Configurazione di 802.1X sugli switch serie SG300

Obiettivo

802.1X è uno standard IEEE che implementa l'autenticazione basata sulla porta. Se una porta utilizza 802.1X, tutti i client che utilizzano tale porta (definiti supplicant) devono presentare credenziali corrette prima di poter accedere alla rete. Un dispositivo che implementa 802.1X (definito autenticatore) deve essere in grado di comunicare con un server RADIUS (Remote Authentication Dial-In User Service) che si trova in un altro punto della rete. Questo server contiene un elenco di utenti validi a cui è consentito l'accesso alla rete; le credenziali inviate dall'autenticatore (fornite dal supplicant) devono corrispondere a quelle in possesso del server RADIUS. In tal caso, il server comunica all'autenticatore di concedere l'accesso all'utente; in caso contrario, l'autenticatore negherà l'accesso.

Lo standard 802.1X è una buona misura di sicurezza per impedire agli utenti indesiderati di accedere alla rete collegandosi a una porta fisica. Affinché 802.1X funzioni correttamente, è necessario che un server RADIUS sia già configurato in un altro punto della rete e che l'autenticatore sia in grado di comunicare con esso.

L'obiettivo di questo documento è mostrare come configurare 802.1X sugli switch serie SG300.

Dispositivi interessati

·Serie SG300 Switch

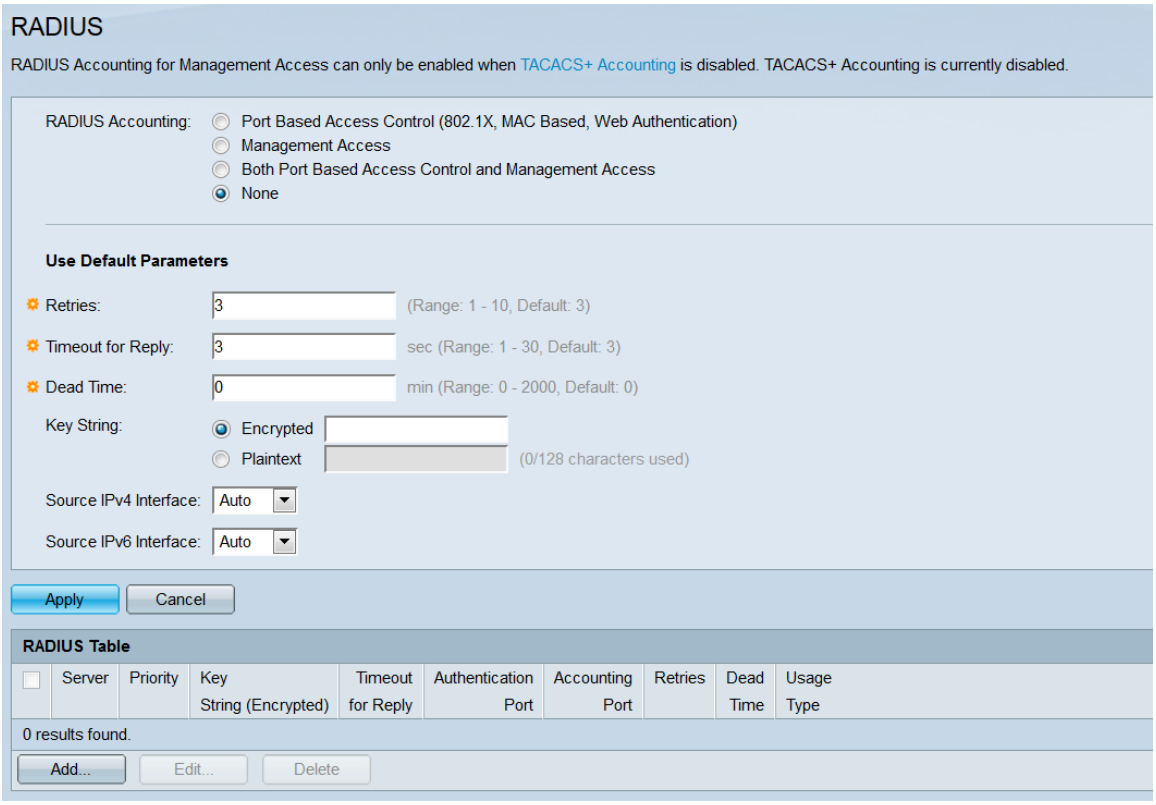
Versione del software

·v1.4.1.3

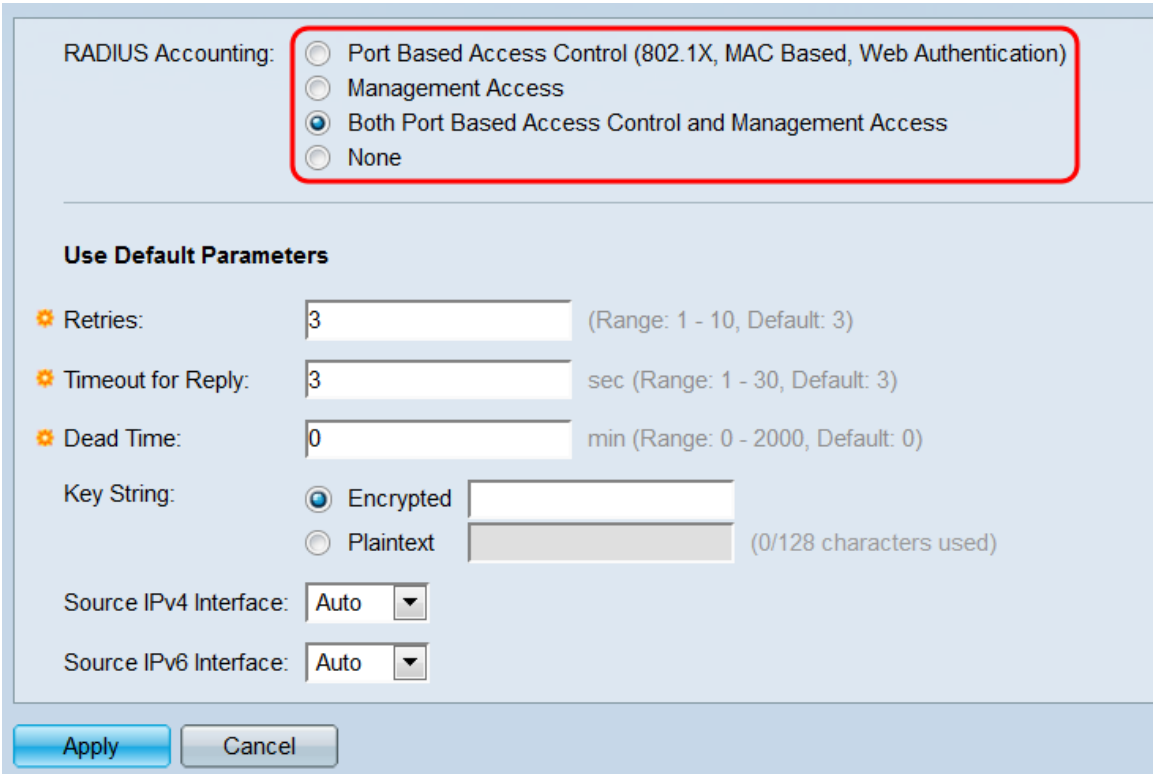
Impostazione dell'autenticazione 802.1X

Aggiunta di un server RADIUS

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > RADIUS**. Viene visualizzata la pagina *RADIUS*.



Passaggio 2. Nel campo *Accounting RADIUS*, scegliere un pulsante di opzione per selezionare il tipo di informazioni di accounting che verranno fornite al server RADIUS. È possibile assegnare a un server RADIUS informazioni di accounting che tengano traccia del tempo di sessione di un utente, delle risorse utilizzate e di altri elementi. L'opzione selezionata non influirà sulle prestazioni di 802.1X.



Le opzioni sono:

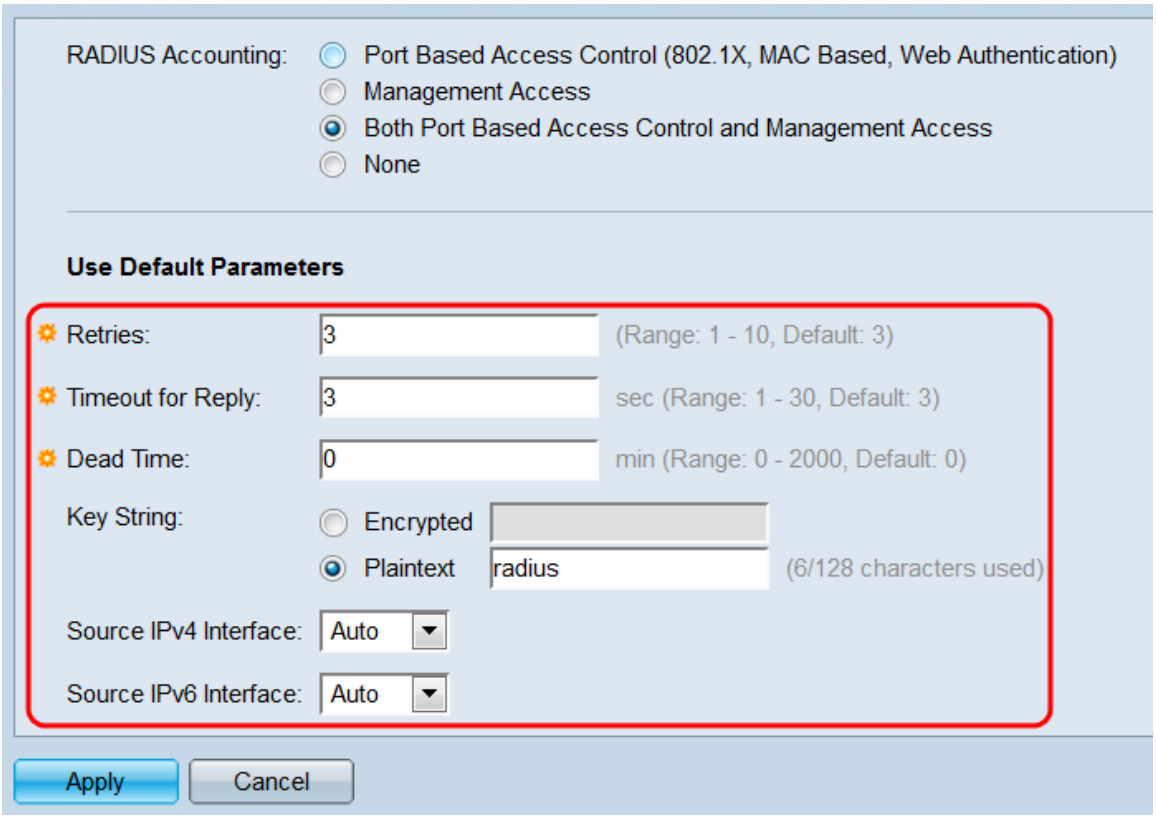
·Controllo degli accessi basato sulle porte - Questa opzione invia al server RADIUS le informazioni di accounting relative alle sessioni autenticate basate sulle porte.

