Configurazione dell'autenticazione 802.1x sugli switch Cisco Business serie 220

Obiettivo

L'obiettivo di questo articolo è mostrare come configurare l'autenticazione 802.1x sugli smart switch Cisco Business serie 220.

Dispositivi interessati | Versione firmware

- Serie CBS220 (DataSheet) | 2.0.0.17

Introduzione

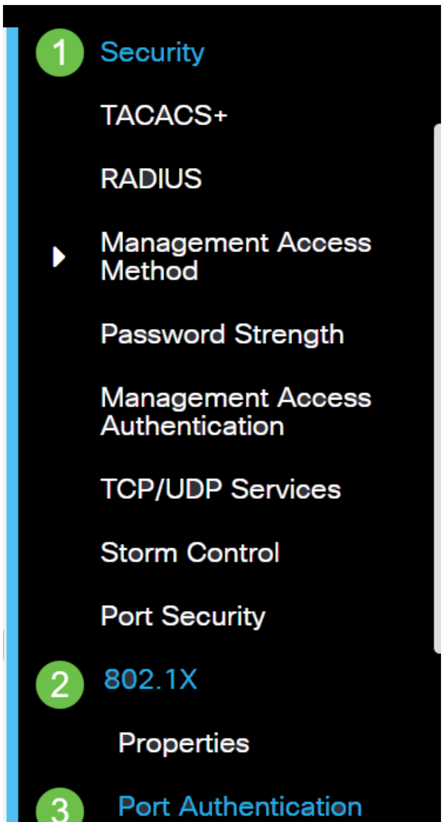
L'autenticazione della porta consente la configurazione dei parametri per ciascuna porta. Poiché alcune modifiche della configurazione sono possibili solo quando la porta è in uno stato di autorizzazione forzata, ad esempio l'autenticazione dell'host, è consigliabile modificare il controllo della porta in Forza autorizzazione prima di apportare le modifiche. Al termine della configurazione, ripristinare lo stato precedente del controllo della porta.

Una porta su cui è definito 802.1x non può diventare membro di un LAG. Impossibile abilitare contemporaneamente 802.1x e Port Security sulla stessa porta. Se si abilita la protezione delle porte su un'interfaccia, non è possibile impostare la modalità automatica per il controllo amministrativo delle porte.

Configura autenticazione porta

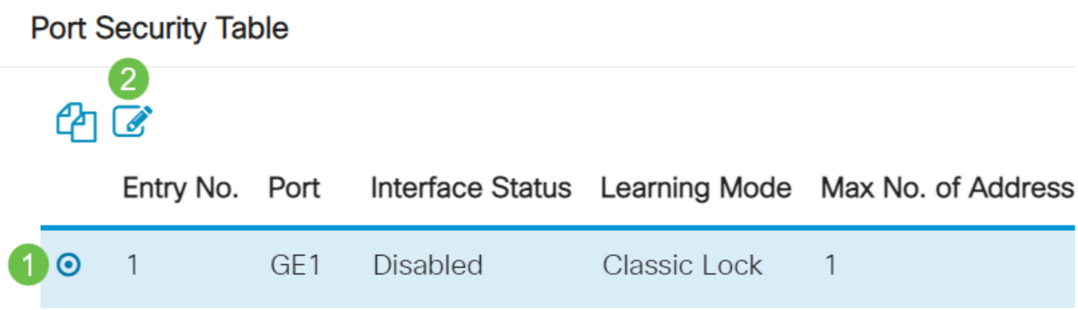
Passaggio 1

Accedere all'interfaccia utente Web dello switch e scegliere **Sicurezza > 802.1x > Autenticazione porta**.



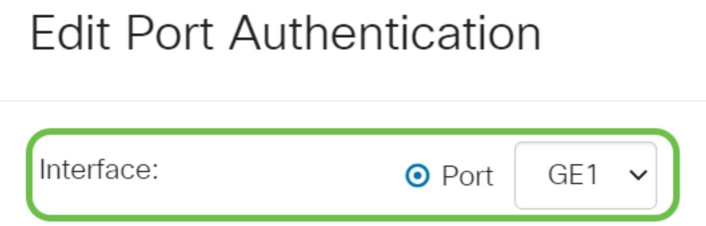
Passaggio 2

Fare clic sul pulsante di opzione della porta che si desidera configurare, quindi fare clic sull'**icona Modifica**.



Passaggio 3

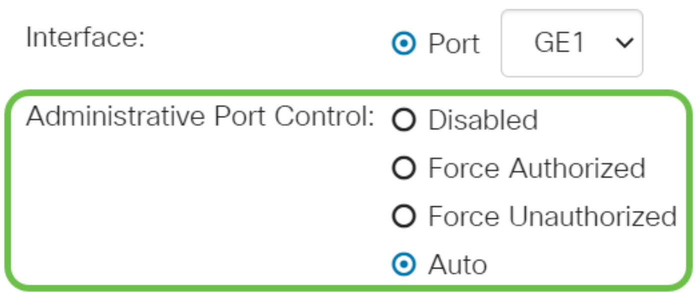
Viene visualizzata la finestra *Modifica autenticazione porta*. Dall'elenco a discesa Interfaccia, verificare che la porta specificata sia quella scelta nel passaggio 2. In caso contrario, fare clic sulla freccia dell'elenco a discesa e scegliere la porta corretta.



