Configurazione dell'autenticazione host e sessione 802.1X sugli switch serie 220/220/300

Obiettivo

802.1X è uno standard IEEE per PNAC (Network Access Control) basato sulle porte che fornisce un metodo di autenticazione alle periferiche connesse alle porte. La pagina Autenticazione host e sessione nell'interfaccia utente grafica di amministrazione dello switch viene usata per definire il tipo di autenticazione da usare per ciascuna porta. L'autenticazione per porta è una funzione che consente a un amministratore di rete di dividere le porte dello switch in base al tipo di autenticazione desiderato. La pagina Host autenticati visualizza le informazioni sugli host autenticati.

In questo documento viene spiegato come configurare l'autenticazione di sessioni e host per singola porta e come visualizzare gli host autenticati nelle impostazioni di sicurezza 802.1X sugli switch gestiti serie 200/220/300.

Dispositivi interessati

- Serie Sx200
- Serie Sx220
- Serie Sx300

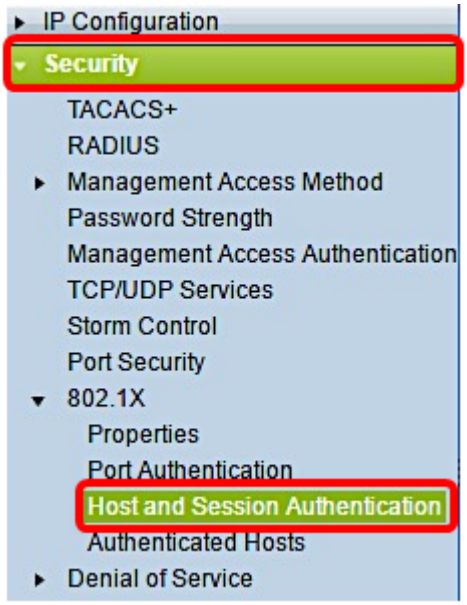
Versione del software

- 1.4.5.02 — Serie Sx200, Serie Sx300
- 1.1.0.14 — Serie Sx220

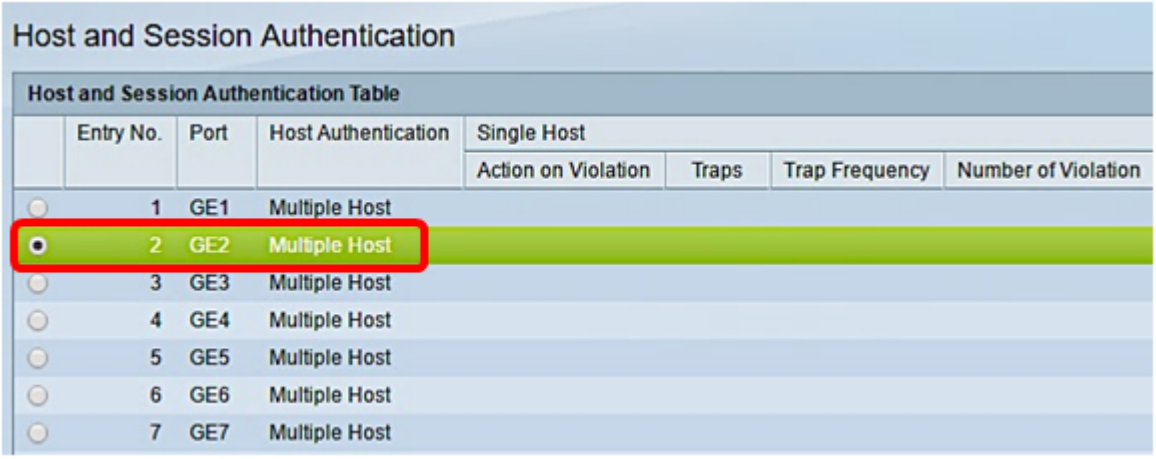
Autenticazione host e sessione

Passaggio 1. Accedere all'utility basata sul Web e scegliere **Sicurezza > 802.1X > Autenticazione host e sessione**.

Nota: le immagini seguenti vengono acquisite dallo Smart Switch SG220-26P.

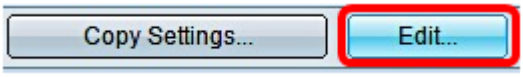


Passaggio 2. Fare clic sul pulsante di opzione della porta che si desidera modificare.

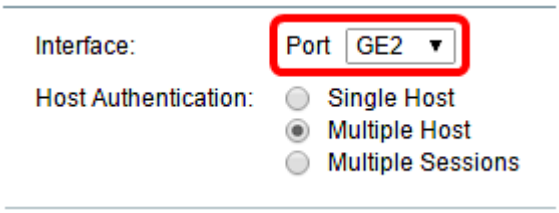


Nota: nell'esempio viene scelta la porta GE2.

Passaggio 3. Fare clic su **Edit** (Modifica) per modificare l'autenticazione host e sessione per la porta specificata.



Passaggio 4. Viene visualizzata la finestra Modifica autenticazione porta. Dall'elenco a discesa Interface (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 destra.