·Accesso alla gestione: questa opzione invia al server RADIUS le informazioni di accounting relative alle sessioni di gestione dello switch.

·Controllo e gestione degli accessi basati sulle porte - Questa opzione invia entrambi i tipi di informazioni di accounting al server RADIUS.

·Nessuno - Non invia informazioni di accounting al server RADIUS.

Passaggio 3. Nell'area *Usa parametri predefiniti* configurare le impostazioni che verranno utilizzate per impostazione predefinita a meno che non venga configurato un server RADIUS aggiunto con impostazioni specifiche. per ciascuna voce server aggiunta allo switch è possibile utilizzare le impostazioni predefinite o impostazioni univoche separate. Per questo articolo verranno utilizzate le impostazioni predefinite definite in questa sezione.



Configurare le impostazioni seguenti:

·Nuovi tentativi - Immettere il numero di tentativi che lo switch eseguirà per contattare un server RADIUS prima di passare al server successivo. Il valore predefinito è 3.

·Timeout per la risposta - Immettere il numero di secondi che lo switch attende per ricevere una risposta dal server RADIUS prima di intraprendere ulteriori azioni (riprovare o rinunciare). Il valore predefinito è 3.

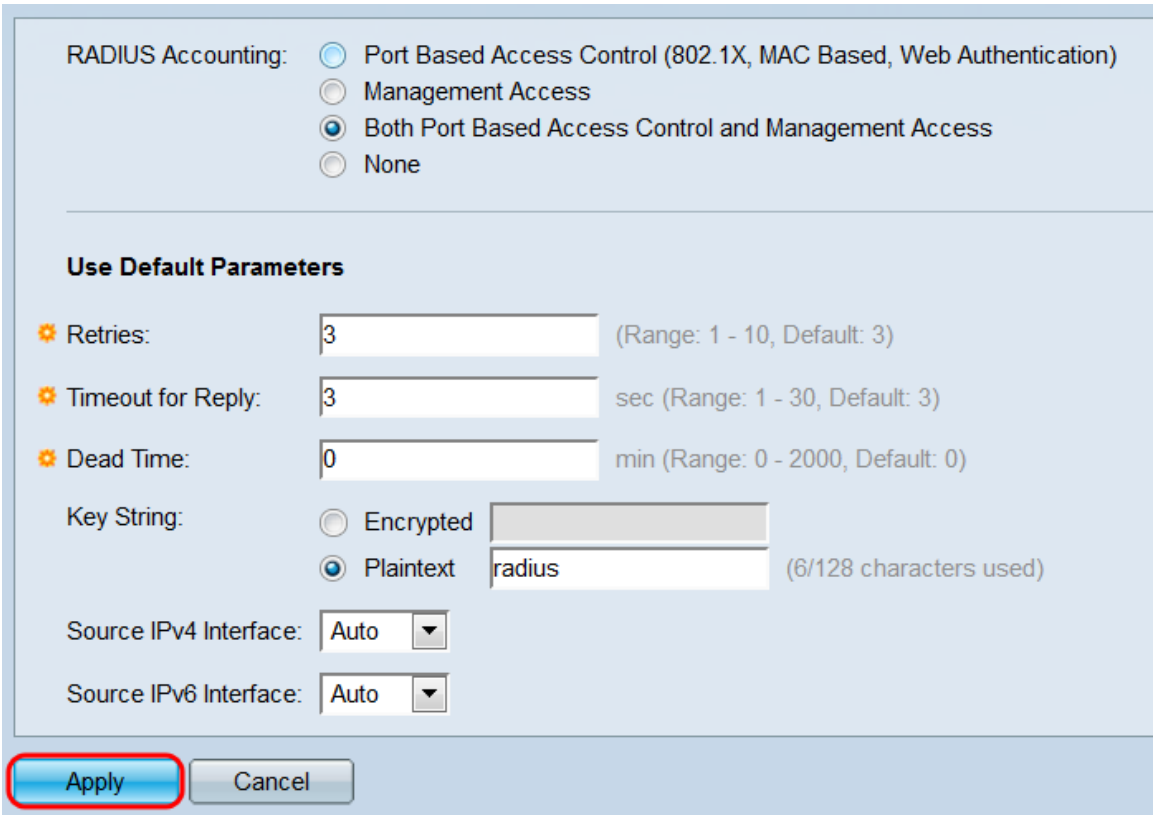
·Tempo inattività: immettere il numero di minuti che devono trascorrere prima che un server RADIUS che non risponde venga trasferito per le richieste di servizio. Il valore predefinito è 0; questo valore indica che il server non viene ignorato.

·Stringa chiave: immettere la chiave segreta utilizzata per l'autenticazione tra lo switch e il server RADIUS. Se si dispone di una chiave crittografata, immetterla utilizzando il pulsante di opzione **Encrypted**; in caso contrario, immettere la chiave in testo normale con il pulsante di opzione **Testo normale**.

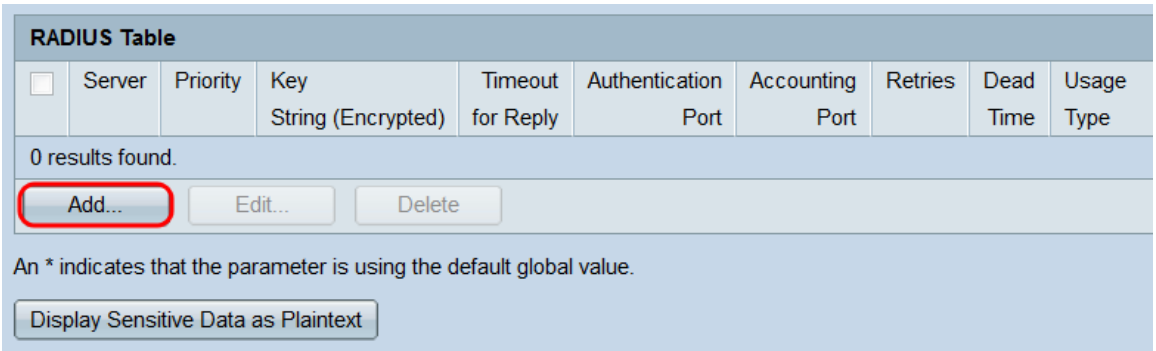
·Interfaccia IPv4/IPv6 di origine: utilizzare questi elenchi a discesa per scegliere l'interfaccia

di origine IPv4/IPv6 da utilizzare per la comunicazione con il server RADIUS. Il valore predefinito è Auto, che utilizzerà l'indirizzo IP di origine predefinito definito sull'interfaccia in uscita.

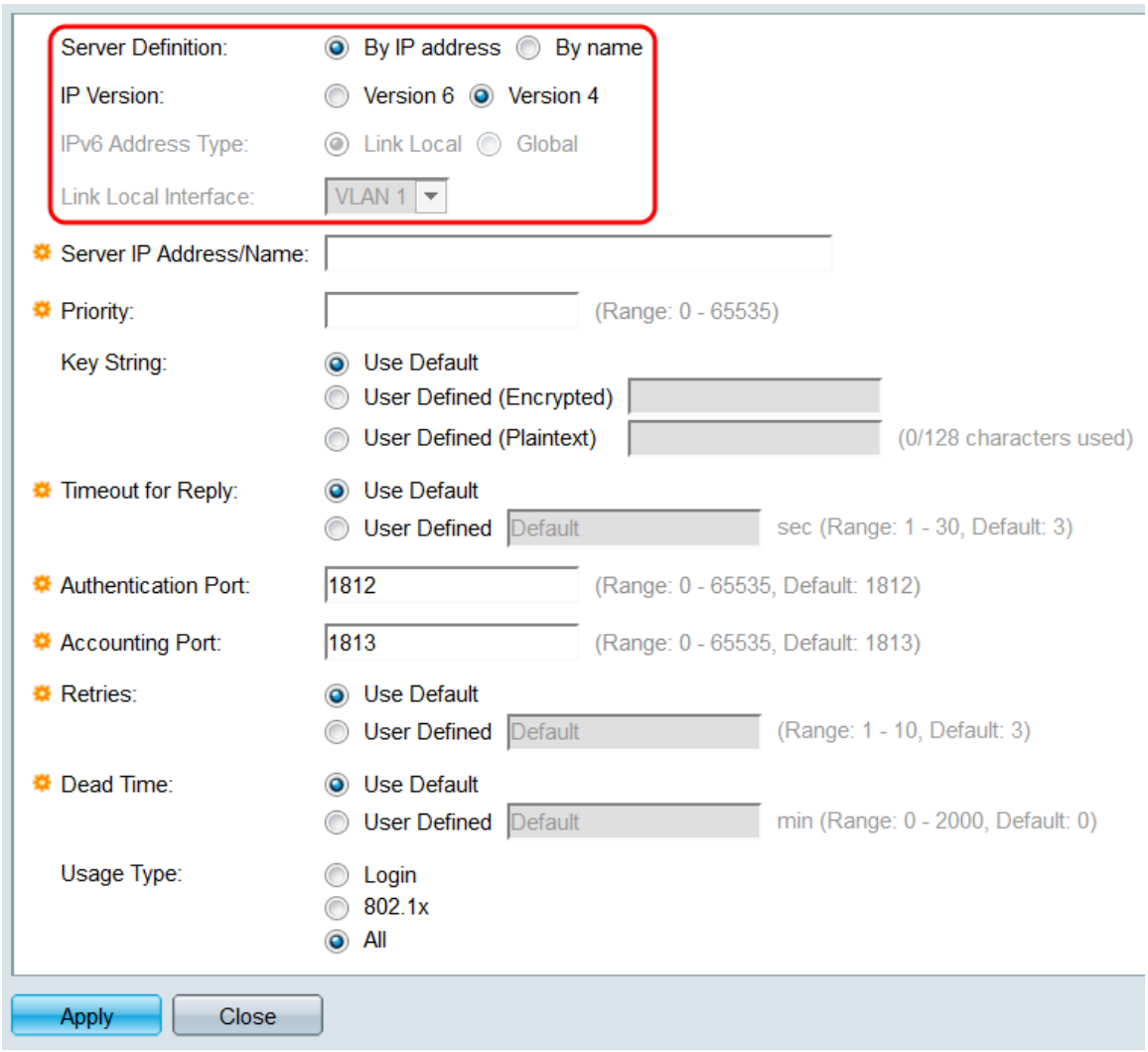
Passaggio 4. Fare clic su **Applica**. Verranno applicate le impostazioni predefinite.