Passaggio 4

Scegliere un pulsante di opzione per il controllo della porta amministrativa. In questo modo viene determinato lo stato di autorizzazione della porta. Le opzioni sono:

- **Disabilitato**: disabilita 802.1x. Si tratta dello stato predefinito.
- **Force Unauthorized** — Nega l'accesso all'interfaccia attivando lo stato non autorizzato sull'interfaccia. Lo switch non fornisce servizi di autenticazione al client tramite l'interfaccia.
- **Auto**: attiva l'autenticazione e l'autorizzazione basate sulle porte sullo switch. L'interfaccia viene spostata tra uno stato autorizzato e uno non autorizzato in base allo scambio di autenticazione tra lo switch e il client.
- **Force Authorized**: autorizza l'interfaccia senza autenticazione.

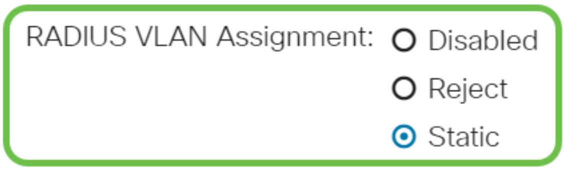


Passaggio 5 (facoltativo)

Selezionare un pulsante di opzione per l'assegnazione della VLAN RADIUS. L'assegnazione della VLAN dinamica verrà abilitata sulla porta specificata. Le opzioni sono:

- **Disabled**: ignora i risultati dell'autorizzazione VLAN e mantiene la VLAN originale dell'host. Questa è l'azione predefinita.
- **Reject**: se la porta specificata riceve un'informazione di autorizzazione VLAN, utilizzerà tale informazione. Tuttavia, se non sono presenti informazioni autorizzate sulla VLAN, l'host viene rifiutato e la VLAN non viene autorizzata.
- **Statico**: se la porta specificata riceve informazioni autorizzate dalla VLAN, utilizzerà queste informazioni. Tuttavia, se non sono presenti informazioni autorizzate sulla VLAN, rimarrà la VLAN originale dell'host.

Se sono presenti informazioni VLAN autorizzate da RADIUS, ma la VLAN non è creata amministrativamente su Device Under Test (DUT), la VLAN verrà creata automaticamente.



Suggerimento rapido: affinché la funzione di assegnazione dinamica della VLAN funzioni, lo switch richiede l'invio da parte del server RADIUS dei seguenti attributi VLAN:

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

Passaggio 6 (facoltativo)

Selezionare la casella di controllo **Enable** (Abilita) per fare in modo che la VLAN guest utilizzi una VLAN guest per le porte non autorizzate.

Passaggio 7

Selezionare la casella di controllo **Attiva** per la riautenticazione periodica. Verranno abilitati i tentativi di riautenticazione delle porte dopo il periodo di riautenticazione specificato.

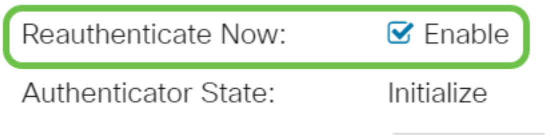
Passaggio 8

Immettere un valore nel campo *Periodo di riautenticazione*. Tempo di riautenticazione della porta espresso in secondi.

Passaggio 9 (facoltativo)

Selezionare la casella di controllo **Riautentica ora** per abilitare la riautenticazione immediata delle porte.

Nel campo Stato autenticatore viene visualizzato lo stato corrente dell'autenticazione.



Se la porta non è in stato Force Authorized o Force Unauthorized, si trova in modalità automatica e l'autenticatore visualizza lo stato dell'autenticazione in corso. Dopo l'autenticazione della porta, lo stato viene visualizzato come Autenticato.

Passaggio 10

Nel campo *Max Hosts*, immettere il numero massimo di host autenticati consentiti sulla porta specifica. Questo valore ha effetto solo in modalità multisessione.

Passaggio 11

Nel campo *Quiet Period* (Periodo di inattività), immettere il numero di secondi durante i quali lo switch rimane in stato di inattività in seguito a uno scambio di autenticazione non riuscito. Quando lo switch è in uno stato non interattivo, non è in ascolto di nuove richieste di autenticazione da parte del client.

Passaggio 12

Nel campo *Rinvio EAP*, immettere il numero di secondi che lo switch attende per la risposta a una richiesta EAP (Extensible Authentication Protocol) o a un frame di identità dal supplicant (client) prima di inviare nuovamente la richiesta.

Passaggio 13

Nel campo *Numero massimo di richieste EAP*, immettere il numero massimo di richieste EAP che possono essere inviate. Se non si riceve una risposta dopo il periodo definito (timeout del supplicant), il processo di autenticazione viene riavviato.

Passaggio 14

Nel campo *Timeout supplicant*, immettere il numero di secondi che devono trascorrere prima che le richieste EAP vengano inviate al supplicant.

Passaggio 15

Nel campo *Timeout server*, immettere il numero di secondi che devono trascorrere prima che lo switch invii nuovamente una richiesta al server di autenticazione.

Passaggio 16

Fare clic su Apply (Applica).

A questo punto, è necessario configurare correttamente l'autenticazione 802.1x sullo switch.

Per ulteriori configurazioni, fare riferimento al Cisco Business serie 220 Switch Administration Guide.

Per visualizzare altri articoli, consultare la pagina di supporto degli switch Cisco Business serie 220