200/220/300系列交換機上的802.1X主機和會話身份驗證配置

目標

802.1X是連線埠型網路存取控制(PNAC)的IEEE標準，為連線到連線埠的裝置提供驗證方法。交換機的管理GUI中的Host and Session Authentication頁面用於定義每個埠使用的身份驗證型別。每埠身份驗證是一種功能，允許網路管理員根據所需的身份驗證型別劃分交換機埠。Authenticated Hosts頁顯示有關已進行身份驗證的主機的資訊。

本文說明如何按連線埠設定主機和作業階段驗證，以及如何在200/220/300系列託管交換器上的802.1X安全設定中檢視已驗證主機。

適用裝置

- Sx200系列
- Sx220系列
- Sx300系列

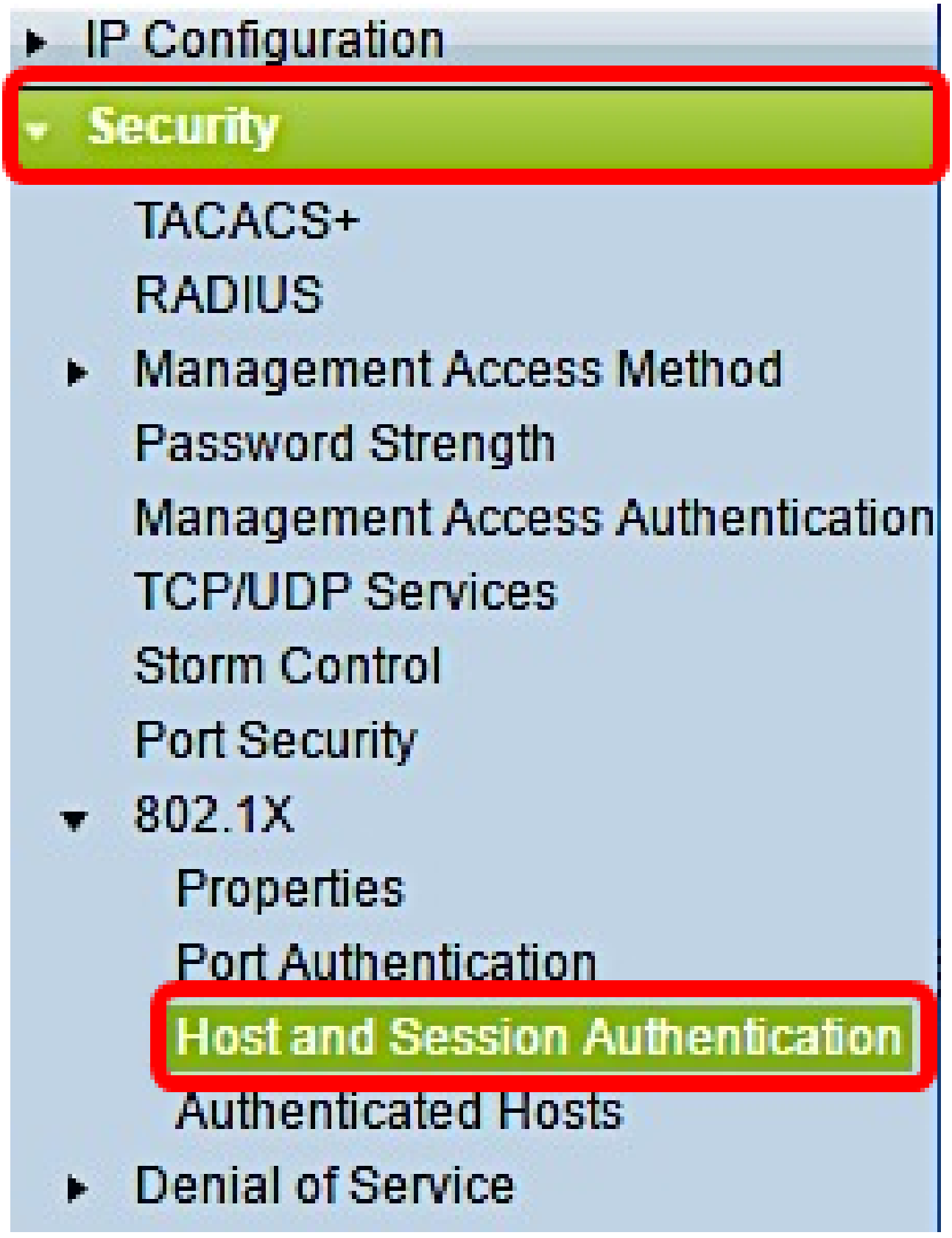
軟體版本