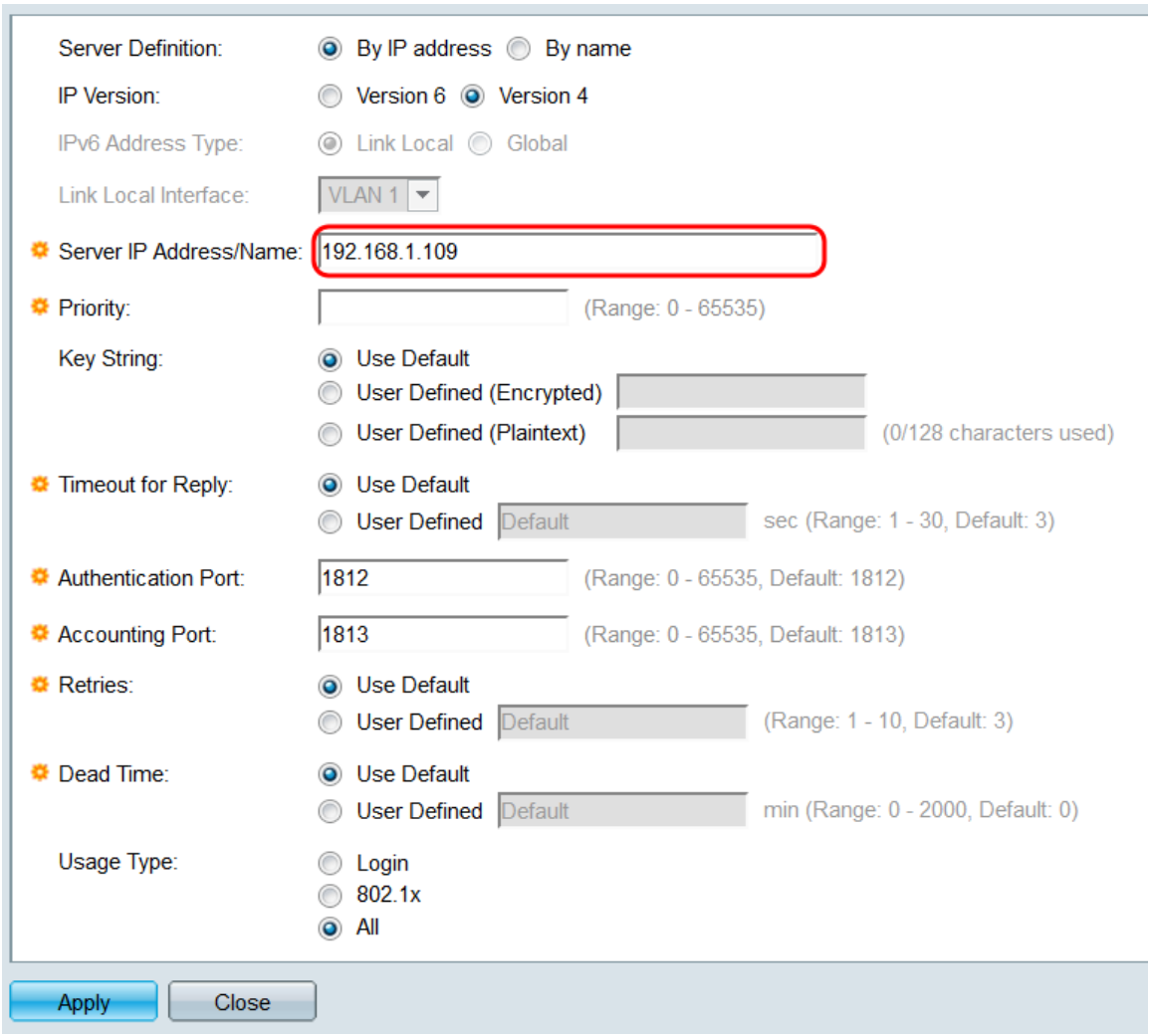
Passaggio 5. La *tabella RADIUS* mostrerà le voci del server RADIUS attualmente configurate sullo switch. Per aggiungere una nuova voce, fare clic sul pulsante **Aggiungi**. Viene visualizzata la finestra *Aggiungi server RADIUS*.



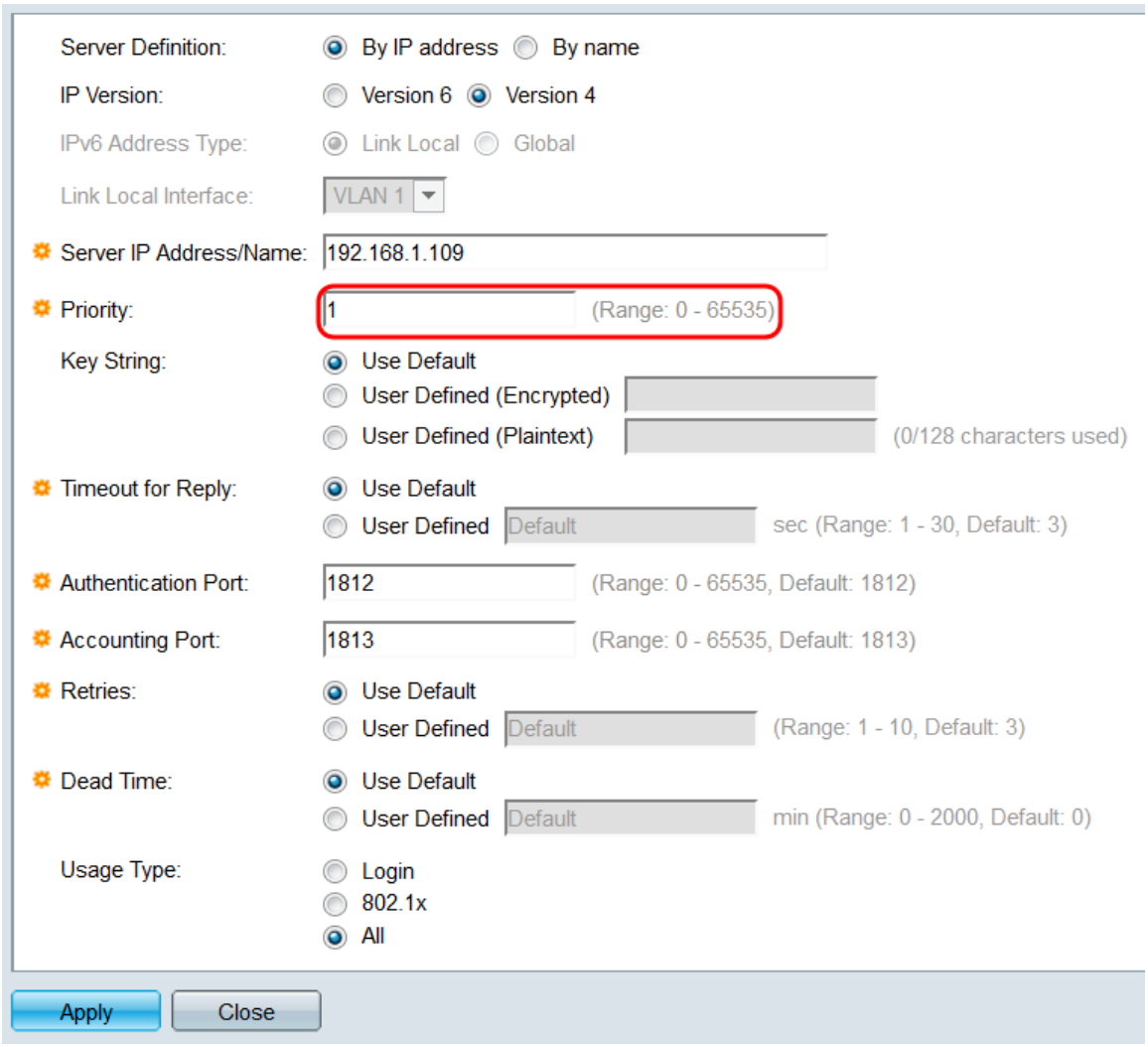
Passaggio 6. Nel campo *Definizione server*, scegliere se contattare il server RADIUS **Per indirizzo IP** o **Per nome** (nomehost). Se è stato selezionato **Per indirizzo IP**, scegliere di utilizzare IPv6 (**versione 6**) o IPv4 (**versione 4**). Se è stata selezionata l'opzione **Versione 6**, utilizzare *Tipo di indirizzo IPv6* e *Collega interfaccia locale* per specificare l'indirizzo IPv6 da utilizzare.



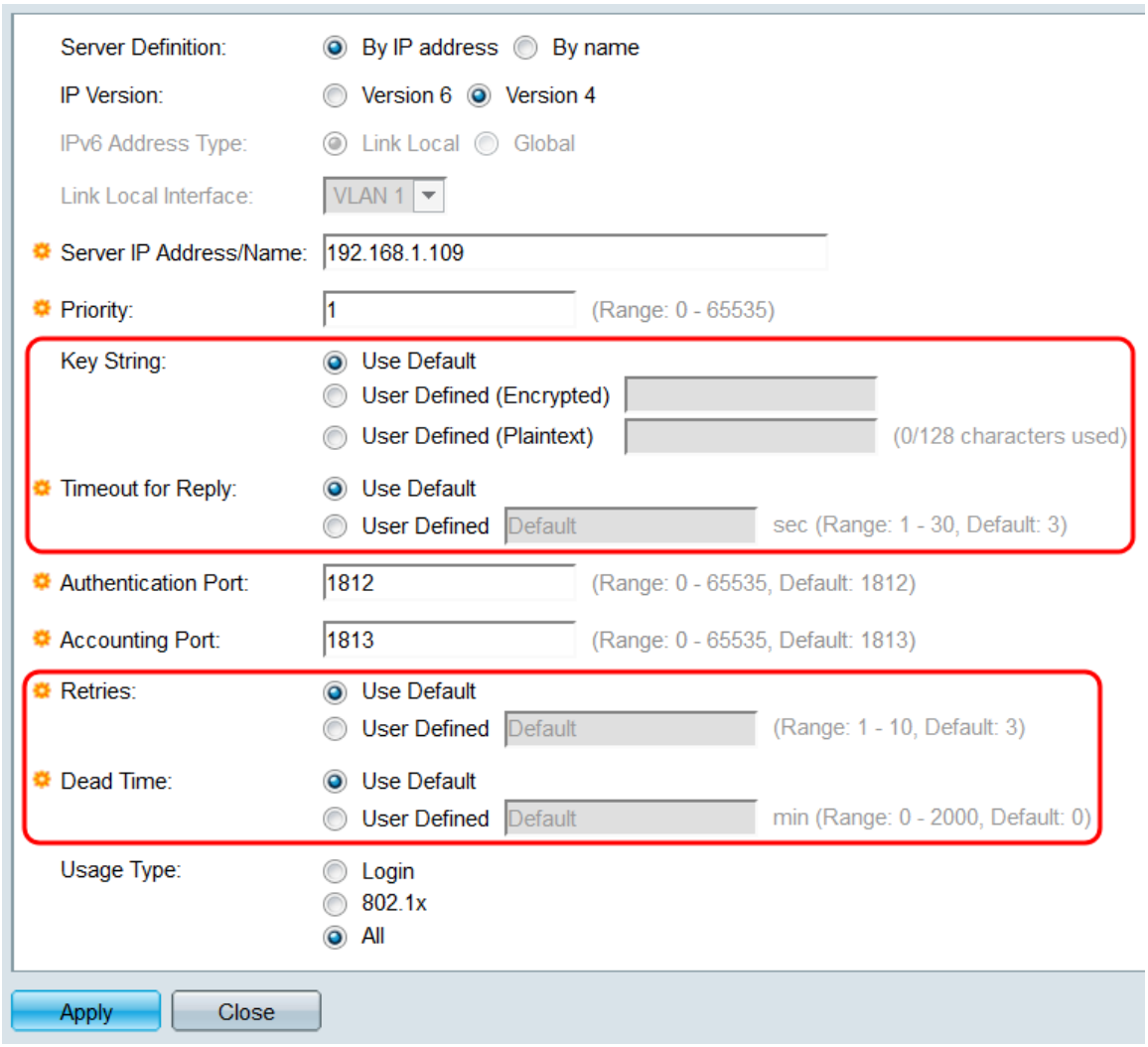
Passaggio 7. Nel campo *Server IP Address/Name* (Indirizzo IP/Nome server), immettere l'indirizzo IP o il nome host del server RADIUS.



