Configurazione dell'autenticazione basata su MAC su uno switch

Obiettivo

802.1X è uno strumento di amministrazione che consente di elencare i dispositivi e garantisce che non vi siano accessi non autorizzati alla rete. In questo documento viene spiegato come configurare l'autenticazione basata su MAC su uno switch con l'interfaccia grafica (GUI). per informazioni su come configurare l'autenticazione basata su MAC con l'interfaccia della riga di comando (CLI), fare clic qui.

Nota: Questa guida è lunga 9 sezioni e 1 sezione per verificare che un host sia stato autenticato. Prendete il caffè, il tè o l'acqua e assicuratevi di avere il tempo sufficiente per rivedere ed eseguire i passi coinvolti.

Per ulteriori informazioni, consultare il glossario.

Come funziona RADIUS?

Esistono tre componenti principali per l'autenticazione 802.1X, un supplicant (client), un autenticatore (dispositivo di rete come uno switch) e un server di autenticazione (RADIUS). RADIUS (Remote Authentication Dial-In User Service) è un server di accesso che utilizza il protocollo di autenticazione, autorizzazione e accounting (AAA) per gestire l'accesso alla rete. RADIUS utilizza un modello client-server in cui le informazioni di autenticazione protetta vengono scambiate tra il server RADIUS e uno o più client RADIUS. Convalida l'identità del client e notifica allo switch se il client è autorizzato o meno ad accedere alla LAN.

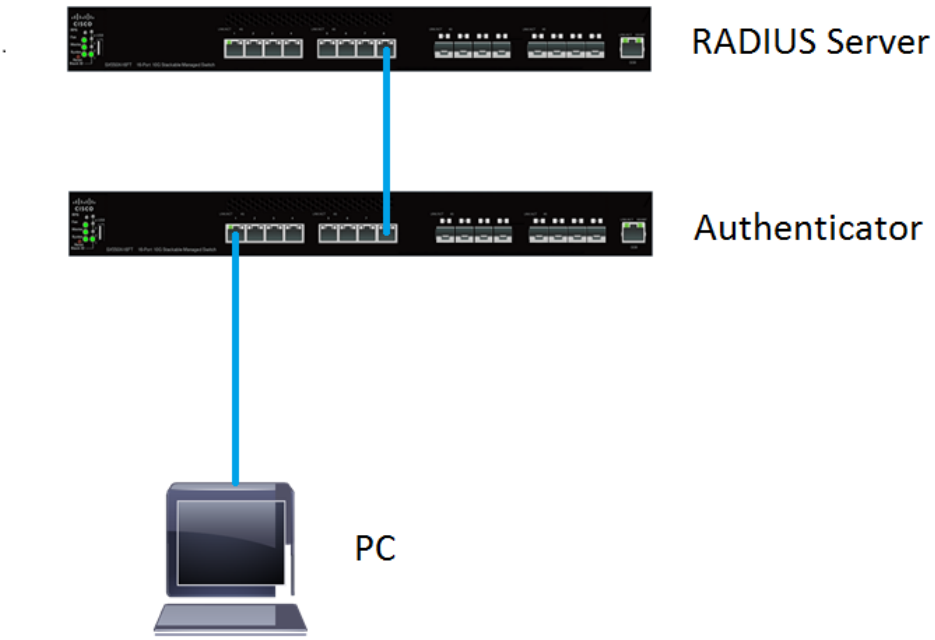
Un autenticatore funziona tra il client e il server di autenticazione. In primo luogo, richiederà informazioni sull'identità al client. In risposta, l'autenticatore verificherà le informazioni con il server di autenticazione. Infine, trasmetterebbe una risposta al cliente. In questo articolo, l'autenticatore è uno switch che include il client RADIUS. Lo switch potrebbe incapsulare e decapsulare i frame EAP (Extensible Authentication Protocol) per interagire con il server di autenticazione.

E per quanto riguarda l'autenticazione basata su MAC?

Nell'autenticazione basata su MAC, quando il richiedente non è in grado di comunicare con l'autenticatore o non è in grado di farlo, utilizza l'indirizzo MAC dell'host per eseguire l'autenticazione. I supplicant basati su MAC vengono autenticati utilizzando RADIUS puro (senza utilizzare EAP). Il server RADIUS dispone di un database host dedicato che contiene solo gli indirizzi MAC consentiti. Anziché considerare la richiesta di autenticazione basata su MAC come autenticazione PAP (Password Authentication Protocol), i server riconoscono tale richiesta in base all'attributo 6 [Service-Type] = 10. Confronteranno l'indirizzo MAC nell'attributo Calling-Station-Id con gli indirizzi MAC memorizzati nel database host.

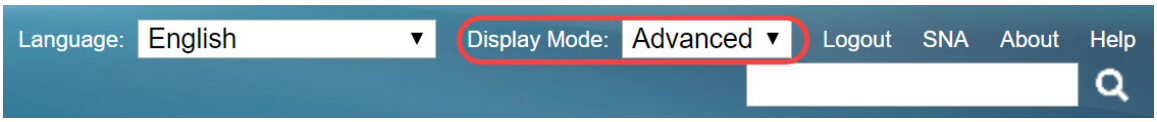
La versione 2.4 offre la possibilità di configurare il formato del nome utente inviato per i supplicant basati su MAC e di definire il metodo di autenticazione EAP o RADIUS puro. In questa versione, è anche possibile configurare il formato del nome utente e configurare una password specifica, diversa dal nome utente, per i supplicant basati su MAC.

Topologia:



Nota: In questo articolo verrà utilizzato il modello SG550X-24 sia per il server RADIUS che per l'autenticatore. Il server RADIUS ha un indirizzo IP statico di 192.168.1.100 e l'autenticatore ha un indirizzo IP statico di 192.168.1.101.

I passaggi descritti in questo documento vengono eseguiti in modalità di visualizzazione **avanzata** . Per passare alla modalità avanzata, andare nell'angolo in alto a destra e selezionare **Avanzate** nell'elenco a discesa *Modalità di visualizzazione*.



Sommario

Dispositivi interessati

- Serie Sx350X

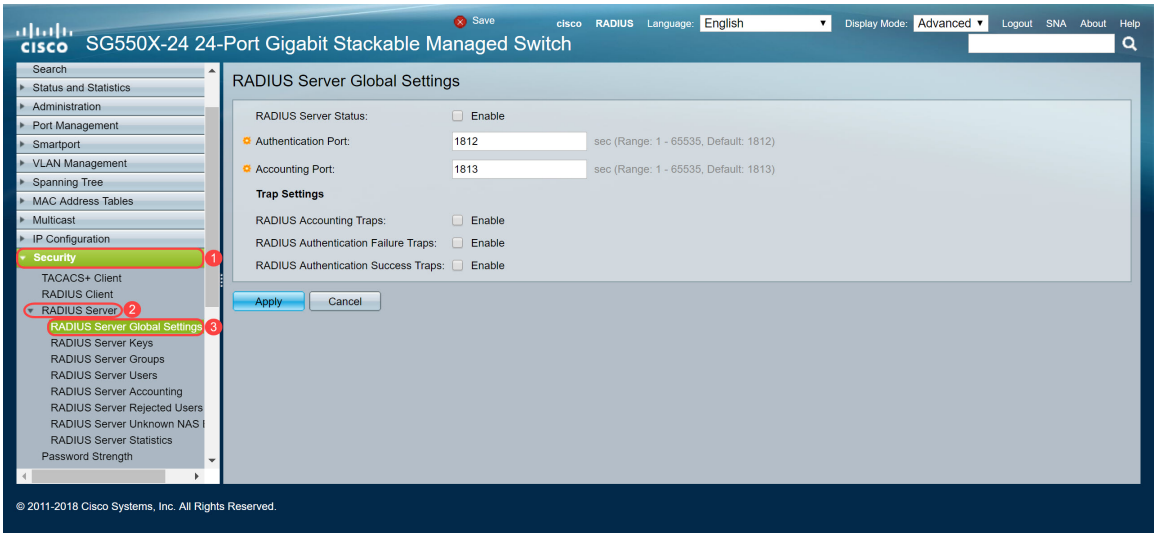
- Serie SG350XG
- Serie Sx550X
- Serie SG550XG

