在RV042、RV042G和RV082 VPN路由器上通過Windows配置Shrew VPN客戶端

目標

虛擬專用網路(VPN)是一種遠端使用者通過Internet虛擬連線到專用網路的方法。客戶端到網關VPN使用VPN客戶端軟體將使用者的台式機或筆記型電腦連線到遠端網路。客戶端到網關VPN連線對於希望安全地遠端連線到辦公室網路的遠端員工非常有用。Shrew VPN Client是在遠端主機裝置上配置的軟體，可提供簡單和安全的VPN連線。

本文檔的目的是向您展示如何為連線到RV042、RV042G或RV082 VPN路由器的電腦配置Shrew VPN客戶端。

注意：本文檔假定您已經在Windows電腦上下載了Shrew VPN客戶端。否則，您需要配置客戶端到網關VPN連線，然後才能開始配置刷新VPN。有關如何配置客戶端到網關VPN的詳細資訊，請參閱為RV042、RV042G和RV082 VPN路由器上的VPN客戶端設定遠端訪問隧道（客戶端到網關）。

適用裝置

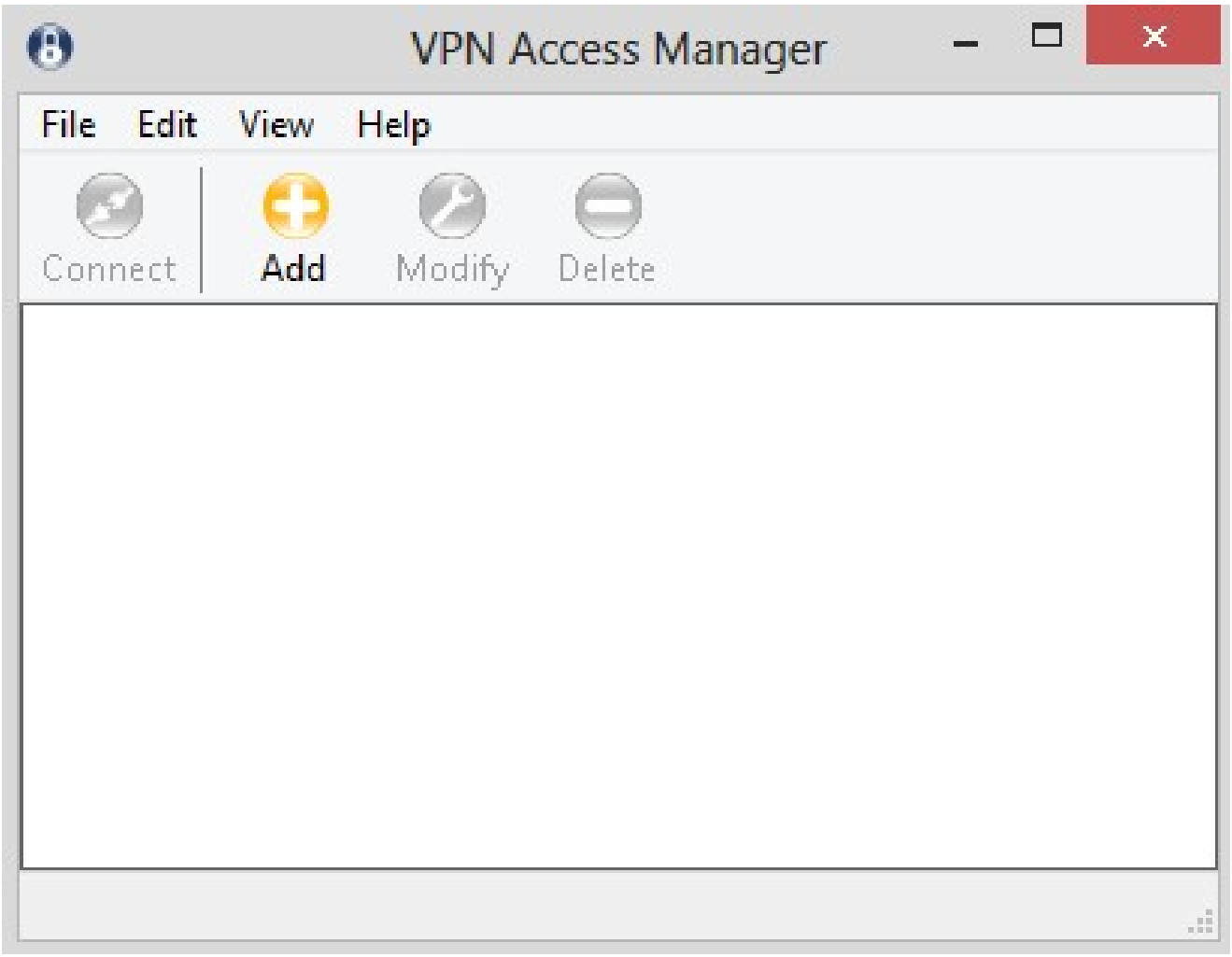
- RV042
- RV042G
- RV082

軟體版本

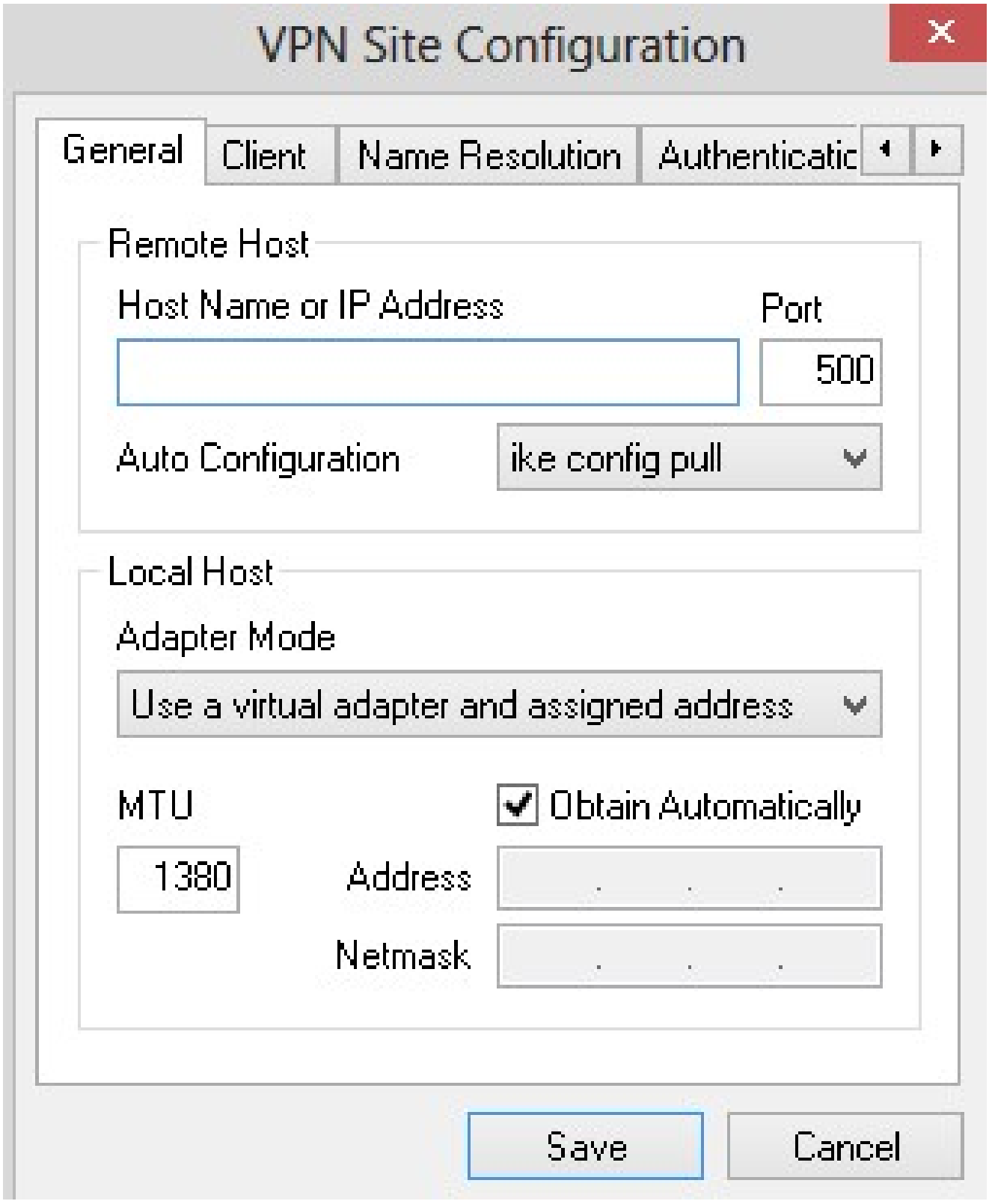
- v4.2.2.08

配置Windows上的Shrew VPN客戶端連線

步驟 1.按一下電腦上的Shrew VPN Client程式並開啟它。Shrew Soft VPN Access Manager視窗開啟：

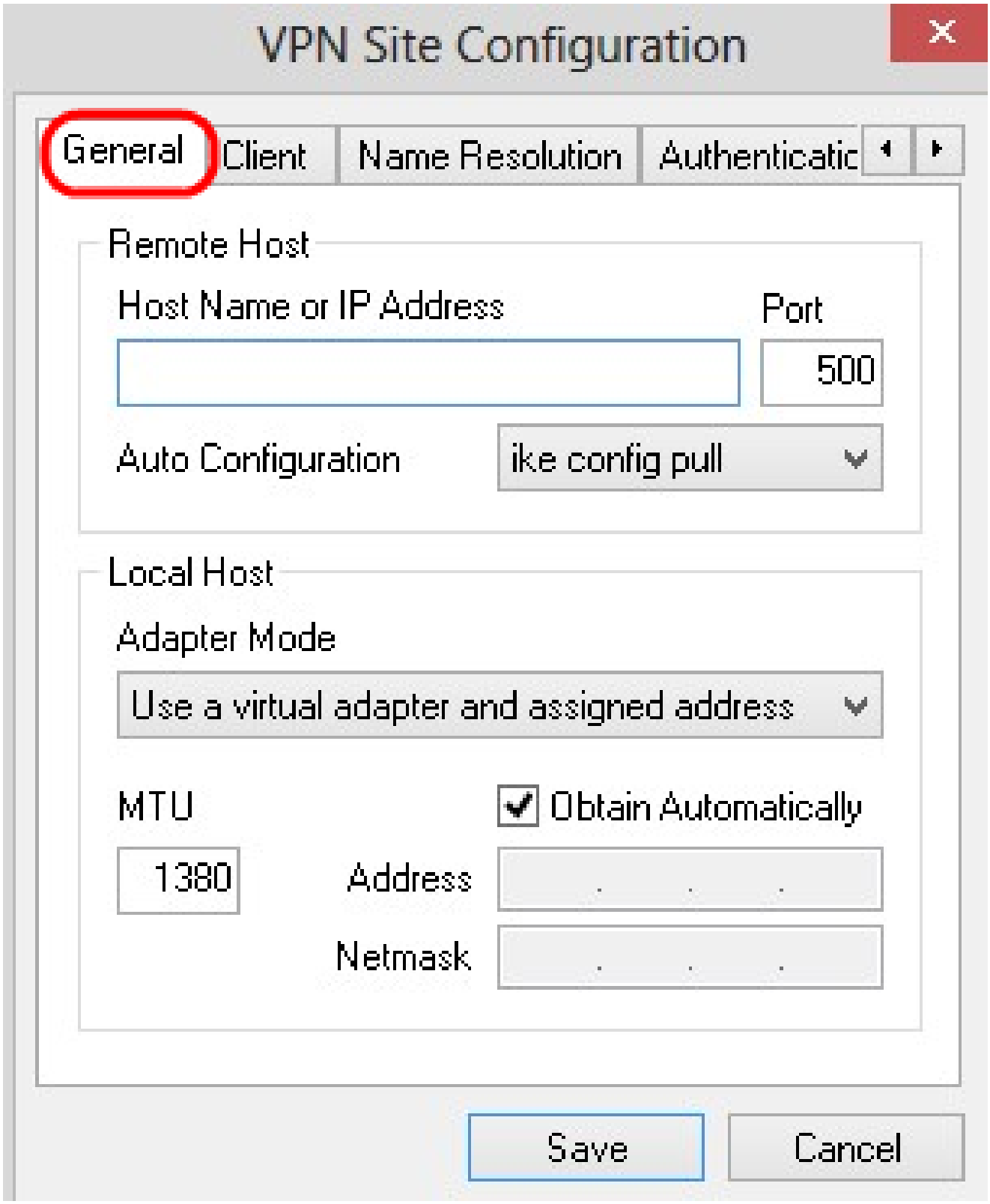


步驟 2.按一下「Add」。出現VPN Site Configuration視窗：



常規配置

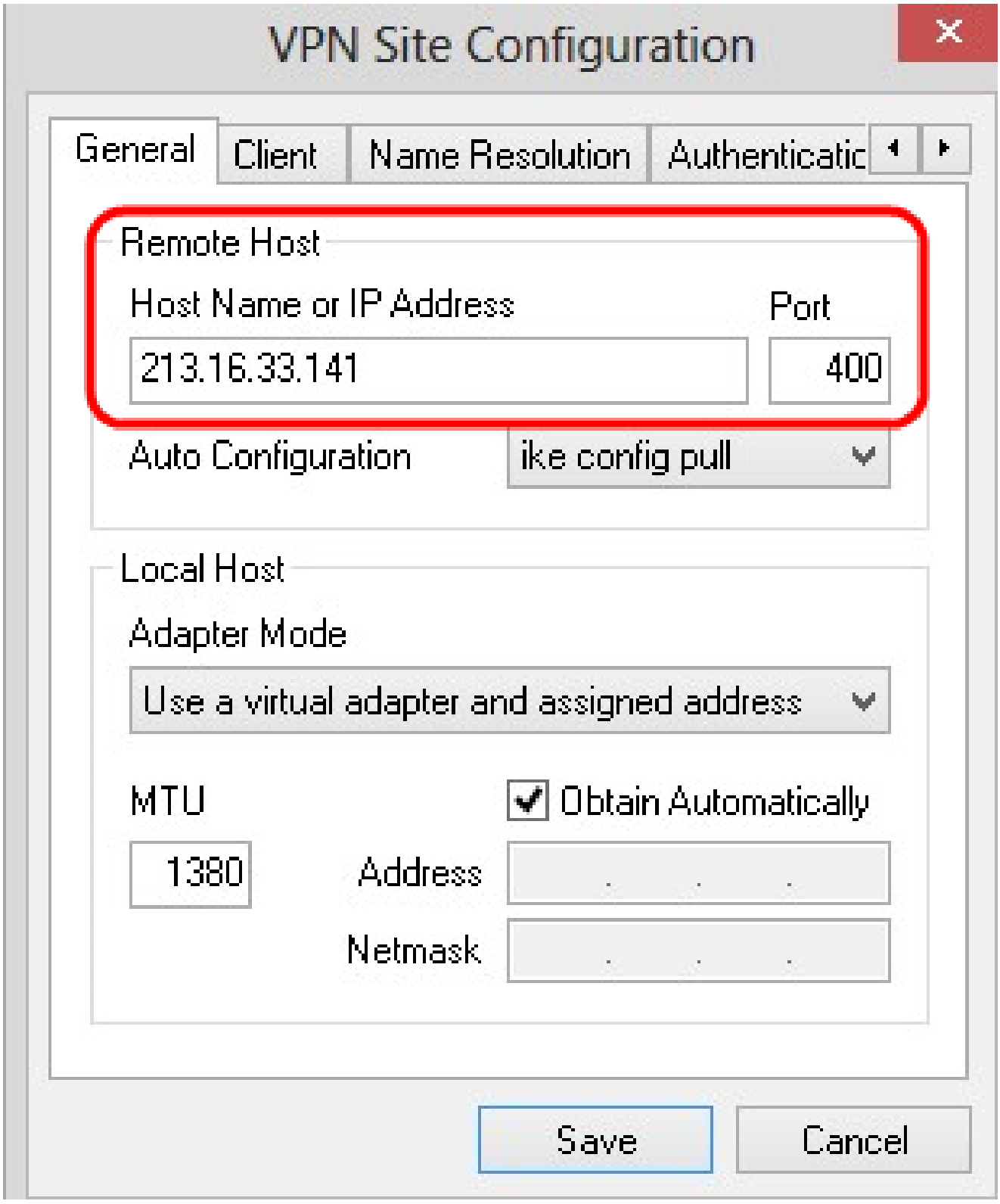
步驟 1.按一下General頁籤。



注意：General部分用於配置遠端和本地主機IP地址。這些引數用於定義客戶端到網關連線的網路引數。

步驟 2.在Host Name or IP Address欄位中，輸入遠端主機IP地址，即已配置WAN的IP地址。

步驟 3.在「Port」欄位中，輸入用於連線的連線埠號碼。圖中所用的埠號為400。



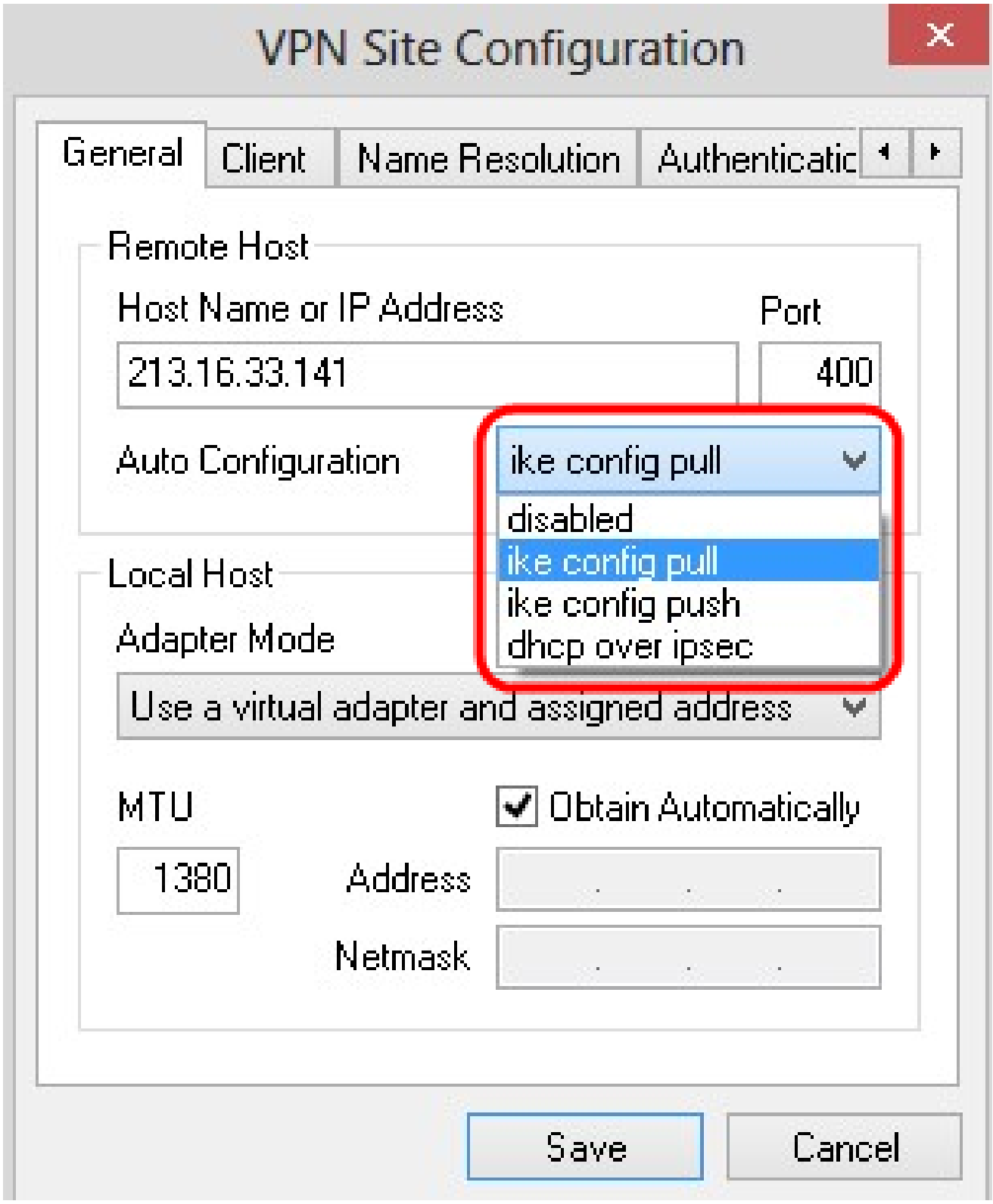
步驟 4.在「Auto Configuration」下拉式清單中選擇所需的組態。