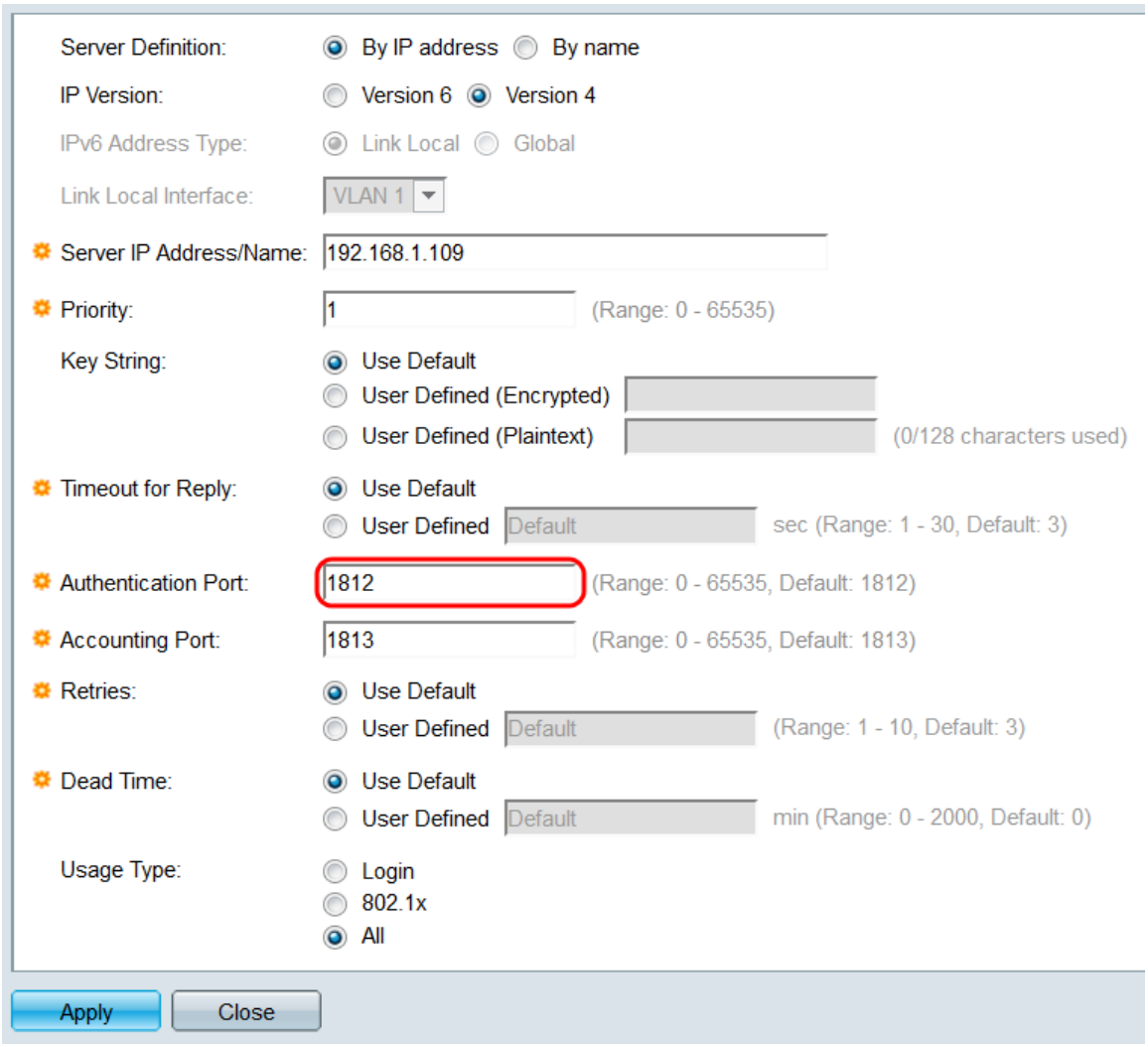
Passaggio 8. Nel campo *Priorità* immettere la priorità che si desidera assegnare al server; lo switch cercherà di contattare il server con la priorità più alta e proseguirà verso il basso fino a quando non incontrerà un server che risponde. L'intervallo è compreso tra 0 e 65535, dove 0 rappresenta la priorità più alta.



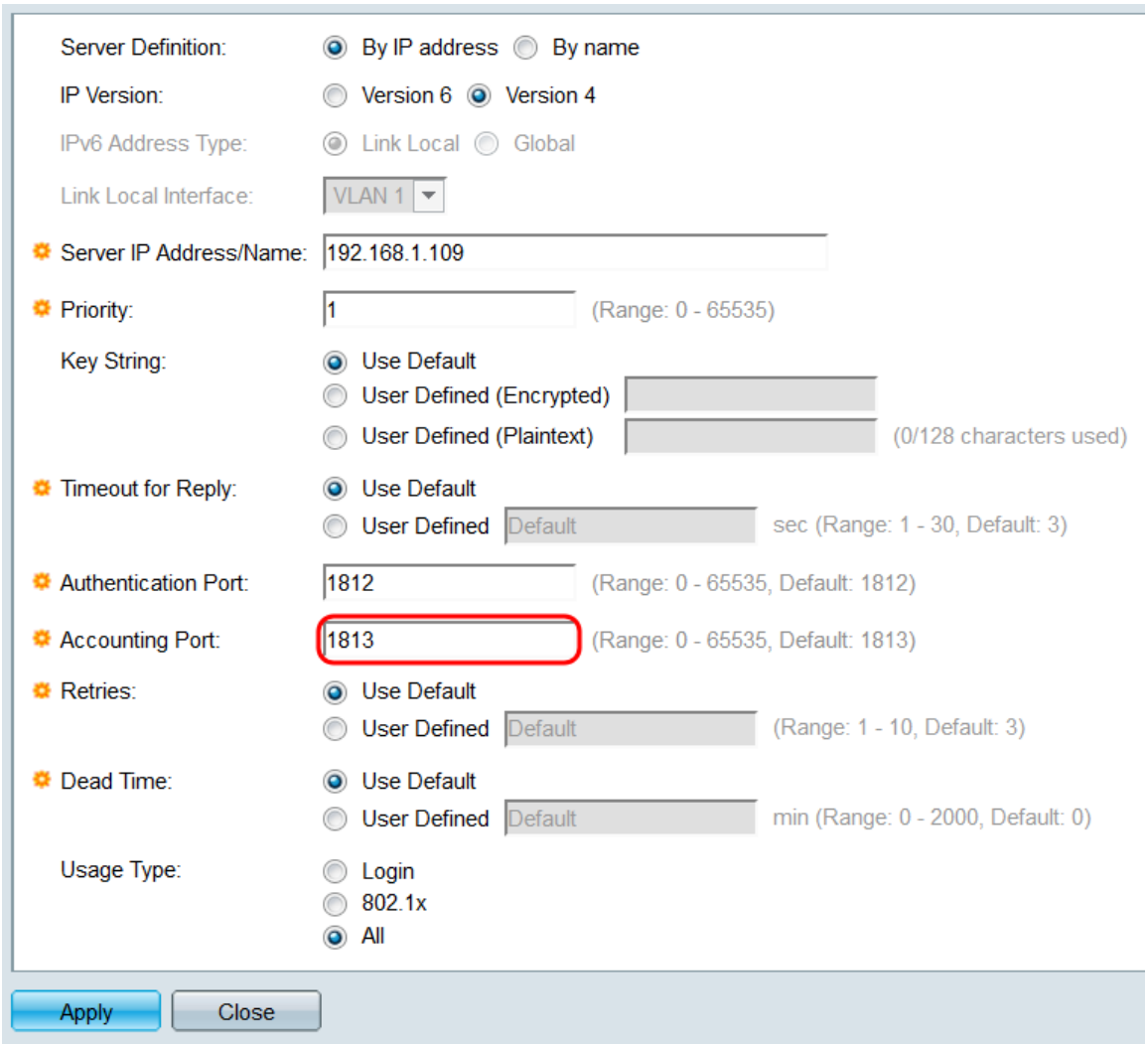
Passaggio 9. Selezionare il pulsante di scelta Utilizza predefinito nei campi Stringa chiave, Timeout per risposta, *Tentativi* e *Tempo morto* per utilizzare le impostazioni configurate in precedenza nella *pagina RADIUS*. È inoltre possibile selezionare i pulsanti di opzione **Definito dall'utente** per configurare impostazioni diverse da quelle predefinite. in questo caso, queste impostazioni verranno utilizzate solo per questo server RADIUS specifico.