- 1.4.5.02 — Sx200系列、Sx300系列
- 1.1.0.14 — Sx220系列

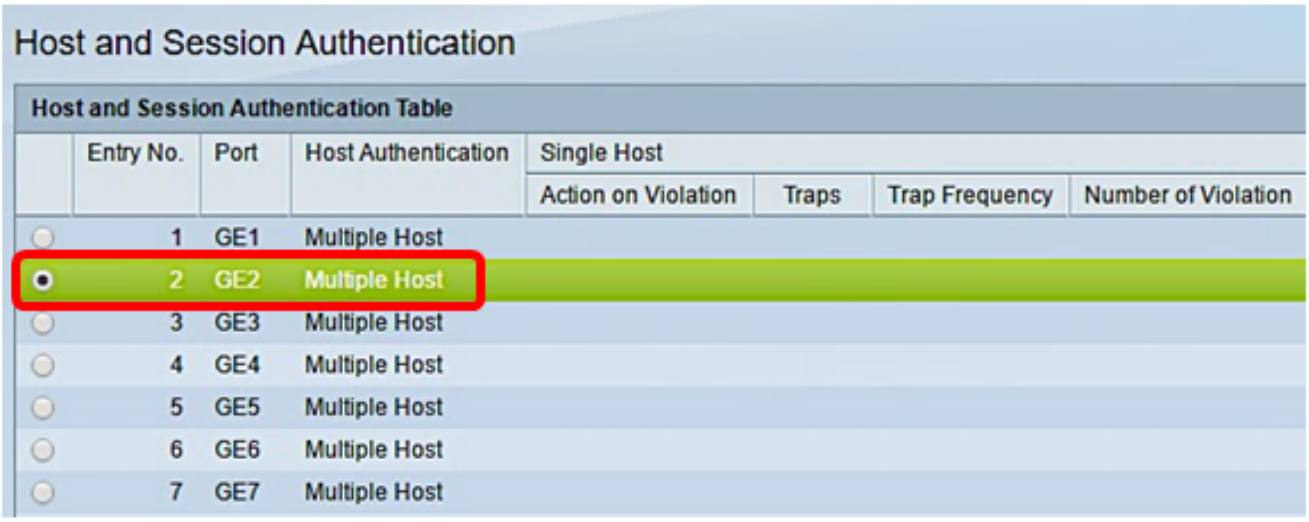
主機和作業階段驗證

步驟 1.登入到基於Web的實用程式，然後選擇Security > 802.1X > Host and Session Authentication。

註：以下影象來自SG220-26P智慧交換機。

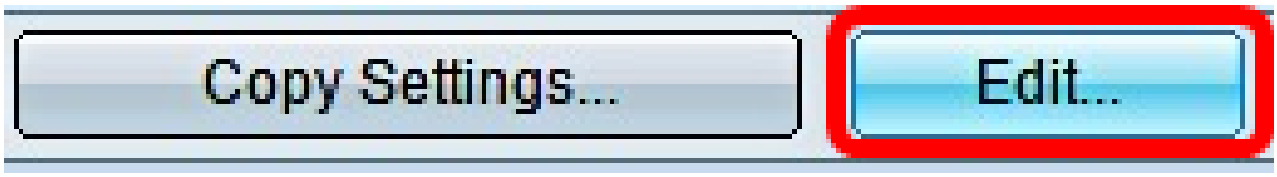


步驟 2.按一下要編輯的埠的單選按鈕。

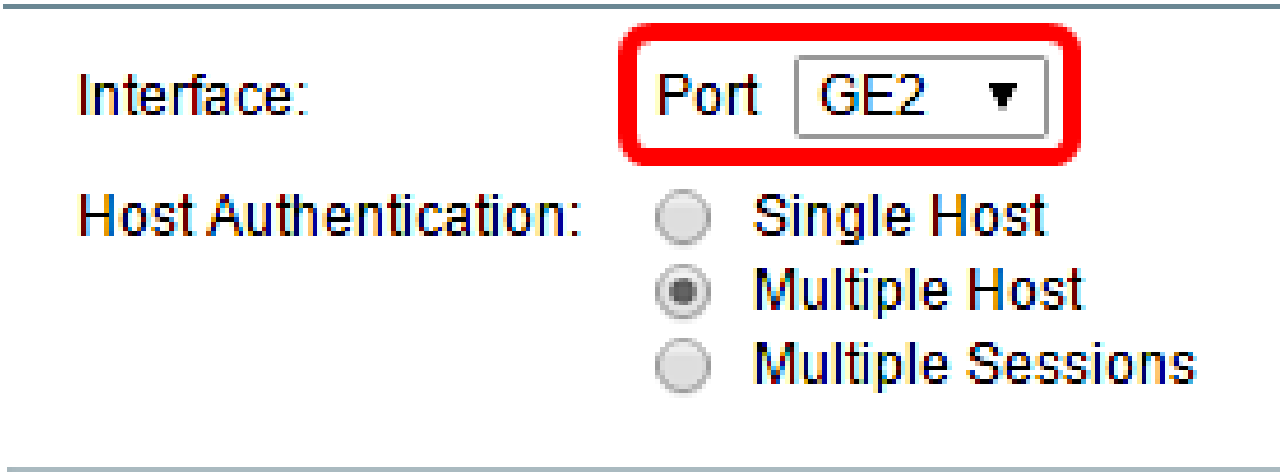


注意：在本示例中，選擇了埠GE2。

步驟 3.按一下Edit以編輯指定埠的主機和會話身份驗證。