·禁用 — 禁用選項禁用任何自動客戶端配置。

· IKE Config Pull — 允許客戶端從電腦設定請求。在電腦支援Pull方法的情況下，請求將返回客戶端支援的設定清單。

· IKE Config Push — 使電腦有機會通過配置過程向客戶端提供設定。在電腦支援Push方法的情況下，請求將返回客戶端支援的設定清單。

· DHCP Over IPSec — 使客戶端有機會通過DHCP over IPSec從電腦請求設定。



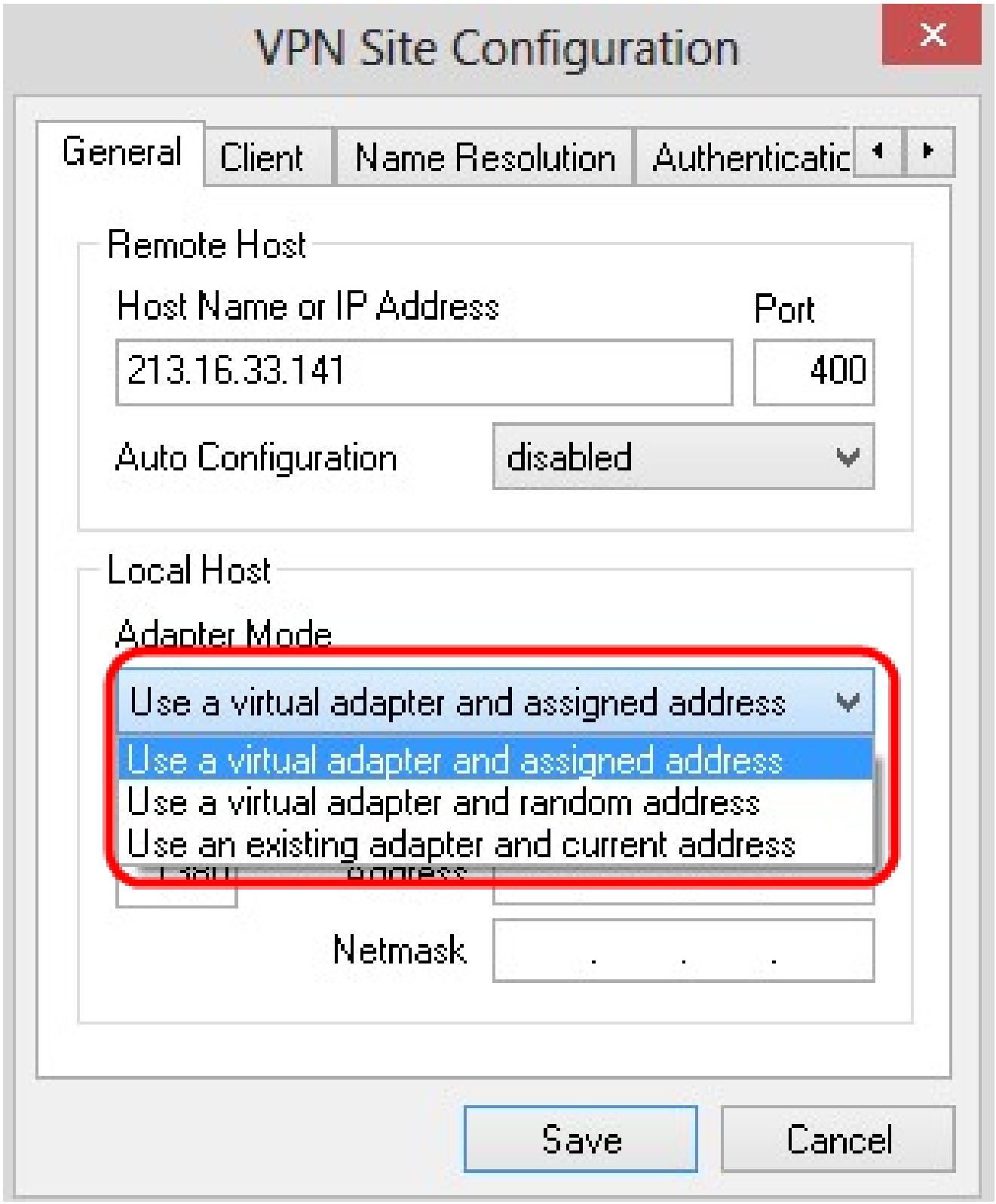
步驟 5.從Adapter Mode下拉選單中，根據Auto Configuration為本地主機選擇所需的介面卡模

式。

·使用虛擬介面卡和分配的地址 — 允許客戶端使用具有指定地址的虛擬介面卡。

·使用虛擬介面卡和隨機地址 — 允許客戶端使用具有隨機地址的虛擬介面卡。

·使用現有介面卡和當前地址 — 使用現有介面卡及其地址。不需要輸入其他資訊。

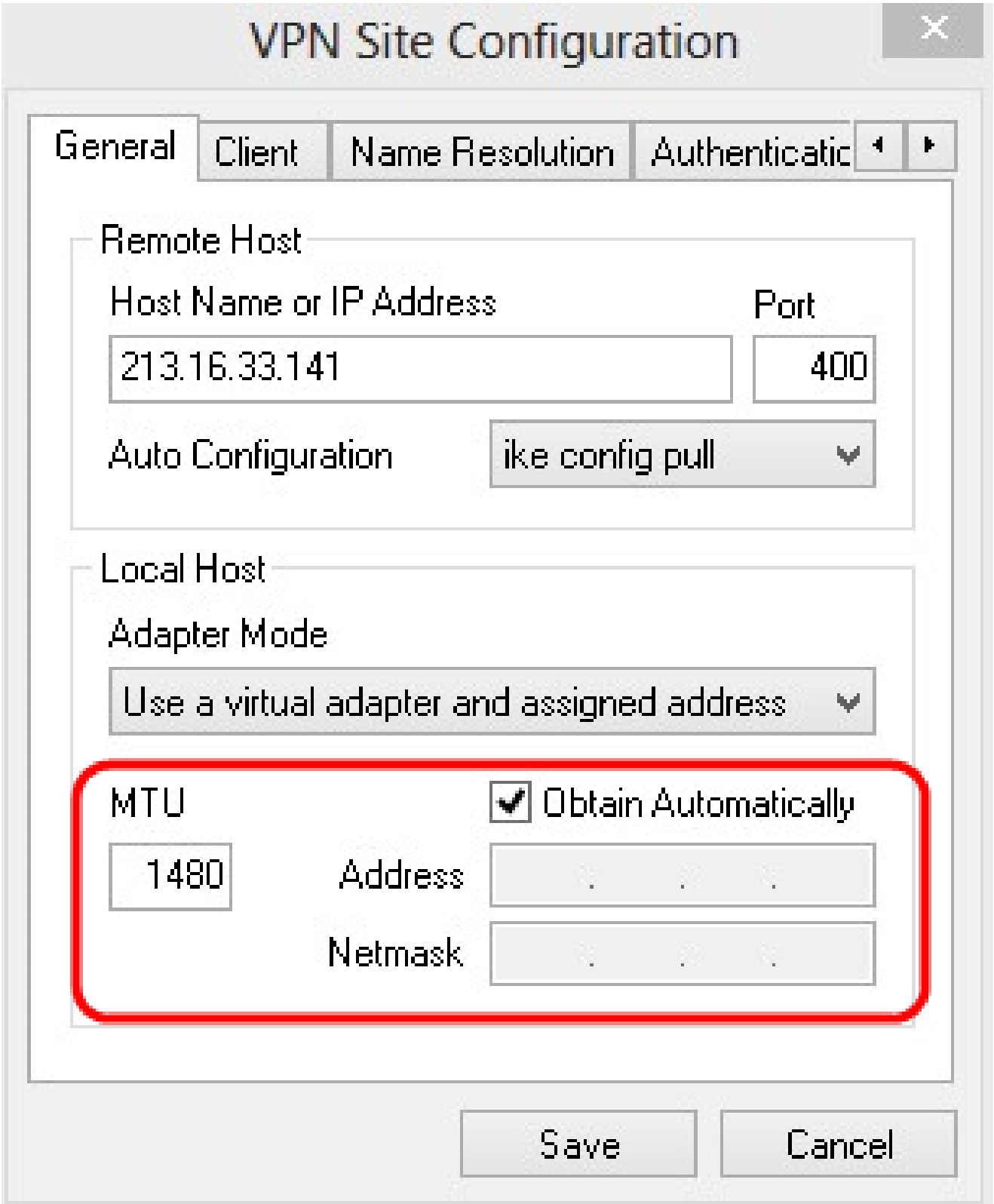


步驟 6.如果從步驟5的Adapter Mode下拉式清單中選擇了Use a Virtual Adapter and Assigned Address，請在MTU欄位中輸入最大傳輸單位(MTU)。最大傳輸單元有助於解決IP分段問題。預設值為 1380。

步驟7.（可選）要通過DHCP伺服器自動獲取地址和子網掩碼，請選中Obtain Automatically覈取方塊。此選項並非對所有配置都可用。

步驟 8.如果從步驟5的Adapter Mode下拉選單中選擇Use a Virtual Adapter and Assigned Address，請在Address欄位中輸入遠端客戶端的IP地址。

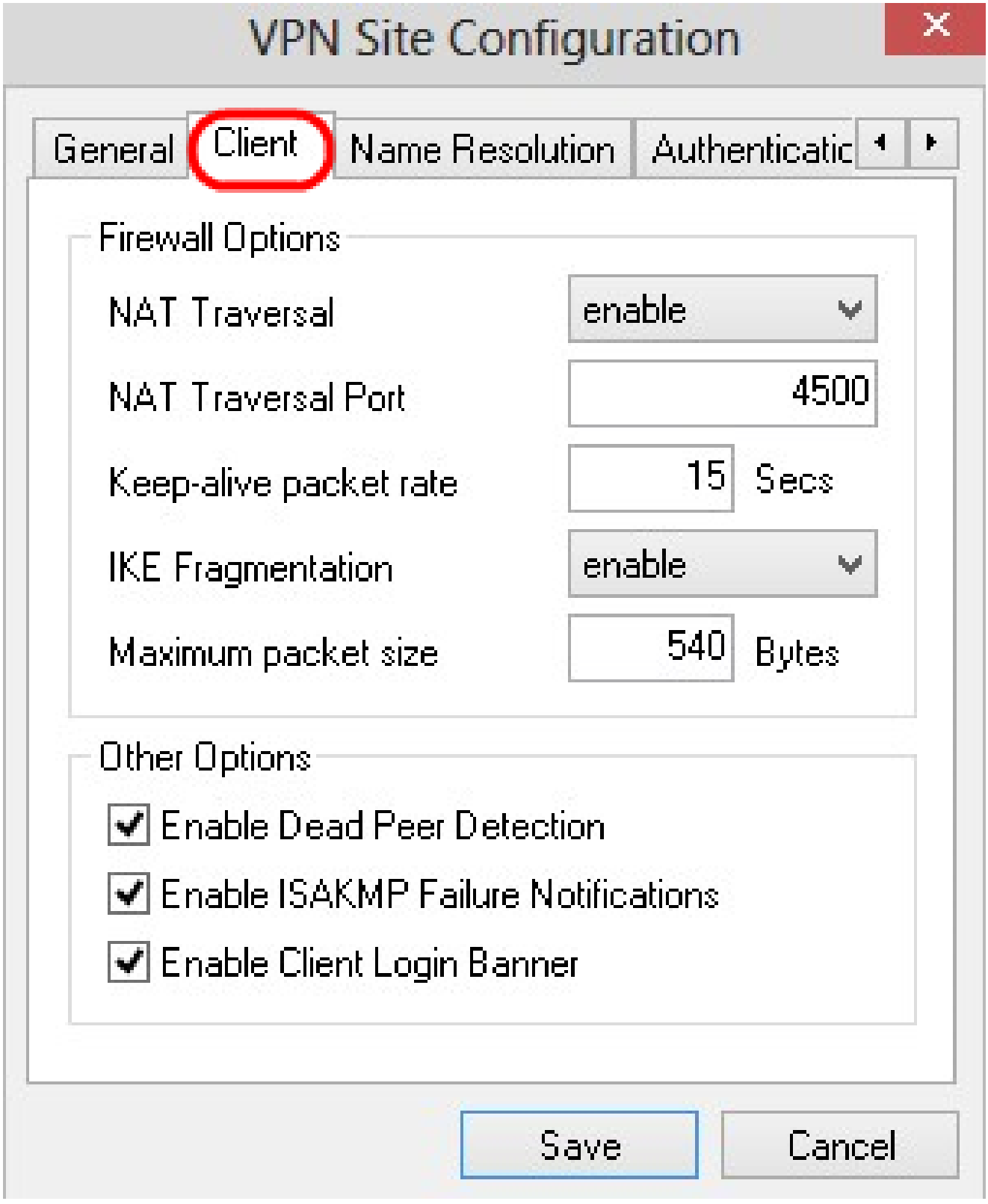
步驟 9.如果從步驟5的Adapter Mode 下拉選單中選擇Use a Virtual Adapter and Assigned Address ，請在Netmask 欄位中輸入遠端客戶端IP地址的子網掩碼。



步驟 10.按一下「Save」以儲存設定。

客戶端配置

步驟 1.按一下Client頁籤。



注意：在客戶端部分，可以配置防火牆選項、失效對等體檢測和ISAKMP（Internet安全關聯和金鑰管理協定）故障通知。這些設定定義手動配置哪些配置選項以及自動獲取哪些配置選項。

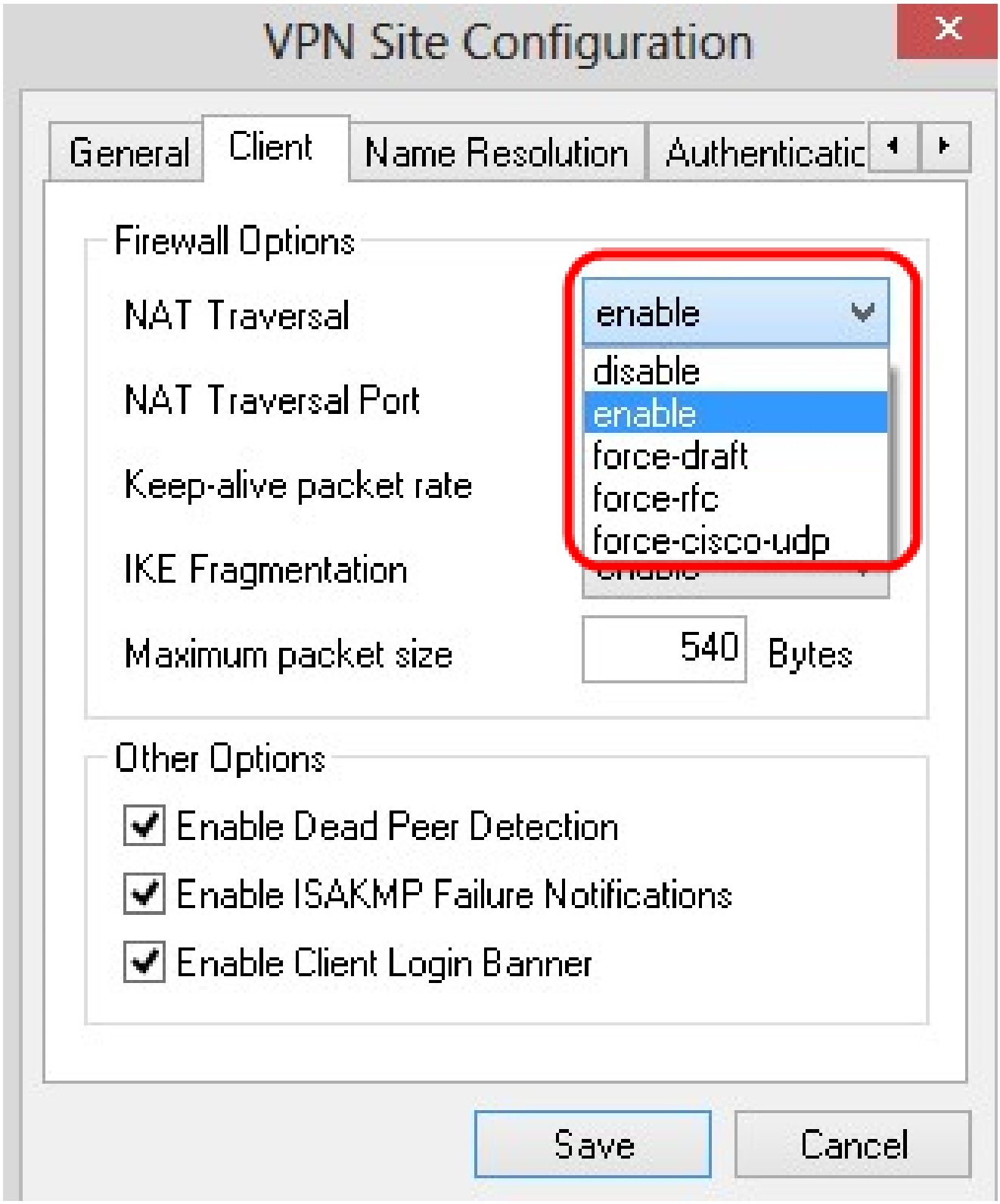
步驟 2.從NAT Traversal下拉選單中選擇適當的NAT（網路地址轉換）遍歷選項。

·禁用 — NAT協定已禁用。

·啟用 — 僅當網關通過協商指示支援時才使用IKE分段。

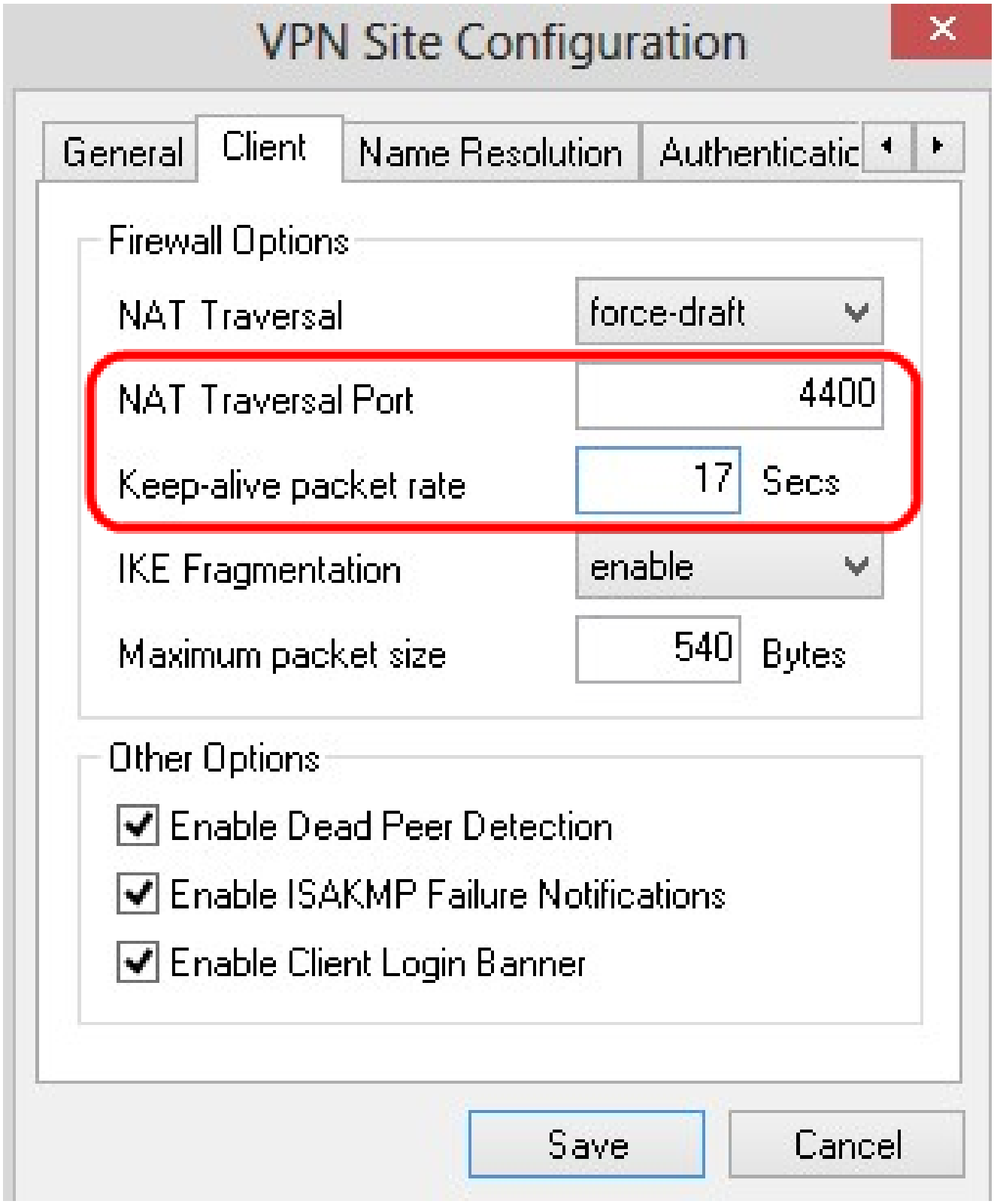
·強制草稿 — NAT協定的草稿版本。如果網關通過協商或檢測NAT來指示支援，則使用此命令。

·強制RFC - NAT協定的RFC版本。如果網關通過協商或檢測NAT來指示支援，則使用此命令。



步驟 3.在NAT Traversal Port欄位中輸入NAT的UDP埠。預設值為 4500。

步驟 4.在「Keep-alive packet rate」欄位中，輸入傳送保持連線封包的速率值。該值以秒為單位。預設值為 30 秒.