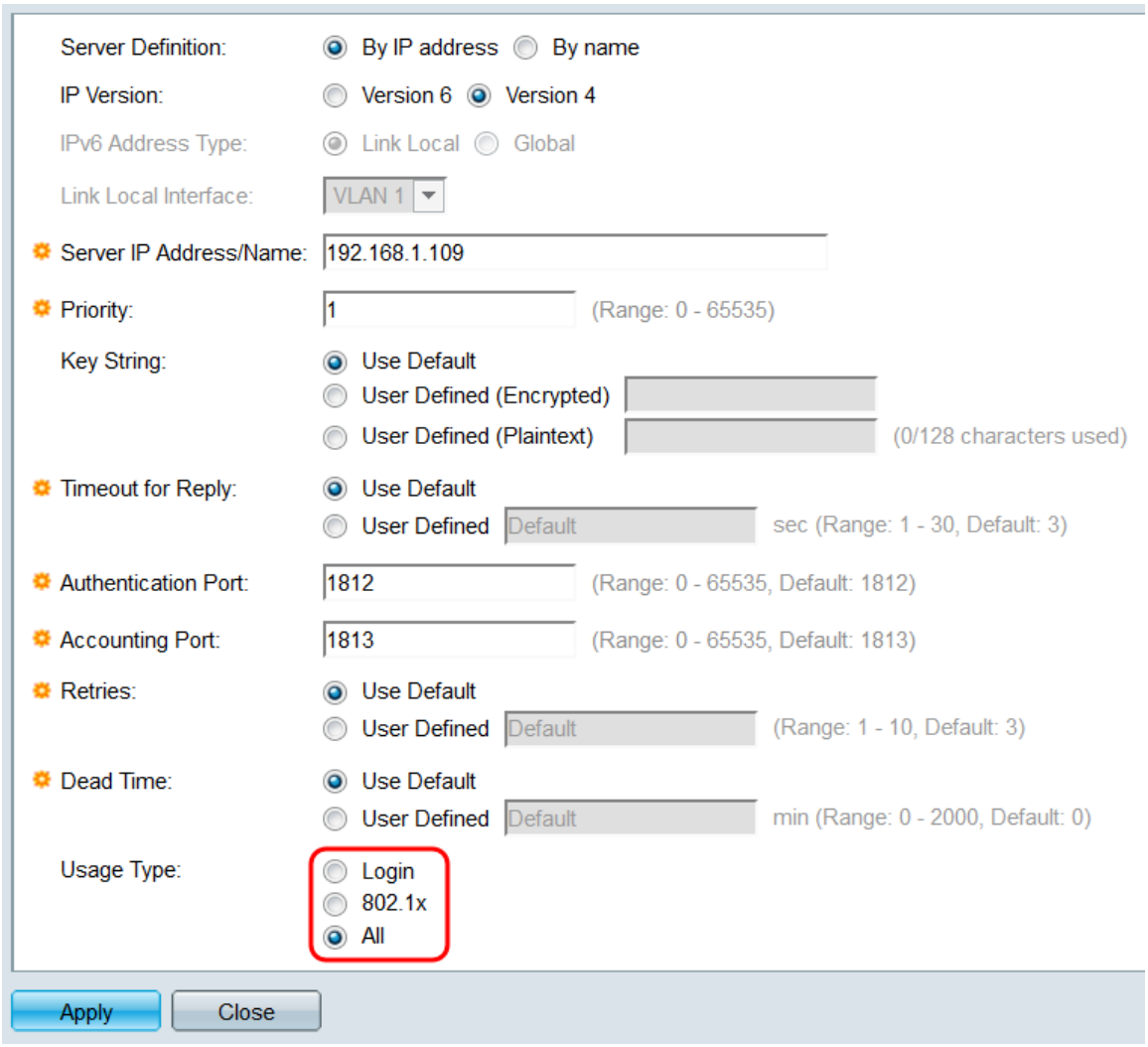
Passaggio 10. Nel campo *Authentication Port* (Porta di autenticazione), specificare la porta che verrà utilizzata per la comunicazione di autenticazione con il server RADIUS. Si consiglia di lasciare la porta predefinita, ossia 1812.



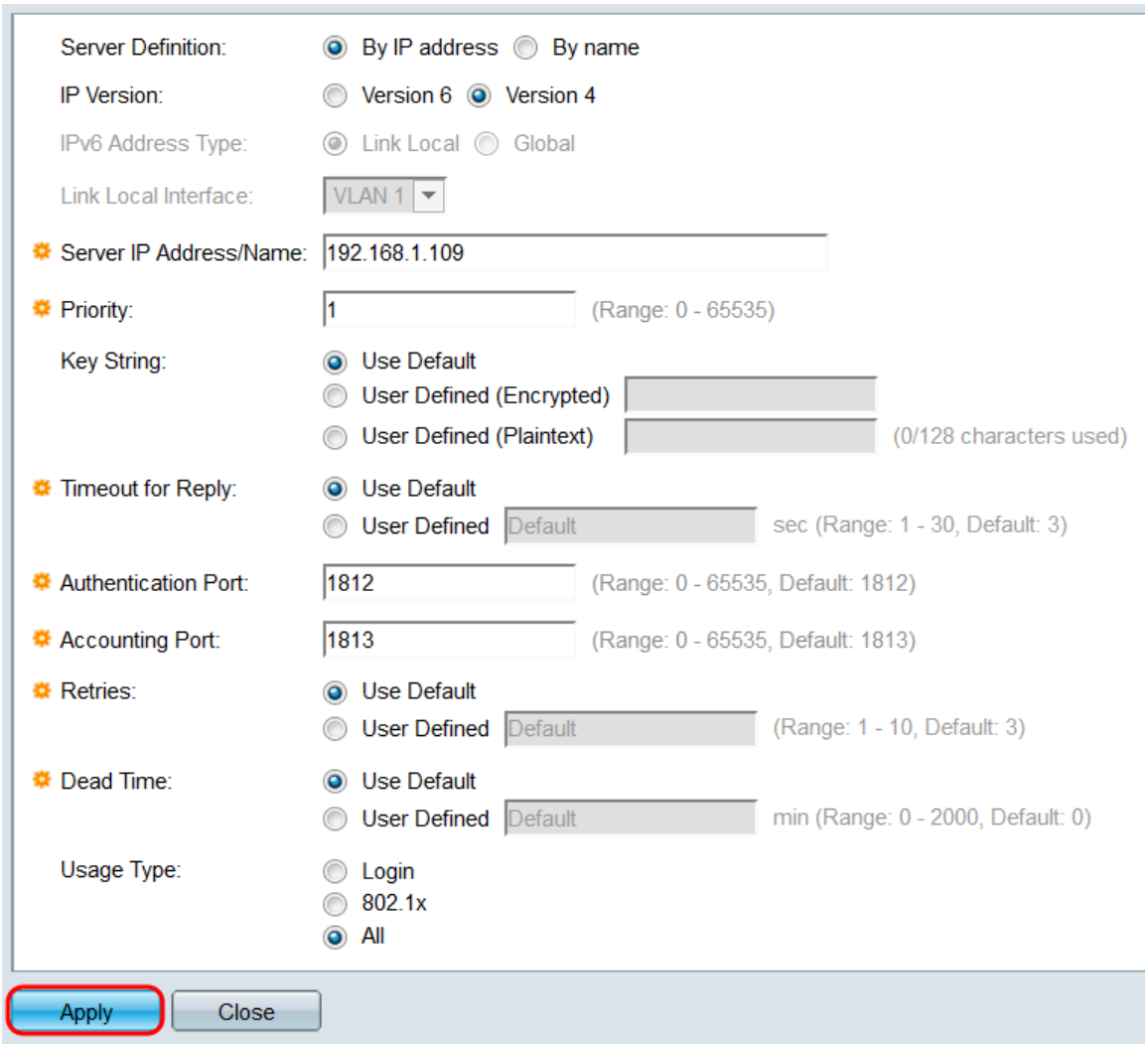
Passaggio 11. Nel campo *Porta di accounting*, specificare la porta che verrà utilizzata per la comunicazione di accounting con il server RADIUS. Si consiglia di lasciare la porta predefinita, 1813.



Passaggio 12. Nel campo *Tipo di utilizzo*, selezionare lo scopo per cui verrà utilizzato il server RADIUS. Quando si configura 802.1X, selezionare il pulsante di opzione **802.1x** o **All** per utilizzare il server RADIUS per l'autenticazione della porta 802.1X.

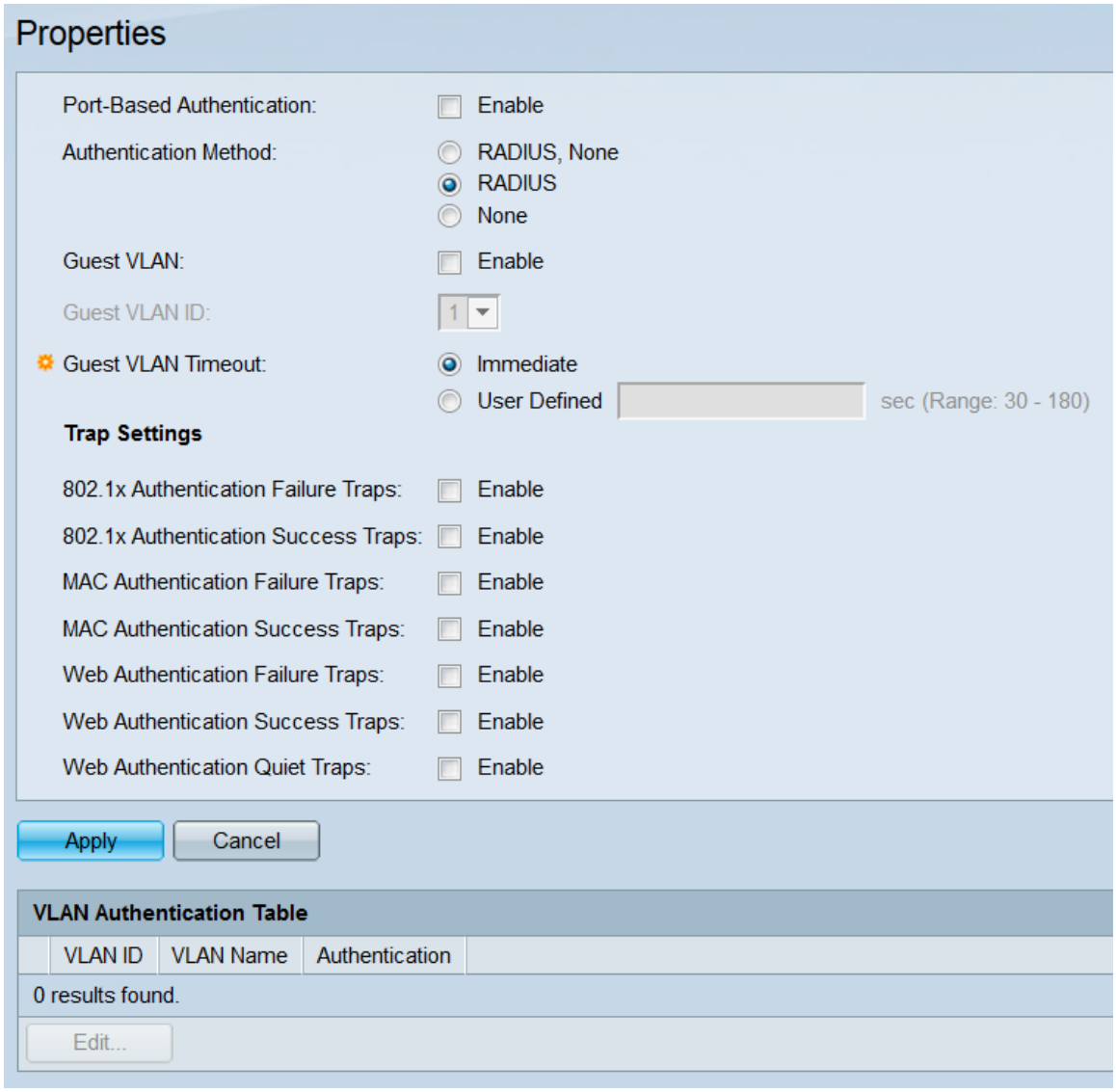


Passaggio 13. Fare clic su **Applica**. Il server verrà aggiunto alla *tabella RADIUS*. Per abilitare l'autenticazione 802.1X basata sulla porta, passare alla sezione successiva.