Versione del software

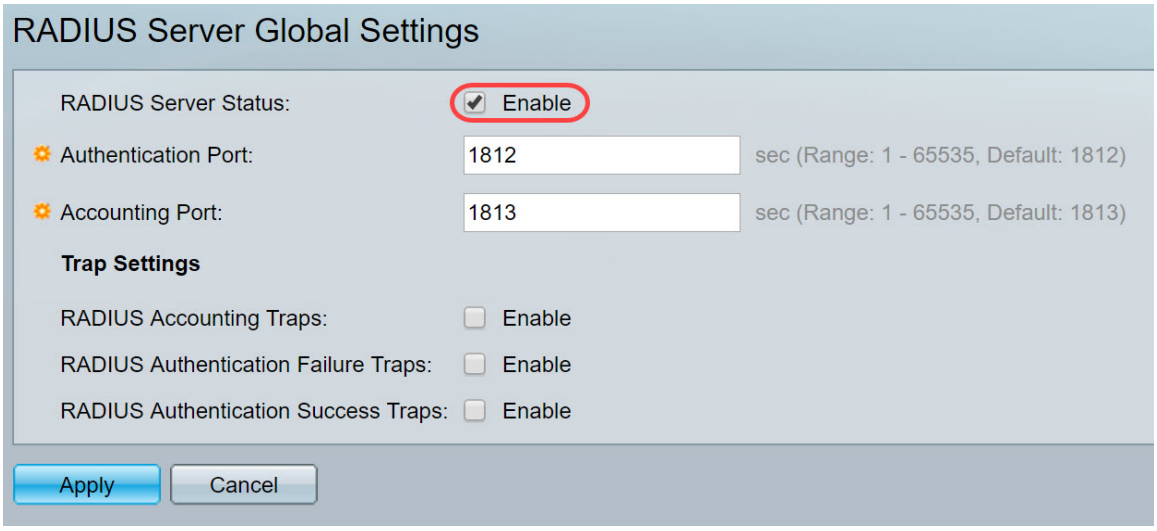
- 2.4.0.94

Impostazioni globali server RADIUS

Passaggio 1. Accedere all'utility basata sul Web dello switch che verrà configurata come server RADIUS e selezionare **Sicurezza > Server RADIUS > Impostazioni globali server RADIUS**.



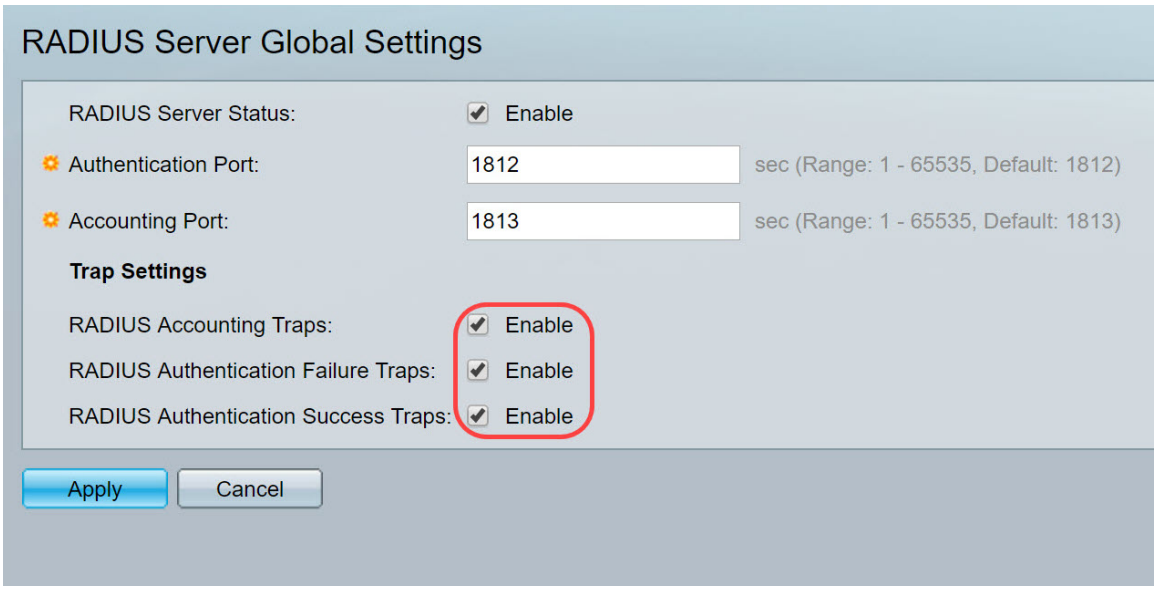
Passaggio 2. Per abilitare lo stato delle funzionalità del server RADIUS, selezionare la casella di controllo **Abilita** nel campo *Stato server RADIUS*.



Passaggio 3. Per generare trap per eventi di accounting RADIUS, accessi non riusciti o accessi riusciti, selezionare la casella di controllo **Abilita** desiderata per generare i trap. I trap sono messaggi di eventi di sistema generati tramite il protocollo SNMP (Simple Network Management Protocol). Quando si verifica una violazione, viene inviata una trap al manager SNMP dello switch. Le impostazioni di trap seguenti sono:

- Registrazioni accounting RADIUS: selezionare per generare registrazioni per eventi di accounting RADIUS.