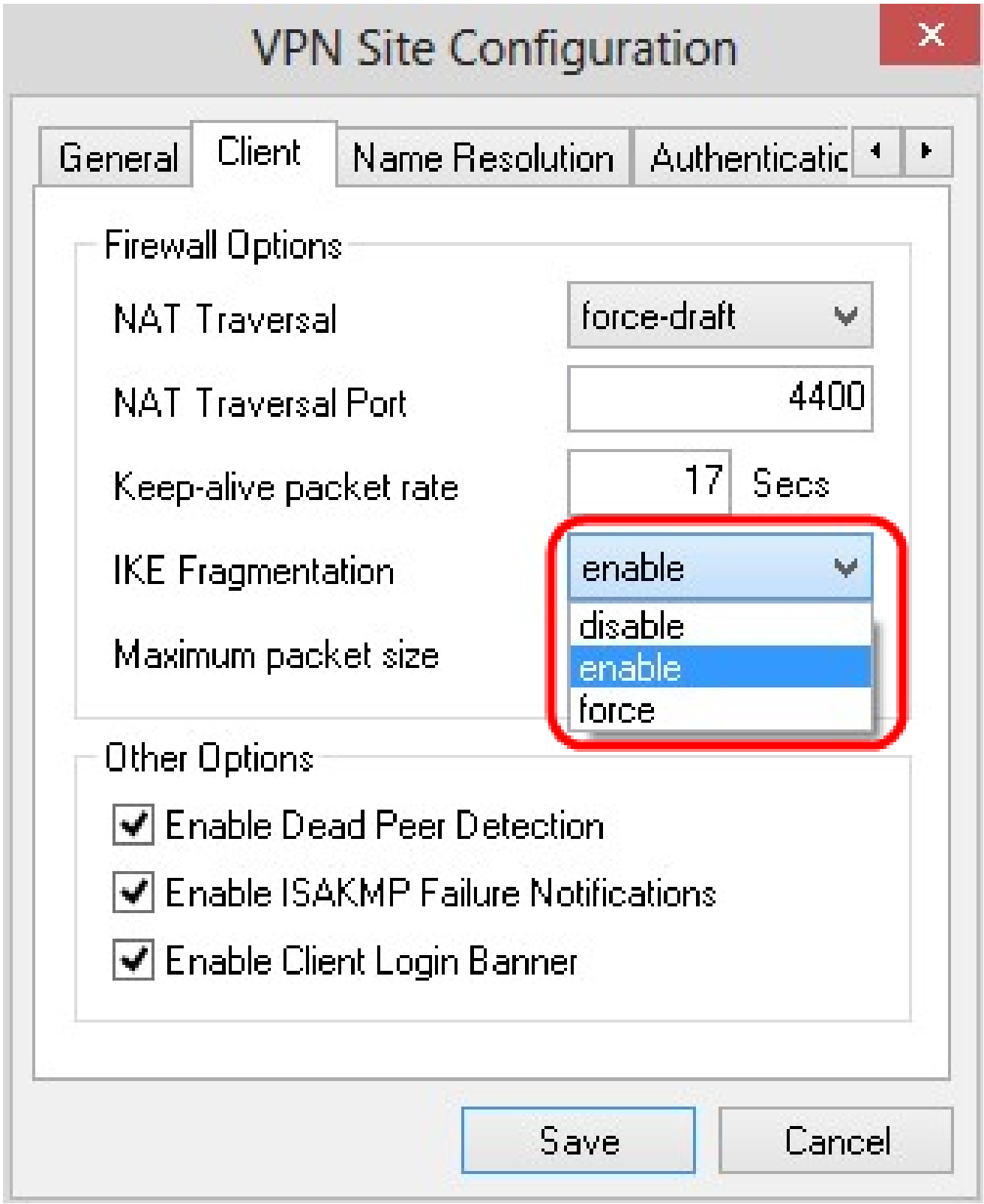


步驟 5.在IKE Fragmentation下拉清單中，選擇適當的選項。

·禁用 — 不使用IKE分段。

·啟用 — 僅當網關通過協商指示支援時才使用IKE分段。

·強制 — 無論指示或檢測如何，都使用IKE分段。



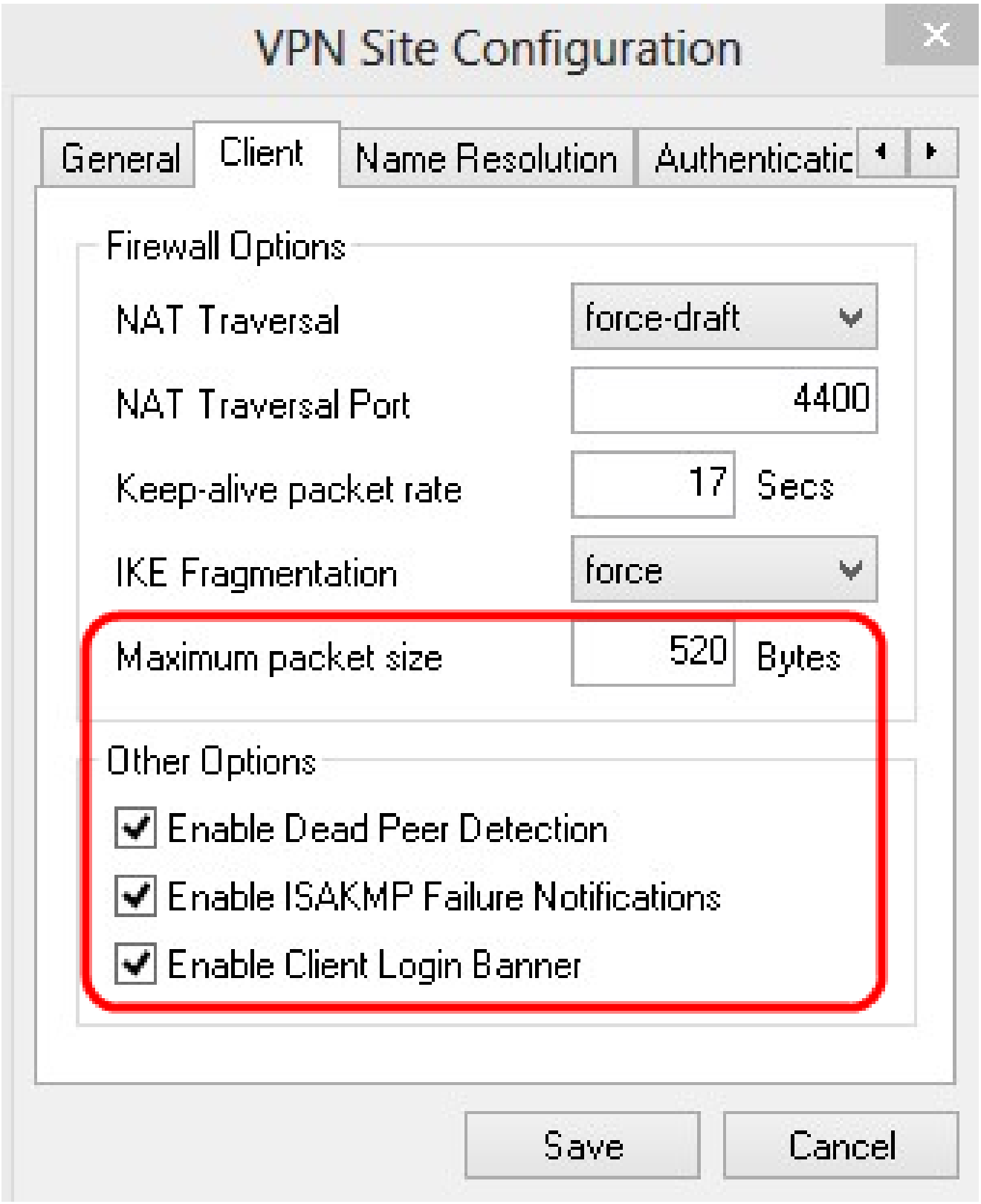
步驟 6.在Maximum packet size欄位中（以位元組為單位）輸入最大資料包大小。如果封包大小大於最大封包大小，則會執行IKE分段。預設值為540位元組。

步驟7.（可選）若要允許電腦和客戶端在另一個無法響應時進行檢測，請選中Enable Dead

Peer Detection覈取方塊。

步驟8.（可選）要通過VPN客戶端傳送故障通知，請選中Enable ISAKMP Failure Notifications覈取方塊。

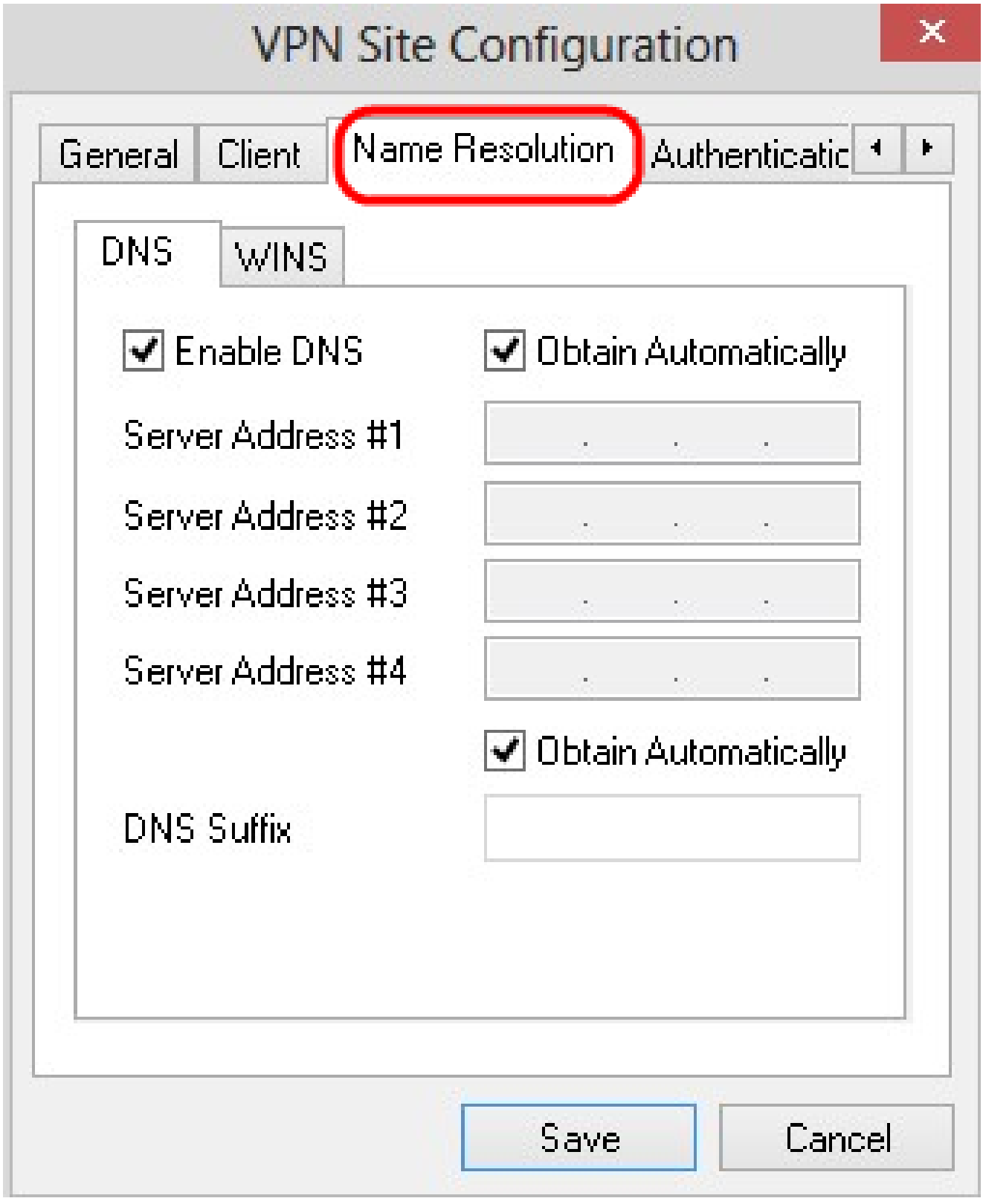
步驟9.（可選）要在與網關建立連線時由客戶端顯示登入橫幅，請選中Enable Client Login 覈取方塊。



