在思科商務220系列交換器上設定802.1x驗證

目標

本文的目的是展示如何在思科商務220系列智慧交換器上設定802.1x驗證。

適用裝置 |韌體版本

- CBS220系列（產品手冊） | 2.0.0.17

簡介

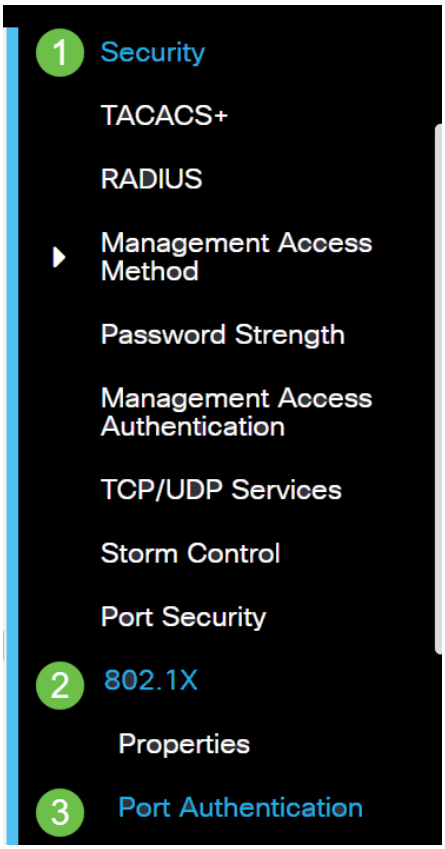
埠身份驗證允許為每個埠配置引數。由於某些配置更改僅在埠處於「強制授權」狀態（如主機身份驗證）時才可能，因此建議您在更改之前將埠控制更改為「強制授權」。配置完成後，將埠控制返回到其先前狀態。

定義了802.1x的埠不能成為LAG的成員。不能在同一埠上同時啟用802.1x和埠安全。如果在介面上啟用埠安全，則管理埠控制不能更改為自動模式。

配置埠身份驗證

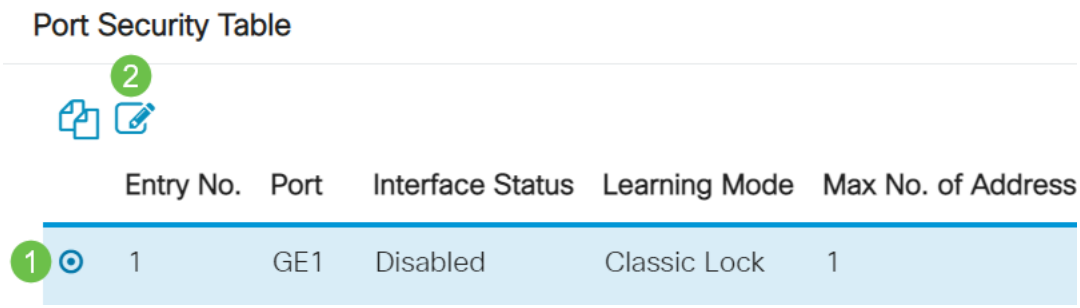
步驟1

登入交換器Web使用者介面(UI)，然後選擇**Security > 802.1x > Port Authentication**。



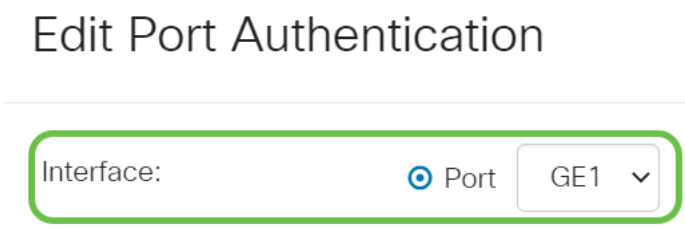
步驟2

點選要配置的埠的單選按鈕，然後點選**編輯圖示**。



步驟3

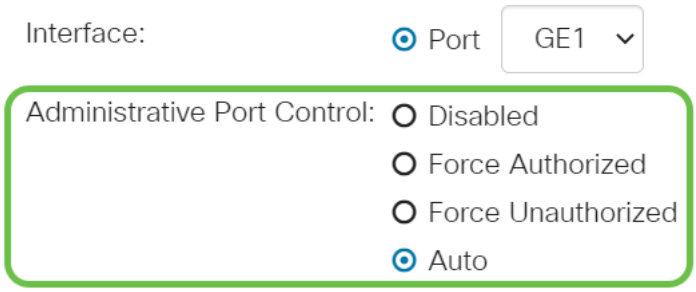
系統將彈出*Edit Port Authentication*視窗。從Interface下拉選單中，確保指定的埠是您在第2步中選擇的埠。否則，按一下下拉箭頭並選擇正確的埠。



