在SG300系列交換機上配置802.1X

目標

802.1X是實施基於埠身份驗證的IEEE標準。如果埠使用802.1X，則使用該埠的任何客戶端（稱為請求方）必須在獲得網路訪問許可權之前提供正確的憑據。實現802.1X的裝置（稱為身份驗證器）必須能夠與網路上其他位置的RADIUS（遠端身份驗證撥入使用者服務）伺服器通訊。此伺服器包含允許訪問網路的有效使用者清單；身份驗證器傳送的任何憑據（由請求方提供）必須與RADIUS伺服器持有的憑據匹配。如果是，則伺服器通知身份驗證器向使用者授予訪問許可權；否則，驗證器將拒絕訪問。

802.1X標準是阻止不需要的使用者通過插入物理埠訪問網路的良好安全措施。請注意，若要使802.1X正常運作，必須在網路上的其他位置設定RADIUS伺服器，且驗證器必須能夠與其通訊。

本文檔旨在向您展示如何在SG300系列交換機上設定802.1X。

適用裝置

·SG300系列交換器

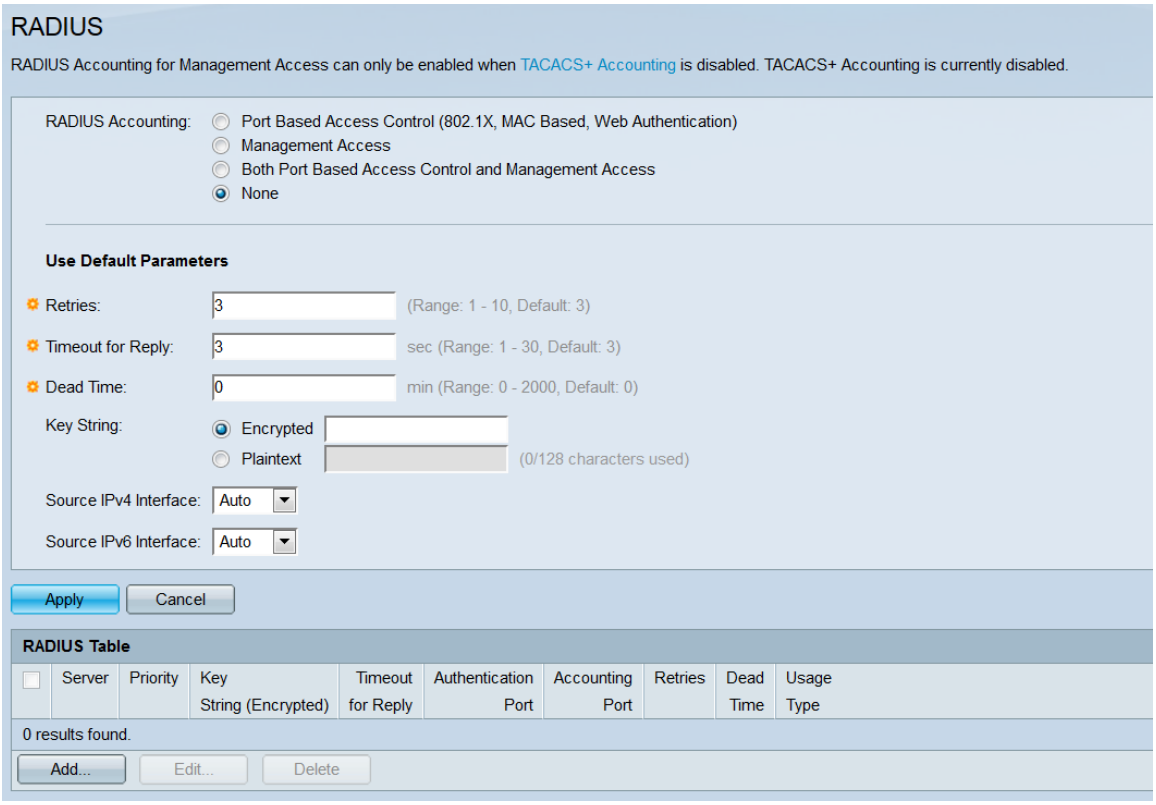
軟體版本

·v1.4.1.3

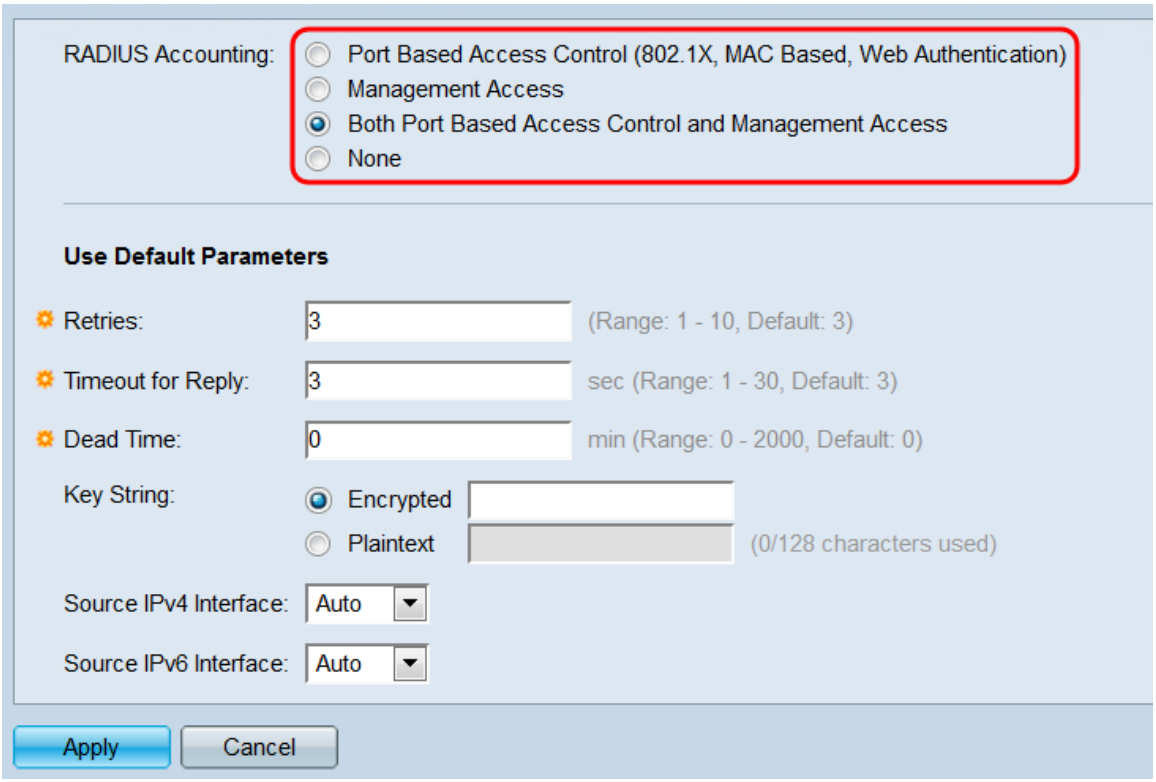
設定802.1X身份驗證

新增RADIUS伺服器

步驟1.登入Web組態公用程式，然後選擇**Security > RADIUS**。*RADIUS*頁面隨即開啟。



步驟2.在*RADIUS Accounting*欄位中，選擇單選按鈕以選擇RADIUS伺服器將提供的記帳資訊型別。可以為RADIUS伺服器提供記帳資訊，用於跟蹤使用者的會話時間、使用者使用的資源和其他內容。此處選擇的選項不會影響802.1X的效能。



選項包括：

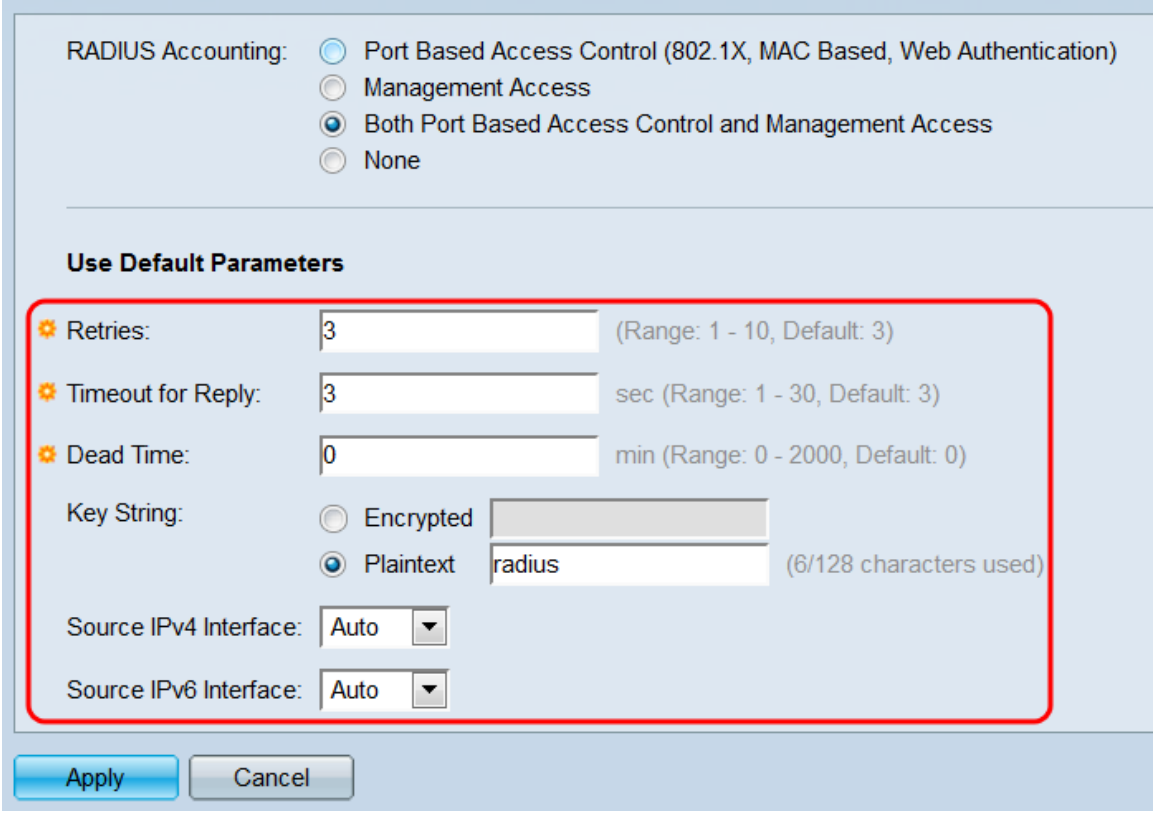
·連線埠型存取控制 — 此選項將有關連線埠型驗證作業階段的計費資訊傳送到RADIUS伺服器。