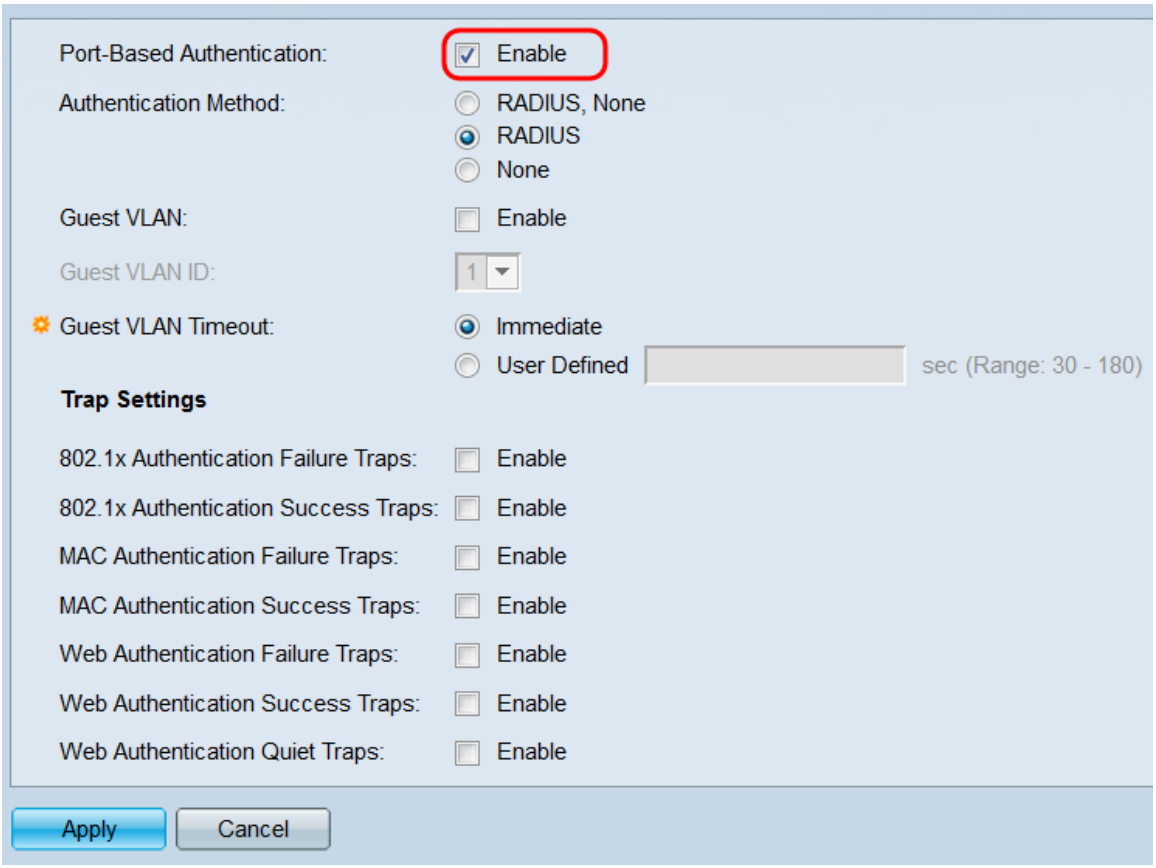


Abilitazione dell'autenticazione basata sulla porta

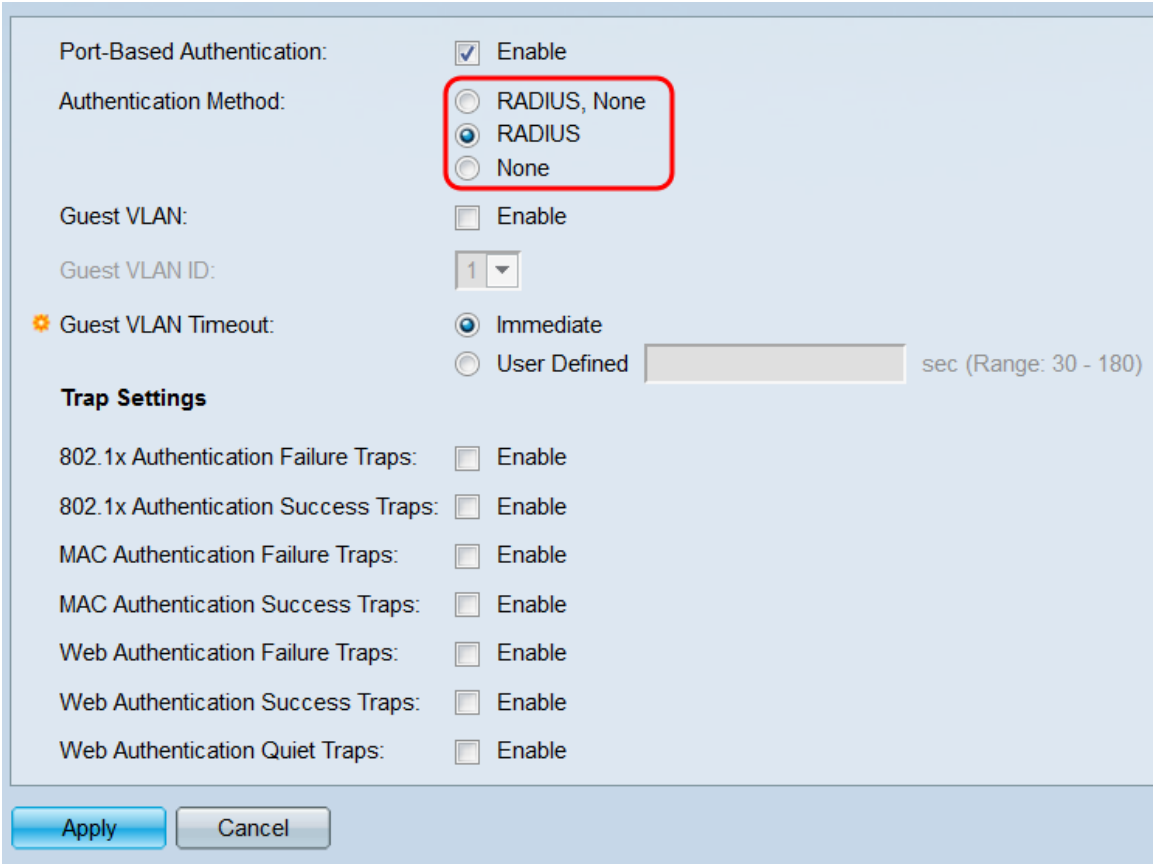
Passaggio 1. Nell'utility di configurazione Web, passare a **Sicurezza > 802.1X/MAC/Web Authentication > Properties** (Protezione > 802.1X/MAC/Autenticazione Web > Proprietà). Viene visualizzata la pagina *Proprietà*.



Passaggio 2. Nel campo *Autenticazione basata sulla porta*, selezionare la casella di controllo **Abilita** per abilitare l'autenticazione basata sulla porta. L'opzione è abilitata per impostazione predefinita.



Passaggio 3. Nel campo *Metodo di autenticazione*, scegliere un pulsante di opzione per determinare come funzionerà l'autenticazione basata sulla porta.



Le opzioni sono:

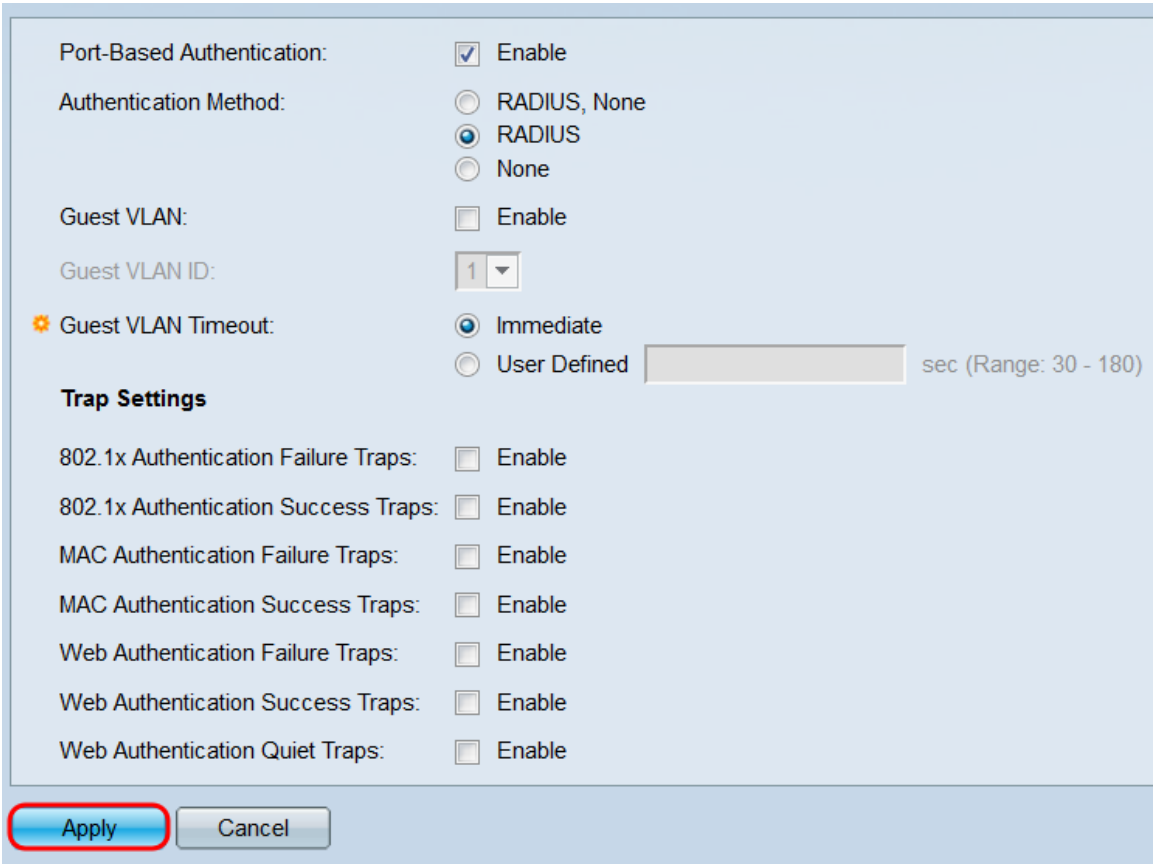
·RADIUS, None - Lo switch tenterà di contattare i server RADIUS definiti nella pagina *RADIUS*. Se non si riceve alcuna risposta dai server, non viene eseguita alcuna

autenticazione e la sessione è consentita. Se il server risponde e le credenziali non sono corrette, la sessione viene negata.