步驟 10.按一下「Save」以儲存設定。

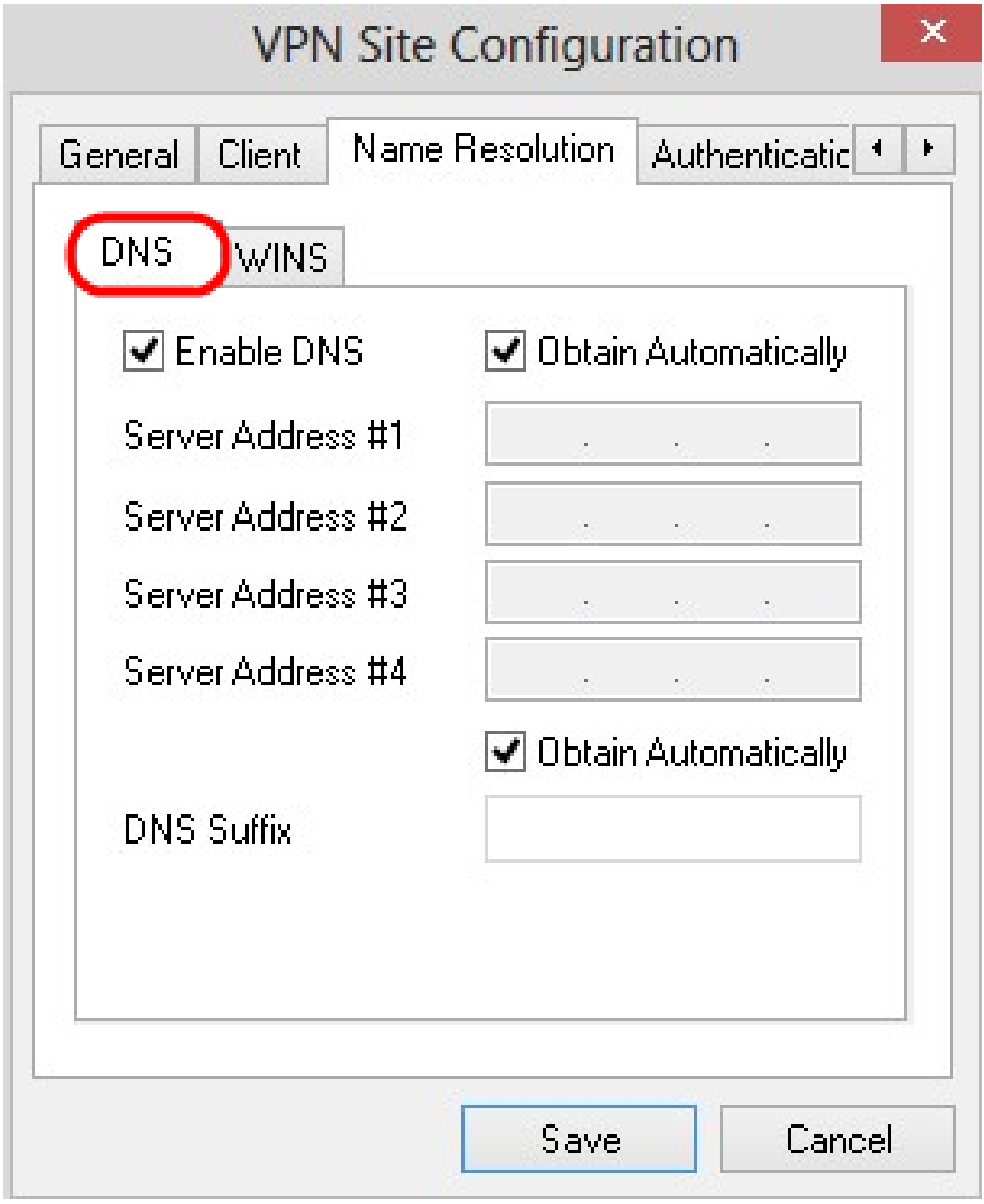
名稱解析配置

步驟 1.按一下Name Resolution頁籤。



注意： Name Resolution部分用於配置DNS（域名系統）和WIN（Windows Internet名稱服務）設定。

步驟 2.按一下DNS選項卡。

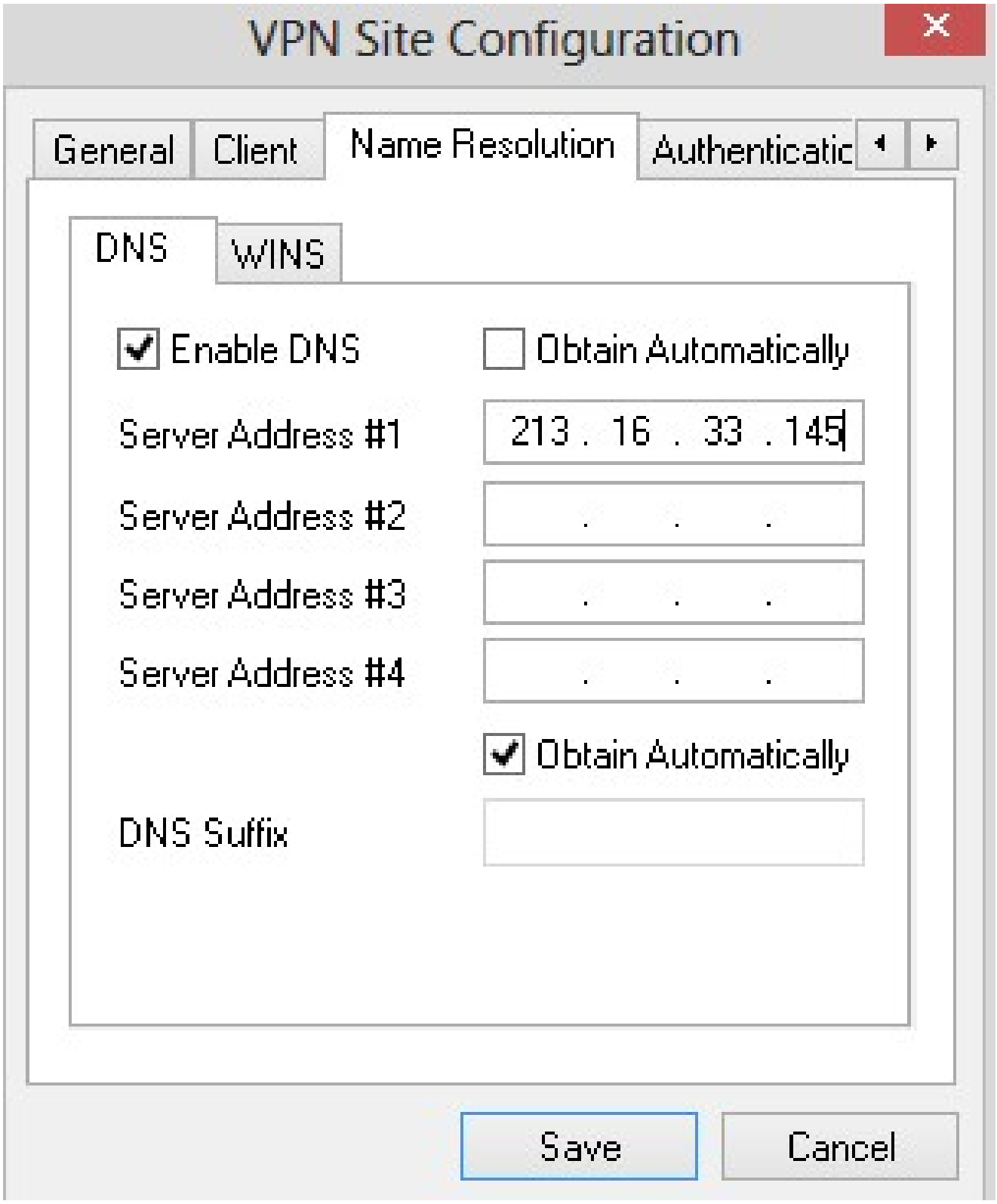


步驟 3.選中Enable DNS以啟用域名系統(DNS)。

步驟4.（可選）若要自動取得DNS伺服器位址，請勾選Obtain Automatically覈取方塊。如果選擇此選項，請跳至步驟6。

步驟 5.在Server Address #1欄位中輸入DNS伺服器地址。如果有其他DNS伺服器，請在其餘

的「伺服器地址」欄位中輸入這些伺服器的地址。

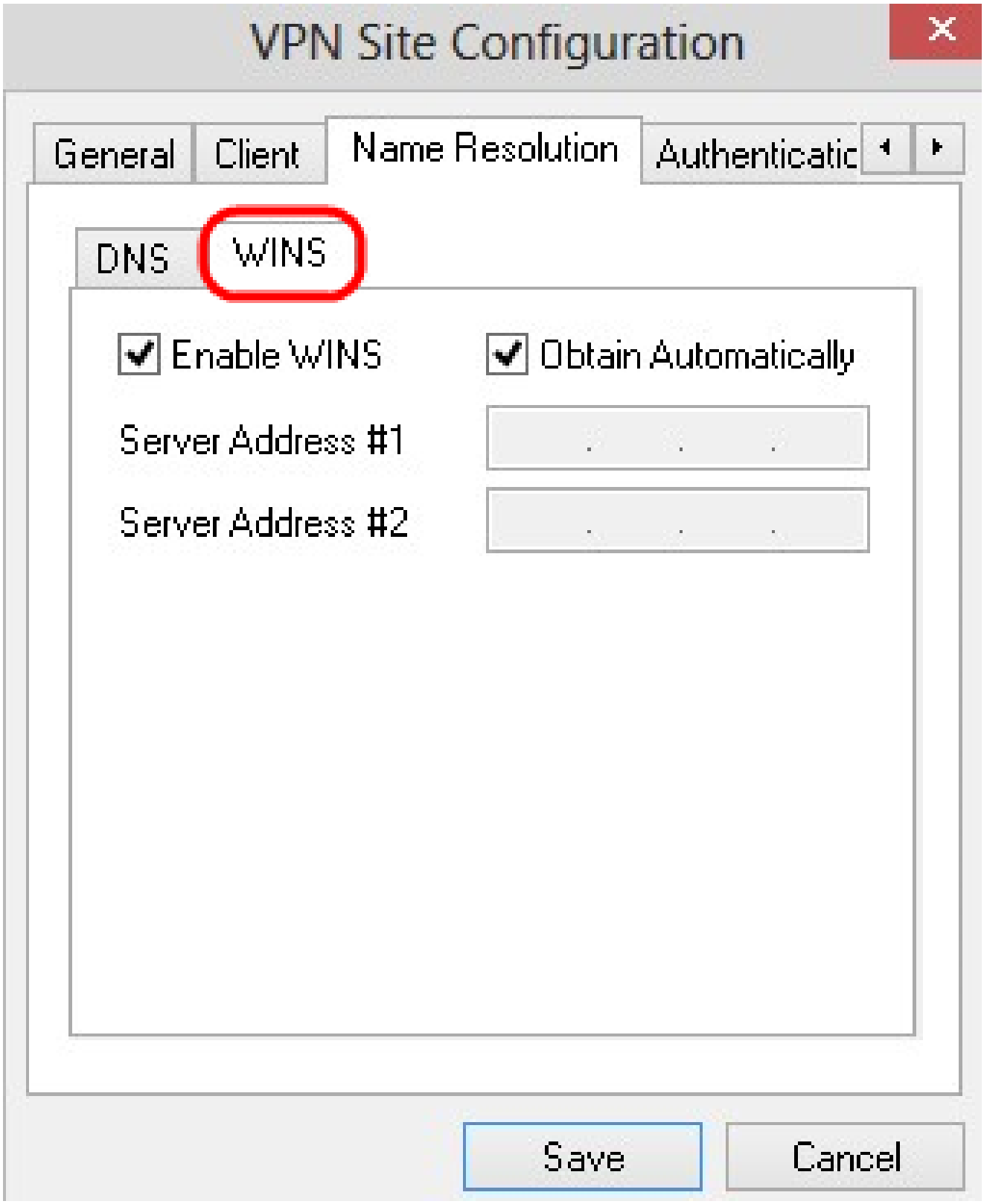


步驟6.（可選）要自動獲取DNS伺服器的字尾，請選中Obtain Automatically覈取方塊。如果選擇此選項，請跳至步驟8。

步驟 7.在「DNS字尾」欄位中輸入DNS服務器的字尾。

步驟 8.按一下「Save」以儲存設定。

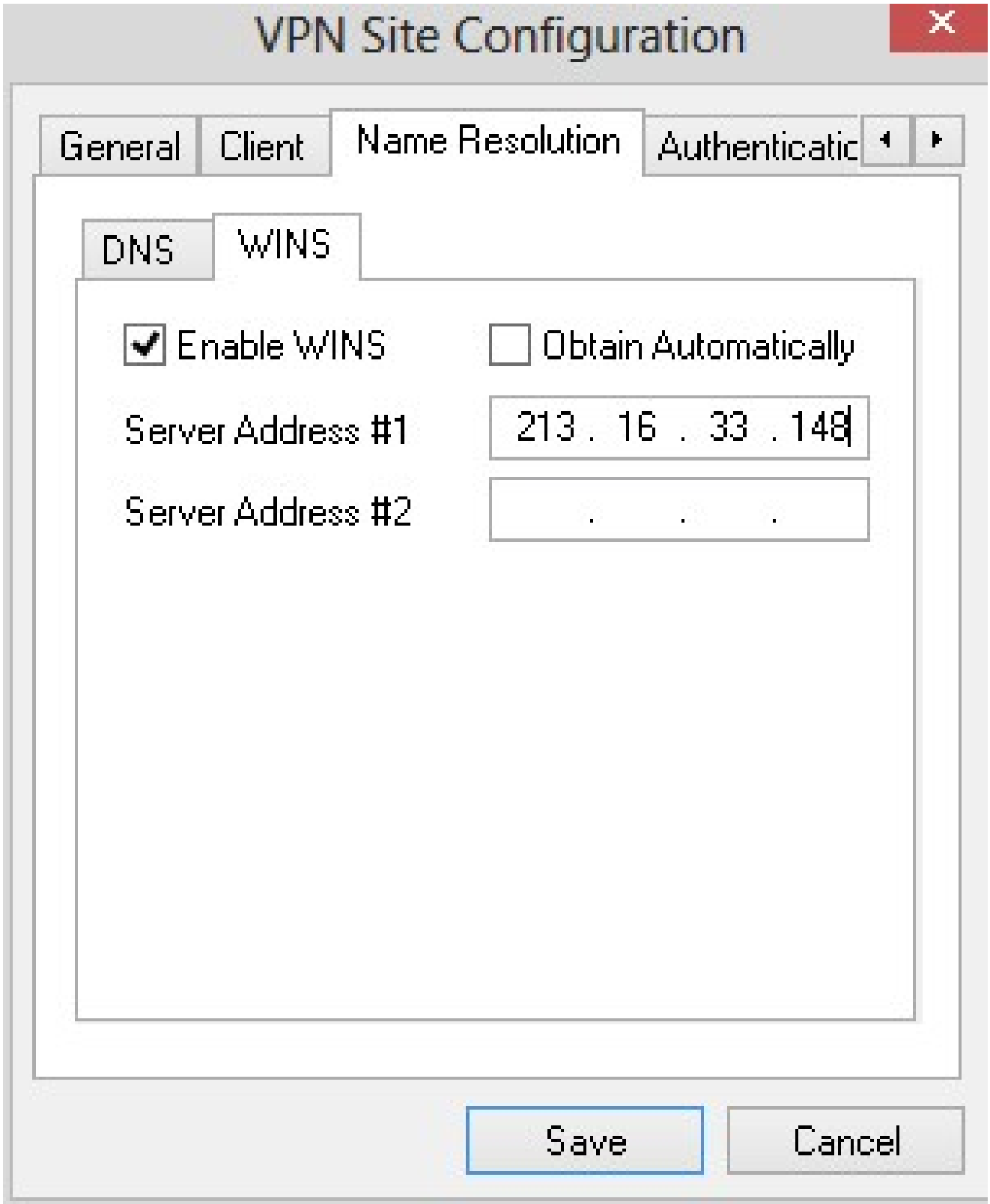
步驟 9.按一下WINS頁籤。



步驟 10.選中Enable WINS以啟用Windows Internet Name Server(WINS)。

步驟11。（可選）要自動獲取DNS伺服器地址，請選中Obtain Automatically覈取方塊。如果選擇此選項，請跳至步驟13。

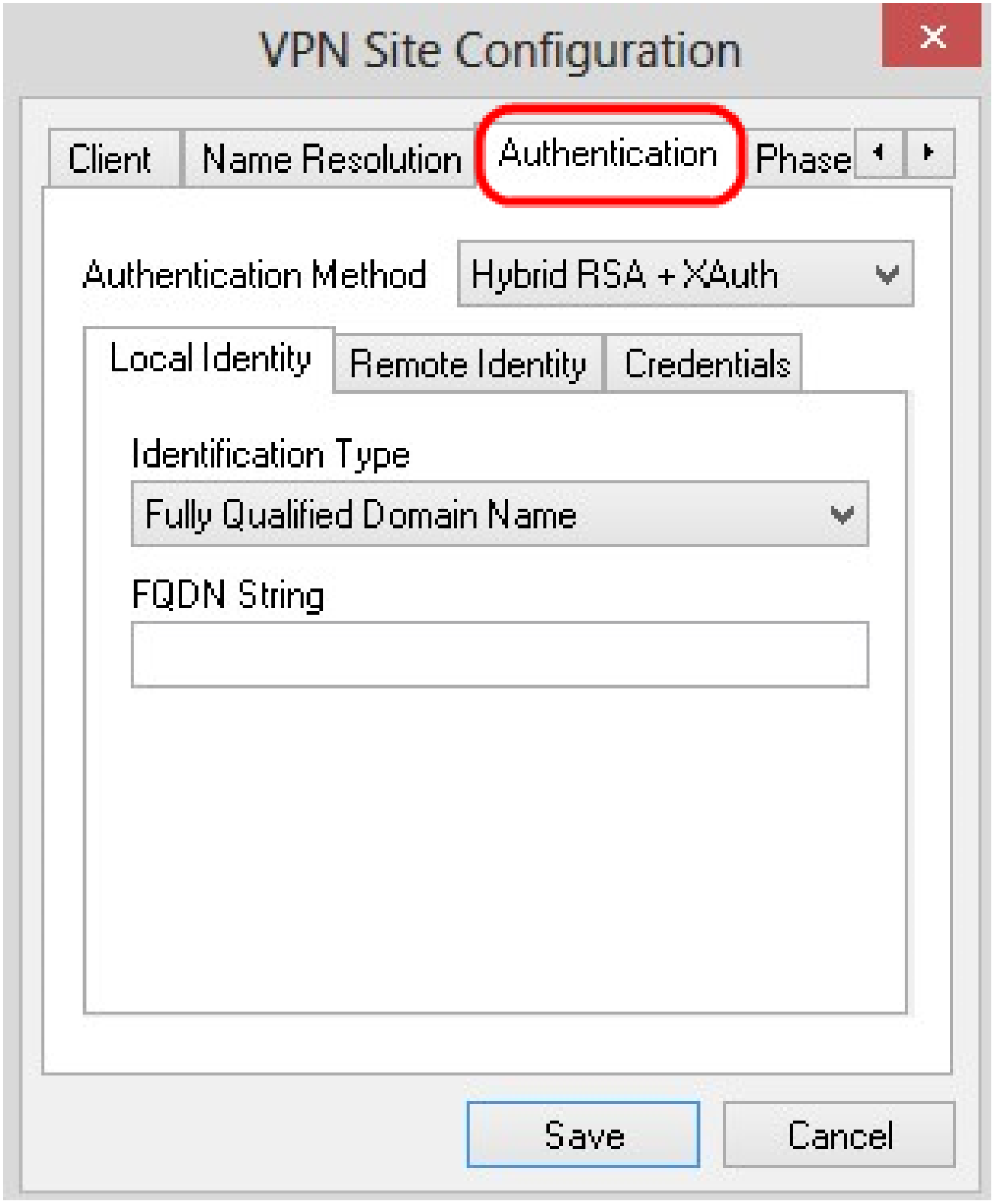
步驟 12.在Server Address #1欄位中輸入WINS伺服器的地址。如果有其他DNS伺服器，在其餘的Server Address欄位中輸入這些服務器的地址。



步驟 13.按一下「Save」以儲存設定。

驗證

步驟 1.按一下Authentication頁籤。



註：在Authentication部分，您可以配置客戶端的引數，使其在嘗試建立ISAKMP SA時處理身份驗證。

步驟 2.從Authentication Method下拉選單中選擇適當的身份驗證方法。

·混合RSA +擴展驗證 — 不需要客戶端憑據。使用者端會驗證閘道。憑據將採用PEM或PKCS12證書檔案或金鑰檔案型別的形式。

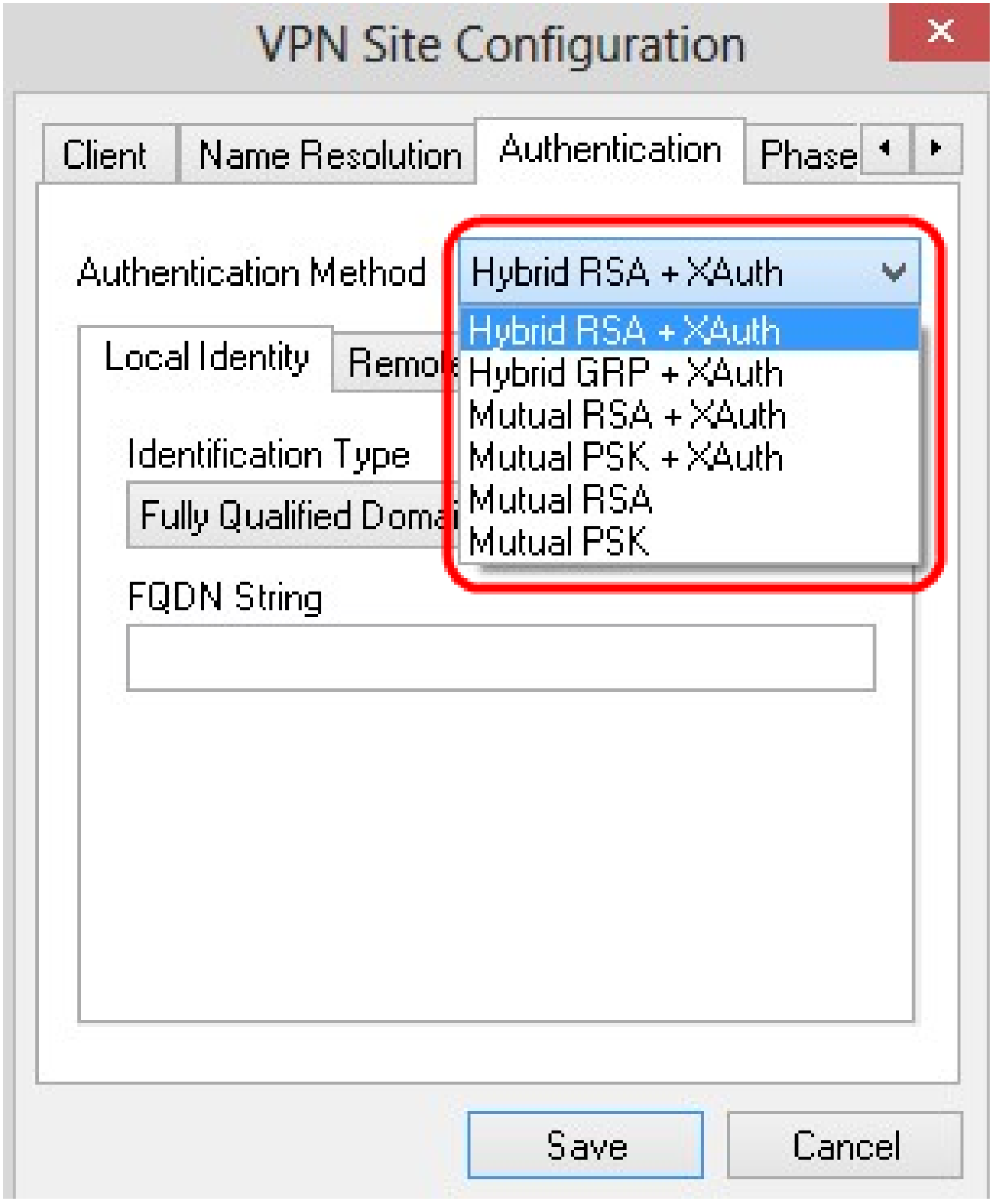
·混合GRP +擴展驗證 — 不需要客戶端憑據。使用者端會驗證閘道。憑證將採用PEM或PKCS12證書檔案和共用金鑰字串的形式。

·雙方RSA +擴展驗證 — 客戶端和網關都需要憑證進行身份驗證。憑證將採用PEM或PKCS12證書檔案或金鑰型別的形式。

·雙方PSK +擴展驗證 — 客戶端和網關都需要憑證進行身份驗證。憑據將採用共用金鑰字串的形式。

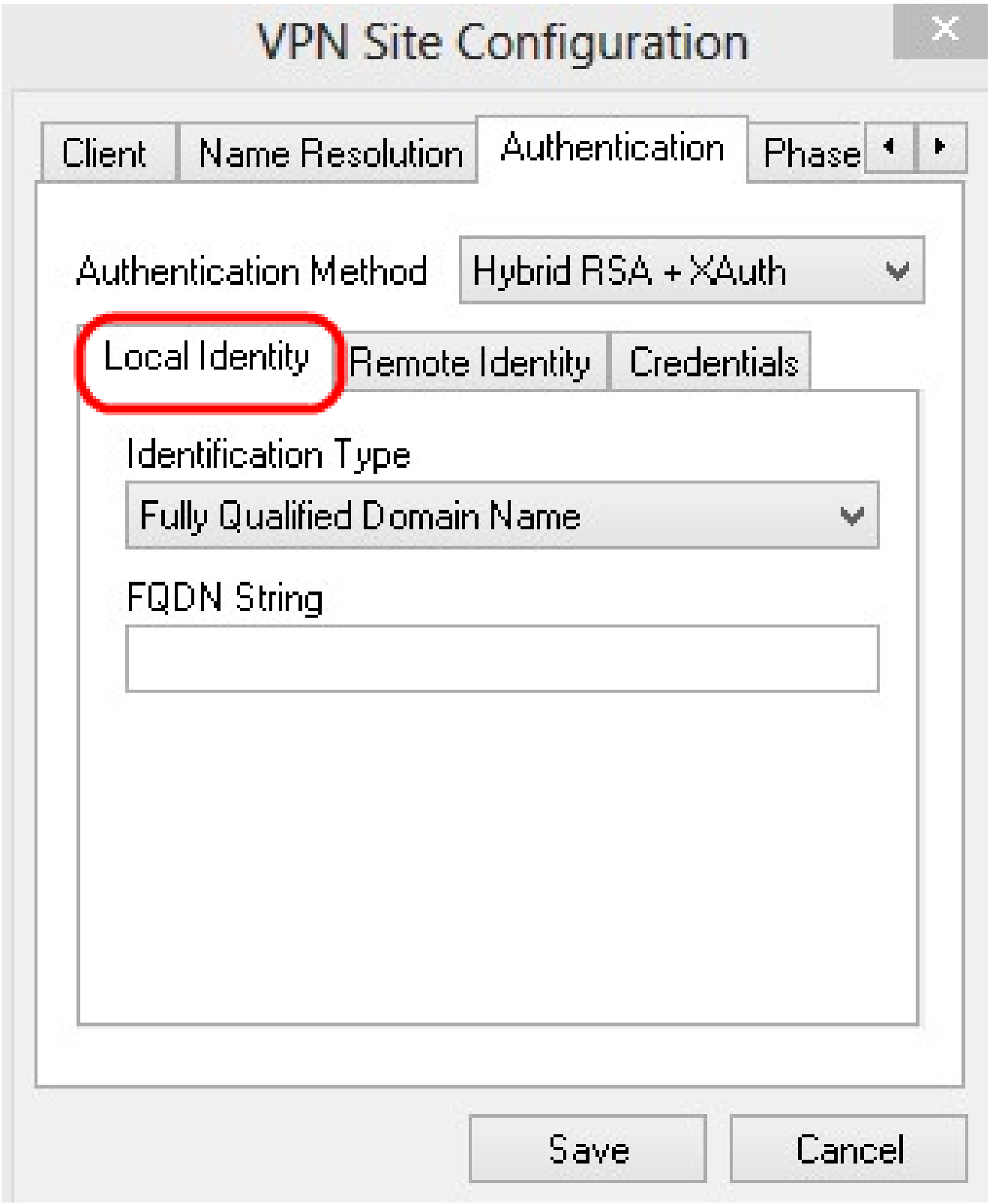
·雙方RSA — 客戶端和網關都需要憑證進行身份驗證。憑證將採用PEM或PKCS12證書檔案或金鑰型別的形式。

·雙向PSK — 客戶端和網關都需要憑證進行身份驗證。憑據將採用共用金鑰字串的形式。



本地身份配置

步驟 1.按一下Local Identity頁籤。



注意：本地身份設定傳送到網關進行驗證的ID。在Local Identity部分中，配置標識型別和FQDN（完全限定域名）字串以確定ID的傳送方式。

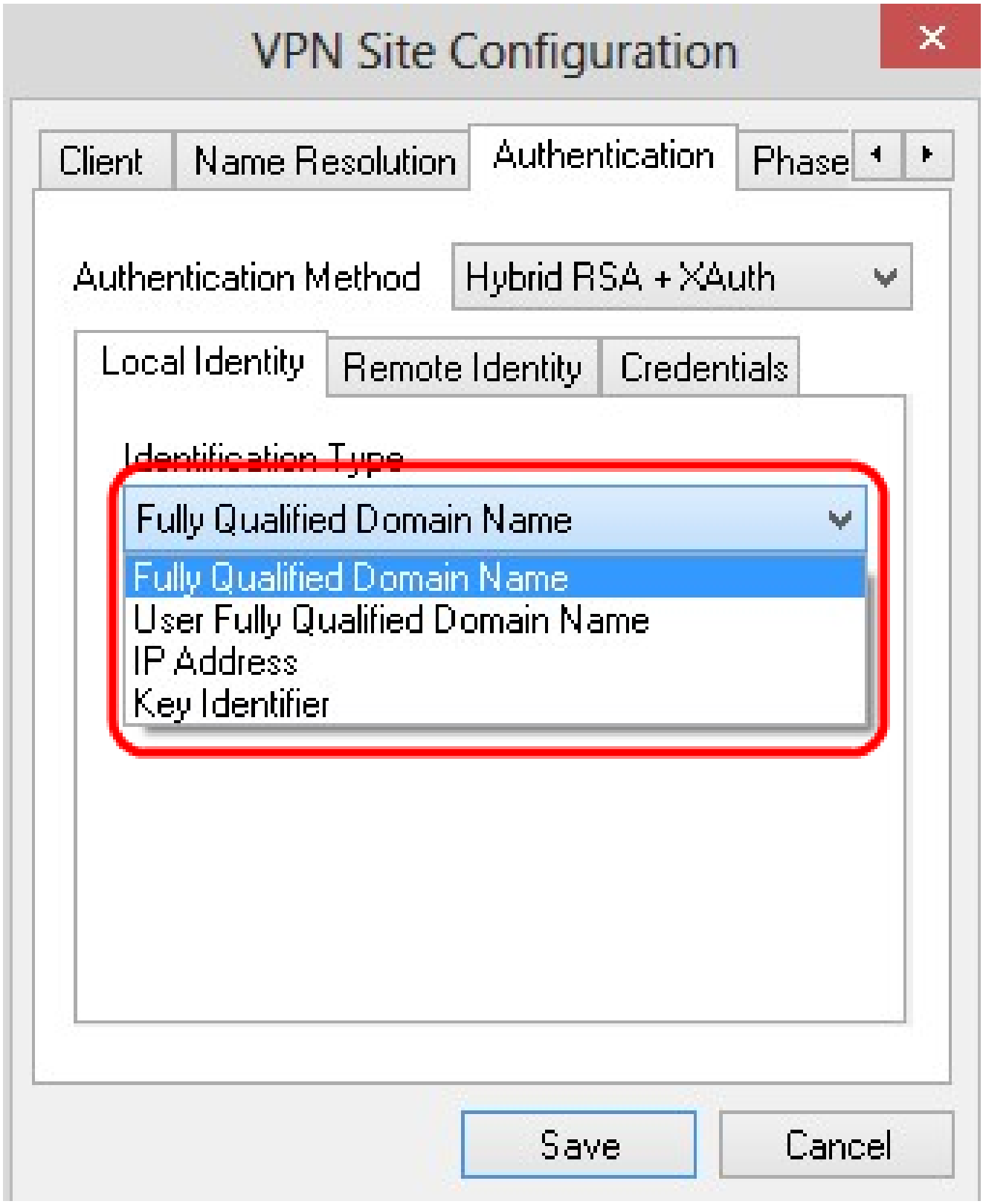
步驟 2.從Identification Type下拉選單中選擇相應的標識選項。並非所有選項對所有身份驗證模式都可用。