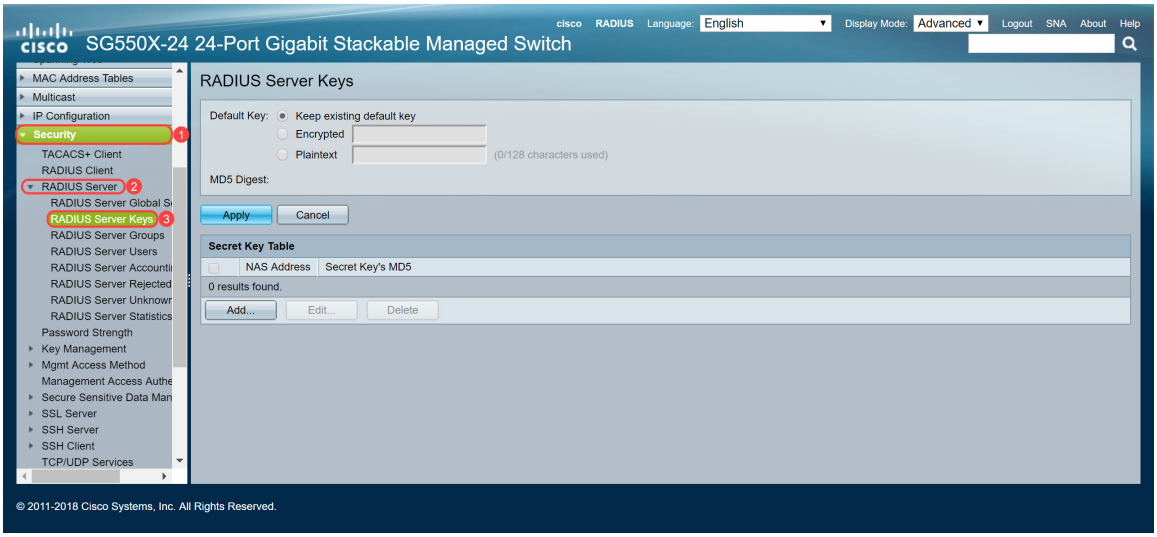
- Trap non riuscite autenticazione RADIUS: selezionare per generare trap per gli accessi non riusciti.
- Trap riuscite autenticazione RADIUS: selezionare per generare trap per gli account di accesso riusciti.



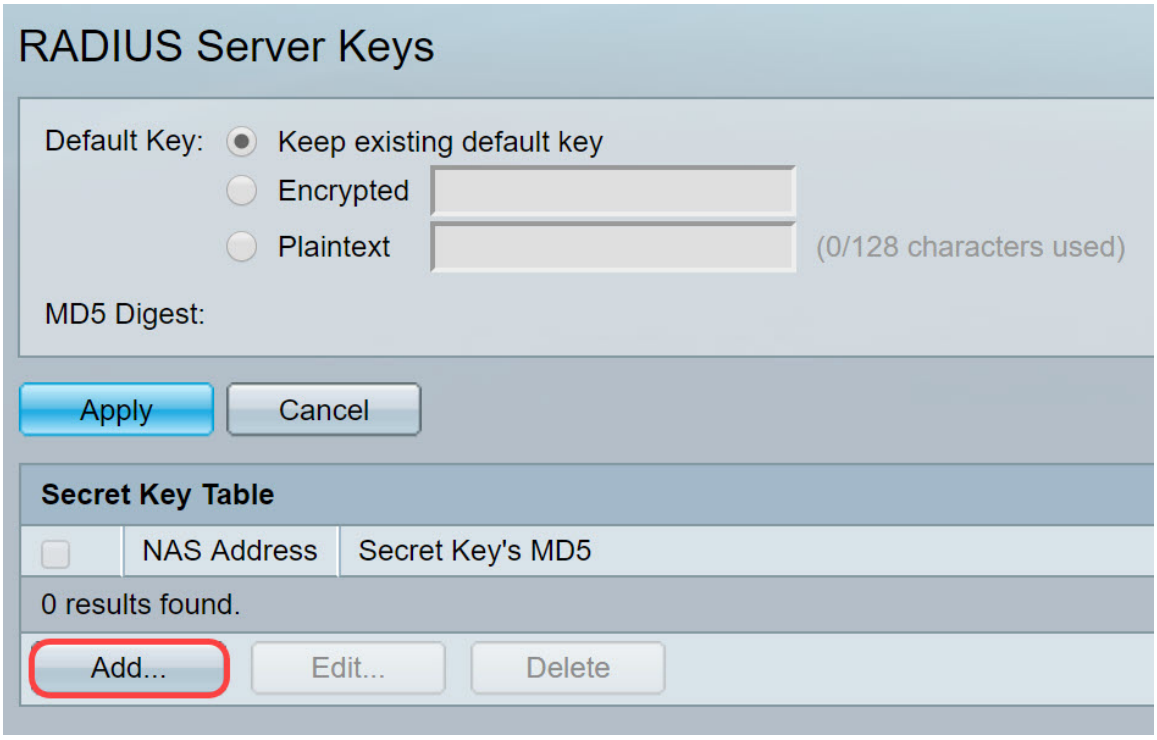
Passaggio 4. Fare clic su **Apply** per salvare le impostazioni.

Chiavi server RADIUS

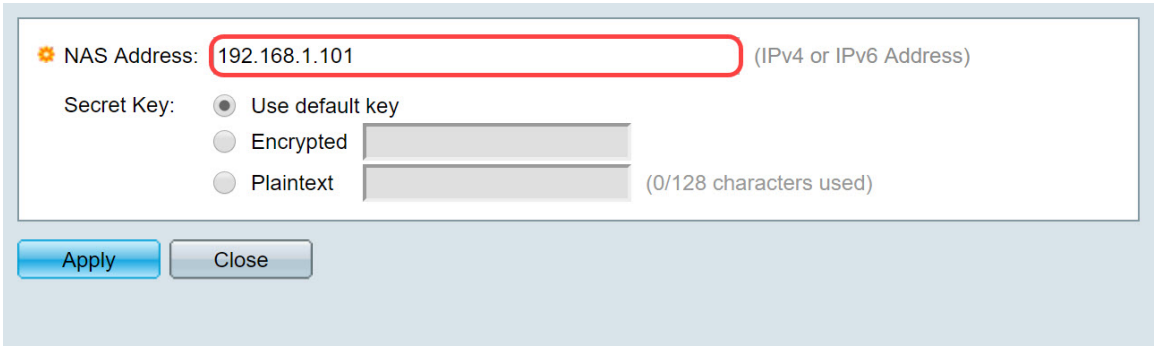
Passaggio 1. Passare a **Sicurezza > Server RADIUS > Chiavi server RADIUS**. Viene visualizzata la pagina *RADIUS Server Key* (Chiave server RADIUS).



Passaggio 2. Nella sezione *Tabella chiavi segrete*, fare clic su **Aggiungi...** per aggiungere una chiave segreta.



Passaggio 3. Viene visualizzata la pagina *Aggiungi chiave segreta*. Nel campo *NAS Address* (Indirizzo NAS), immettere l'indirizzo dello switch contenente il client RADIUS. Nell'esempio, verrà usato l'indirizzo IP 192.168.1.101 come client RADIUS.