·管理訪問 — 此選項將有關交換機管理會話的記帳資訊傳送到RADIUS伺服器。

·基於埠的訪問控制和管理訪問 — 此選項將兩種型別的記帳資訊傳送到RADIUS伺服器。

·無 — 不向RADIUS伺服器傳送記帳資訊。

步驟3.在*Use Default Parameters*區域中，配置將預設使用的設定，除非新增的RADIUS伺服器配置了它自己的特定設定；您新增到交換機的每個伺服器條目都可以使用預設設定或單獨的唯一設定。對於這篇文章，我們將使用本節中定義的預設設定。



配置以下設定：

·重試 — 輸入交換機在移動到下一台伺服器之前嘗試聯絡RADIUS伺服器的次數。預設值為3。

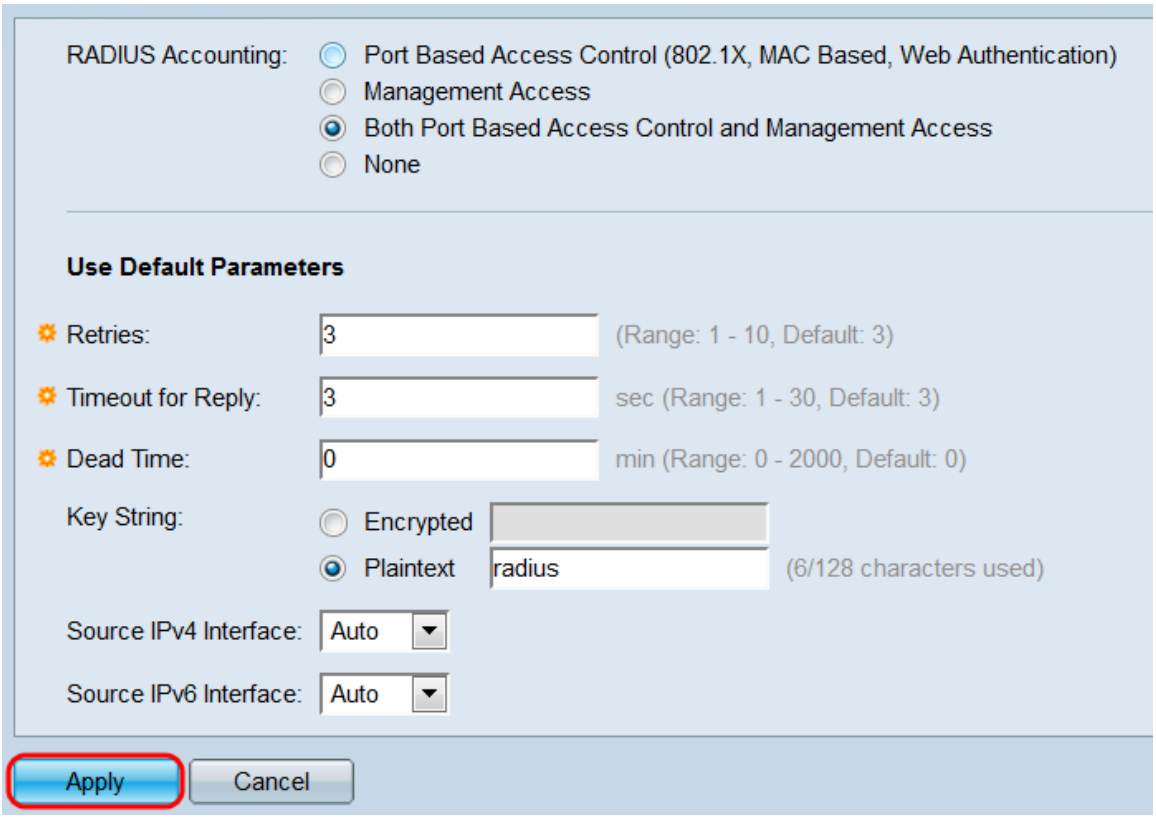
·應答超時 — 輸入交換機在採取進一步操作（重試或放棄）之前等待來自RADIUS伺服器的應答的秒數。 預設值為3。

·Dead Time — 輸入無響應的RADIUS伺服器傳遞服務請求之前經過的分鐘數。預設值為0;該值表示伺服器不會被繞過。

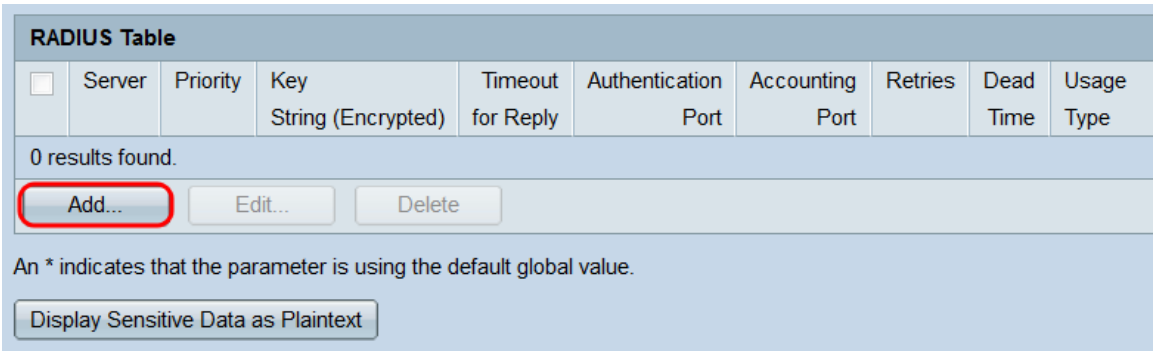
·金鑰字串 — 輸入用於在交換機和RADIUS伺服器之間進行身份驗證的金鑰。如果您有加密的金鑰，請使用**Encrypted**單選按鈕輸入；否則，請使用**Plaintext**單選按鈕輸入明文金鑰。

·源IPv4/IPv6介面 — 使用這些下拉選單選擇與RADIUS伺服器通訊時將使用的IPv4/IPv6源介面。預設值為Auto，將使用傳出介面上定義的預設源IP地址。