·完全限定域名 — 本地標識的客戶端標識基於完全限定域名。如果選擇此選項，請執行步驟3，然後跳至步驟7。

·使用者完全限定域名 — 本地身份的客戶端標識基於使用者完全限定域名。如果選擇此選項，請執行步驟4，然後跳至步驟7。

· IP地址 — 本地身份的客戶端標識基於IP地址。如果選中Use a discovered local host address，將自動發現IP地址。如果選擇此選項，請執行步驟5，然後跳至步驟7。

·金鑰識別符號 — 基於金鑰識別符號標識本地客戶端的客戶端識別符號。如果選擇此選項，請執行步驟6和步驟7。



步驟 3.在FQDN String欄位中輸入完全限定的域名作為DNS字串。

步驟 4.在UFQDN String欄位中輸入使用者完全限定的域名作為DNS字串。

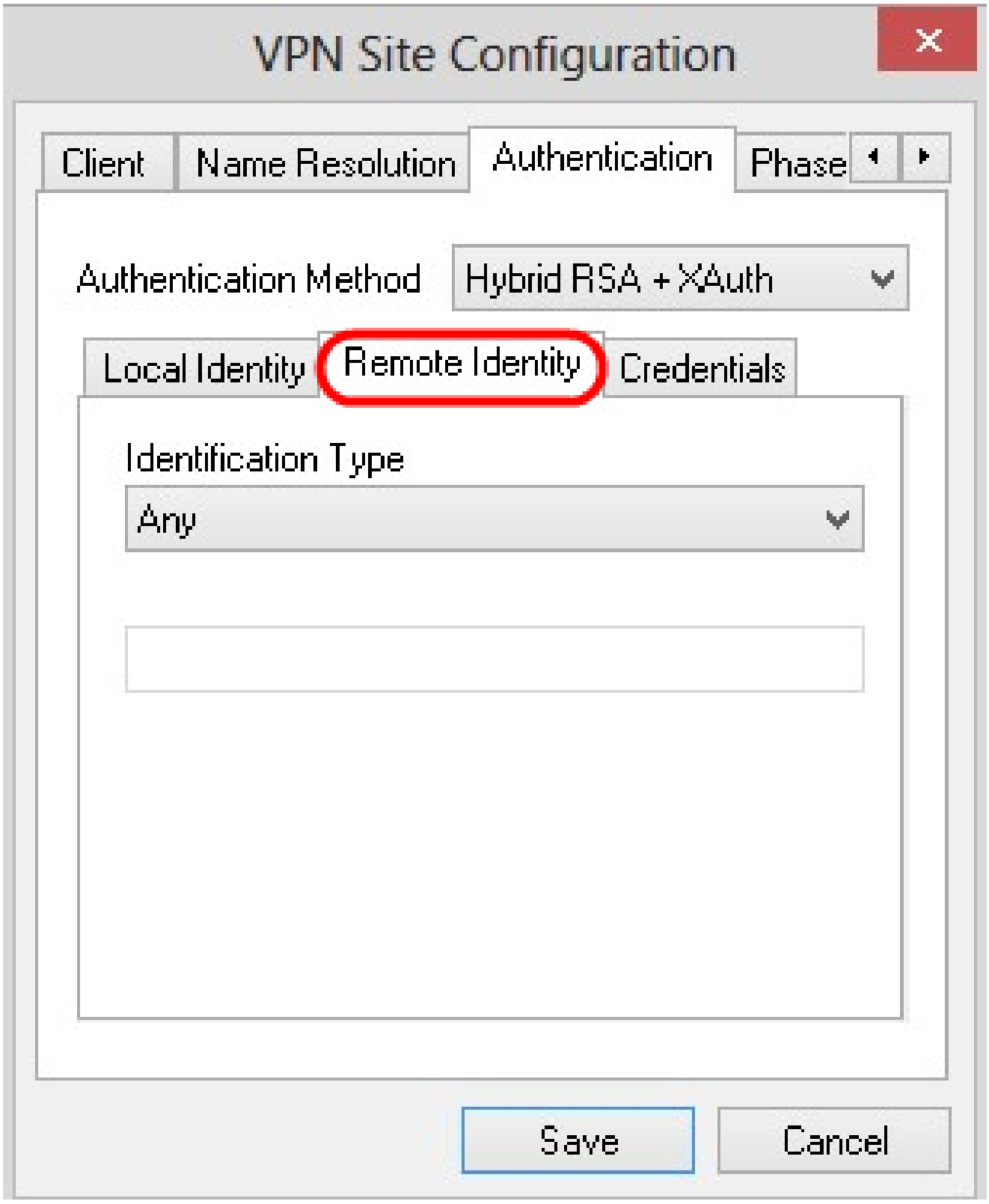
步驟 5.在UFQDN字串欄位中輸入IP地址。

步驟 6.在Key ID String（金鑰ID字串）中輸入用於標識本地客戶端的金鑰識別符號。

步驟 7.按一下「Save」以儲存設定。

遠端身份配置

步驟 1.按一下Remote Identity頁籤。



注意：遠端身份從網關驗證ID。在Remote Identity部分中，將標識型別配置為確定ID的驗證方式。

步驟 2.從Identification Type下拉選單中選擇相應的標識選項。

· Any — 遠端客戶端可以接受任何值或ID進行身份驗證。

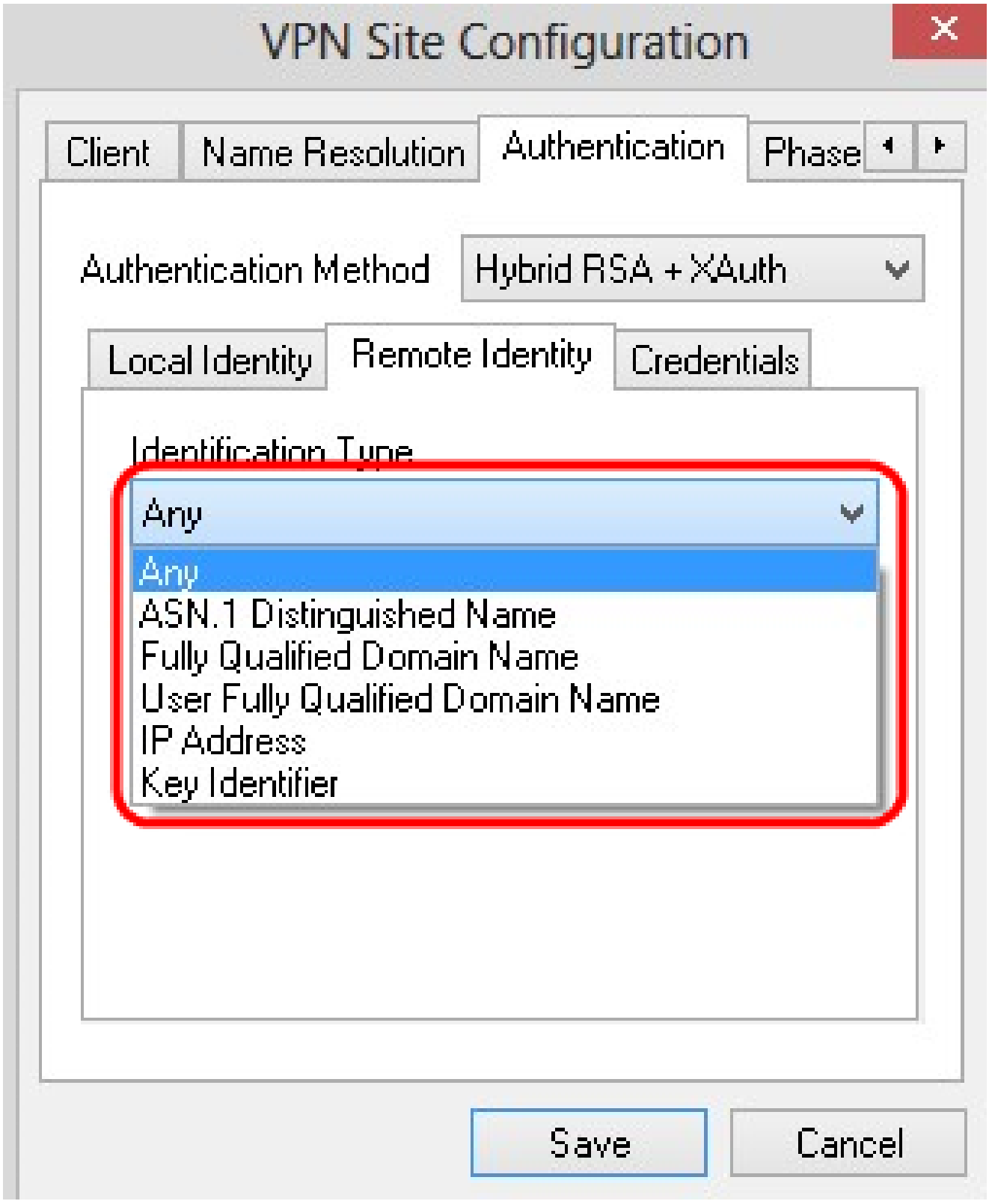
· ASN.1可分辨名稱 — 從PEM或PKCS12證書檔案自動標識遠端客戶端。只有在Authentication一節的步驟2中選擇了RSA身份驗證方法時，才能選擇此選項。選中Use the subject in the received certificate but don't compare it with a specific value覈取方塊以自動接收證書。如果選擇此選項，請執行步驟3，然後跳至步驟8。

·完全限定域名 — 遠端標識的客戶端標識基於完全限定域名。只有在Authentication一節的步驟2中選擇PSK身份驗證方法時，才能選擇此選項。如果選擇此選項，請執行步驟4，然後跳至步驟8。

·使用者完全限定域名 — 遠端身份的客戶端標識基於使用者完全限定域名。只有在Authentication一節的步驟2中選擇PSK身份驗證方法時，才能選擇此選項。如果選擇此選項，請執行步驟5，然後跳至步驟8。

· IP地址 — 遠端身份的客戶端標識基於IP地址。如果選中Use a discovered local host address，將自動發現IP地址。如果選擇此選項，請執行步驟6，然後跳至步驟8。

·金鑰識別符號 — 基於金鑰識別符號來標識遠端客戶端的客戶端識別符號。如果選擇此選項，請執行步驟7和步驟8。



步驟 3.在ASN.1 DN字串欄位中輸入ASN.1 DN字串。

步驟 4.在FQDN String欄位中輸入完全限定的域名作為DNS字串。

步驟 5.在UFQDN字串欄位中輸入使用者完全限定的域名（DNS字串）。

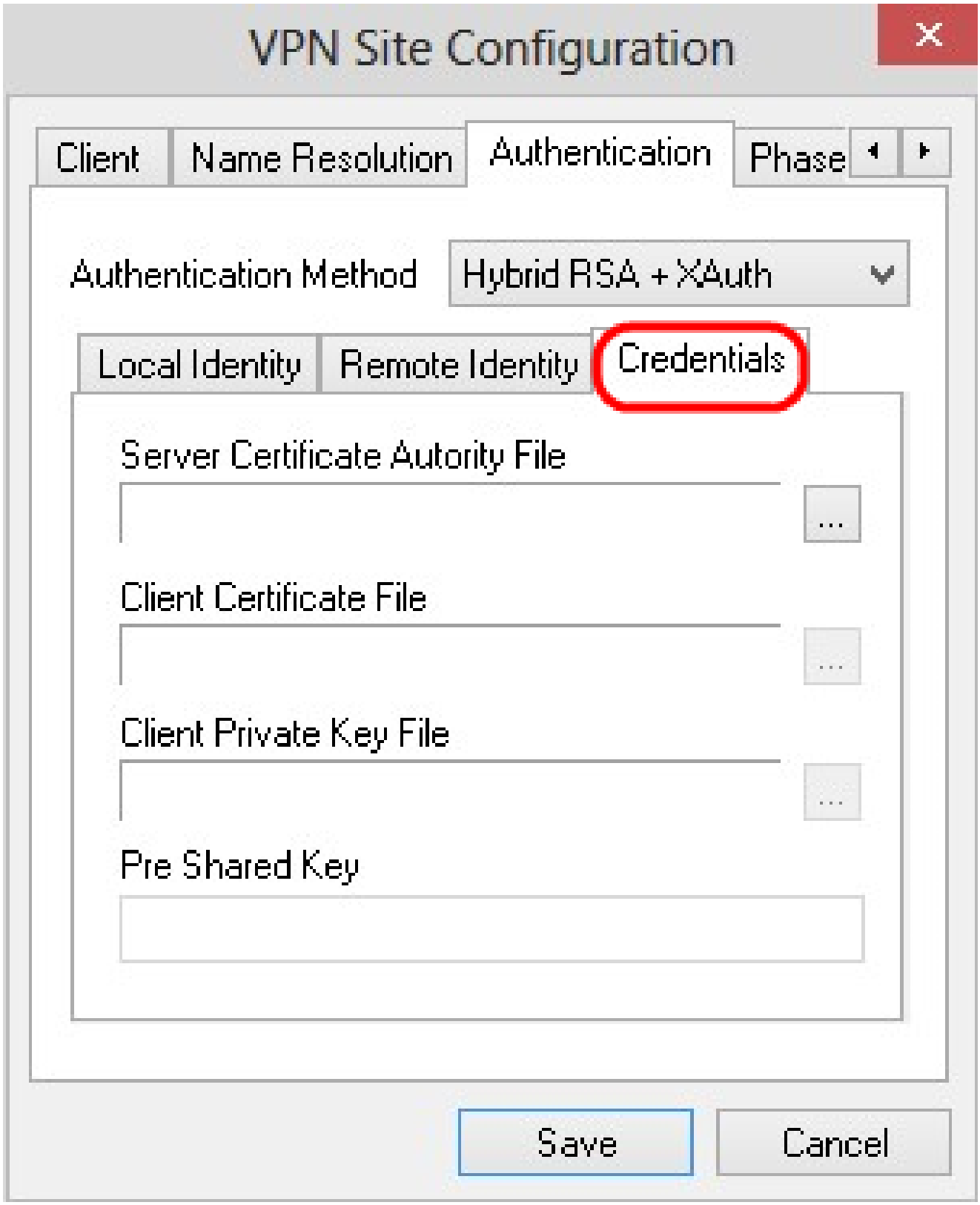
步驟 6.在UFQDN String欄位中輸入IP地址。

步驟 7.在Key ID String欄位中輸入用於標識本地客戶端的金鑰識別符號。

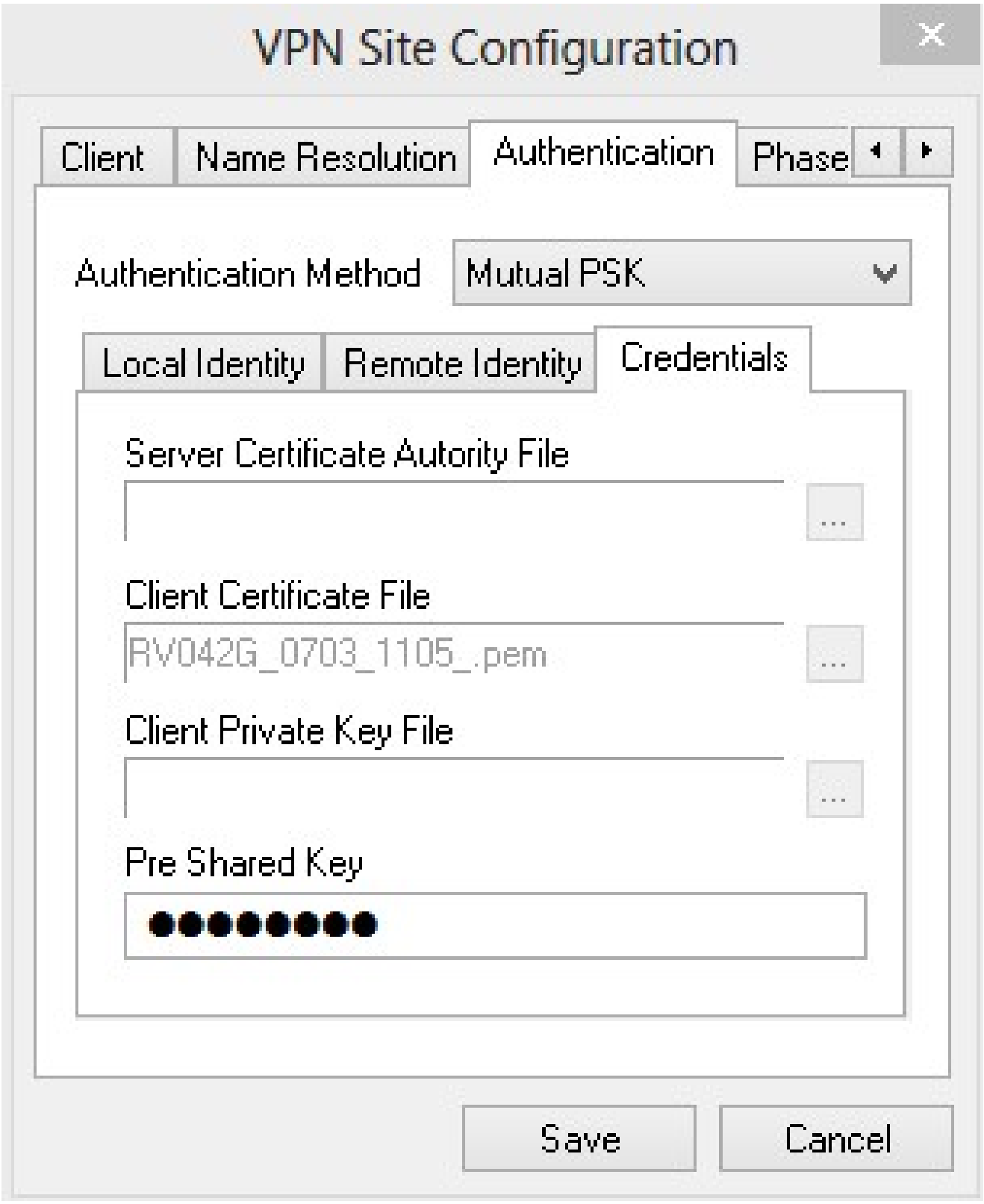
步驟 8.按一下「Save」以儲存設定。

憑證配置

步驟 1.按一下Credentials頁籤。



注意：在Credentials部分，配置預共用金鑰。



步驟 2.要選擇伺服器證書檔案，請按一下Server Certificate Authority File 欄位旁邊的...圖示，然後選擇在PC上儲存伺服器證書檔案的路徑。