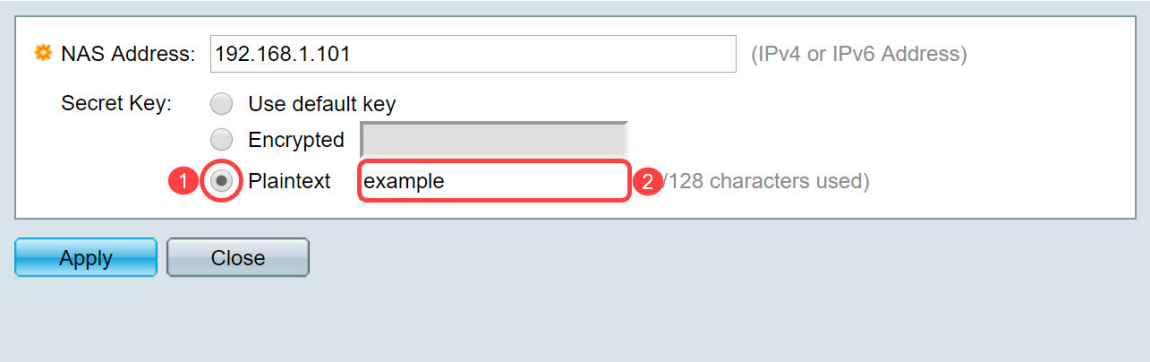


Passaggio 4. Selezionare uno dei pulsanti di opzione utilizzati come *chiave privata*. Le opzioni seguenti sono:

- Usa chiave predefinita - Per i server specificati, il dispositivo tenta di autenticare il client RADIUS utilizzando la stringa di chiave predefinita esistente.
- Crittografato: per crittografare le comunicazioni utilizzando MD5 (Message-Digest Algorithm 5), immettere la chiave in formato crittografato.
- Testo normale — immettere la stringa chiave in modalità testo normale.

In questo esempio verrà selezionato *Testo normale* e verrà utilizzata la parola **esempio** come *chiave segreta*. Dopo aver premuto apply (Applica), la chiave sarà in formato crittografato.

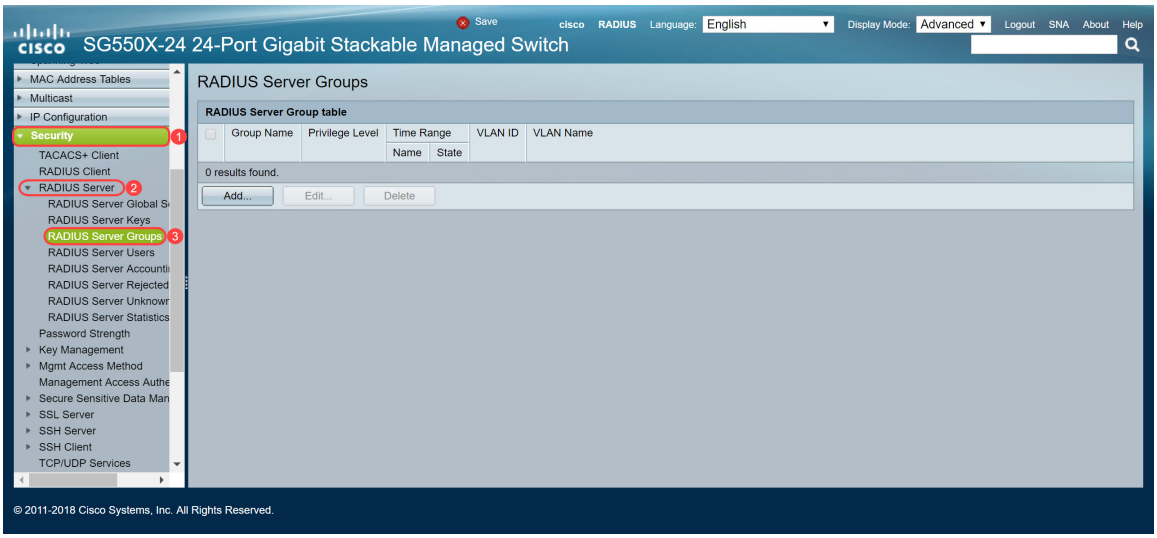
Nota: Non è consigliabile utilizzare la parola **example** come chiave segreta. Utilizzare una chiave più forte. È possibile utilizzare fino a 128 caratteri. Se la tua password è troppo complessa per essere ricordata allora è una buona password, ma è ancora meglio se la puoi trasformare in una passphrase memorabile con caratteri speciali e numeri che sostituiscono le vocali — "P@55w0rds@reH@rdT0Remember". Si consiglia di non utilizzare parole presenti in un dizionario. È consigliabile scegliere una frase e scambiare alcune lettere per caratteri speciali e numeri. Per ulteriori informazioni, fare riferimento a questo post del blog Cisco.



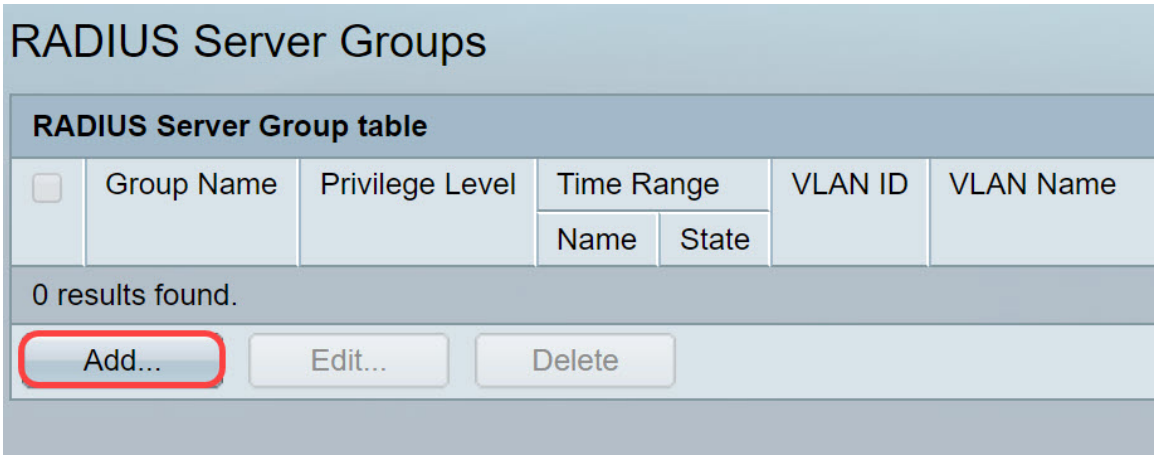
Passaggio 5. Fare clic su **Apply** per salvare la configurazione. La chiave segreta è ora crittografata con MD5. MD5 è una funzione hash crittografica che accetta un dato e crea un output esadecimale univoco che in genere non è riproducibile. MD5 utilizza un valore hash a 128 bit.

