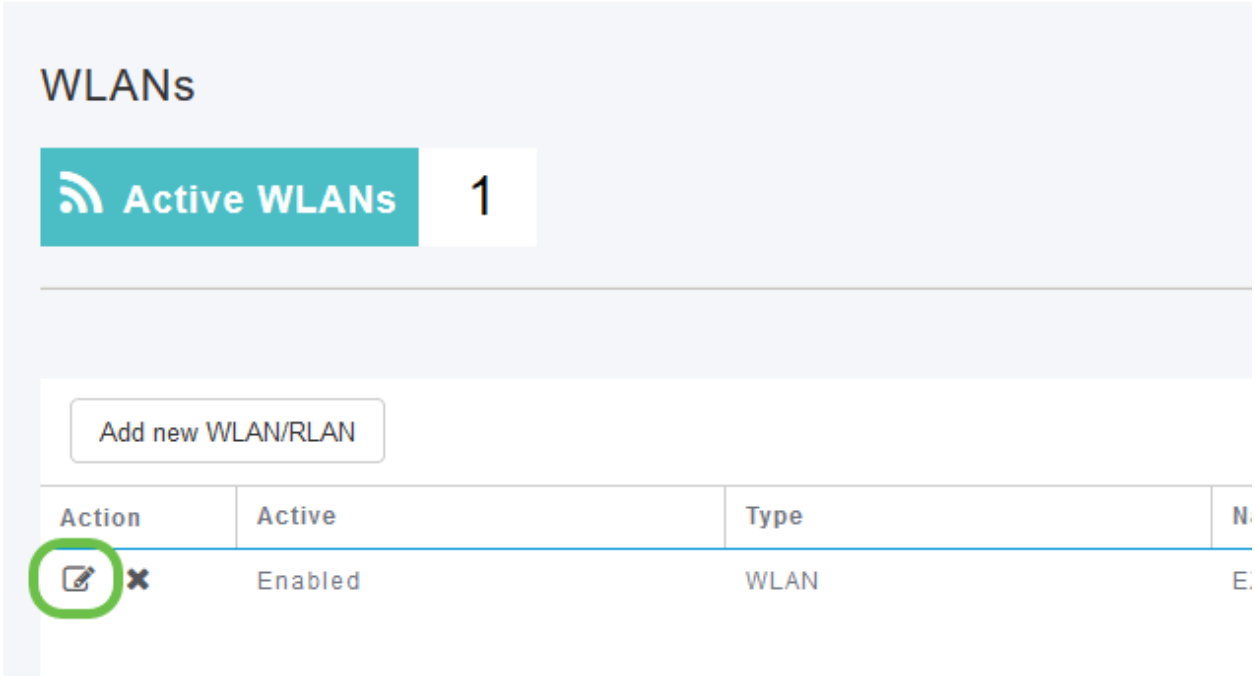


以下內容與按一下無線設定連結時看到的內容相似：



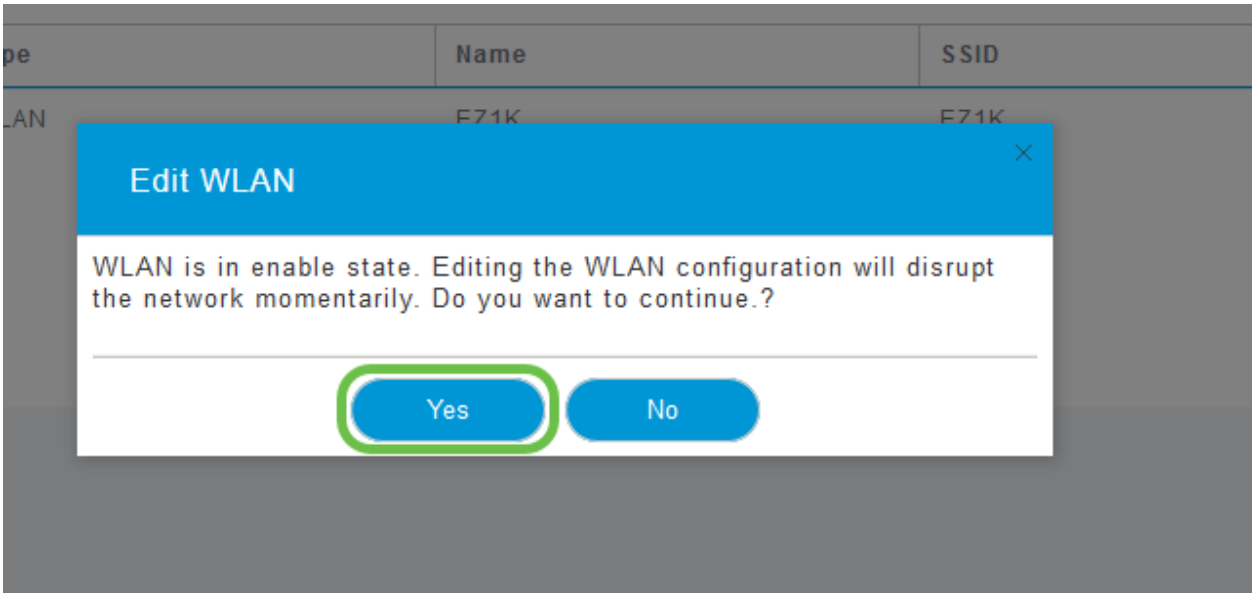
步驟2

決定要將哪個WLAN用於該應用，然後按一下其左側的**edit**圖示。



步驟3

彈出式選單可能如下圖所示。這條重要消息可能會暫時影響您網路上的服務。按一下**Yes**向前移動。

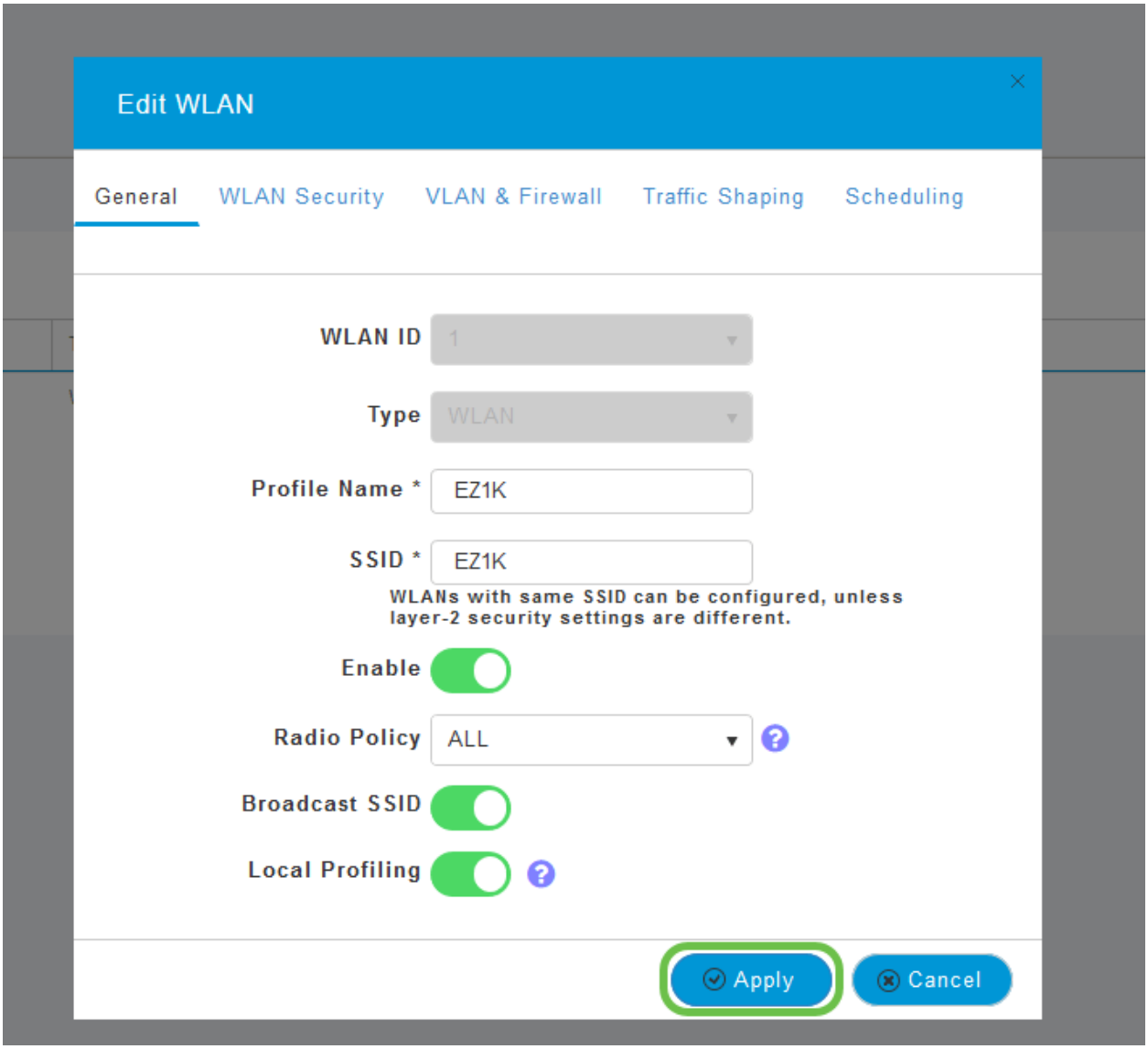


步驟4

通過按一下「本地分析」(Local Profiling)**切換按鈕來切**換客戶端分析。