步驟 3.要選擇客戶端證書檔案，請按一下客戶端證書檔案欄位旁邊的...圖示，然後選擇在PC上儲存客戶端證書檔案的路徑。

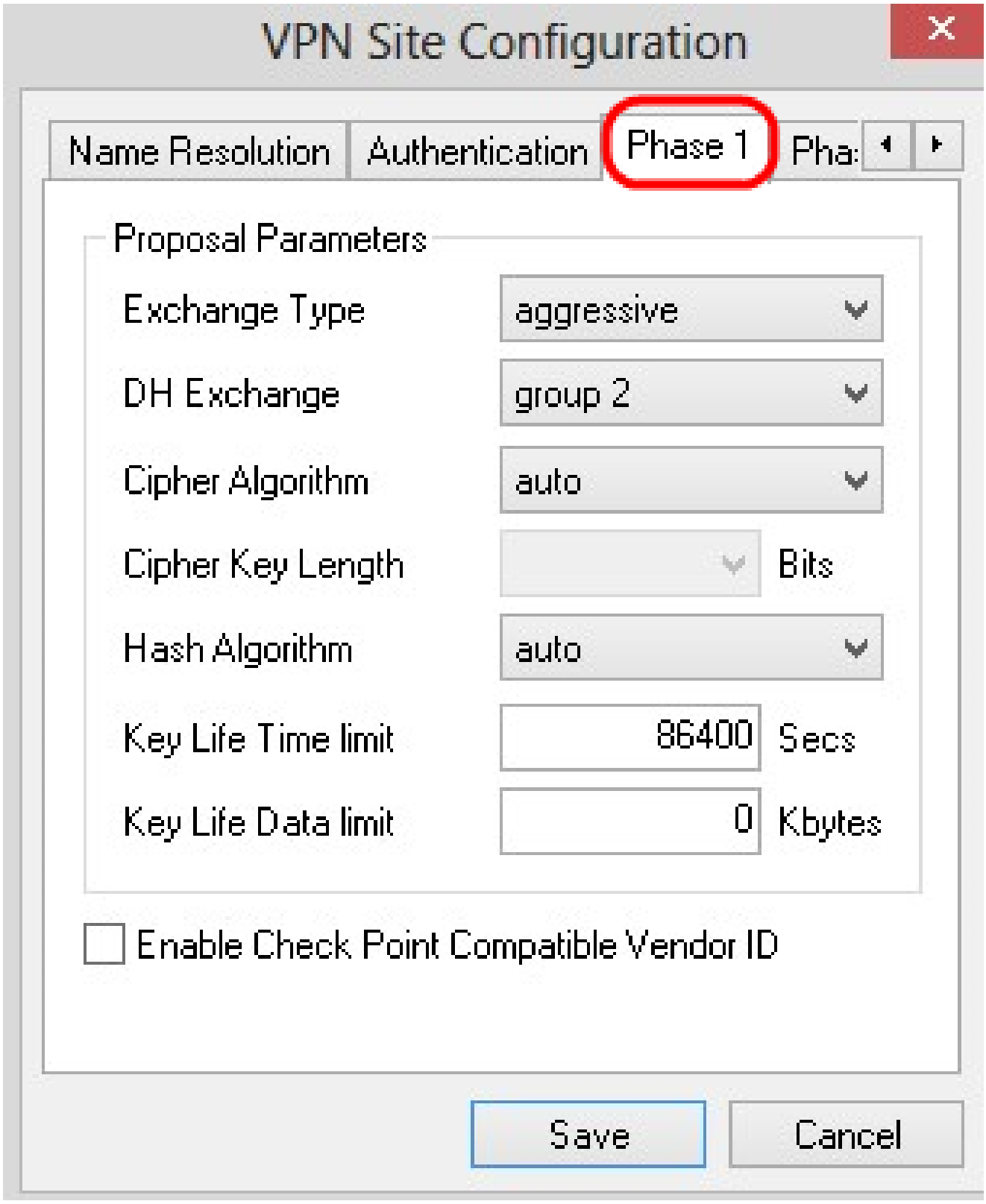
步驟 4. 要選擇客戶端私鑰檔案，請點選客戶端私鑰檔案欄位旁邊的...圖示，然後選擇在PC中儲存客戶端私鑰檔案的路徑。

步驟 5.在PreShared Key欄位中輸入預共用金鑰。此金鑰應與配置隧道時使用的金鑰相同。

步驟 6.按一下「Save」以儲存設定。

第1階段配置

步驟 1.按一下Phase 1頁籤。

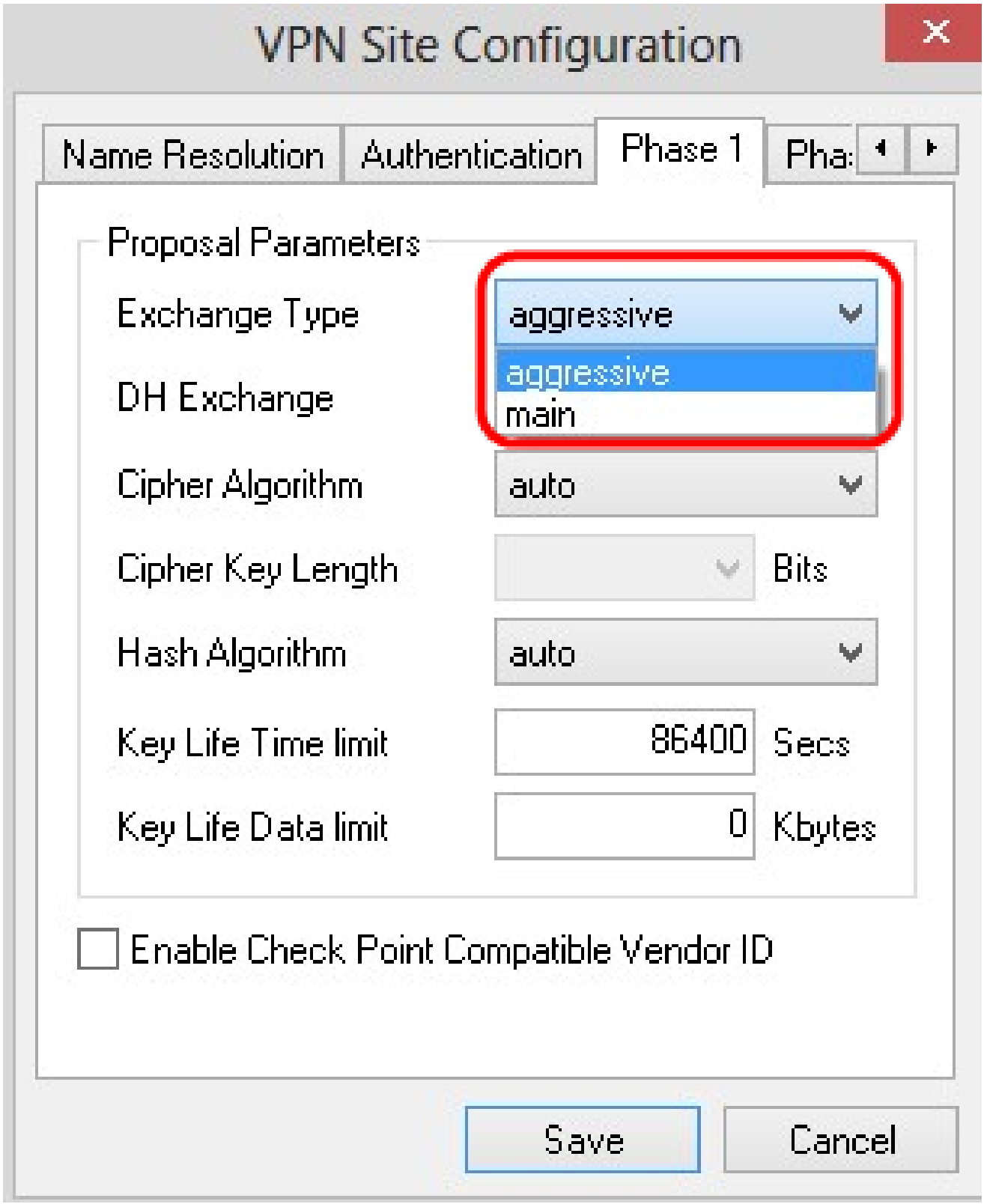


注意：在Phase 1部分，您可以配置引數，以便可以建立帶有客戶端網關的ISAKMP SA。

步驟 2.從Exchange Type下拉選單中選擇適當的金鑰交換型別。

·主要 — 對等體的身份受到保護。

·攻擊性 — 對等體的身份沒有保障。



步驟 3.在DH Exchange下拉選單中，選擇在VPN連線的配置期間選擇的適當組。

步驟 4.在「Cipher Algorithm」下拉選單中，選擇在VPN連線配置期間選擇的適當選項。

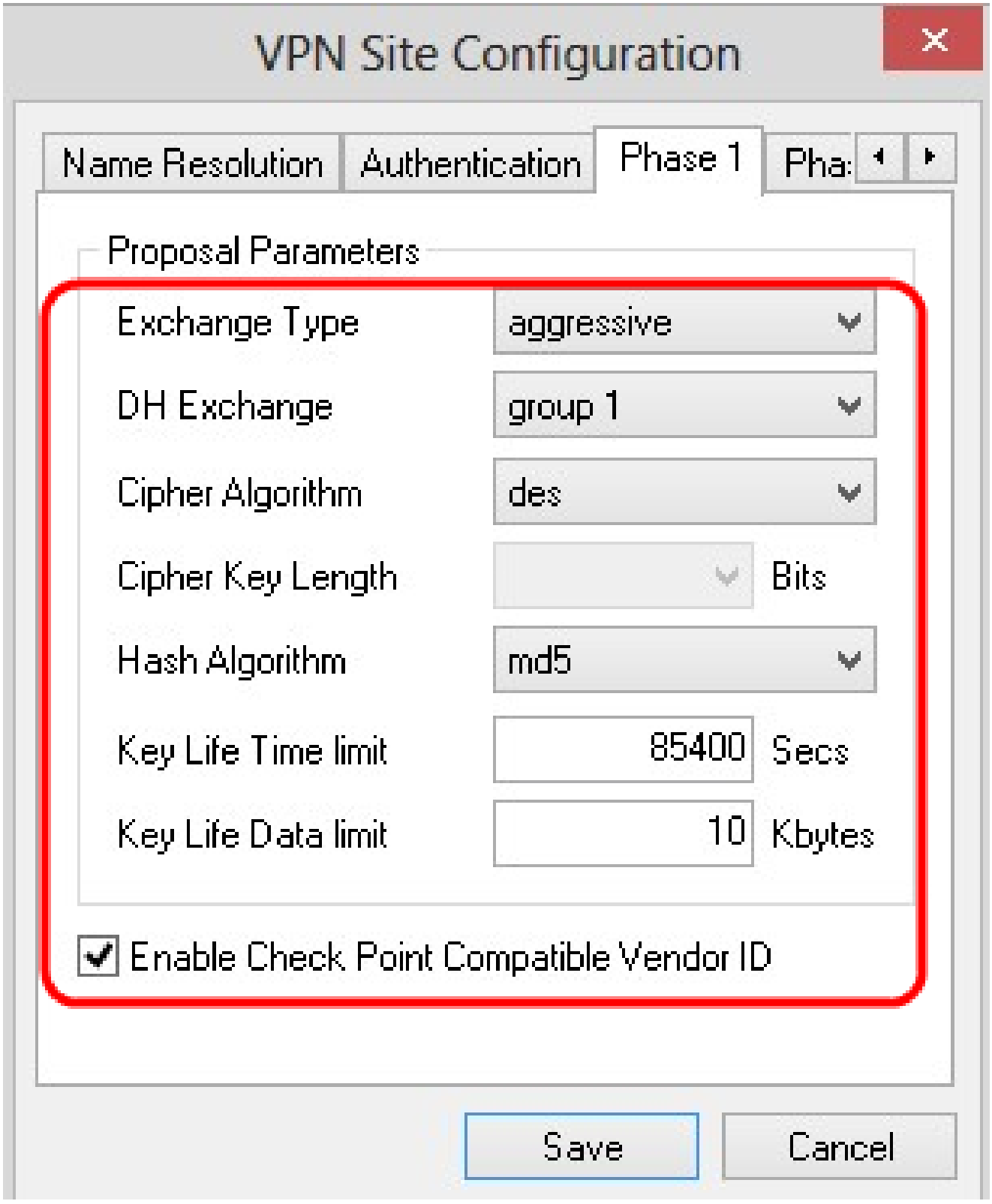
步驟 5.在「Cipher Key Length」下拉選單中，選擇與配置VPN連線期間選擇的選項的金鑰長度匹配的選項。

步驟 6.在「Hash Algorithm」下拉選單中，選擇在配置VPN連線期間選擇的選項。

步驟 7.在Key Life Time limit欄位中，輸入在配置VPN連線時使用的值。

步驟 8.在「關鍵壽命資料限制」欄位中，輸入要保護的值（以千位元組為單位）。預設值為0，表示關閉該功能。

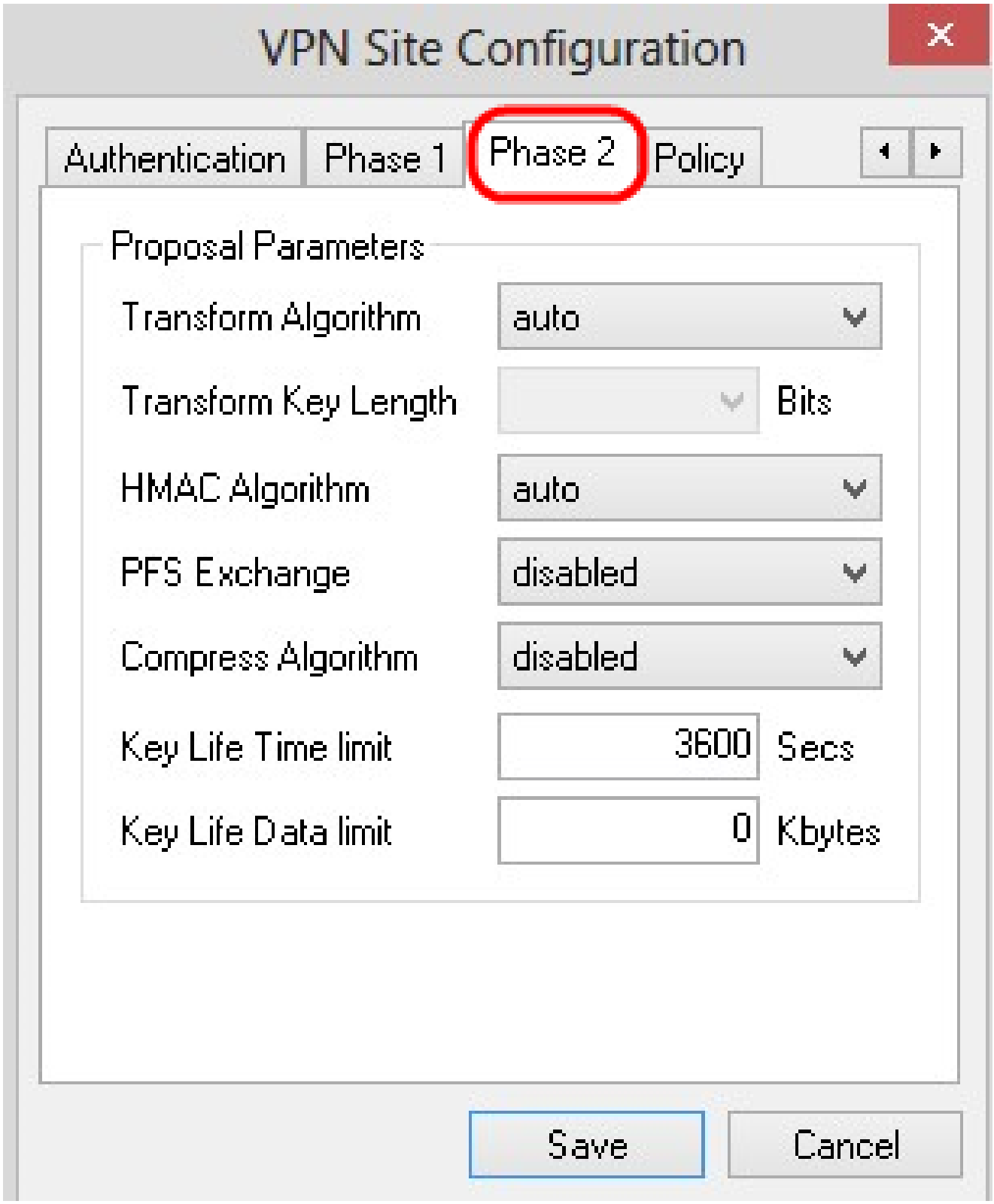
步驟9.（可選）選中Enable Check Point Compatible Vendor ID覈取方塊。



步驟 10.按一下「Save」以儲存設定。

第2階段配置

步驟 1.按一下Phase 2頁籤。



注意：在Phase 2部分，可以配置引數，以便可以建立具有遠端客戶端網關的IPsec SA。

步驟 2.在Transform Algorithm下拉選單中，選擇在配置VPN連線期間選擇的選項。

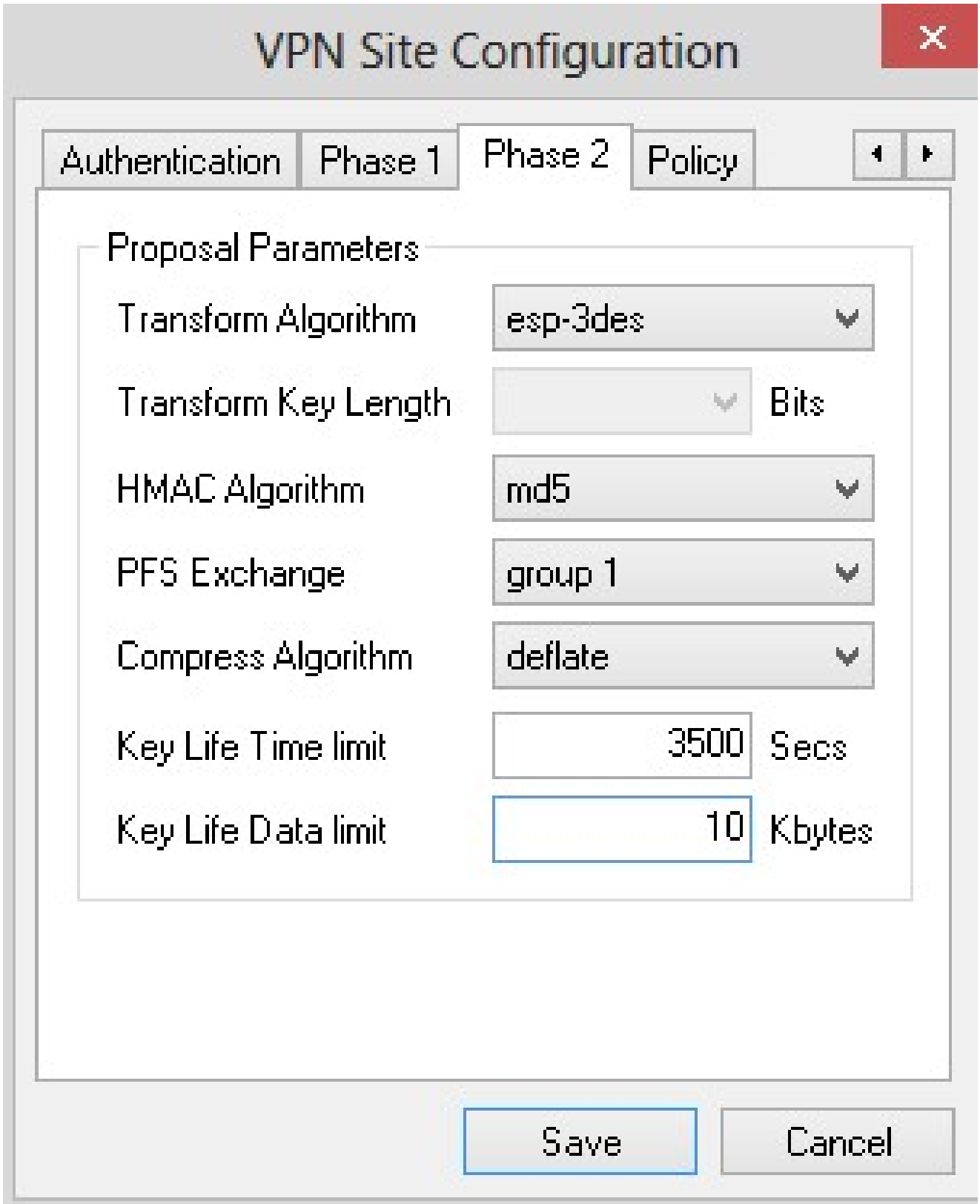
步驟 3.在Transform Key Length下拉選單中，選擇與配置VPN連線期間所選擇的選項的金鑰長度匹配的選項。