Gruppi di server RADIUS

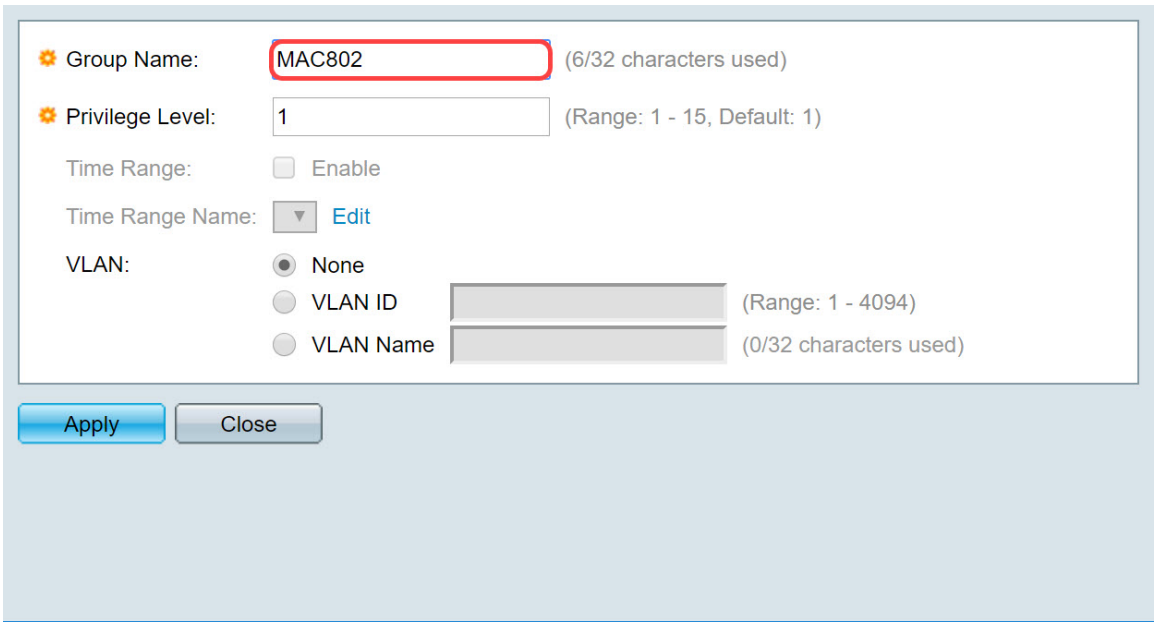
Passaggio 1. Passare a **Sicurezza > Server RADIUS > Gruppi di server RADIUS**.



Passaggio 2. Fare clic su **Aggiungi...** per aggiungere un nuovo gruppo di server RADIUS.

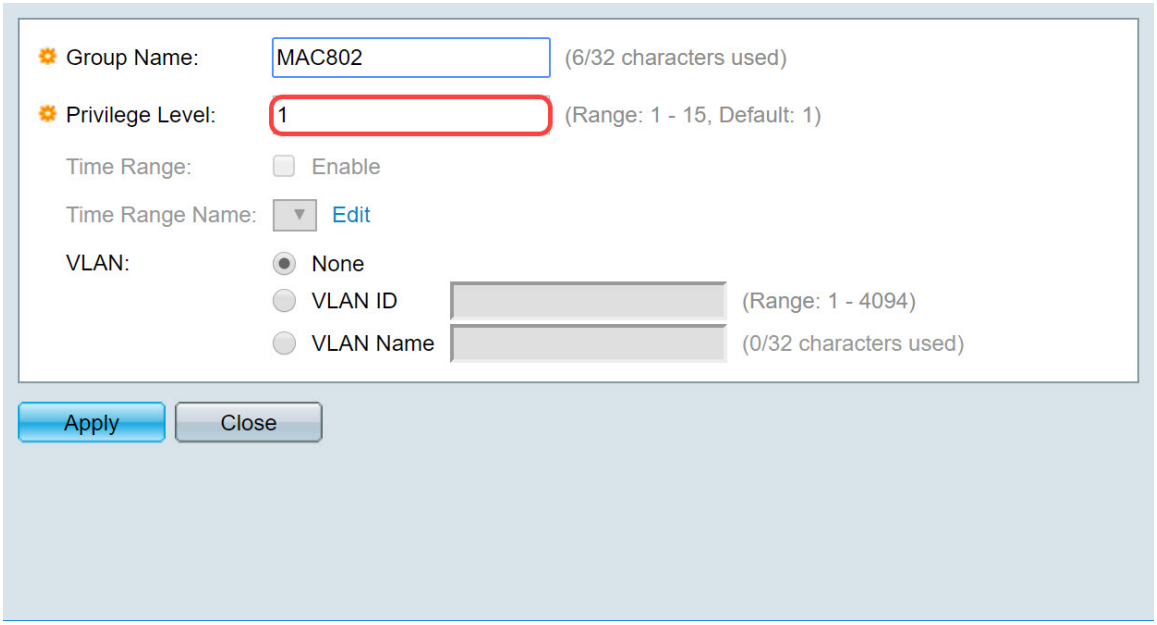


Passaggio 3. Viene visualizzata la pagina *Aggiungi gruppo di server RADIUS*. Immettere un nome per il gruppo. In questo esempio verrà utilizzato **MAC802** come nome del gruppo.



Passaggio 4. Inserire il livello di privilegi di accesso alla gestione del gruppo nel campo *Livello di privilegio*. L'intervallo è compreso tra 1 e 15, dove 15 è il privilegio più privilegiato e il valore predefinito è 1. In questo esempio il livello di privilegio rimarrà impostato su 1.

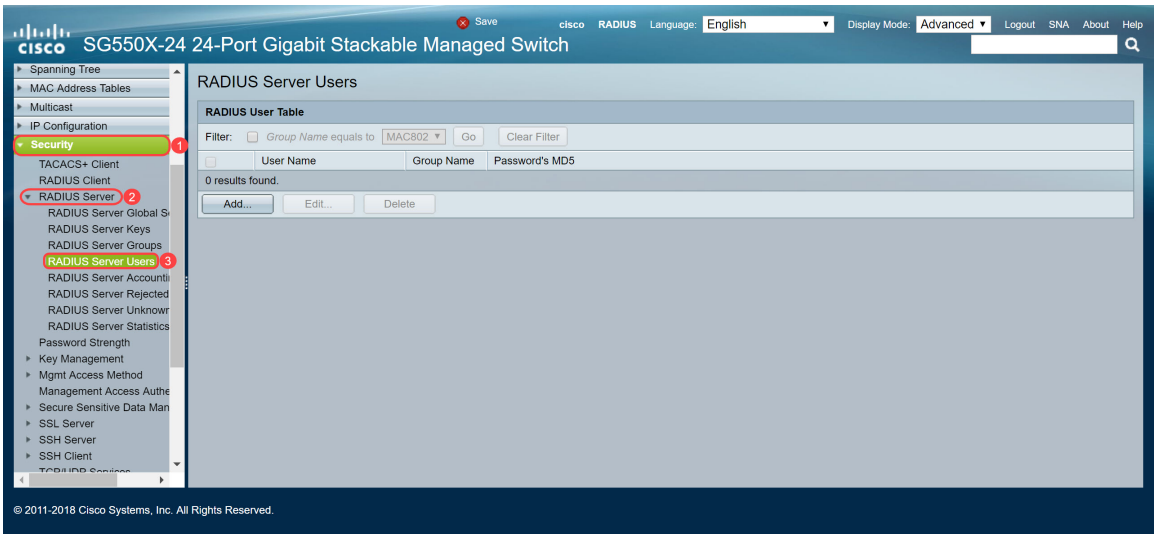
Nota: In questo articolo non configureremo l'*intervallo di tempo* o la *VLAN*.