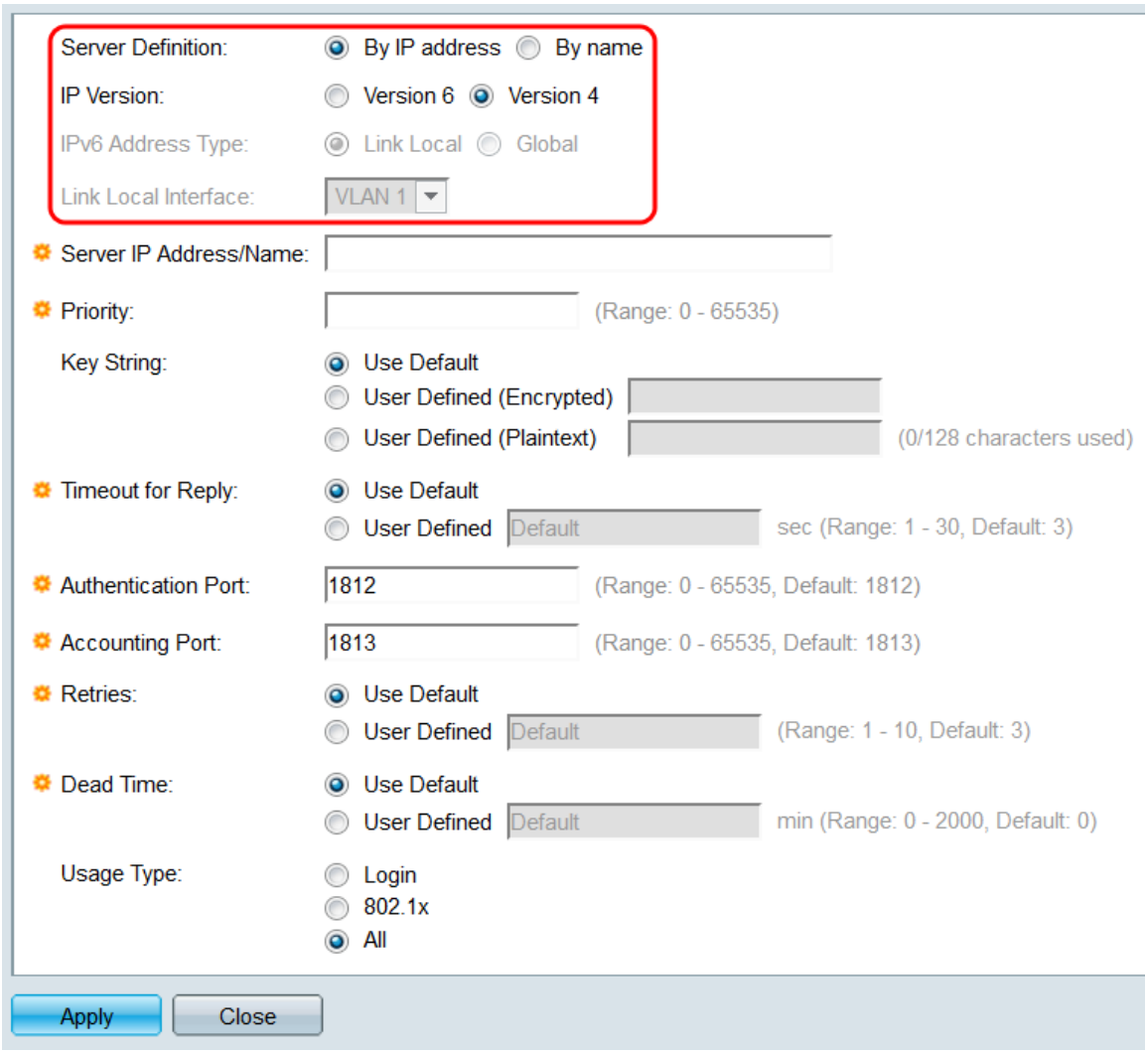
步驟4.按一下**Apply**。將應用預設設定。



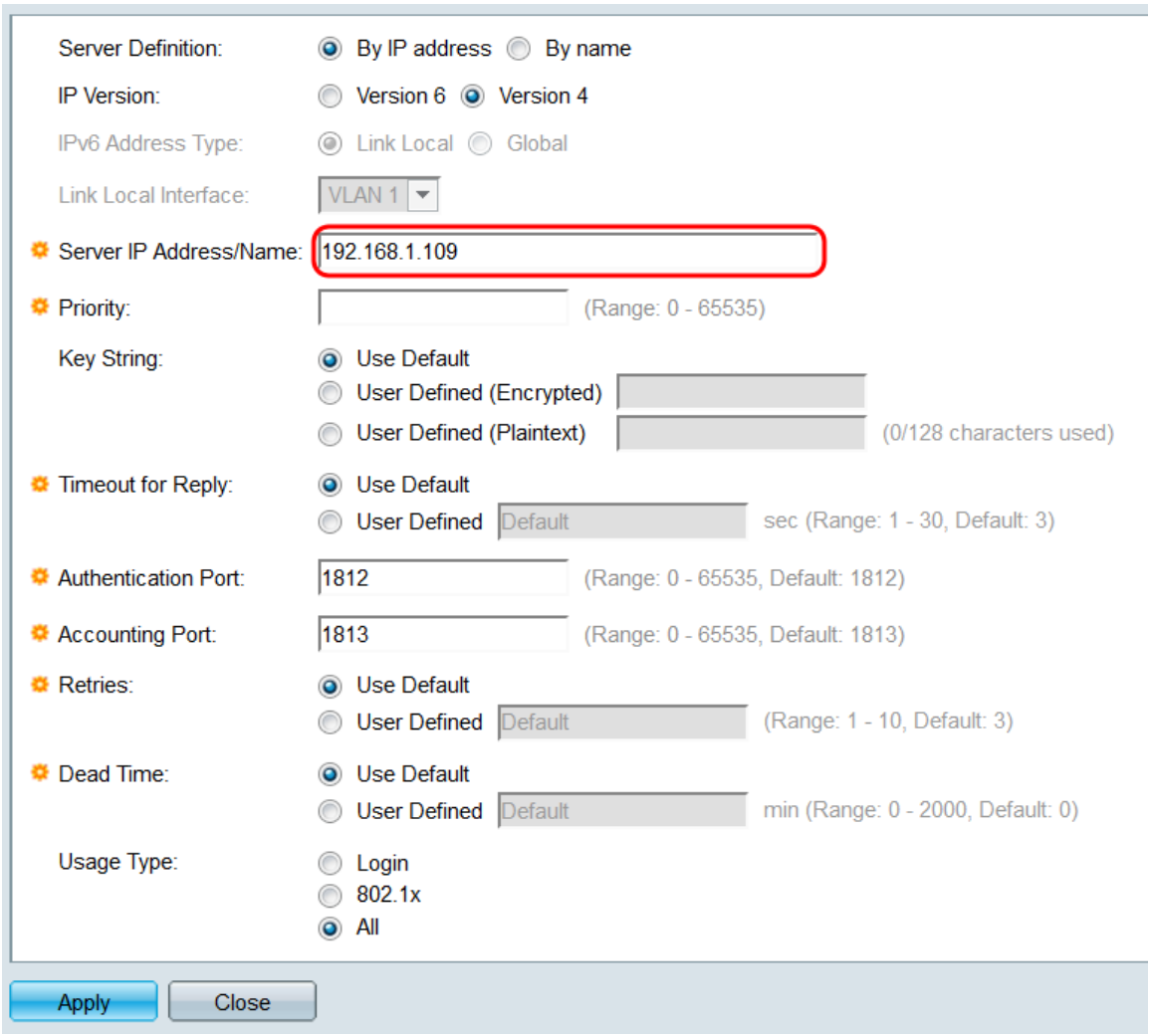
步驟5. *RADIUS表*會顯示交換器上目前設定的RADIUS伺服器專案。要新增新條目，請按一下**新增.....**按鈕。將會開啟*新增RADIUS伺服器*視窗。



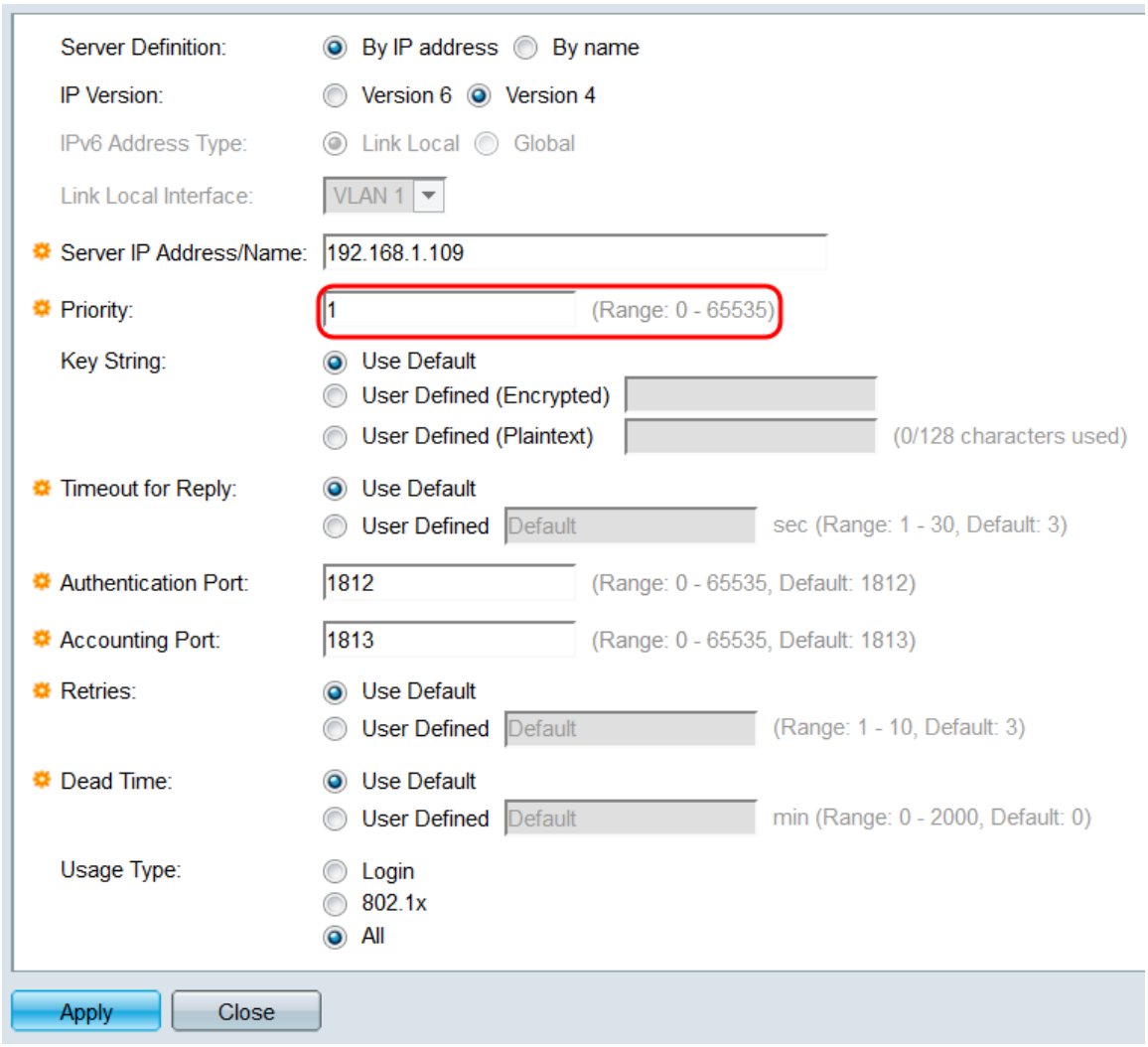
步驟6.在*Server Definition*欄位中，選擇是按IP位址還是**按名稱（主機名稱）聯絡RADIUS伺服器。** 如果選擇**By IP address**，請選擇使用IPv6(**版本6**)或IPv4(**版本4**)。 如果選擇了**版本6**，請使用*IPv6地址型別*和*Link Local Interface*指定將使用的IPv6地址。



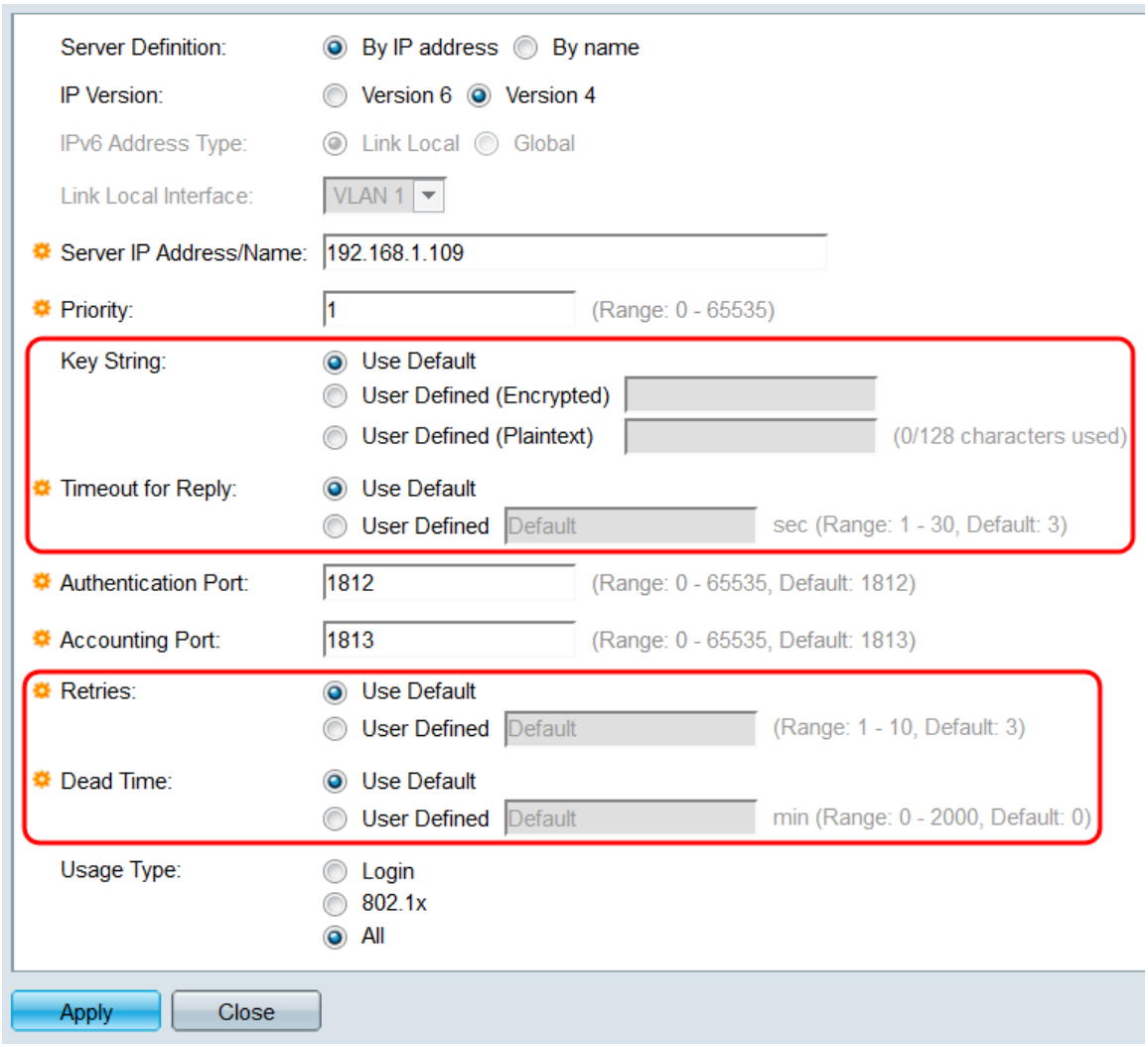
步驟7.在「*Server IP Address/Name*」欄位中，輸入RADIUS伺服器的IP位址或主機名稱。