步驟 4.系統將彈出Edit Port Authentication視窗。從Interface下拉選單中，確保指定的埠是您在第2步中選擇的埠。否則，按一下下拉箭頭並選擇正確的埠。

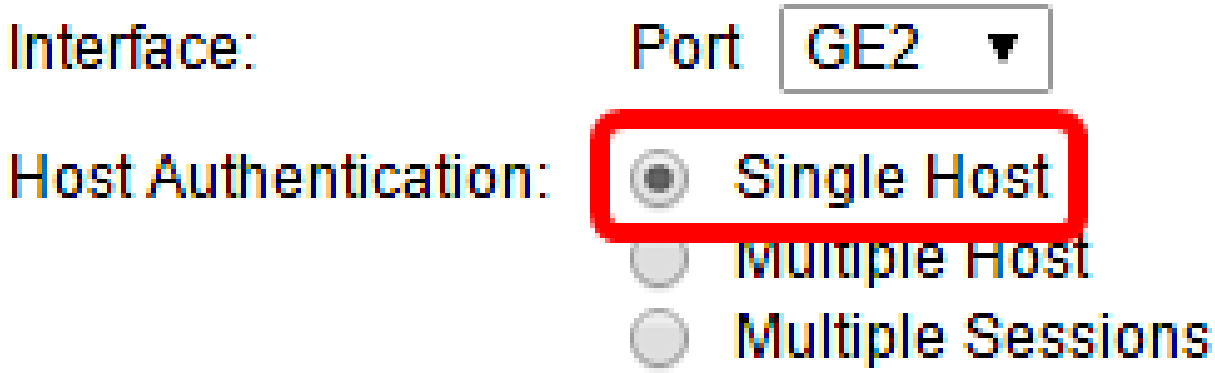


註：如果使用200或300系列，將顯示「編輯主機和會話身份驗證」視窗。

步驟 5.在Host Authentication欄位中點選與所需身份驗證模式對應的單選按鈕。選項包括：

- 單一主機 — 交換機僅授予單個授權主機對該埠的訪問許可權。
- 多主機(802.1X) — 多個主機可以訪問單個埠。這是預設模式。交換機只需要授權第一台主機，然後連線到該埠的所有其他客戶端都可以訪問網路。如果身份驗證失敗，則會拒絕第一台主機和所有連線的客戶端訪問網路。
- 多個作業階段 — 多個主機可以存取單一連線埠，但每個主機都必須通過驗證。