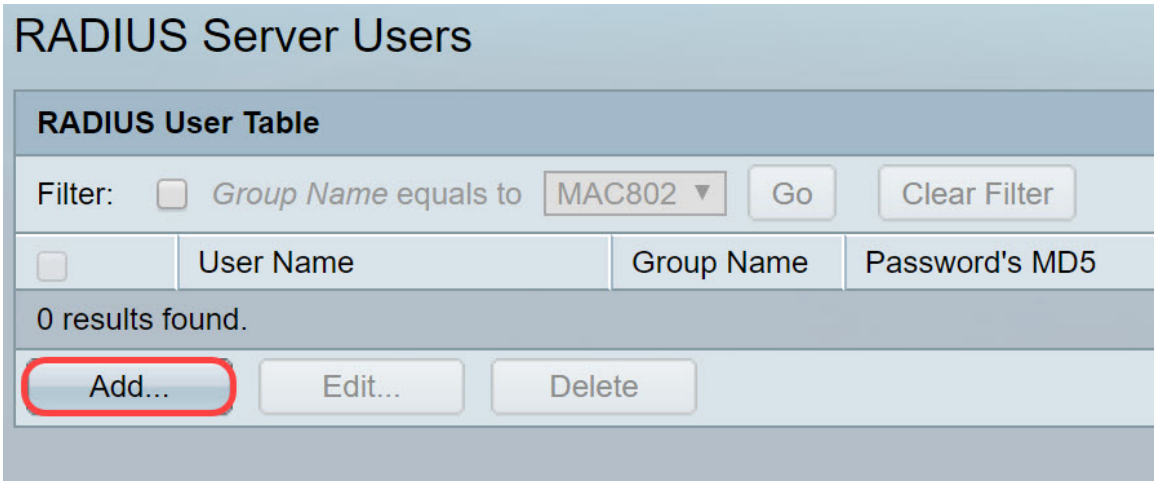
Passaggio 5. Fare clic su **Apply** per salvare le impostazioni.

Utenti server RADIUS

Passaggio 1. Passare a **Sicurezza > Server RADIUS > Utenti server RADIUS** per configurare gli utenti per RADIUS.

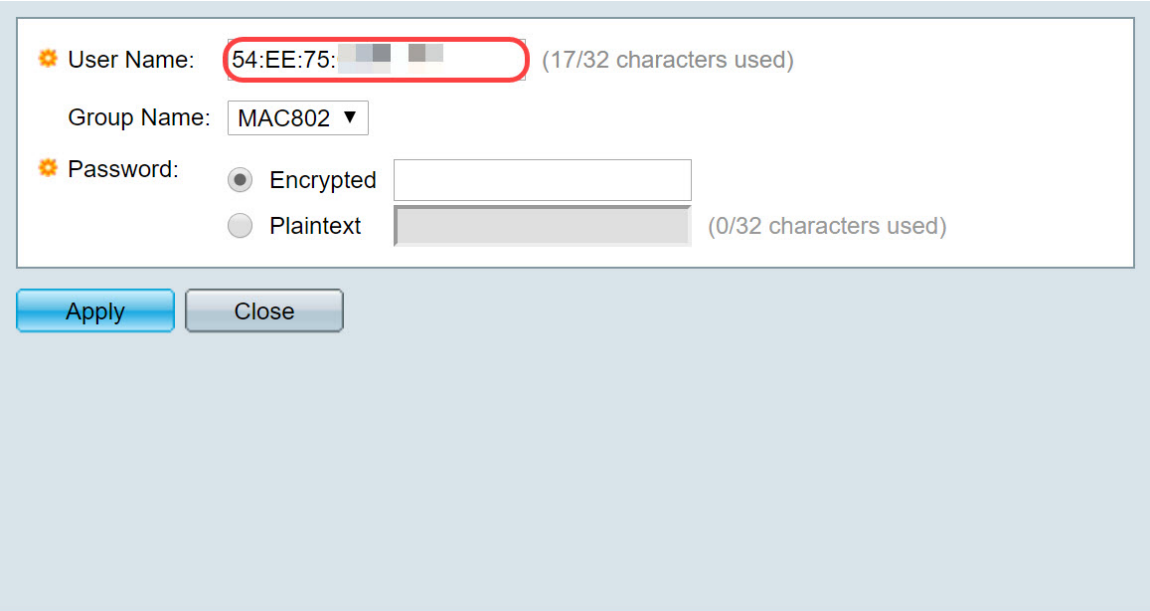


Passaggio 2. Fare clic su **Aggiungi...** per aggiungere un nuovo utente.

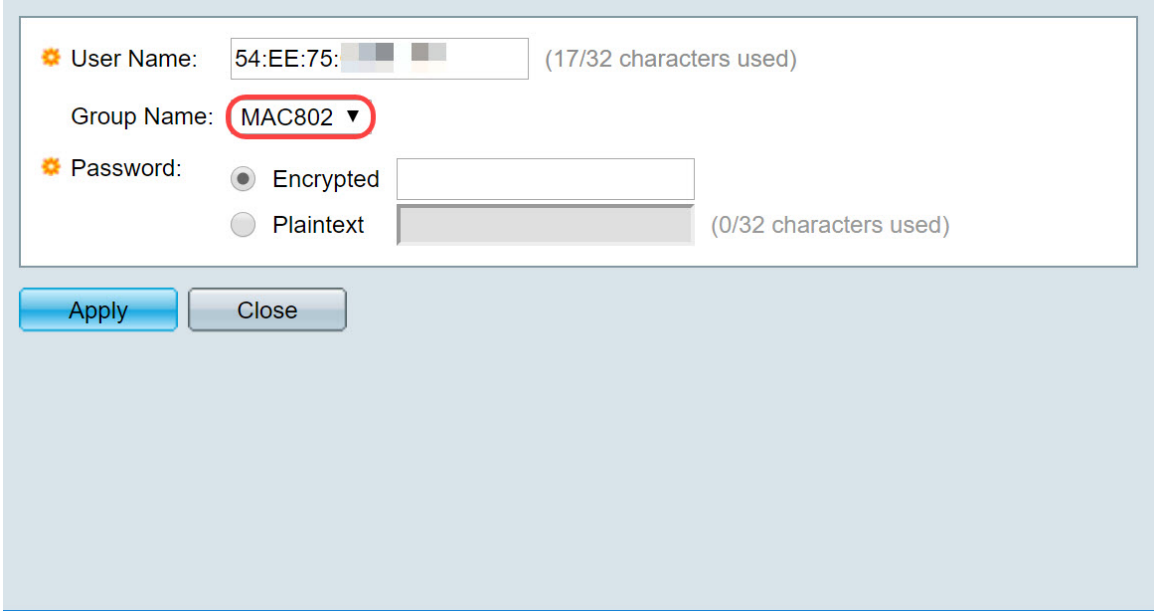


Passaggio 3. Viene visualizzata la pagina *Aggiungi utente server RADIUS*. Nel campo *Nome utente*, immettere l'indirizzo MAC di un utente. In questo esempio, verrà utilizzato l'indirizzo MAC Ethernet nel computer.

Nota: Una parte dell'indirizzo MAC è stata sfocata.



Passaggio 4. Selezionare un gruppo nell'elenco a discesa *Nome gruppo*. Come evidenziato nel passaggio 3 della sezione Gruppo server RADIUS, verrà selezionato **MAC802** come nome del gruppo per questo utente.