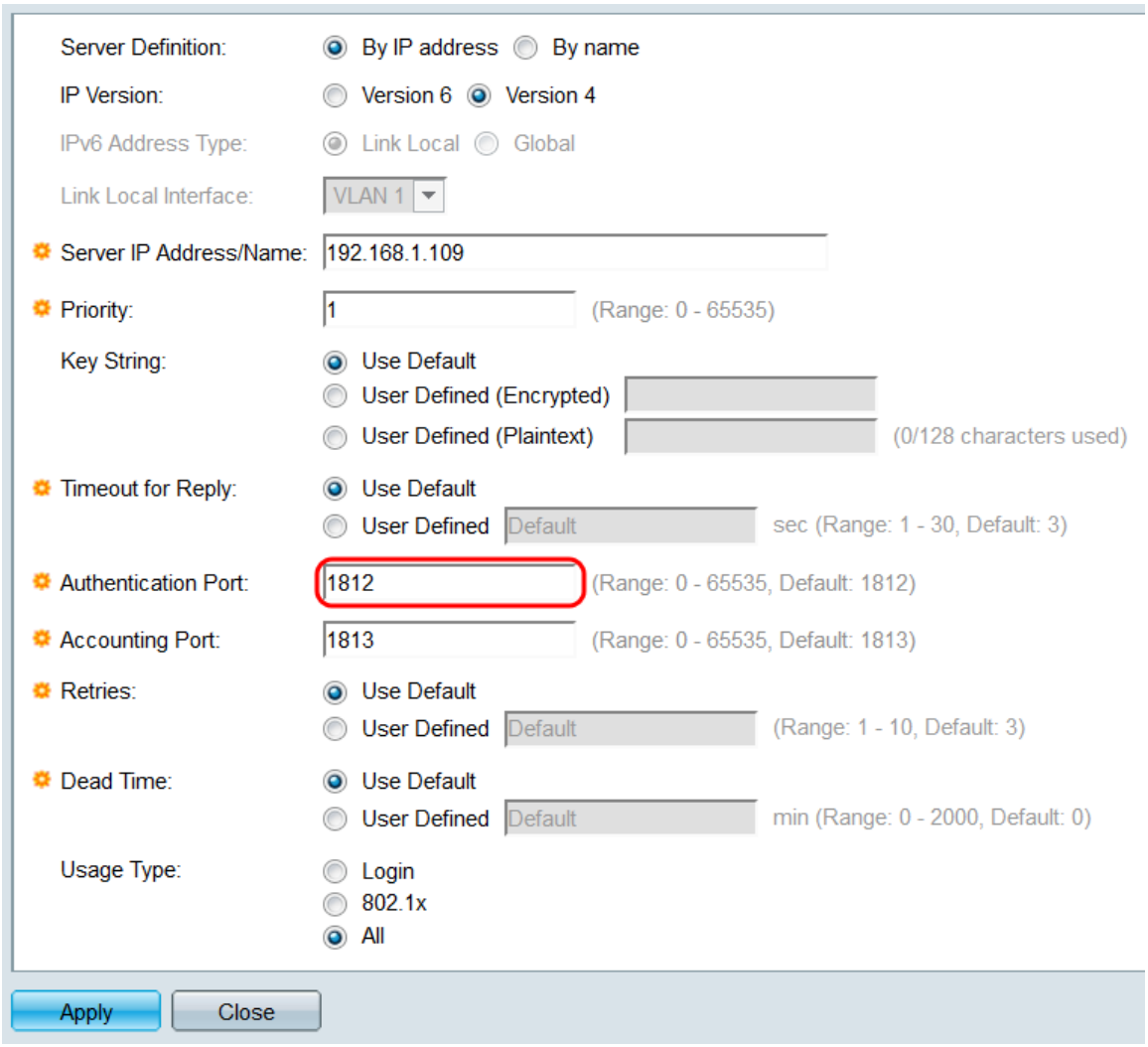
步驟8.在*優先順序*欄位中，輸入您要指派給此伺服器的優先順序；交換機將嘗試聯絡具有最高優先順序的伺服器，並繼續關閉清單，直到它遇到響應伺服器。範圍為0 - 65535，其中0表示最高優先順序。



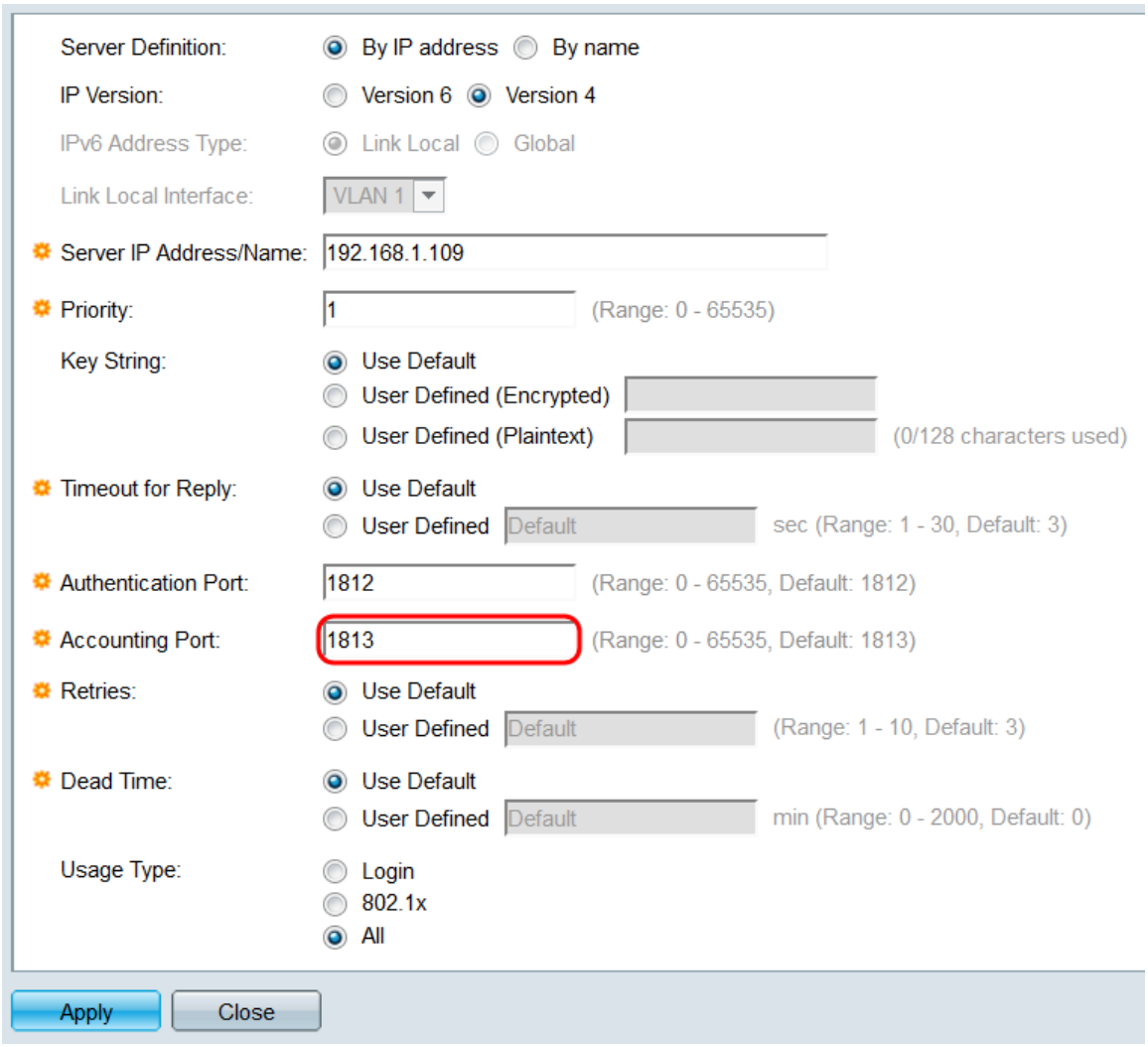
步驟9.選擇Key String、Timeout for Reply、*Retries*和*Dead Time*欄位中的Use Default單選按鈕，以使用以前在RADIUS頁中配置的設定。您還可以選擇**User Defined**單選按鈕以配置不同於預設值的設定；如果執行此操作，這些設定將僅用於此特定RADIUS伺服器。