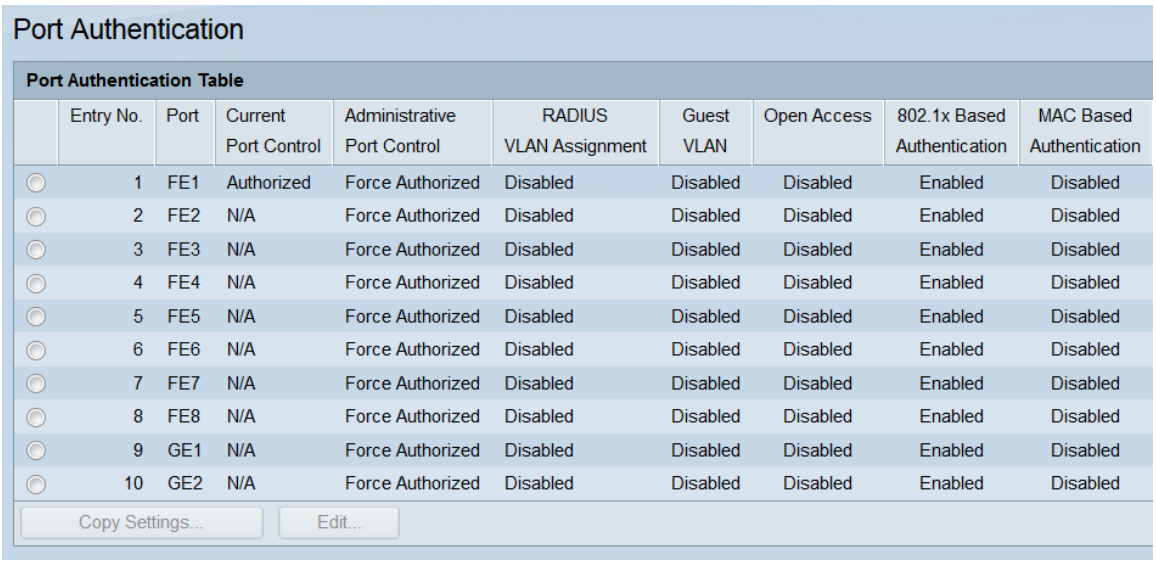
·RADIUS - Lo switch tenterà di contattare i server RADIUS definiti nella pagina *RADIUS*. Se non si riceve alcuna risposta dai server, la sessione viene negata. Questa opzione è consigliata per l'implementazione 802.1X più sicura.

·Nessuno: non viene eseguita alcuna autenticazione. Tutte le sessioni saranno consentite. Questa opzione non implementa 802.1X.

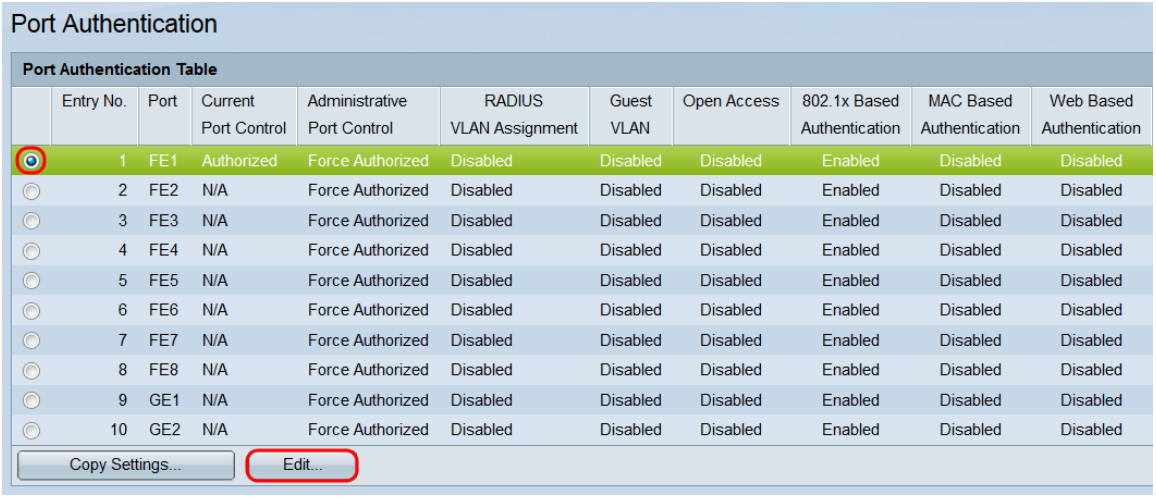
Passaggio 4. Fare clic su **Applica**.



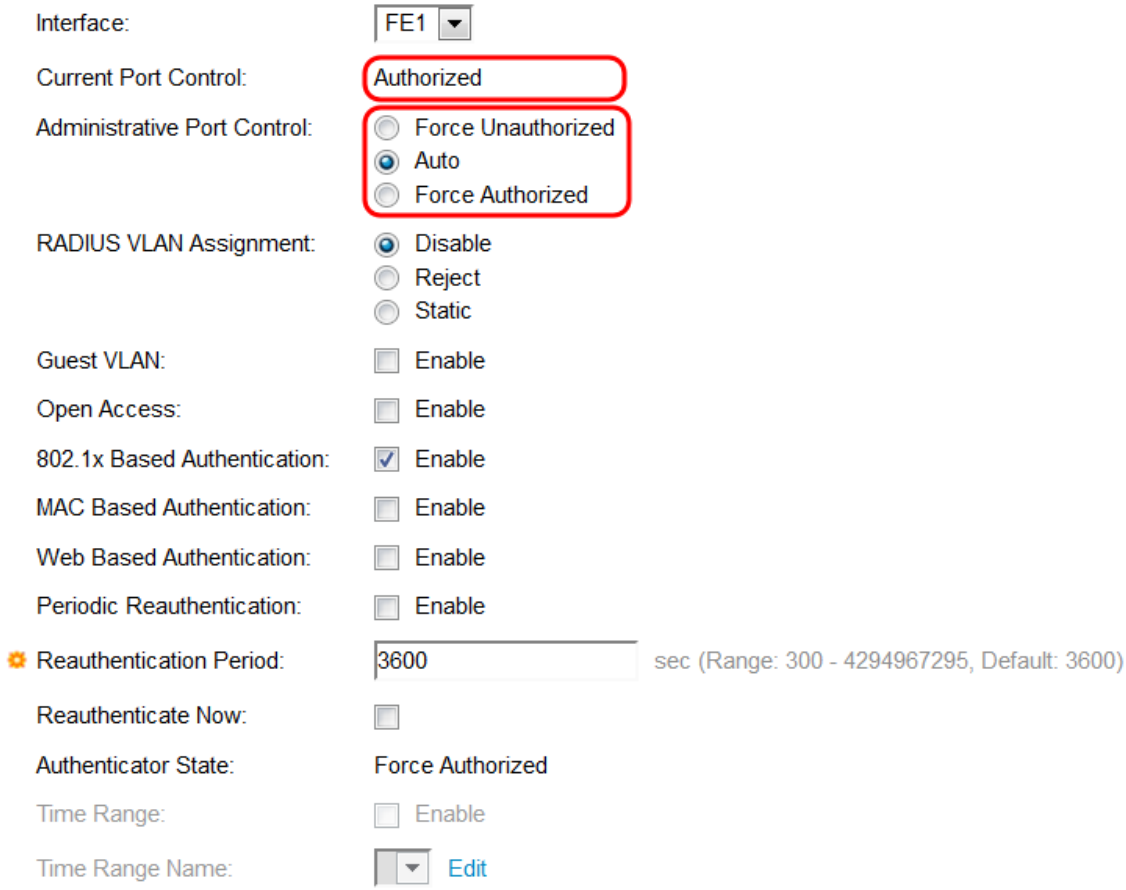
Passaggio 5. Passare a **Sicurezza > Autenticazione 802.1X/MAC/Web > Autenticazione porta**. Si apre la pagina *Port Authentication* (Autenticazione porta).



Passaggio 6. Selezionare la porta da configurare selezionando il relativo pulsante di opzione nella *tabella Port Authentication* e facendo clic sul pulsante **Edit...**. Viene visualizzata la finestra *Modifica autenticazione porta*.



Passaggio 7. Nel campo *Controllo porta amministrativa*, scegliere un pulsante di opzione per determinare come la porta autorizzerà le sessioni. Nel campo *Controllo porta corrente* viene visualizzato lo stato di autorizzazione corrente della porta selezionata.