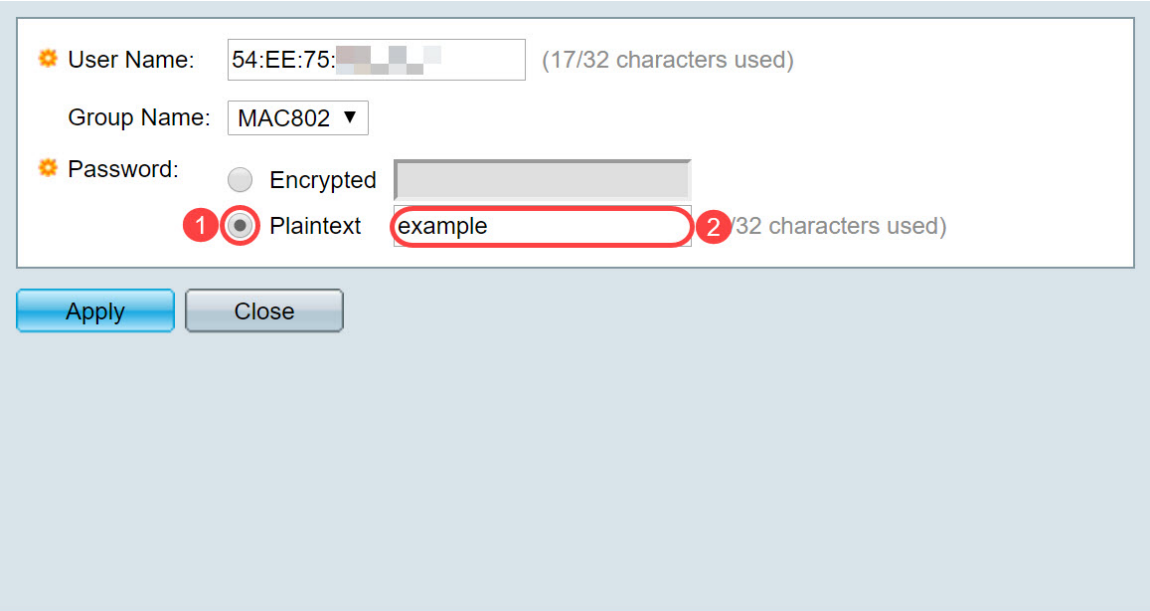


Passaggio 5. Selezionare uno dei seguenti pulsanti di opzione:

- Crittografia: una chiave viene utilizzata per crittografare le comunicazioni tramite MD5. Per utilizzare la crittografia, immettere la chiave in forma crittografata.
- Testo normale — se non si dispone di una stringa di chiave crittografata (da un altro dispositivo), immettere la stringa di chiave in modalità testo normale. La stringa della chiave crittografata viene generata e visualizzata.

Verrà selezionato *Testo normale* come password per questo utente e verrà digitato **esempio** come password in testo normale.

Nota: Non è consigliabile utilizzare **example** come password in testo normale. È consigliabile utilizzare una password più complessa.

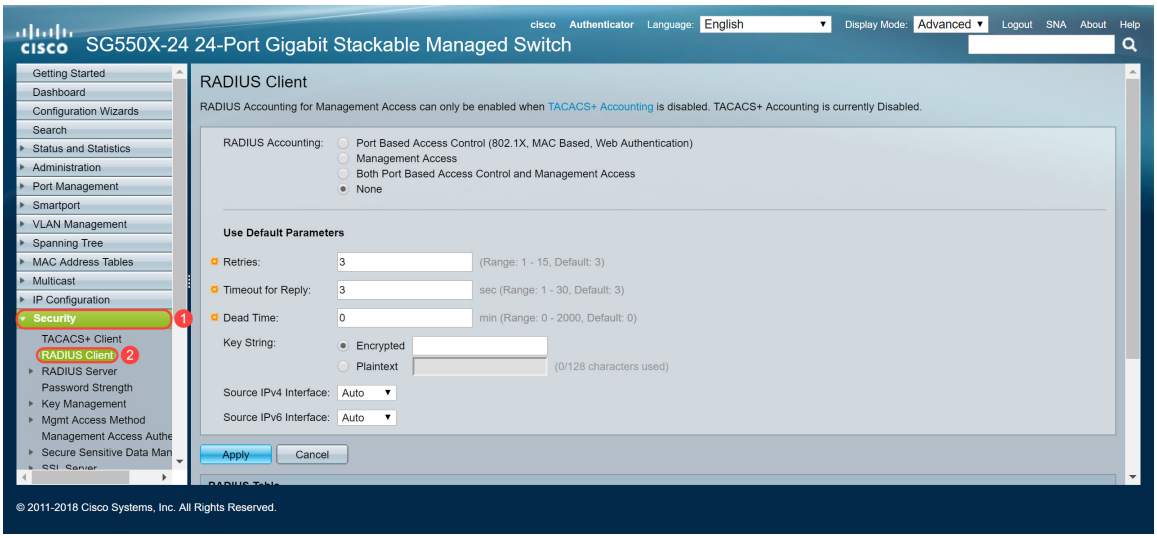


Passaggio 6. Al termine della configurazione, fare clic su **Applica**.

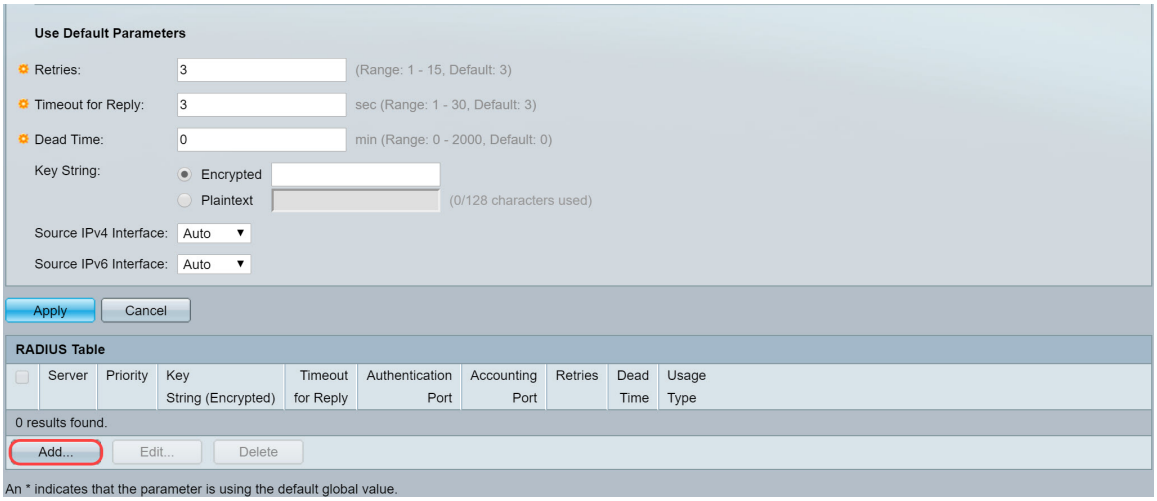
La configurazione del server RADIUS è terminata. Nella sezione successiva, il secondo switch verrà configurato come autenticatore.