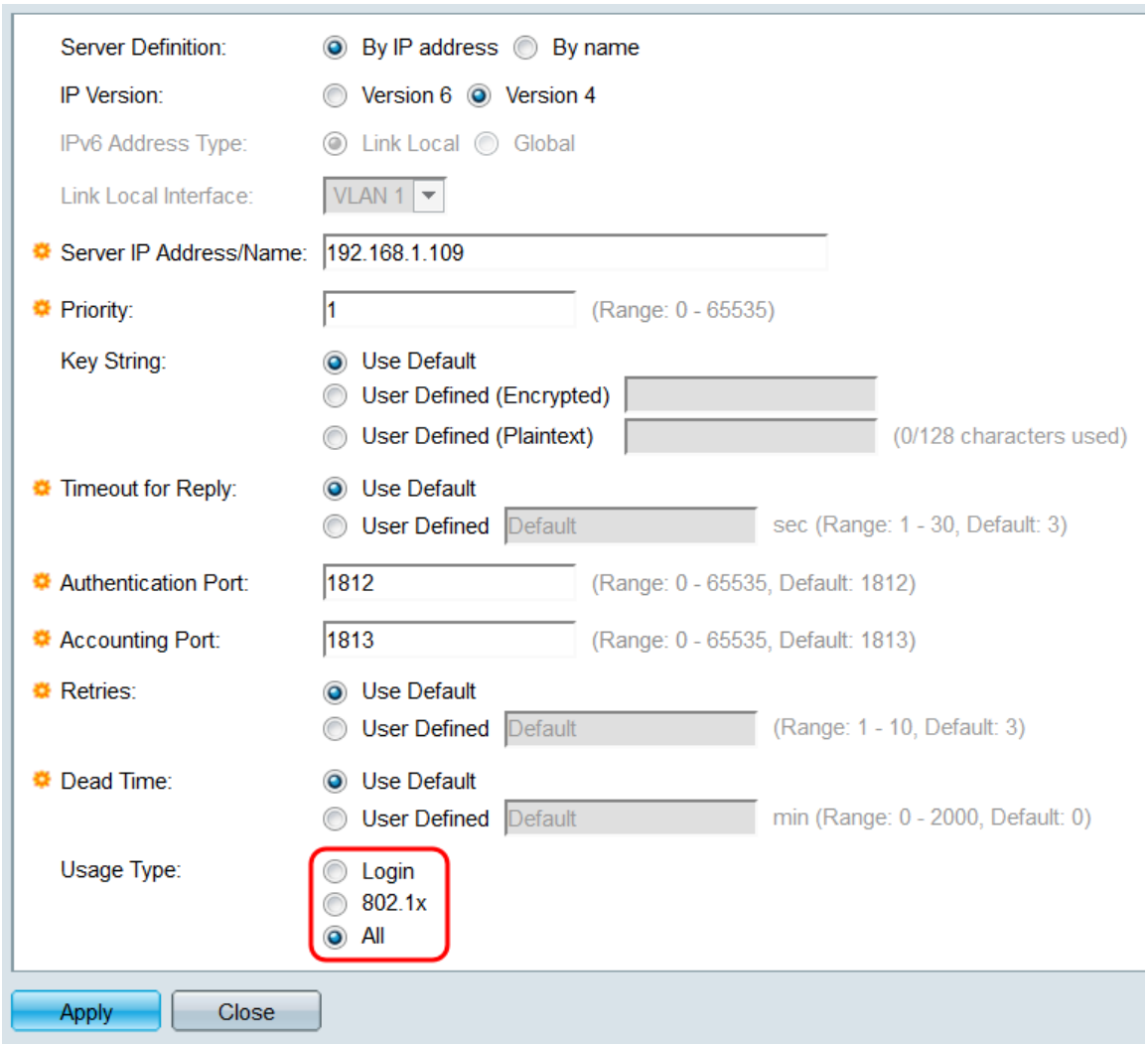
步驟10.在*Authentication Port*欄位中，指定將用於與RADIUS伺服器進行驗證通訊的連線埠。建議將此選項保留在預設埠1812上。



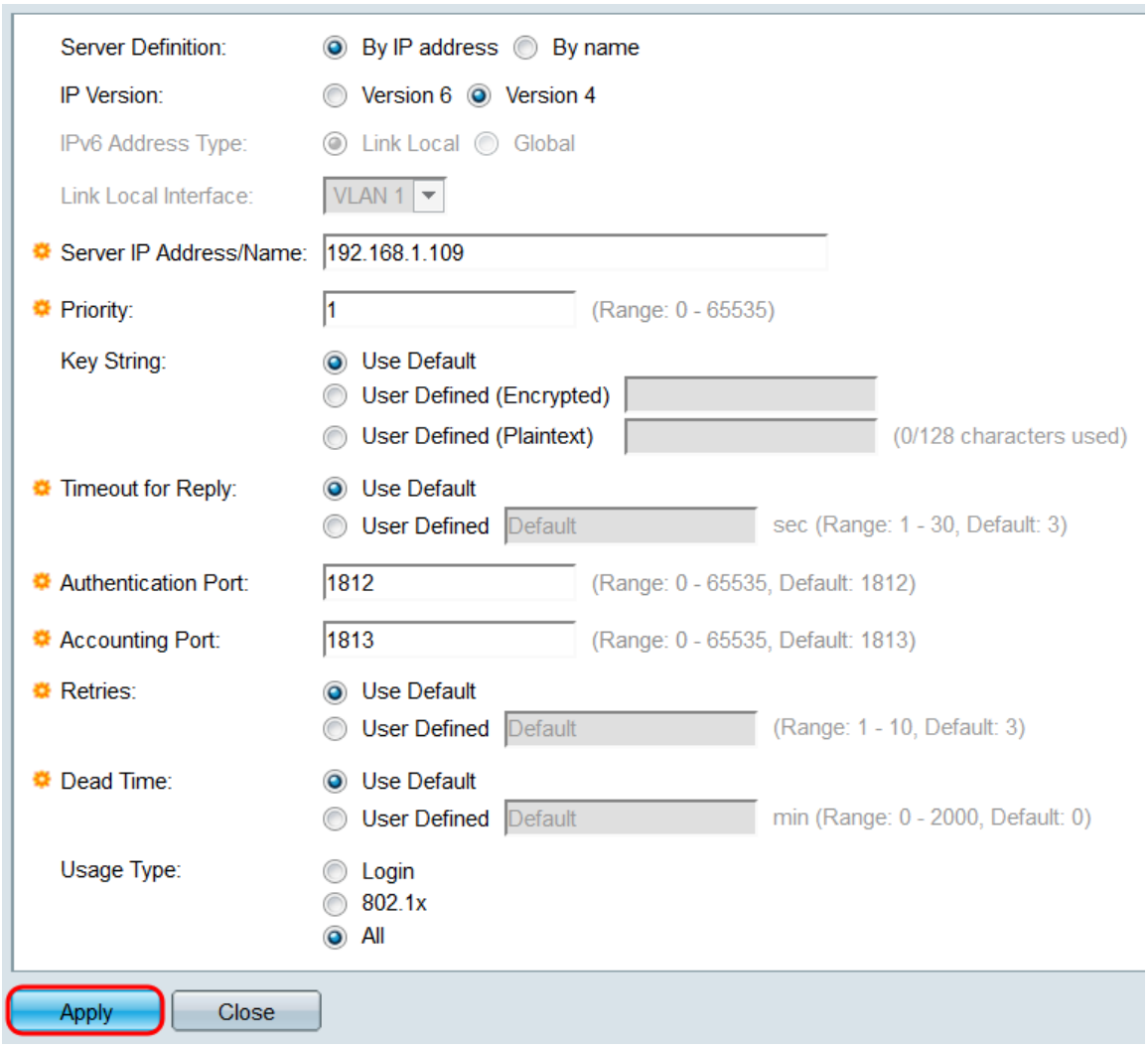
步驟11.在*Accounting Port*欄位中，指定將用來與RADIUS伺服器進行計費通訊的連線埠。建議將此選項保留在預設埠1813上。



步驟12.在*Usage Type*欄位中，選擇RADIUS伺服器將使用的用途。配置802.1X時，選擇**802.1x**或**All**單選按鈕以使用RADIUS伺服器進行802.1X埠身份驗證。