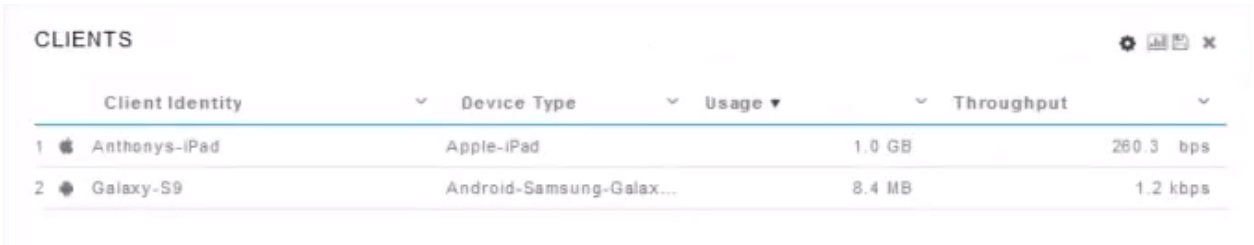
步驟5

按一下「Apply」。



步驟6

按一下左側的**Monitoring**部分選單項。您將看到客戶端資料開始顯示在*Monitoring*頁籤的儀表板中。



結論

現在，您已完成安全網路的設定。多麼美好的感受啊！現在花一分鐘慶祝一下然後開始工作！

我們希望為我們的客戶帶來最好的體驗，因此您對此主題有任何意見或建議，請向我們傳送電子郵件至思科內容團隊。

如果您想閱讀其他文章和文檔，請檢視您的硬體的支援頁面：

- 含PoE的Cisco RV345P VPN路由器
- 思科商務140AC存取點
- 思科商務142ACM網狀延伸器