Le opzioni sono:

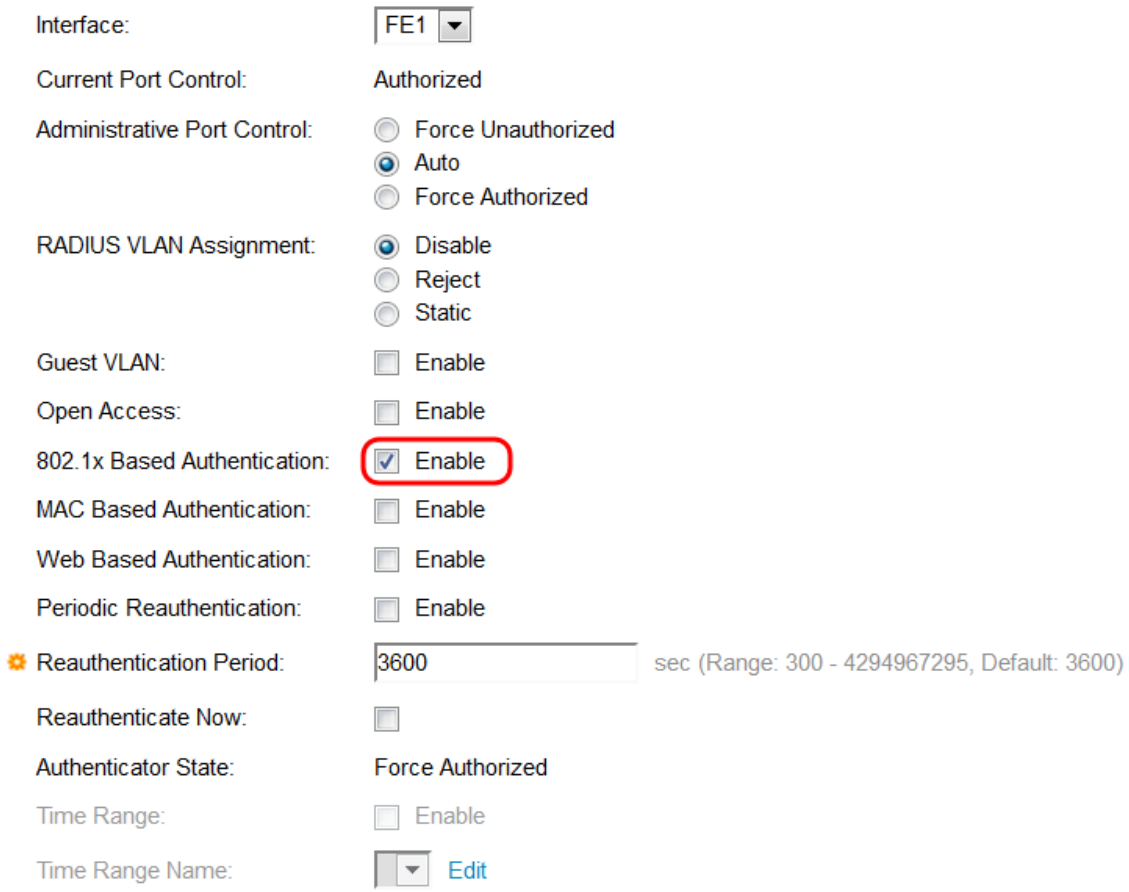
·Force Unauthorized (Imponi non autorizzati) - Sposta l'interfaccia in uno stato non autorizzato. Il dispositivo non fornisce l'autenticazione ai client connessi a questa porta e nega l'accesso.

·Auto - Abilita l'autenticazione basata sulla porta per la porta selezionata. Sposta l'interfaccia tra autorizzati e non autorizzati a seconda dell'esito della procedura di autenticazione.

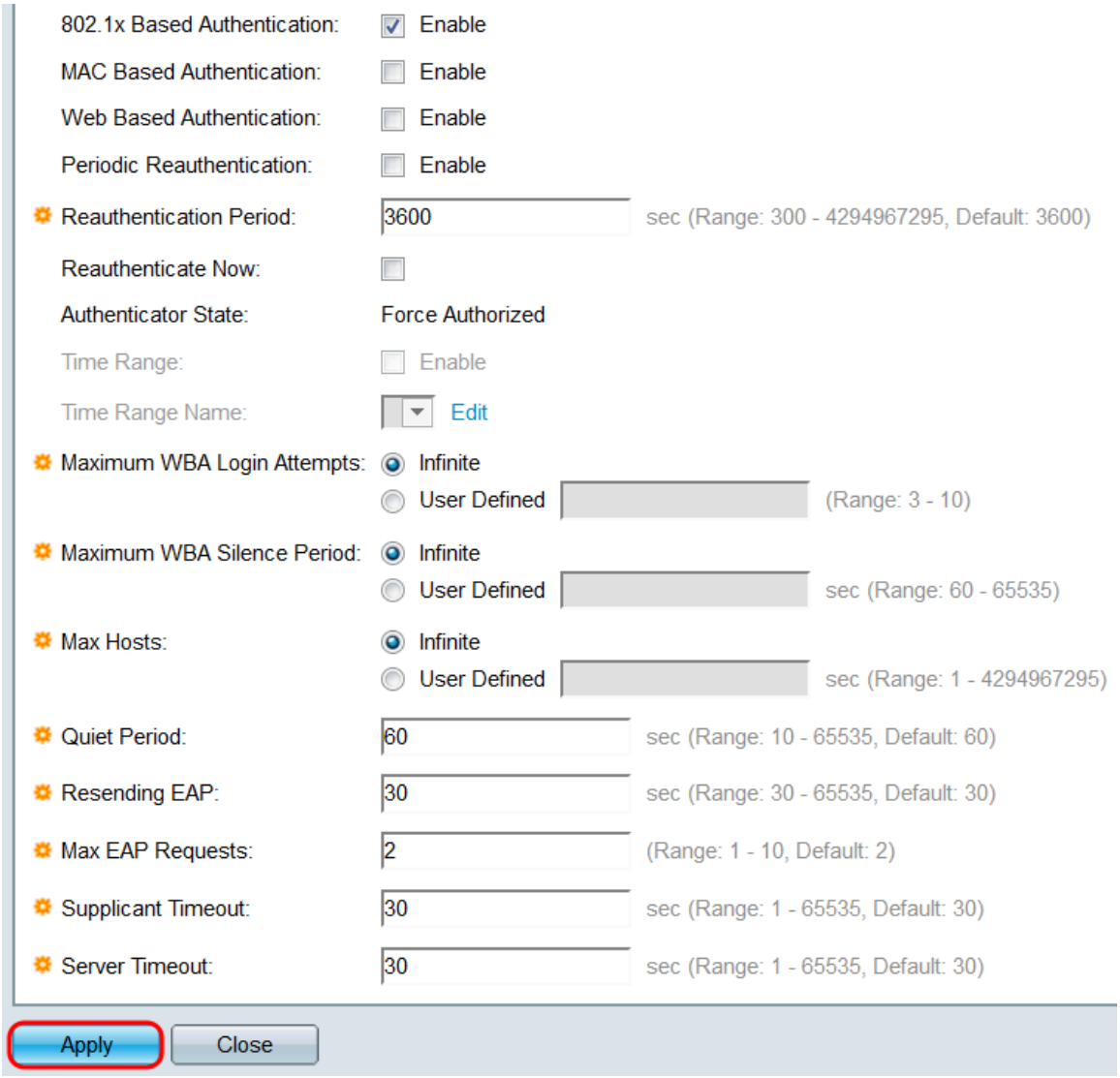
Scegliere questa opzione per implementare 802.1X.

·Force Authorized - Attiva lo stato autorizzato dell'interfaccia. Il dispositivo fornirà l'accesso a tutti i client che si connettono a questa porta senza autenticazione.

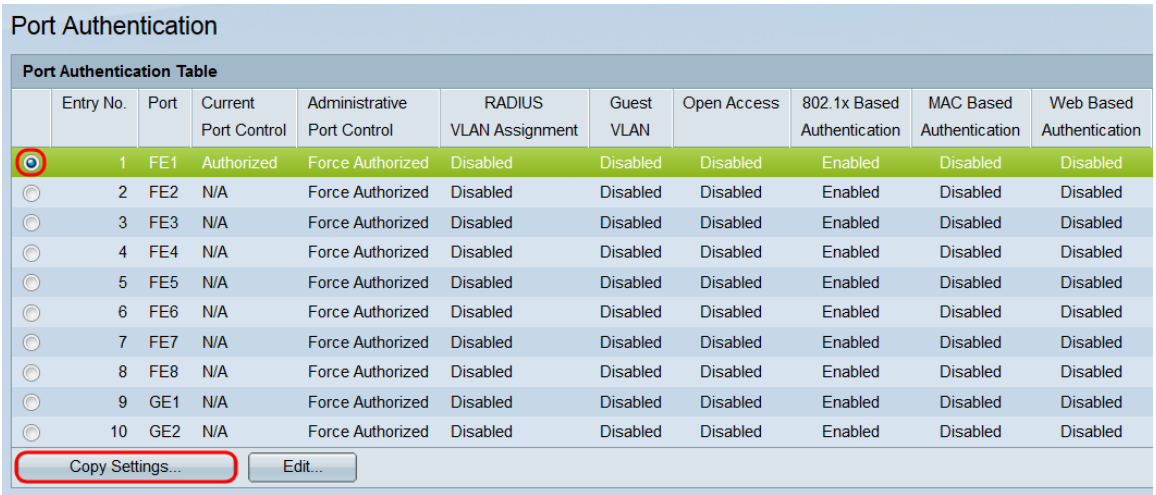
Passaggio 8. Selezionare la casella di controllo **Abilita** nel campo *Autenticazione basata su 802.1X* per abilitare l'autenticazione 802.1X per la porta selezionata.



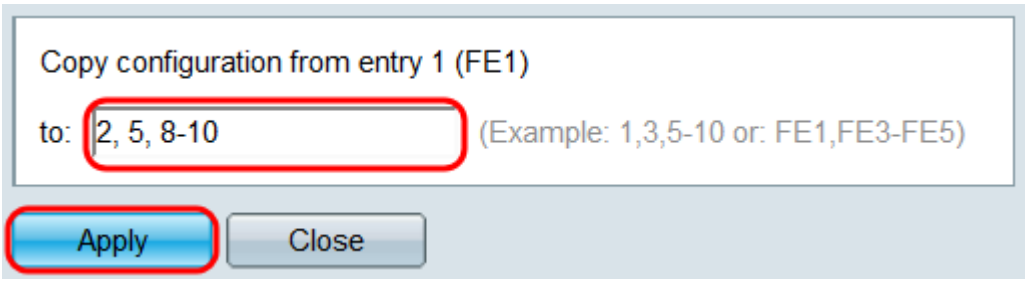
Passaggio 9. Fare clic su **Applica**. La porta dovrebbe essere ora completamente configurata per l'autenticazione basata sulla porta 802.1X ed è pronta per iniziare l'autenticazione di tutti i client che si connettono a essa. Utilizzare il campo *Interface* (Interfaccia) per selezionare una porta diversa da configurare senza tornare alla pagina *Port Authentication* (Autenticazione porta).



Passaggio 10. Per copiare rapidamente le impostazioni di una porta su un'altra porta o intervallo di porte, fare clic sul pulsante di opzione della porta che si desidera copiare nella *tabella Autenticazione porta* e fare clic sul pulsante **Copia impostazioni...**. Viene visualizzata la finestra *Copia impostazioni*.



Passaggio 11. Nel campo di testo, immettere la porta o le porte (separate da virgole) in cui copiare le impostazioni. È inoltre possibile specificare un intervallo di porte. Quindi, fare clic su **Applica** per copiare le impostazioni.



Qui è disponibile un video relativo a questo articolo...

[Fare clic qui per visualizzare altre Tech Talks di Cisco]