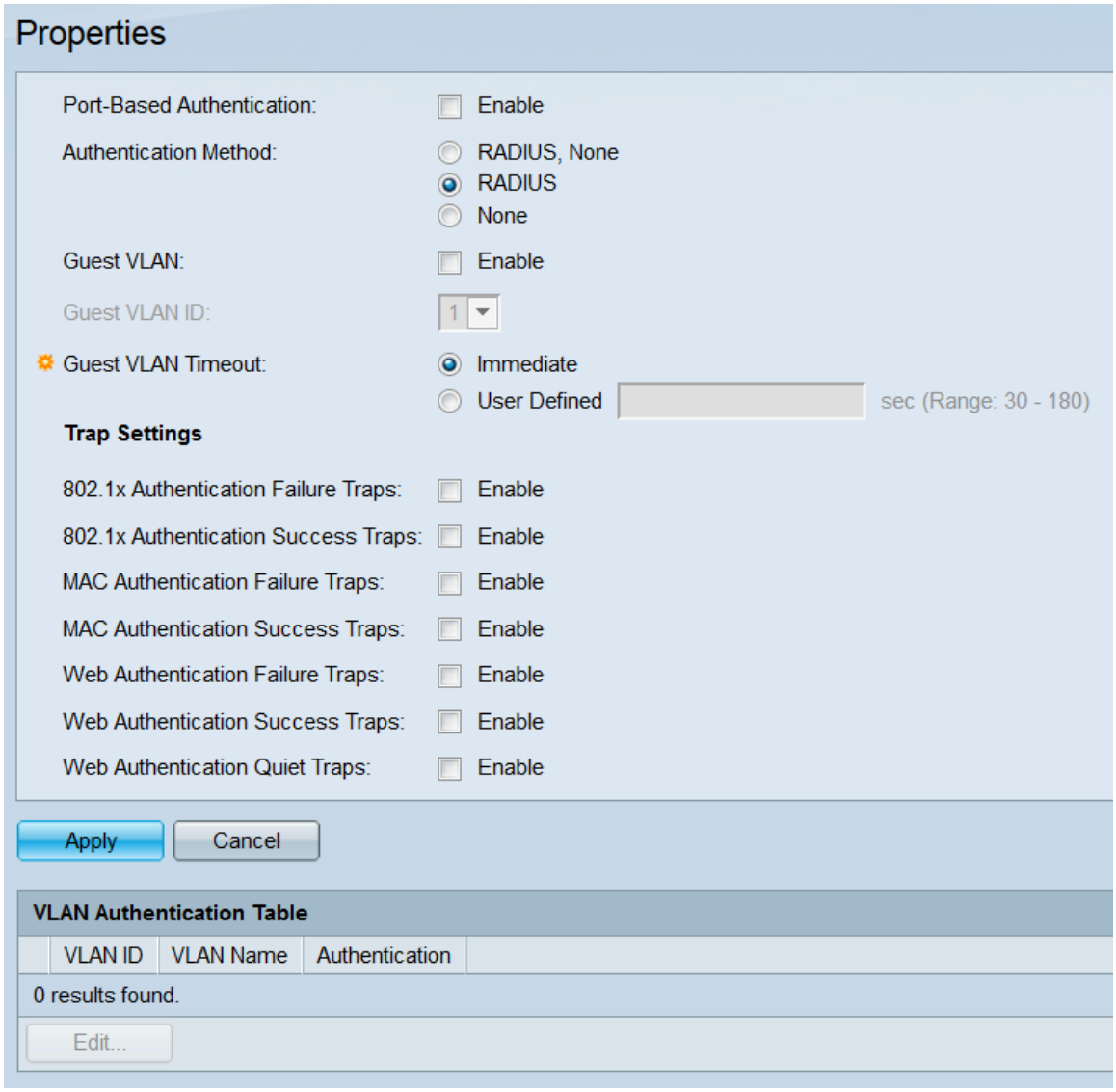


步驟13.按一下**Apply**。伺服器將新增到*RADIUS*表。要啟用基於埠的802.1X身份驗證，請繼續下一部分。

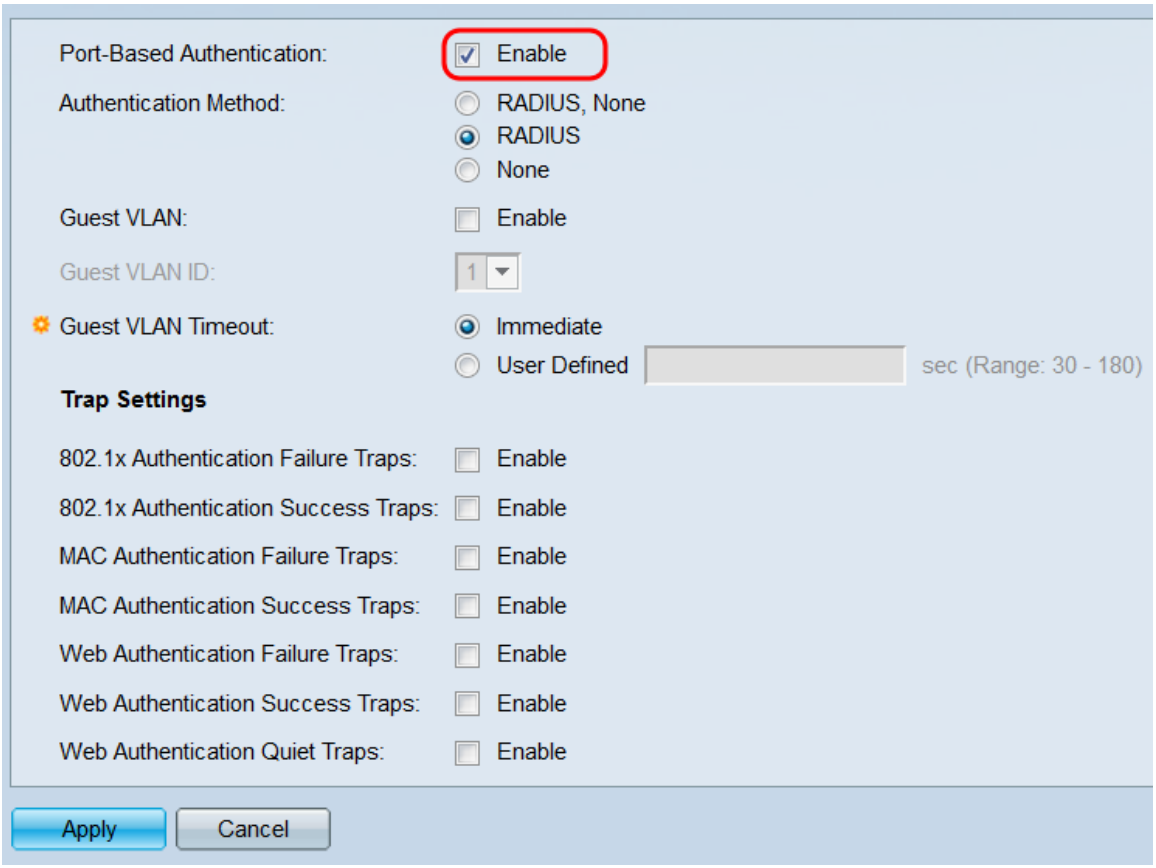


啟用基於埠的身份驗證

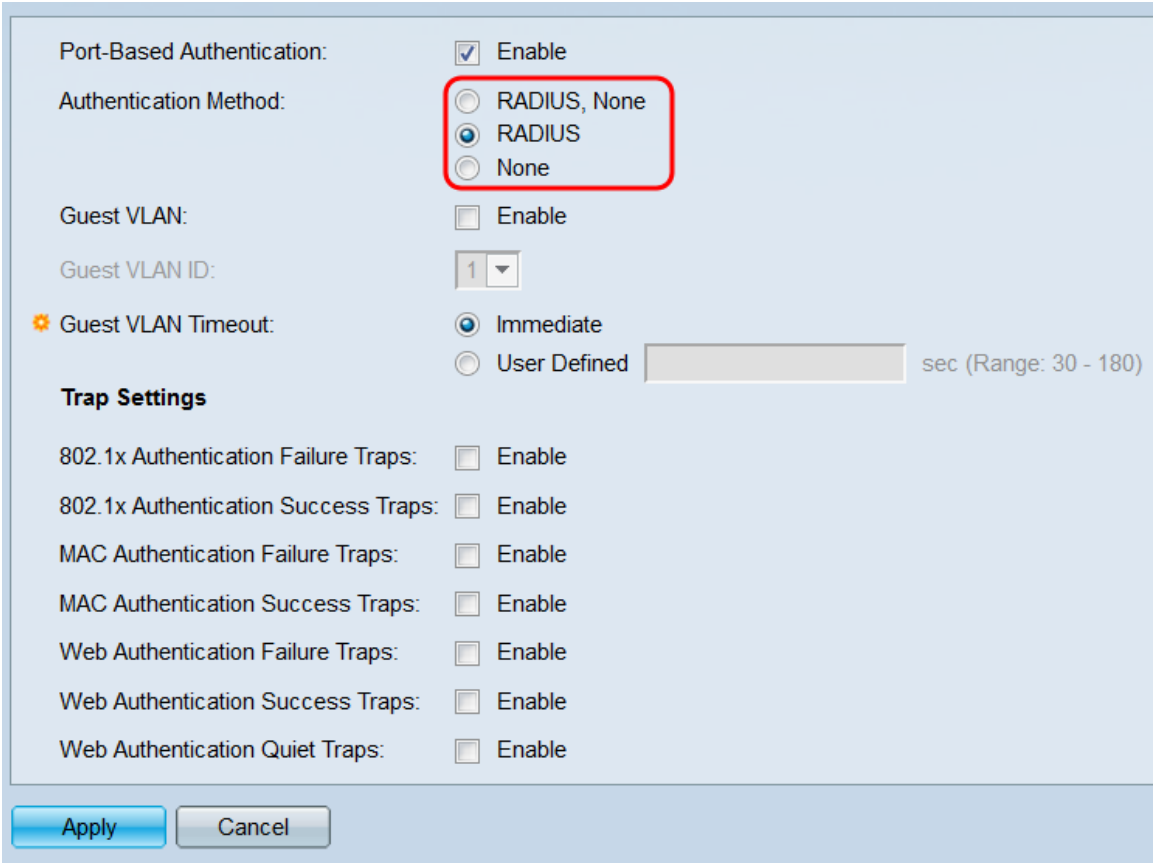
步驟1.在Web配置實用程式中，轉到**安全> 802.1X/MAC/Web身份驗證>屬性**。*Properties*頁面隨即開啟。



步驟2.在*Port-Based Authentication*欄位中，勾選**Enable**覈取方塊以啟用基於埠的身份驗證。預設情況下啟用。



步驟3.在*Authentication Method*欄位中，選擇單選按鈕以判斷連線埠型驗證的工作方式。



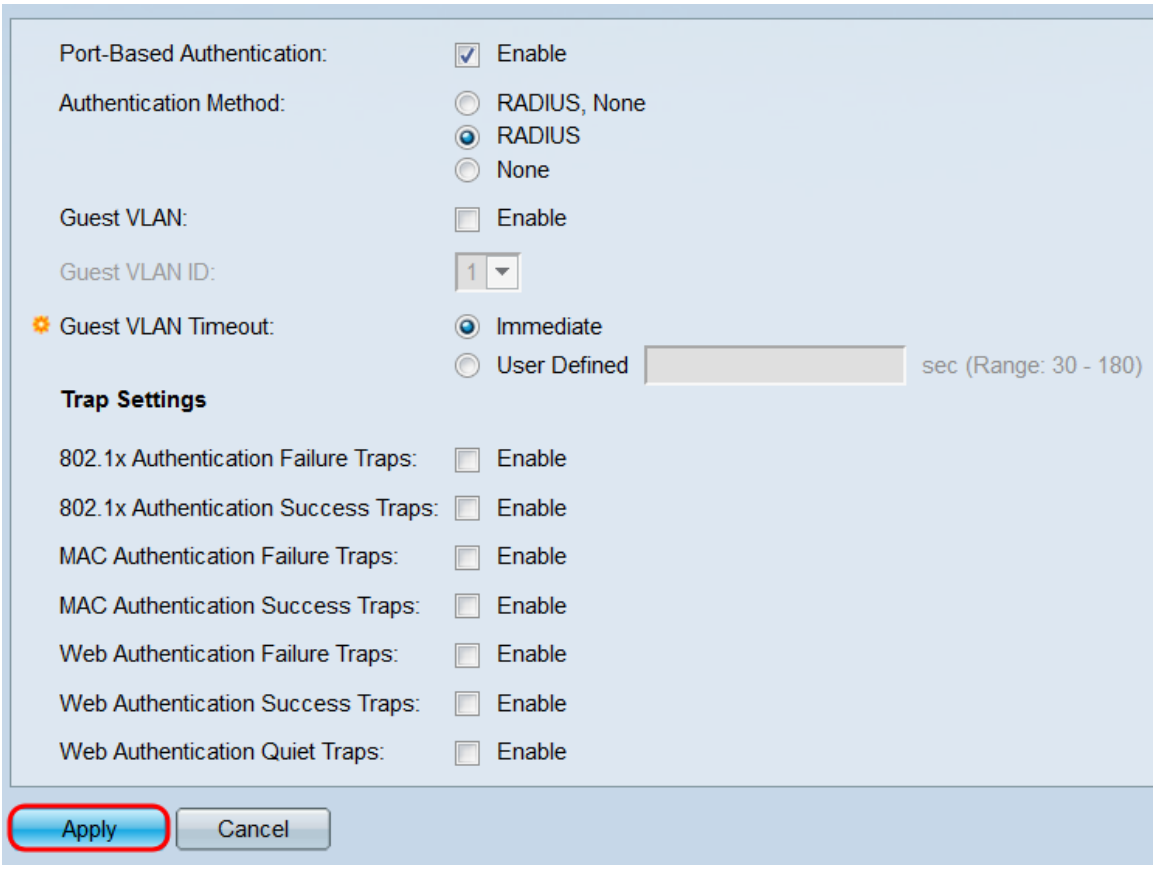
選項包括：

·RADIUS， None — 交換機將嘗試聯絡*RADIUS*頁上定義的RADIUS伺服器。如果未收到來自伺服器的響應，則不執行身份驗證並允許會話。如果伺服器有響應，並且憑據不正確，則會話會被拒絕。