步驟4

選擇管理埠控制的單選按鈕。這將確定埠授權狀態。選項包括：

- **Disabled** — 禁用802.1x。這是預設狀態。
- **強制未授權**(Force Unauthorized) — 通過將介面移至未授權狀態來拒絕介面訪問。交換機不通過介面向客戶端提供身份驗證服務。
- **自動** — 在交換器上啟用連線埠型驗證和授權。根據交換機和客戶端之間的身份驗證交換，該介面在已授權或未授權狀態之間移動。
- **強制授權** — 授權介面而不進行身份驗證。

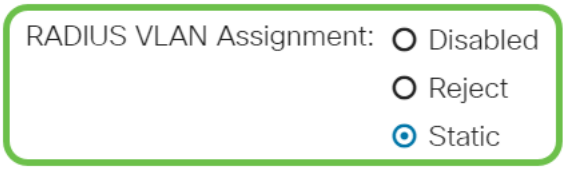


第5步（可選）

選擇RADIUS VLAN分配的單選按鈕。這將啟用指定埠上的動態VLAN分配。選項包括：

- **Disabled** — 忽略VLAN授權結果並保留主機的原始VLAN。這是預設操作。
- **拒絕** — 如果指定的埠收到VLAN授權資訊，它將使用該資訊。但是，如果沒有VLAN授權資訊，則會拒絕主機並使其未授權。
- **Static** — 如果指定的埠收到VLAN授權資訊，它將使用該資訊。但是，如果沒有VLAN授權資訊，它將保留主機的原始VLAN。

如果存在來自RADIUS的VLAN授權資訊，但是未在測試裝置(DUT)上管理性建立VLAN，則系統將自動建立VLAN。



快速提示：要使「動態VLAN分配」功能生效，交換機要求RADIUS伺服器傳送以下VLAN屬性：

- [64] Tunnel-Type = VLAN（型別13）
- [65] Tunnel-Medium-Type = 802（型別6）
- [81] Tunnel-Private-Group-Id = VLAN ID

第6步（可選）

勾選**Enable**覈取方塊，使訪客VLAN將訪客VLAN用於未授權的埠。

第7步

選中**Enable**覈取方塊以定期重新驗證。這將啟用在指定的重新身份驗證時間段後埠重新身份驗證嘗試。

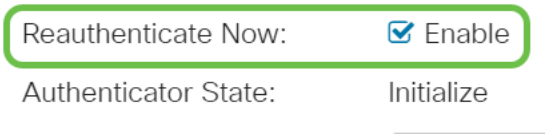
步驟8

在*Reauthentication Period*欄位中輸入值。這是重新驗證連線埠的時間（以秒為單位）。

第9步（可選）

選中**Reauthenticate Now**覈取方塊以啟用即時埠重新身份驗證。

Authenticator State欄位顯示身份驗證的當前狀態。



如果埠未處於Force Authorized或Force Unauthorized狀態，則該埠處於Auto Mode並且驗證器顯示正在進行的驗證狀態。連線埠通過驗證後，狀態顯示為「Authenticated」。

步驟10

在「*Max Hosts*」欄位中，輸入特定連線埠上允許的最大已驗證主機數量。該值僅在多會話模式下生效。

步驟11

在「*Quiet Period*」欄位中，輸入交換器在驗證交換失敗後保持安靜狀態的秒數。當交換機處於安靜

狀態時，這意味著交換機沒有偵聽來自客戶端的新身份驗證請求。

步驟12

在「*Reending EAP*」欄位中，輸入交換機在重新傳送請求之前等待請求方（客戶端）對可擴展身份驗證協定(EAP)請求或身份幀的響應的秒數。

步驟13

在*Max EAP Requests*欄位中，輸入可以傳送的最大EAP請求數。如果在定義的時間段（請求方超時）之後未收到響應，身份驗證過程將重新啟動。

步驟14

在*Supplicant Timeout*欄位中，輸入將EAP請求重新傳送到請求方之前經過的秒數。

步驟15

在「*Server Timeout*」欄位中，輸入交換器將要求重新傳送到驗證伺服器之前經過的秒數。

步驟16

按一下「Apply」。

現在，您應該在交換機上成功配置802.1x身份驗證。

如需更多設定，請參閱思科商務220系列交換器管理指南。

如果您想檢視其他文章，請檢視思科商務220系列交換器支援頁面