註：在本示例中，選擇單主機。

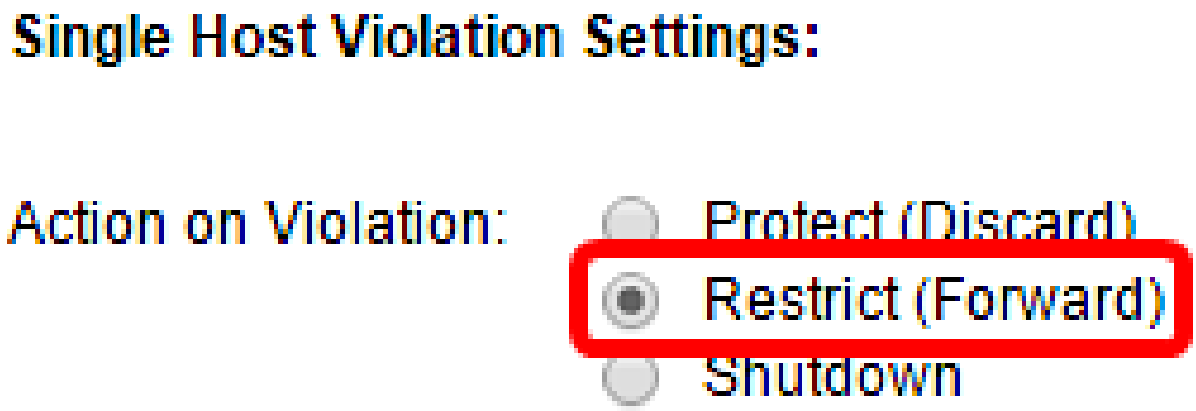


注意：如果選擇多個主機或多個會話，請跳至步驟9。

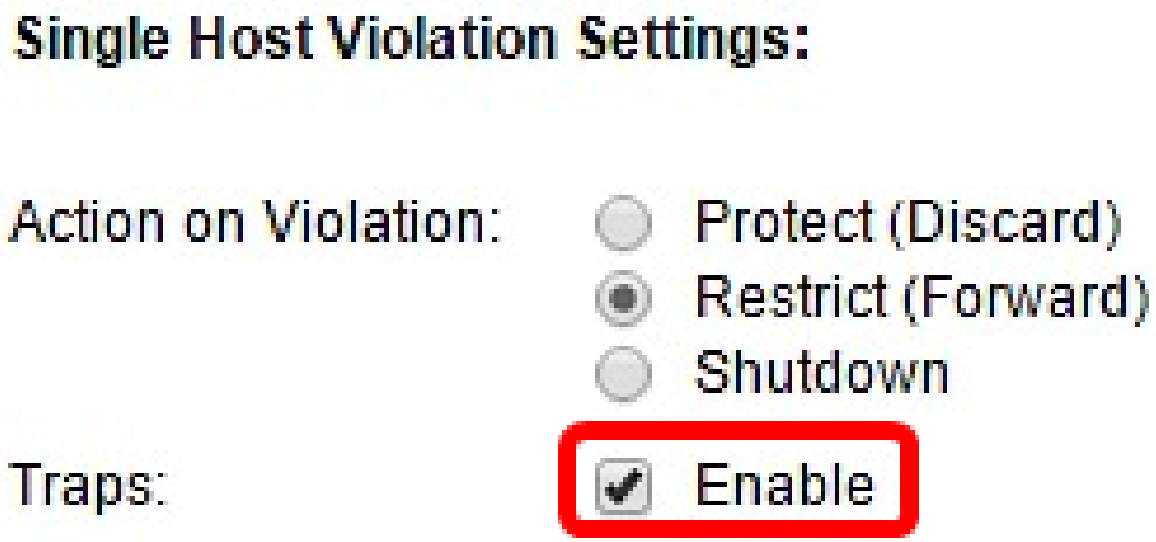
步驟 6.在Single Host Violation Settings區域中，點選與所需Action on Violation對應的單選按鈕。如果資料包來自的MAC地址與原始請求方的MAC地址不匹配的主機，則會發生衝突。發生這種情況時，該操作將決定從不屬於原始請求方的主機到達的資料包會發生什麼情況。選項包括：

- 保護（丟棄）— 丟棄資料包。這是預設操作。
- Restrict（轉發）— 提供訪問並轉發資料包。
- Shutdown — 封鎖封包並關閉連線埠。連線埠會一直關閉，直到重新啟用或交換器重新開機為止。

註：在此示例中，選擇Restrict(Forward)。



步驟7.（可選）選中Traps欄位中的Enable以啟用陷阱。陷阱是生成的簡單網路管理協定(SNMP)消息，用於報告系統事件。發生違規時，陷阱會傳送到交換器的SNMP管理員。