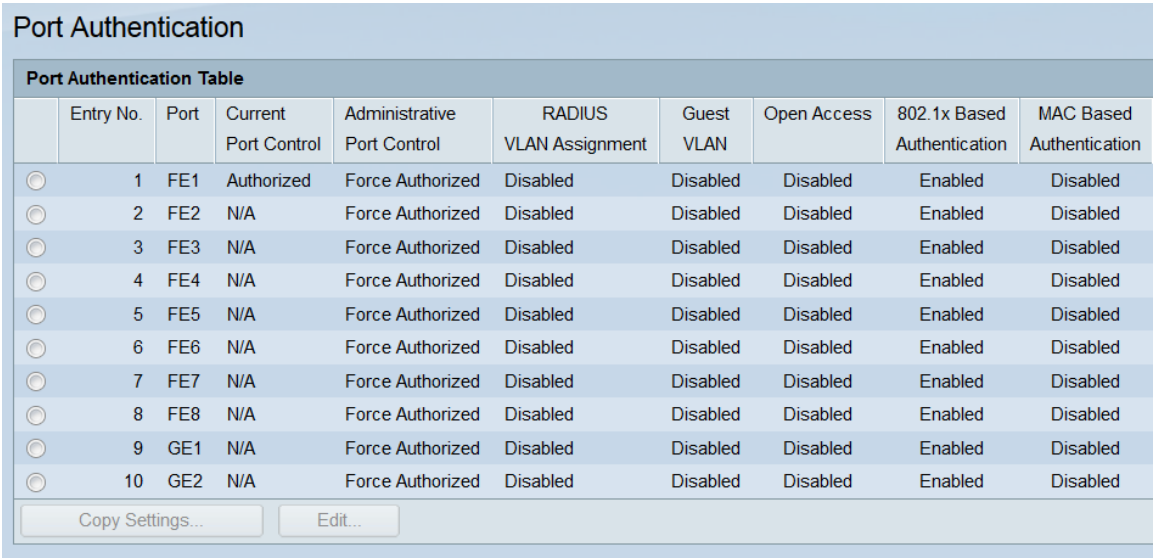
·RADIUS — 交換機將嘗試聯絡*RADIUS*頁面上定義的RADIUS伺服器。如果沒有收到來自伺服器的響應，會話將被拒絕。對於最安全的802.1X實施，建議使用此選項。

·無 — 不執行身份驗證。允許所有會話。此選項不會實現802.1X。

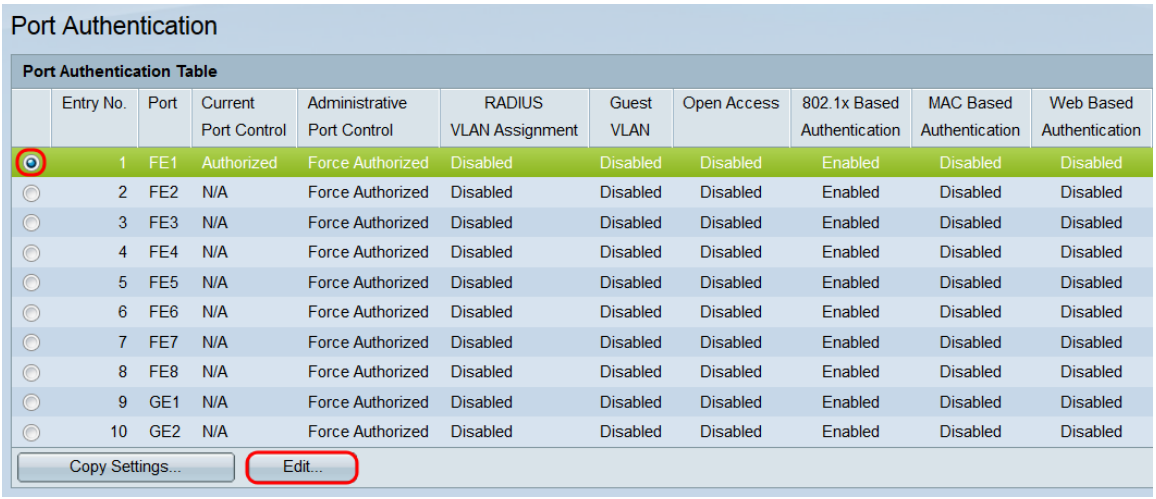
步驟4.按一下**Apply**。



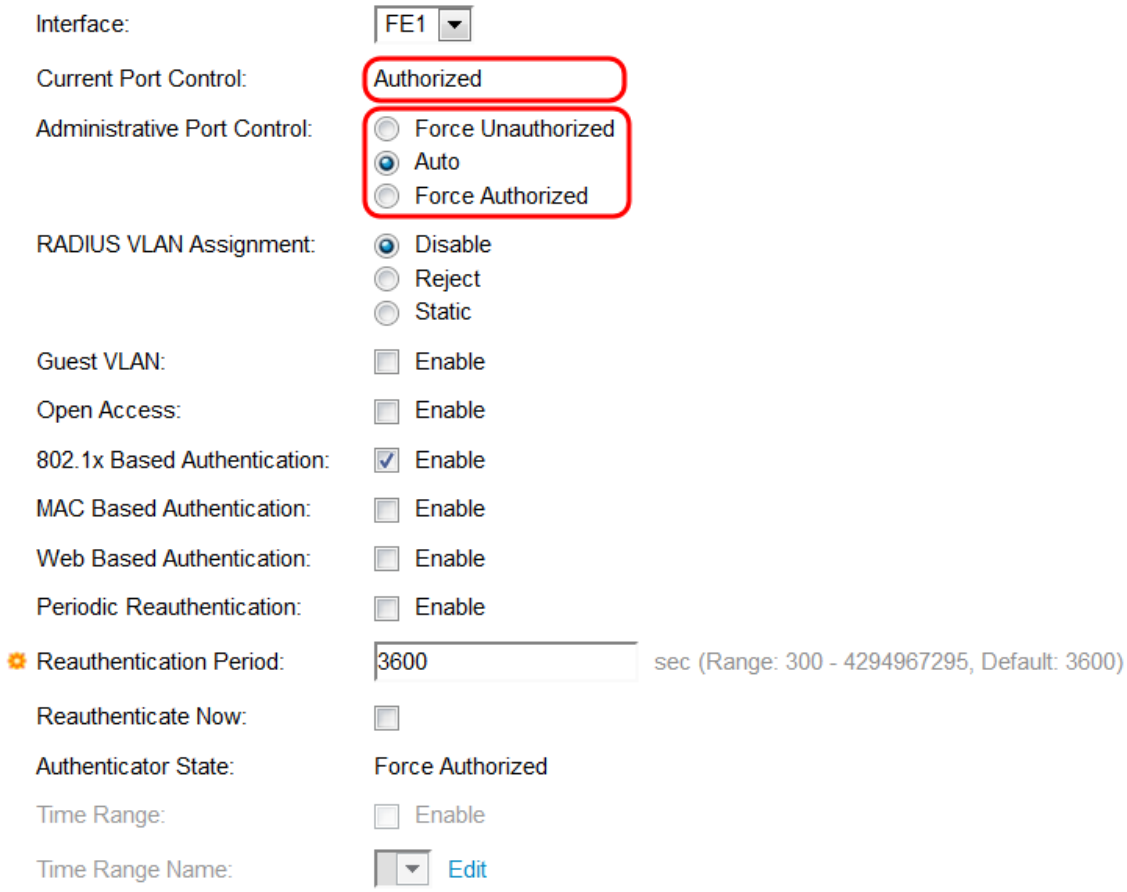
步驟5.導覽至**Security > 802.1X/MAC/Web Authentication > Port Authentication**。*Port Authentication*頁面隨即開啟。



步驟6.在*Port Authentication Table*中選擇要配置的埠，然後點選**Edit...**按鈕。*Edit Port Authentication*視窗開啟。



步驟7.在*Administrative Port Control*欄位中，選擇單選按鈕以確定連線埠如何授權作業階段。*Current Port Control*欄位顯示所選連線埠的目前授權狀態。