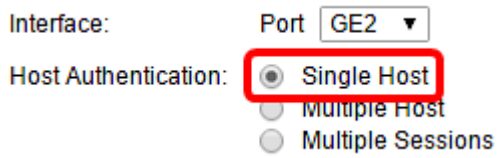


Nota: se si utilizza la serie 200 o 300, viene visualizzata la finestra Modifica autenticazione host e sessione.

Passaggio 5. Fare clic sul pulsante di opzione corrispondente alla modalità di autenticazione desiderata nel campo *Autenticazione host*. Le opzioni sono:

- Host singolo: lo switch concede l'accesso alla porta solo a un host autorizzato.
- Multiple Host (802.1X): più host possono accedere alla singola porta. Questa è la modalità predefinita. Lo switch richiede l'autorizzazione solo del primo host, quindi tutti gli altri client connessi alla porta hanno accesso alla rete. Se l'autenticazione ha esito negativo, l'accesso alla rete verrà negato al primo host e a tutti i client collegati.
- Sessioni multiple: più host possono accedere alla singola porta, ma ogni host deve essere autenticato.

Nota: nell'esempio riportato viene scelto Host singolo.

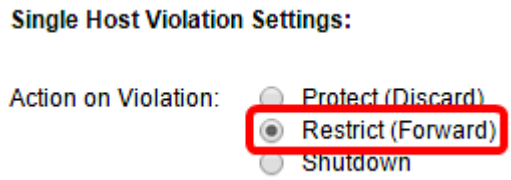


Nota: se si sceglie Più host o Sessioni multiple, andare al passo 9.

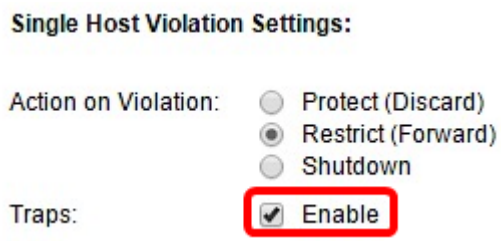
Passaggio 6. Nell'area Impostazioni violazione host singolo, fare clic sul pulsante di opzione corrispondente all'azione in caso di violazione desiderata. Una violazione si verifica se i pacchetti arrivano da un host il cui indirizzo MAC non corrisponde a quello del supplicant originale. In questo caso, l'azione determina cosa succede ai pacchetti provenienti da host che non sono considerati il supplicant originale. Le opzioni sono:

- Proteggi (Elimina) — scarta i pacchetti. Questa è l'azione predefinita.
- Restrict (Forward) - Fornisce l'accesso e inoltra i pacchetti.
- Shutdown — blocca i pacchetti e chiude la porta. La porta rimane inattiva finché non viene riattivata o finché lo switch non viene riavviato.

Nota: in questo esempio, è stato scelto Limita (inoltra).



Passaggio 7. (Facoltativo) Selezionare **Attiva** nel campo *Registrazioni* per attivare le registrazioni. I trap sono messaggi SNMP (Simple Network Management Protocol) generati per segnalare eventi di sistema. Quando si verifica una violazione, viene inviata una trap al manager SNMP dello switch.



Passaggio 8. Nel campo *Frequenza trap*, immettere il tempo desiderato, in secondi, tra le

trap inviate. In questo modo viene definita la frequenza di invio delle trap.

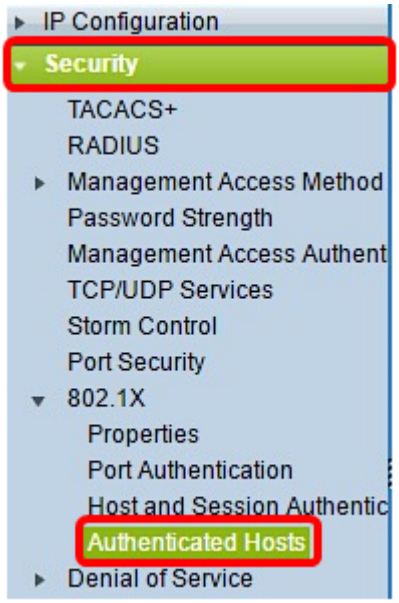
Nota: nell'esempio vengono usati 30 secondi.

Passaggio 9. Fare clic su Apply (Applica).

A questo punto, è necessario configurare l'autenticazione dell'host e della sessione sullo switch.

Visualizzazione degli host autenticati

Passaggio 1. Accedere all'utility basata sul Web e scegliere **Sicurezza > 802.1X > Host autenticato**.



La tabella Host autenticati visualizza le informazioni riportate di seguito per gli host autenticati.

- Nome utente — specifica il nome supplicant autenticato sulla porta.

- Porta - specifica il numero della porta a cui è connesso il supplicant.
- Session Time: specifica l'intero tempo in cui il richiedente è stato connesso alla porta. Il formato è GG:HH:MM:SS (Day:Hour:Minute:Second).
- Metodo di autenticazione — specifica il metodo utilizzato per l'autenticazione. I valori possibili sono:
- Nessuno — specifica che il supplicant non è stato autenticato.
- Radius: specifica che il supplicant è stato autenticato dal server RADIUS.
- Indirizzo MAC — specifica l'indirizzo MAC del supplicant.
- ID VLAN: per specificare la VLAN a cui appartiene l'host. La colonna VLAN ID è disponibile solo sugli switch Smart Plus serie 220.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).