步驟 4.在「HMAC Algorithm」下拉選單中，選擇在配置VPN連線期間選擇的選項。

步驟 5.在PFS Exchange下拉選單中，選擇在配置VPN連線期間選擇的選項。

步驟 6.在Key Life Time Limit欄位中，輸入在配置VPN連線期間使用的值。

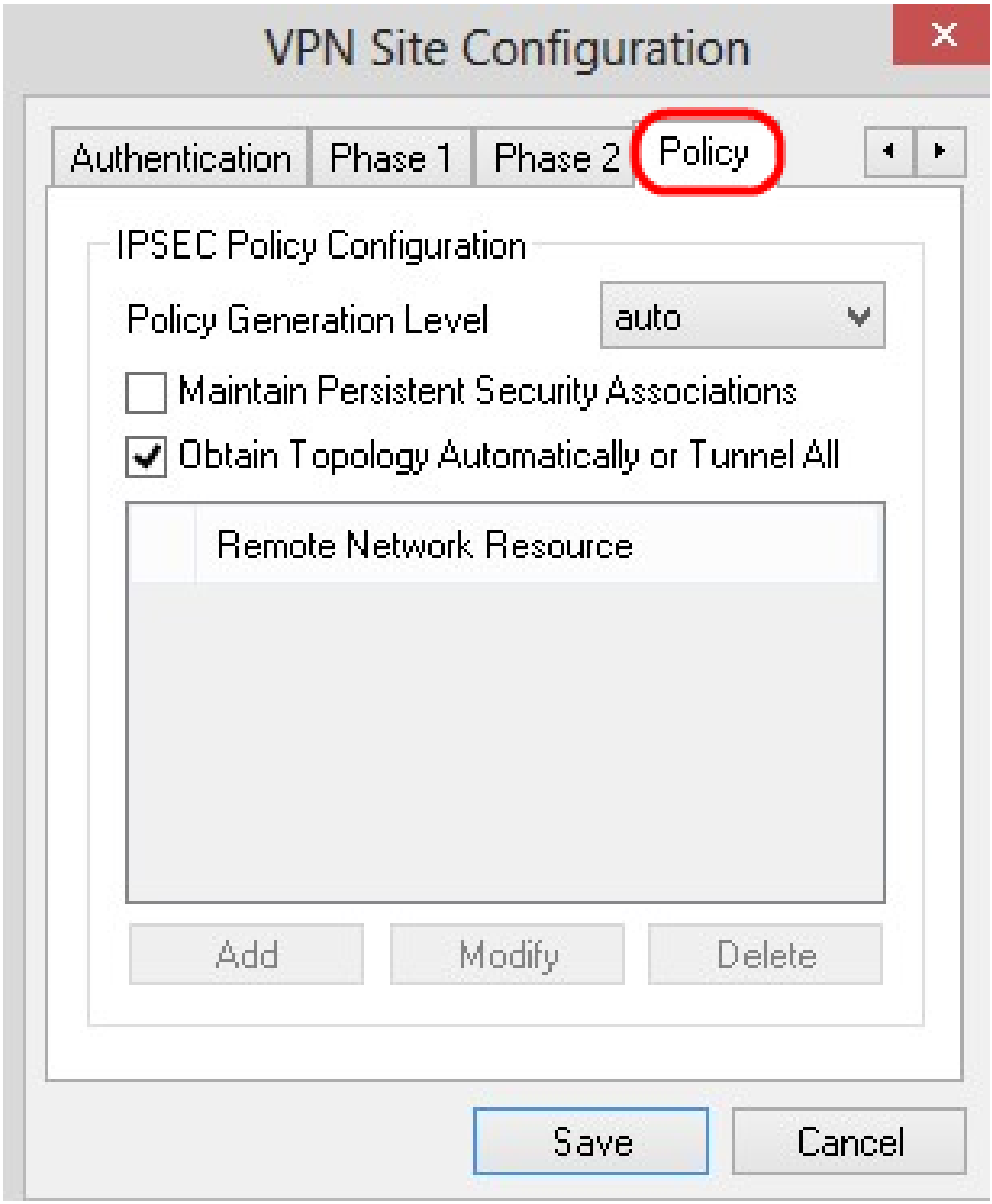
步驟 7.在「Key Life Data limit」欄位中，輸入要保護的值（以千位元組為單位）。預設值為0，表示關閉該功能。



步驟 8.按一下「Save」以儲存設定。

策略配置

步驟1.按一下Policy頁籤。



注意：在Policy部分中定義了IPSEC策略，這是客戶端與主機進行站點配置通訊所必需的。

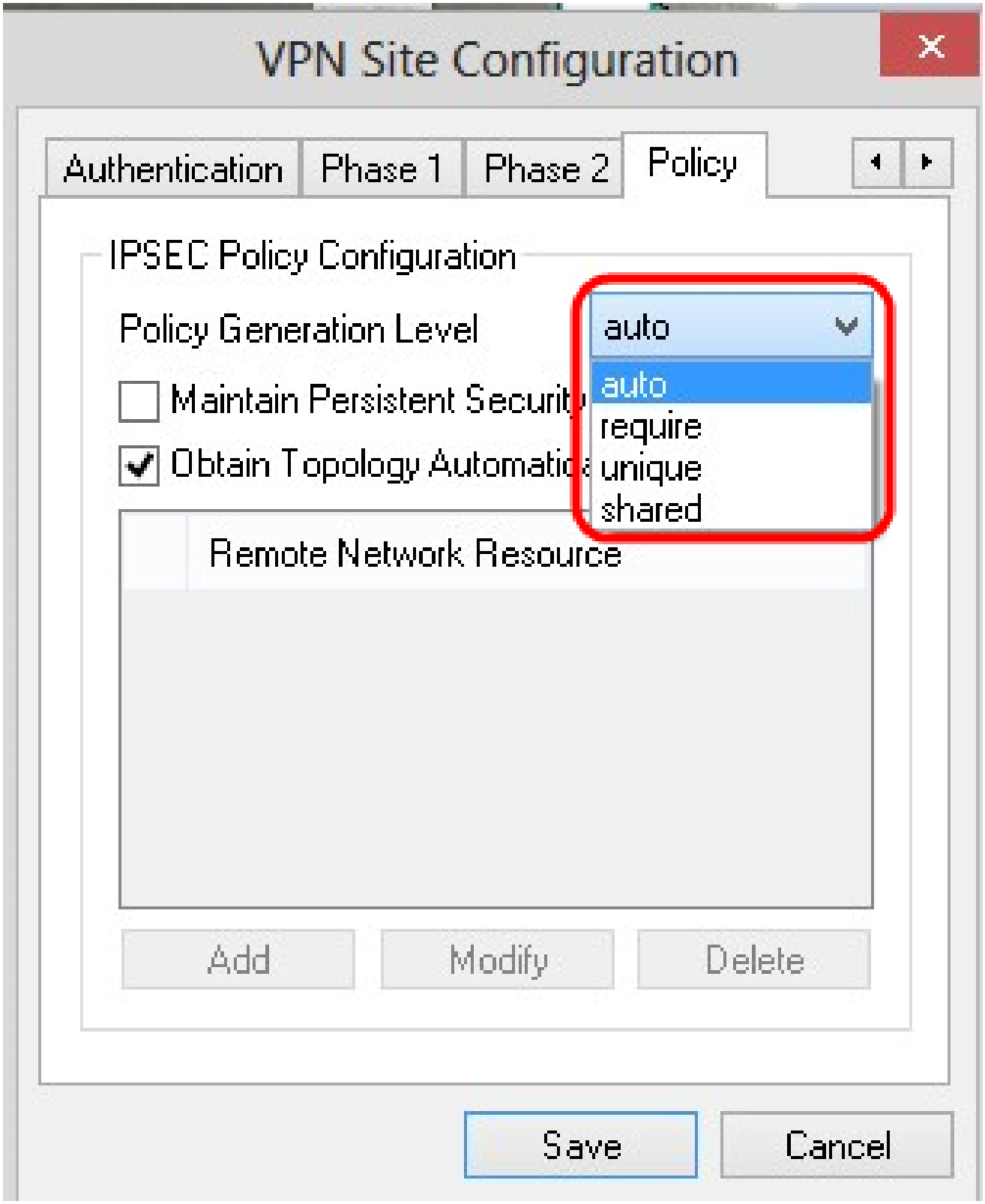
步驟 2.在Policy Generation Level下拉選單中，選擇適當的選項。

·自動 — 自動確定必要的IPsec策略級別。

·要求 — 不會協商每個策略的唯一安全關聯。

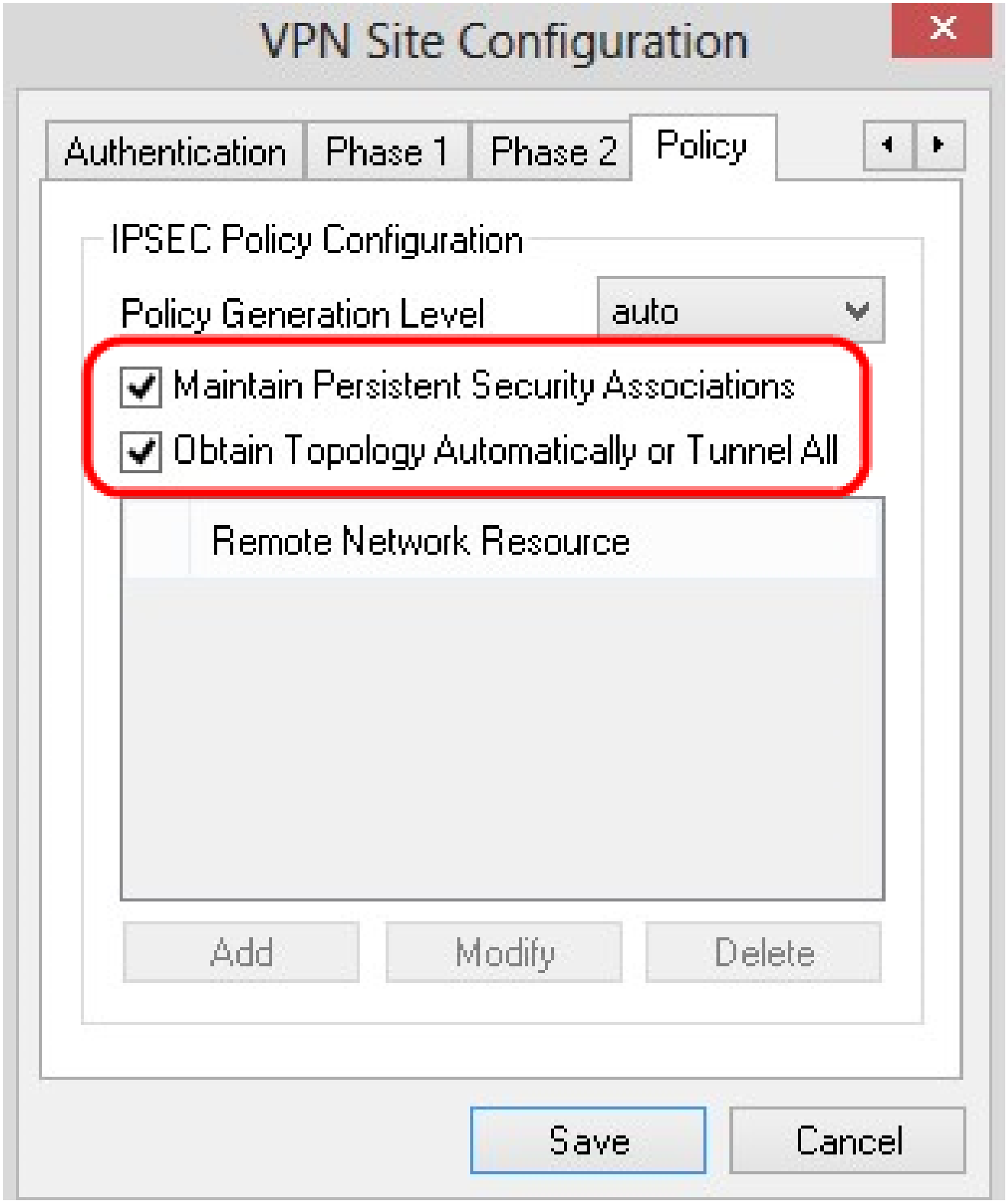
·唯一 — 協商每個策略的唯一安全關聯。

·共用 — 在必要級別生成適當的策略。

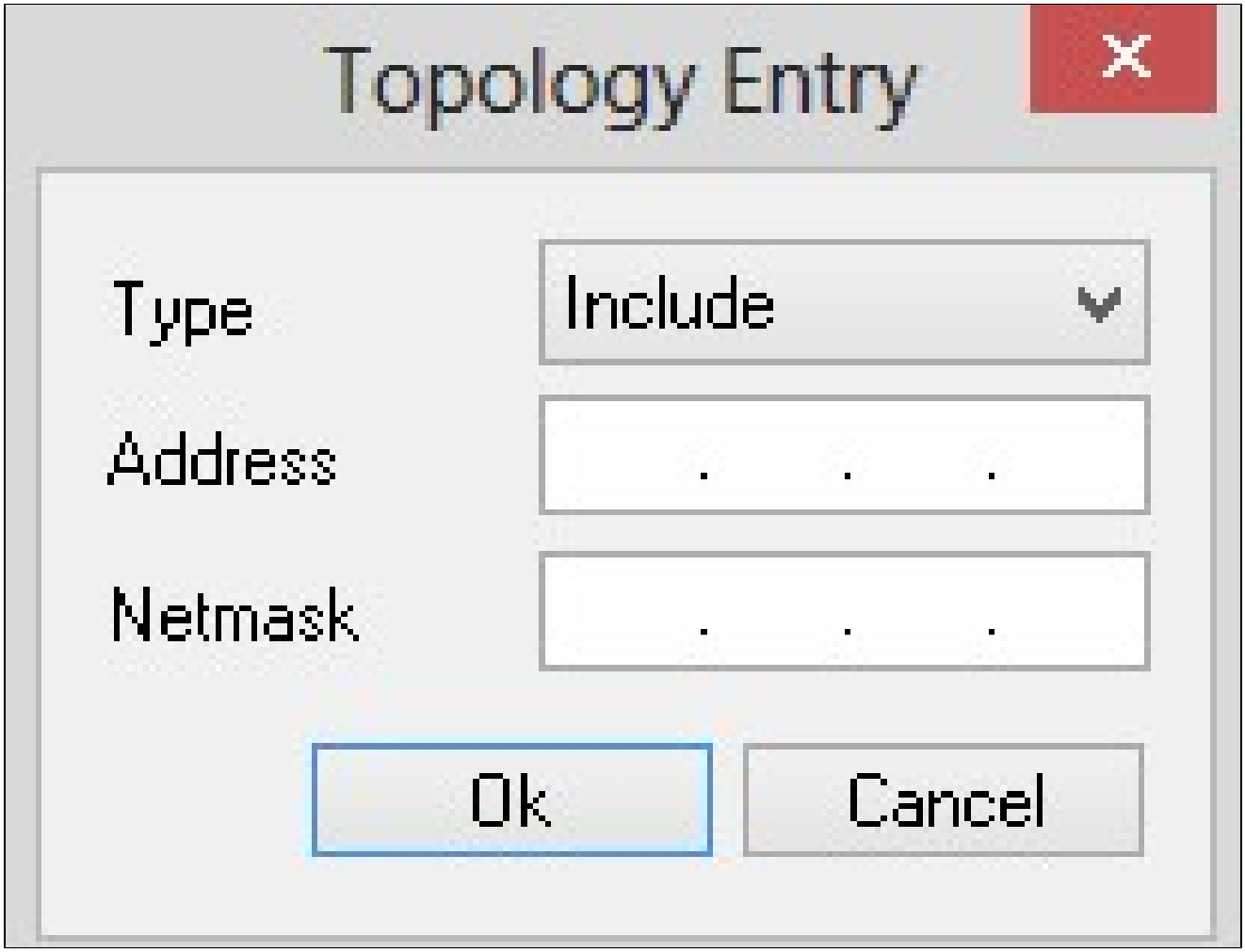


步驟3.（可選）要更改IPSec協商，請選中Maintain Persistent Security Associations覈取方塊。如果啟用，則會在連線後直接為每個策略進行協商。如果禁用，則根據需要進行協商。

步驟4.（可選）要從裝置接收自動提供的網路清單，或要將所有資料包預設傳送到RV0XX，請選中Obtain Topology Automatically或Tunnel All覈取方塊。如果未選中，則必須手動執行配置。如果選中此覈取方塊，請跳至步驟10。



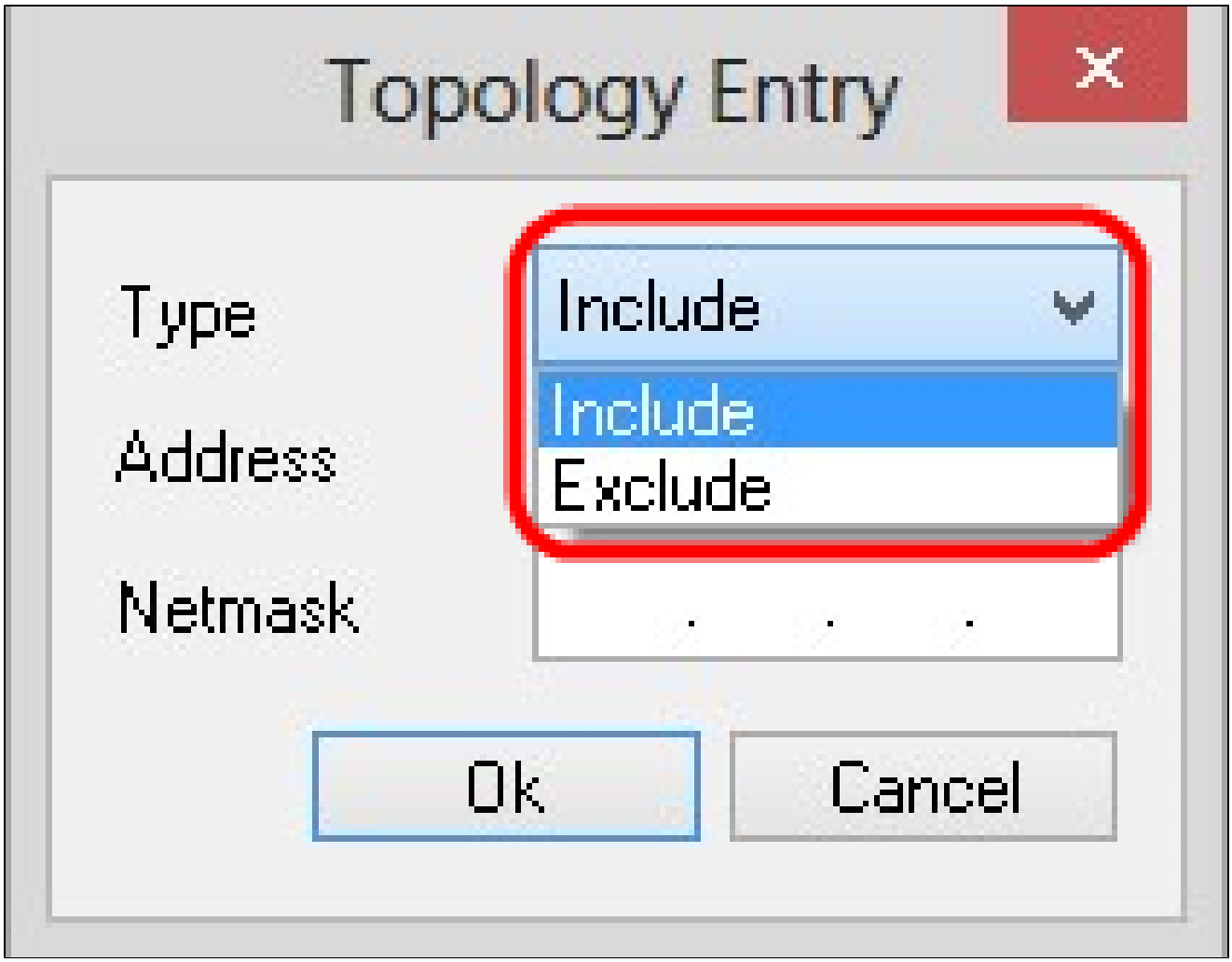
步驟 5.按一下Add將拓撲條目新增到表中。出現Topology Entry視窗。