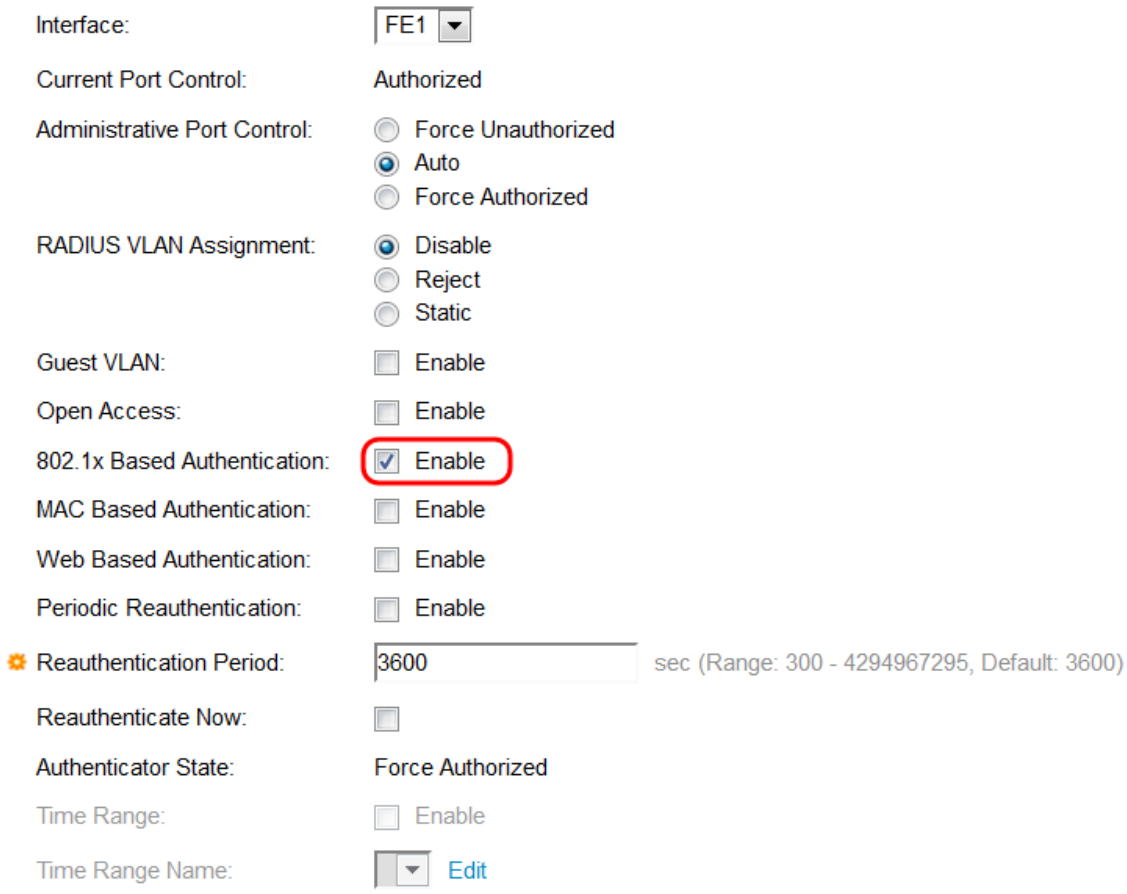
選項包括：

·強制未授權 — 將介面移至未授權狀態。裝置不向連線到此埠的任何客戶端提供身份驗證，並拒絕訪問。

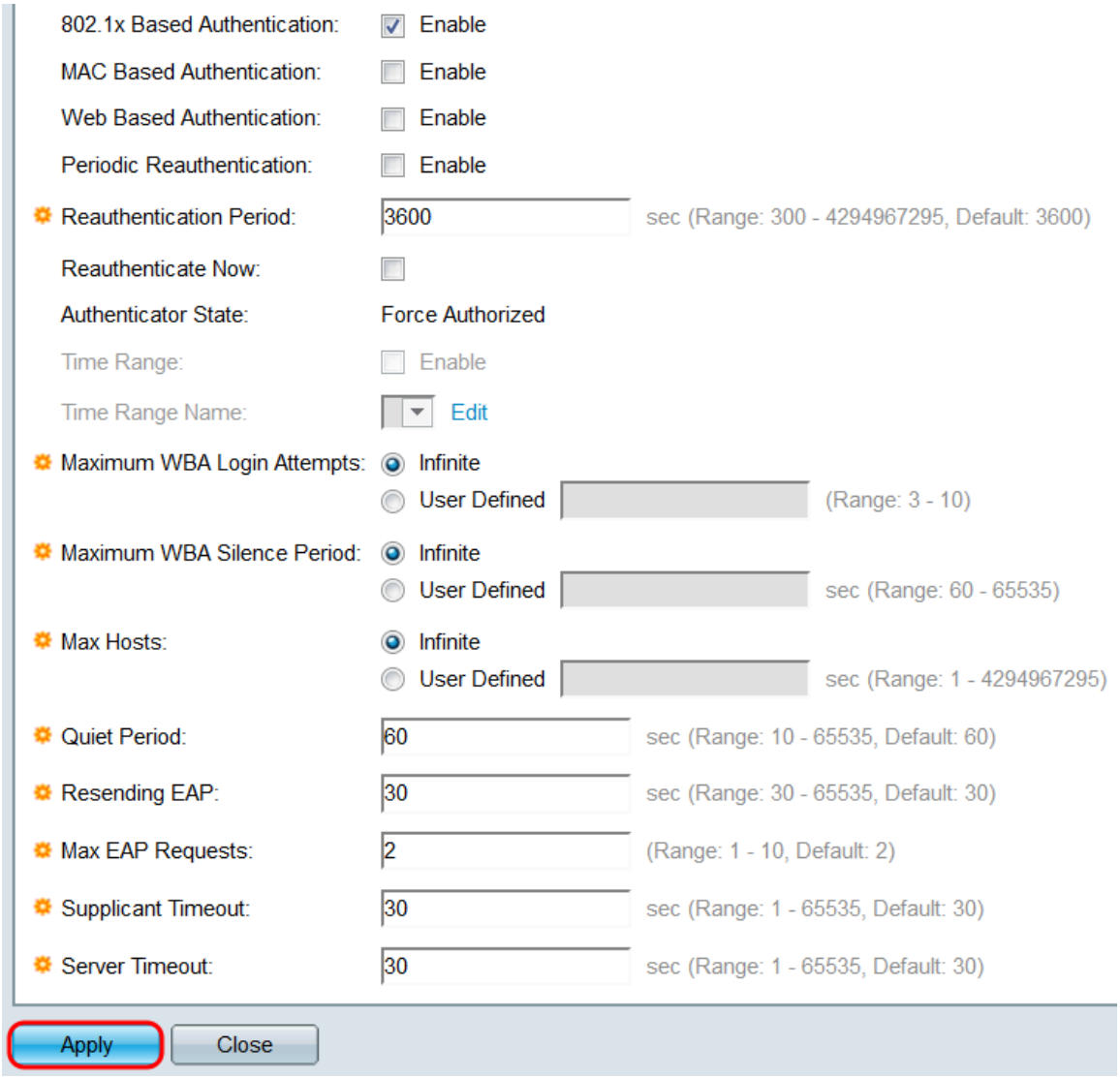
·自動 — 為所選埠啟用基於埠的身份驗證。根據身份驗證過程的結果，在已授權和未授權之間移動介面。選擇此選項以實現802.1X。

·強制授權 — 將介面移至授權狀態。裝置將提供對連線到此埠的任何客戶端的訪問而無需身份驗證。

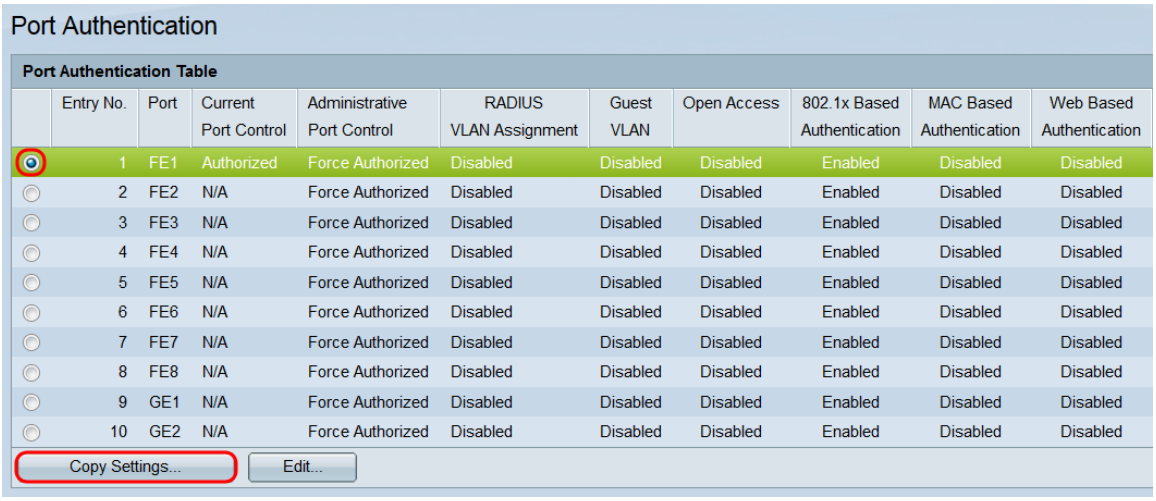
步驟8.選中*802.1X Based Authentication*欄位中的**Enable**覈取方塊，為所選埠啟用802.1X身份驗證。



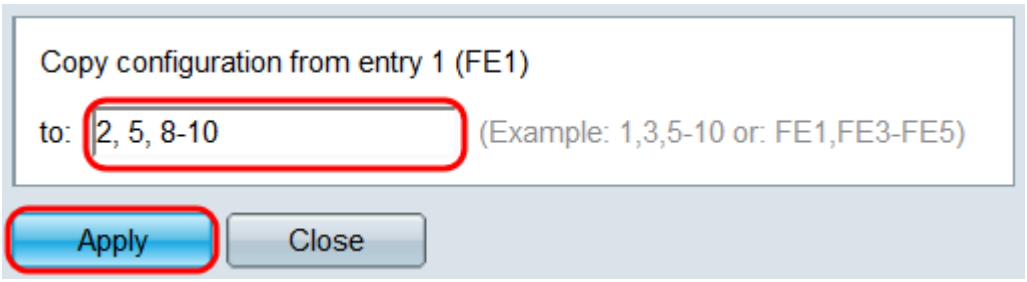
步驟9.按一下**Apply**。埠現在應完全配置為基於802.1X埠的身份驗證，並且已準備好開始驗證連線到該埠的任何客戶端。使用*Interface*欄位選擇要設定的不同連線埠，而不是回到*Port Authentication*頁面。



步驟10.如果要將連線埠的設定快速複製到另一個連線埠或連線埠範圍，請在「*連線埠驗證表*」中按一下要複製的連線埠的單選按鈕，然後按一下「**Copy Settings...**」按鈕。*Copy Settings*視窗開啟。



步驟11.在文本欄位中，輸入要複製設定的埠（用逗號分隔）。您還可以指定埠範圍。然後，按一下**Apply**複製設定。



檢視與本文相關的影片……

[按一下此處檢視思科的其他技術對話]