步驟 8.在Trap Frequency欄位中輸入已傳送陷阱之間所允許的所需時間（以秒為單位）。這定義了陷阱的傳送頻率。

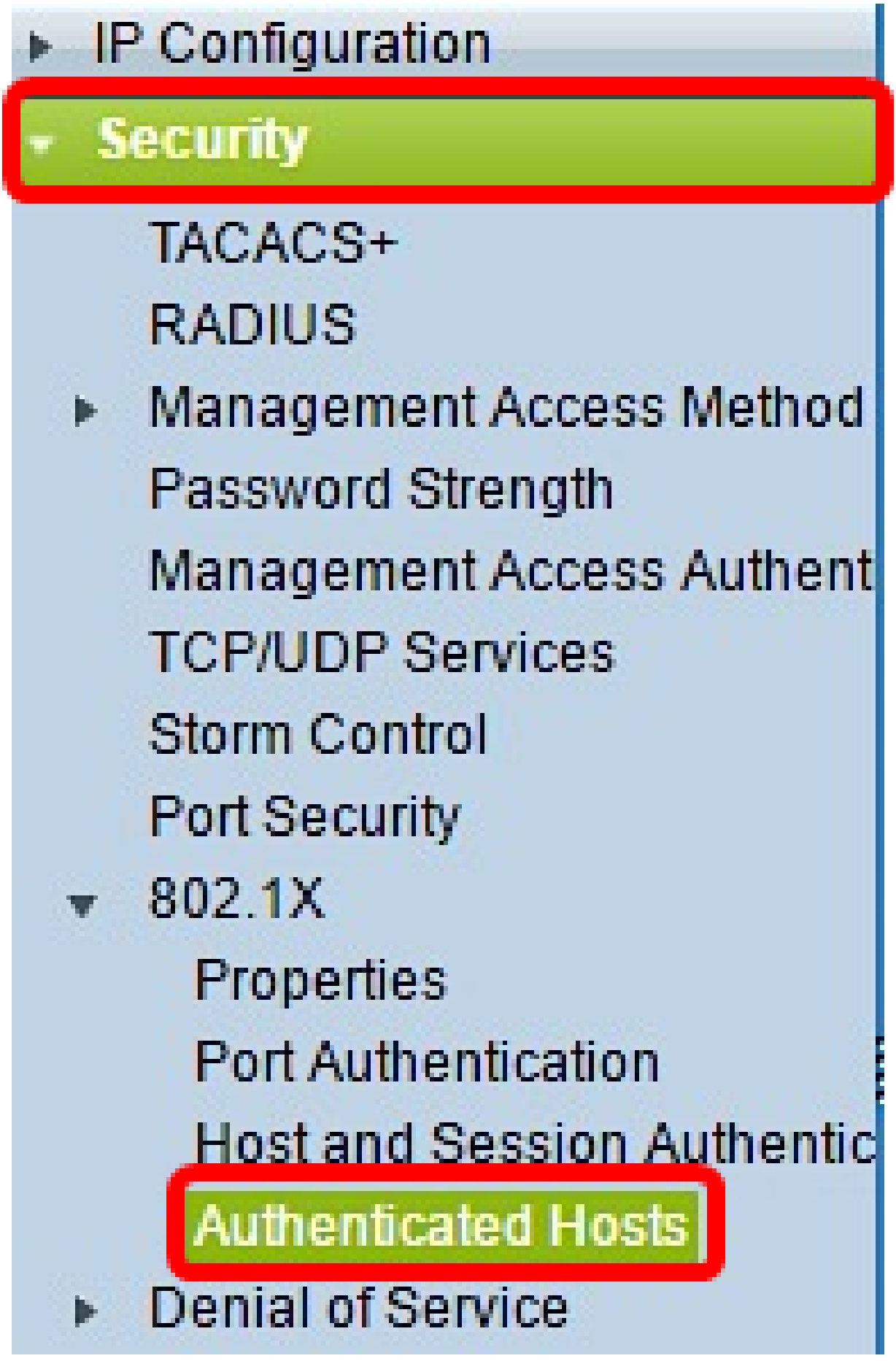
註：在本示例中，使用30秒。

步驟 9.按一下「Apply」。

現在，您應該在交換機上配置主機和會話身份驗證。

檢視經過驗證的主機

步驟 1.登入到基於Web的實用程式，然後選擇Security > 802.1X > Authenticated Host。


IP Configuration
Security
TACACS+
RADIUS
Management Access Method
Password Strength
Management Access Authent
TCP/UDP Services
Storm Control
Port Security
802.1X
Properties
Port Authentication
Host and Session Authentic
Authenticated Hosts
Denial of Service

Authenticated Hosts表顯示已驗證主機的以下資訊。

- 使用者名稱 — 指定在埠上經過身份驗證的請求方名稱。
- Port — 指定請求方所連線的埠號。
- Session Time — 指定請求方連線到埠的整個時間。格式為 DD:HH:MM:SS(Day:Hour:Minute:Second)。
- Authentication Method — 指定用於驗證的方法。可能的值為：
- None — 指定請求方未通過身份驗證。
- Radius — 指定請求方已由RADIUS伺服器進行驗證。
- MAC地址 — 指定請求方的MAC地址。
- VLAN ID — 指定主機所屬的VLAN。VLAN ID列僅在220系列Smart Plus交換機中可用。

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）。