步驟 6.在「Type」下拉式清單中，選擇適當的選項。

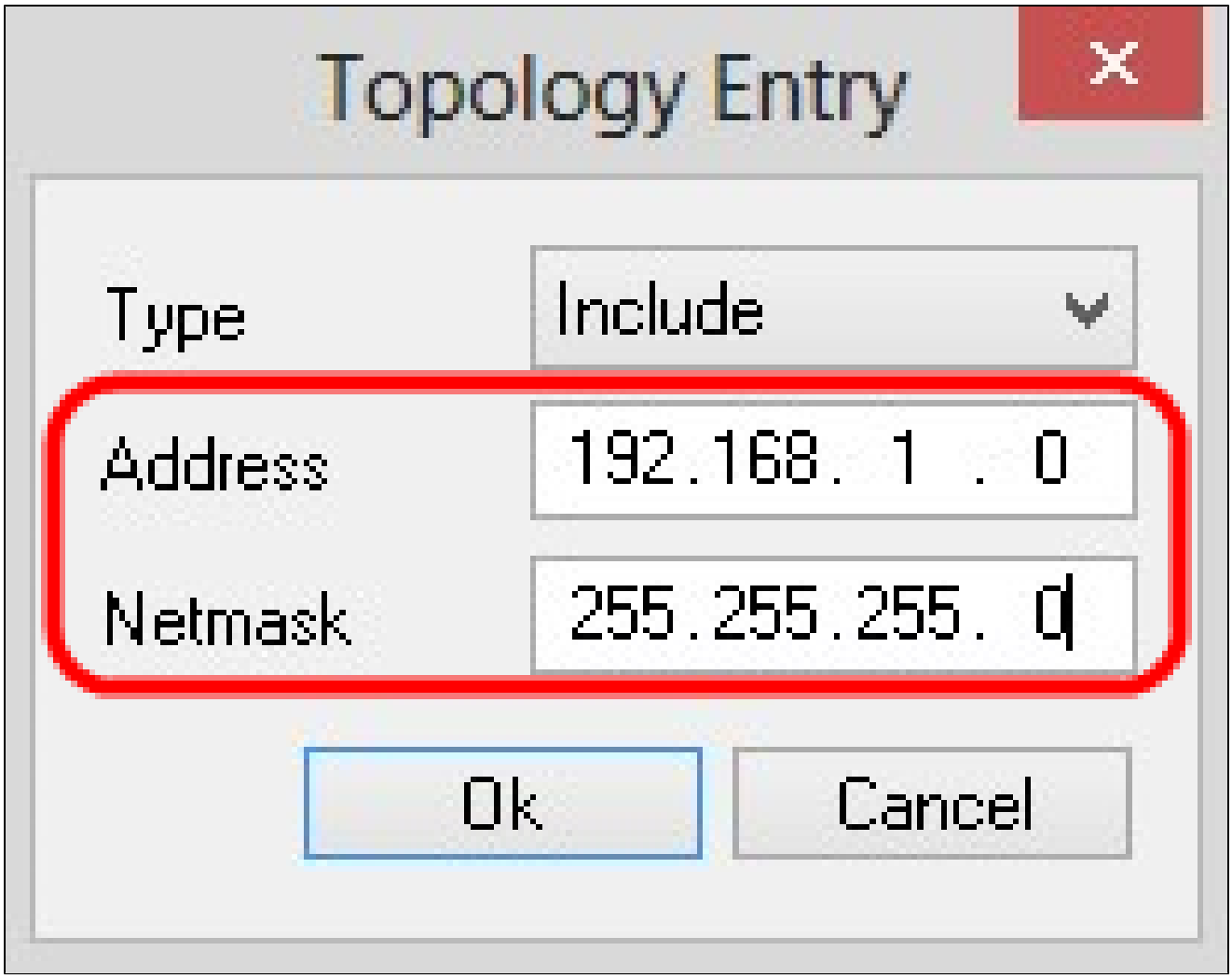
·包括 — 通過VPN網關訪問網路。

·排除 — 通過本地連線訪問網路。

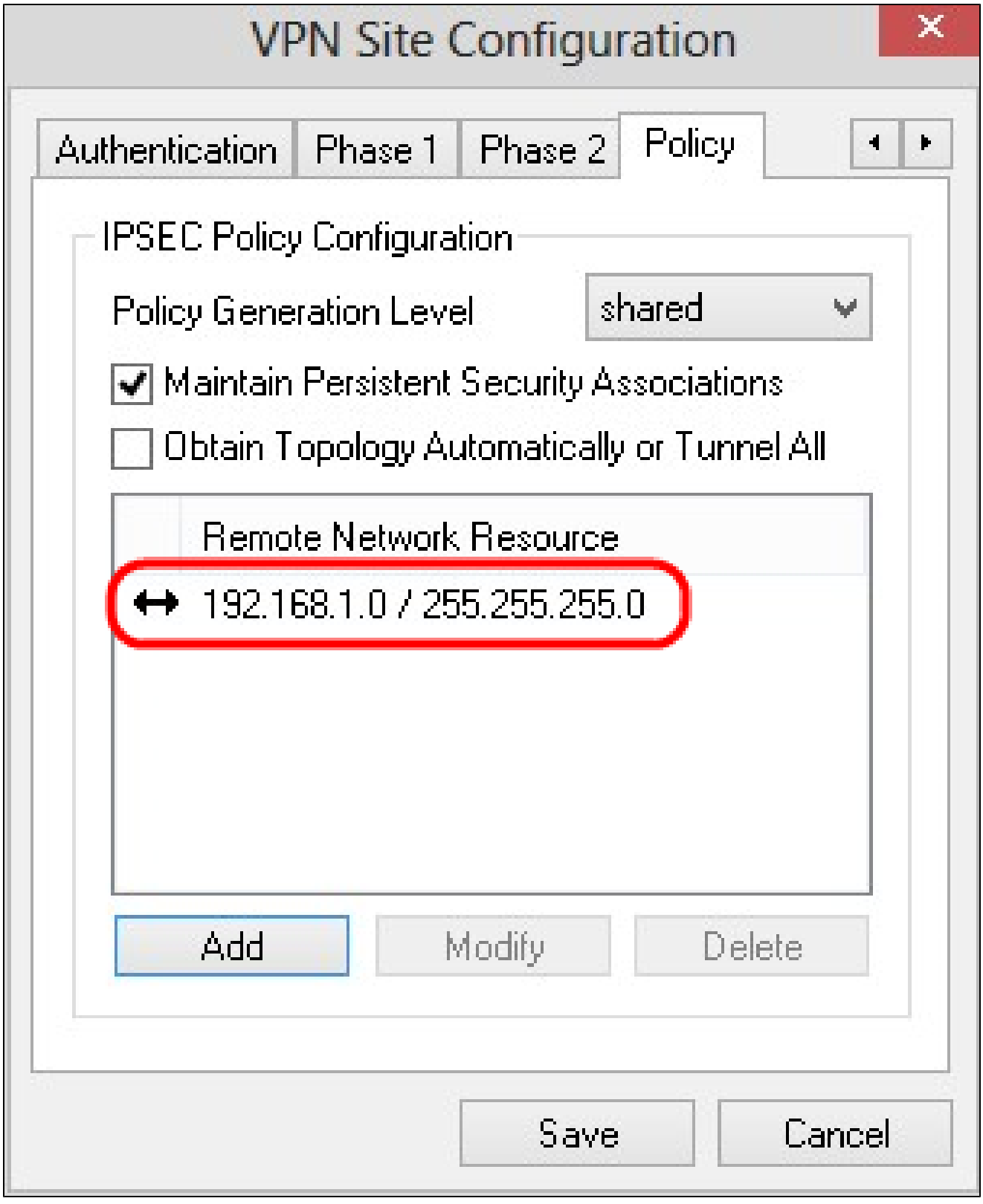


步驟 7.在Address欄位中，輸入RV0XX的IP地址。

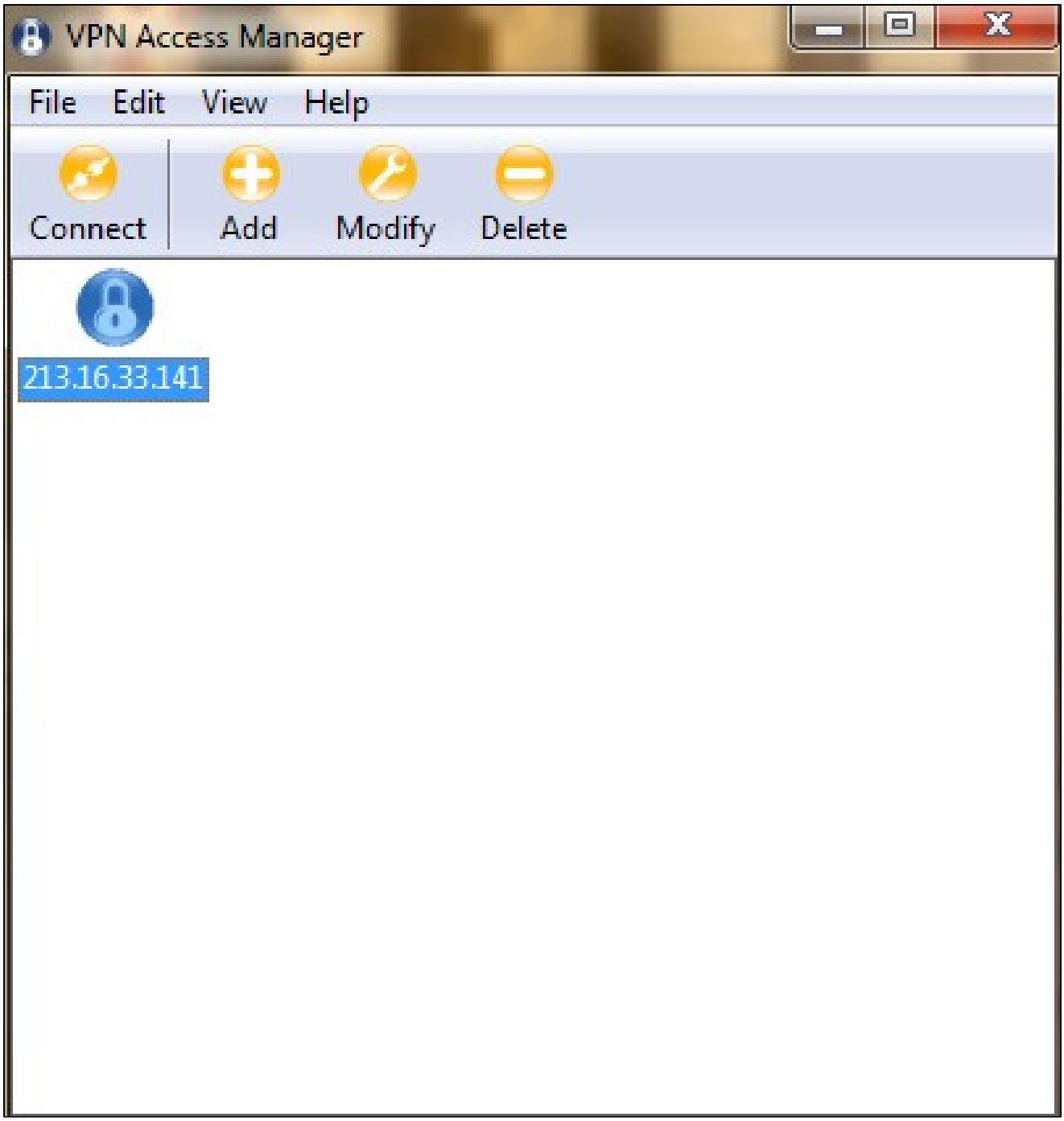
步驟 8.在Netmask欄位中輸入裝置的子網掩碼地址。



步驟 9.按一下「OK」（確定）。RV0XX的IP地址和子網掩碼地址顯示在Remote Network Resource清單中。



步驟 10.按一下Save，該操作將使用者返回到顯示新VPN連線的VPN Access Manager視窗。

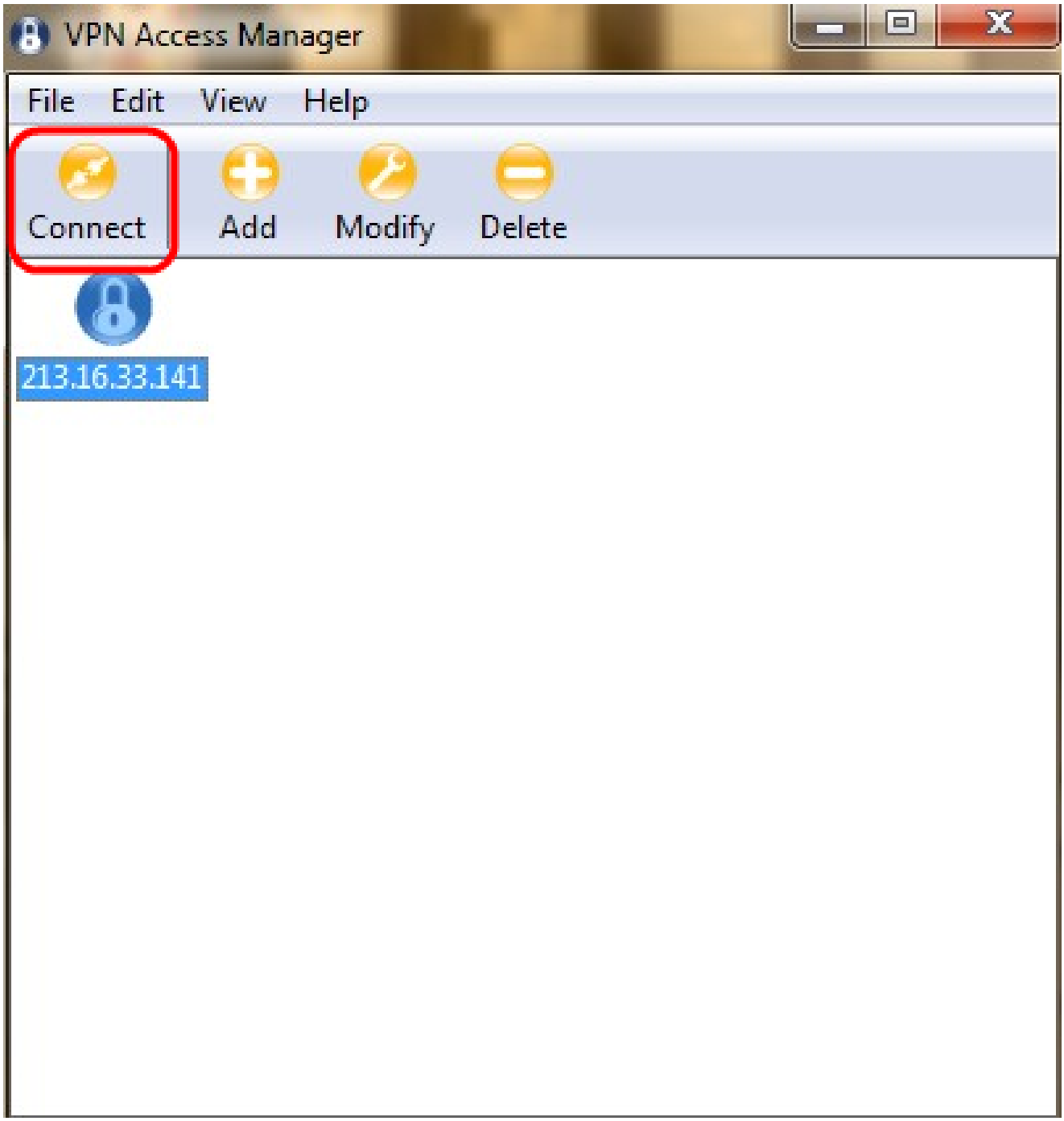


連線

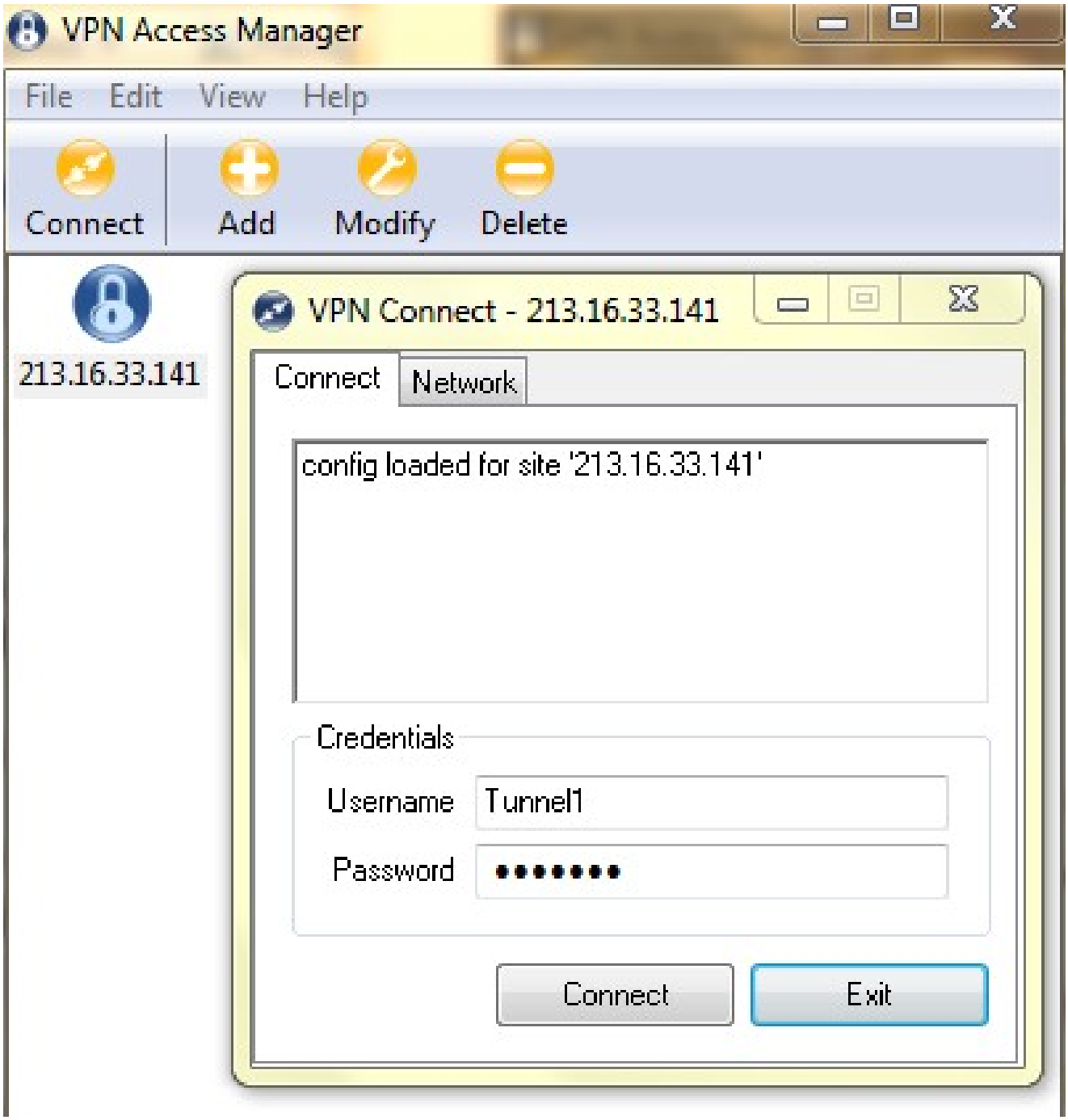
本節介紹如何在配置所有設定後設定VPN連線。所需的登入資訊與裝置上配置的VPN客戶端訪問資訊相同。

步驟 1.按一下所需的VPN連線。

步驟 2.按一下「Connect」。



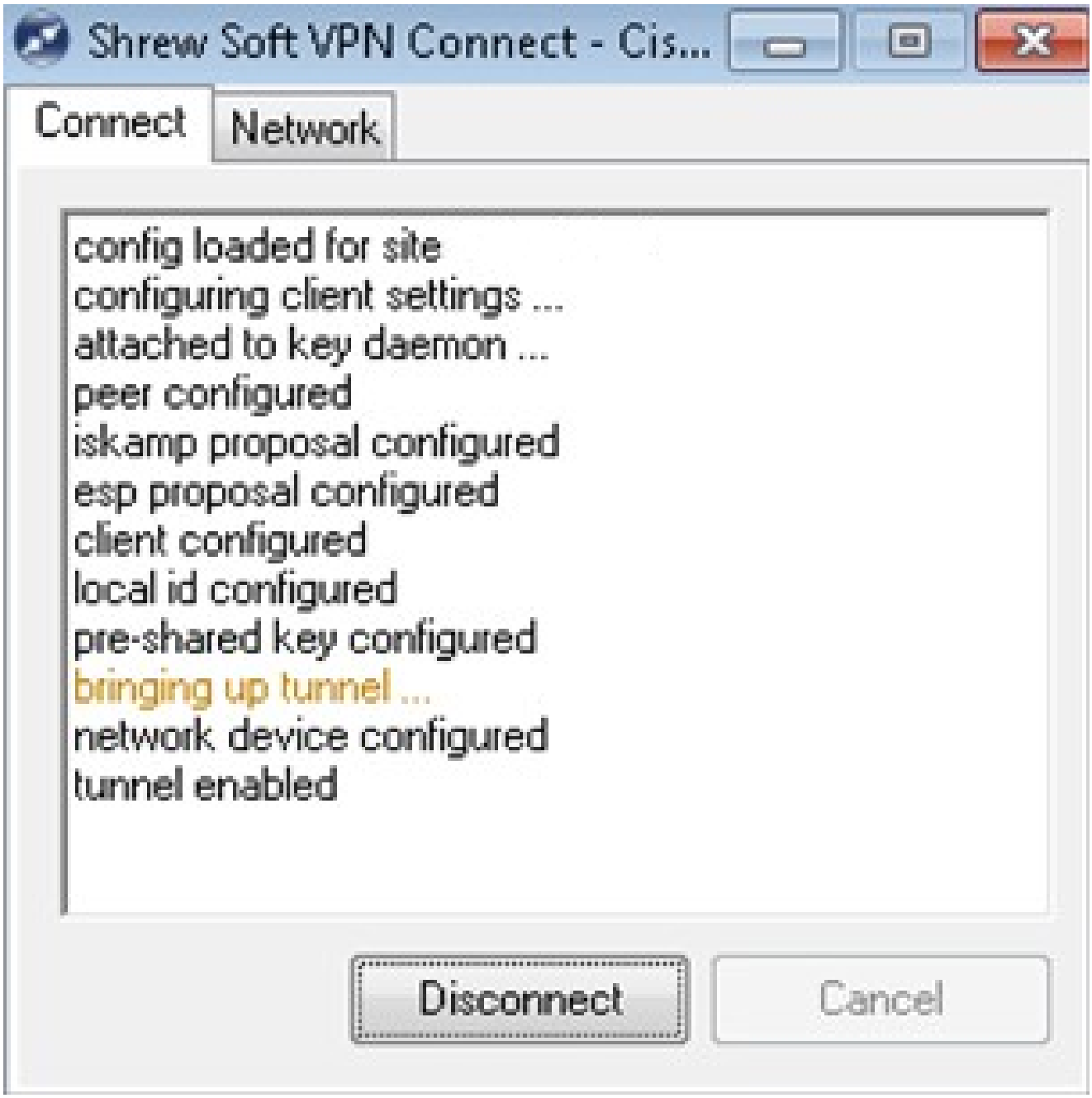
出現VPN Connect視窗：



步驟 3.在Username欄位中輸入VPN的使用者名稱。

步驟 4.在Password 欄位中輸入VPN使用者帳戶的密碼。

步驟 5.按一下「Connect」。出現Shrew Soft VPN Connect視窗：



步驟6。（可選）若要停用連線，請按一下Disconnect。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。