Client RADIUS

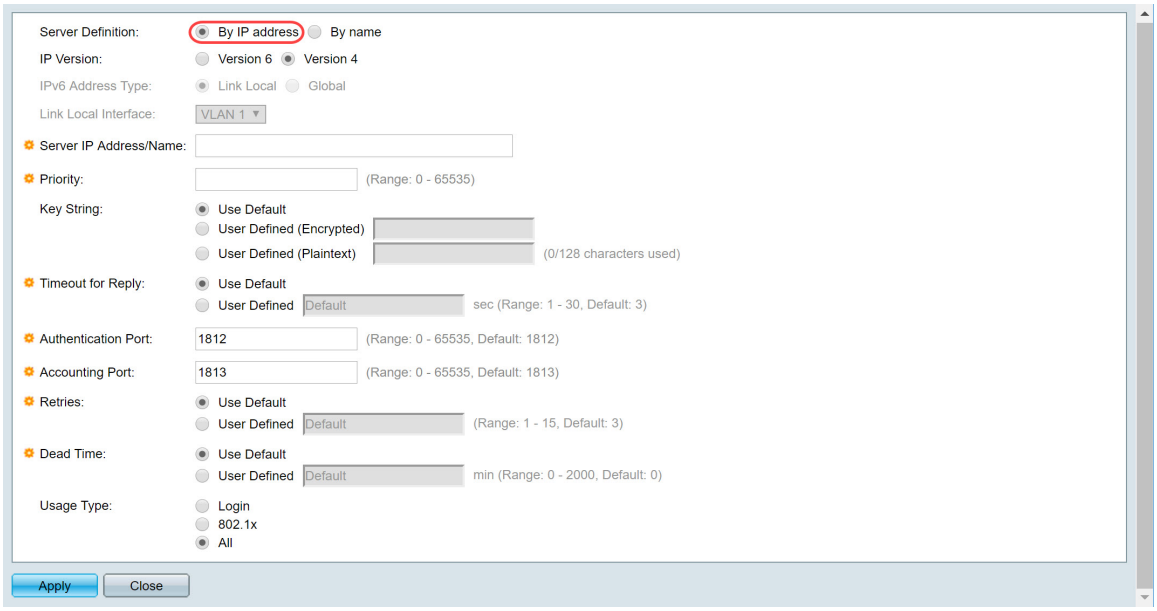
Passaggio 1. Accedere all'utility basata sul Web dello switch che verrà configurata come autenticatore e selezionare **Sicurezza > Client RADIUS**.



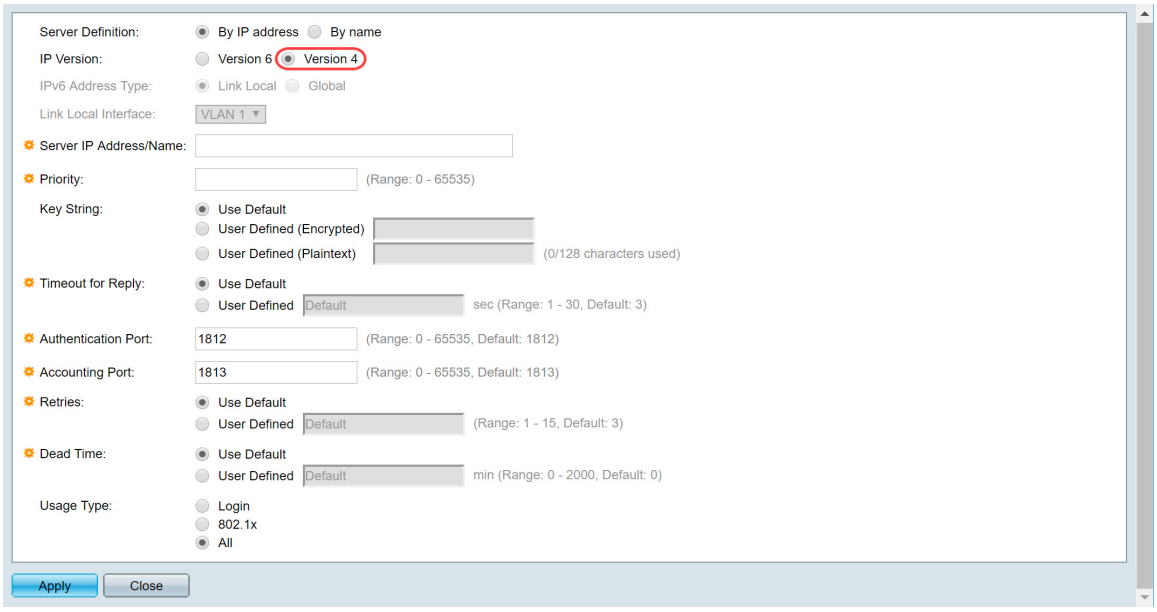
Passaggio 2. Scorrere fino alla sezione *Tabella RADIUS*, quindi fare clic su **Aggiungi...** per aggiungere un server RADIUS.



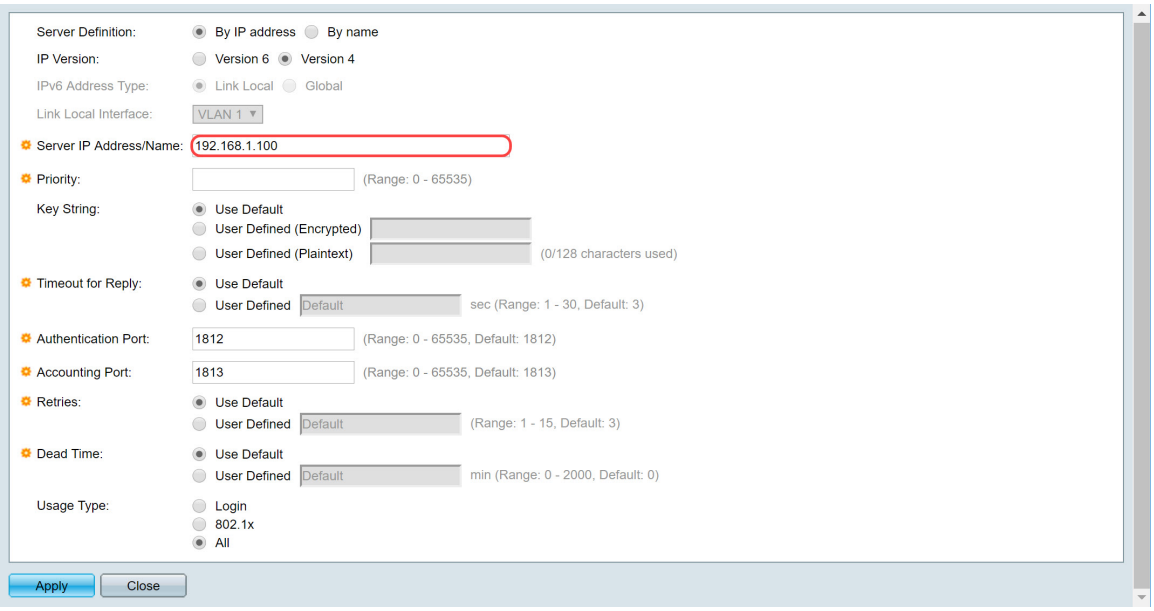
Passaggio 3. (Facoltativo) Selezionare se specificare il server RADIUS in base all'indirizzo IP o al nome nel campo *Definizione server*. Nell'esempio, verrà mantenuta la selezione predefinita **Per indirizzo IP**.



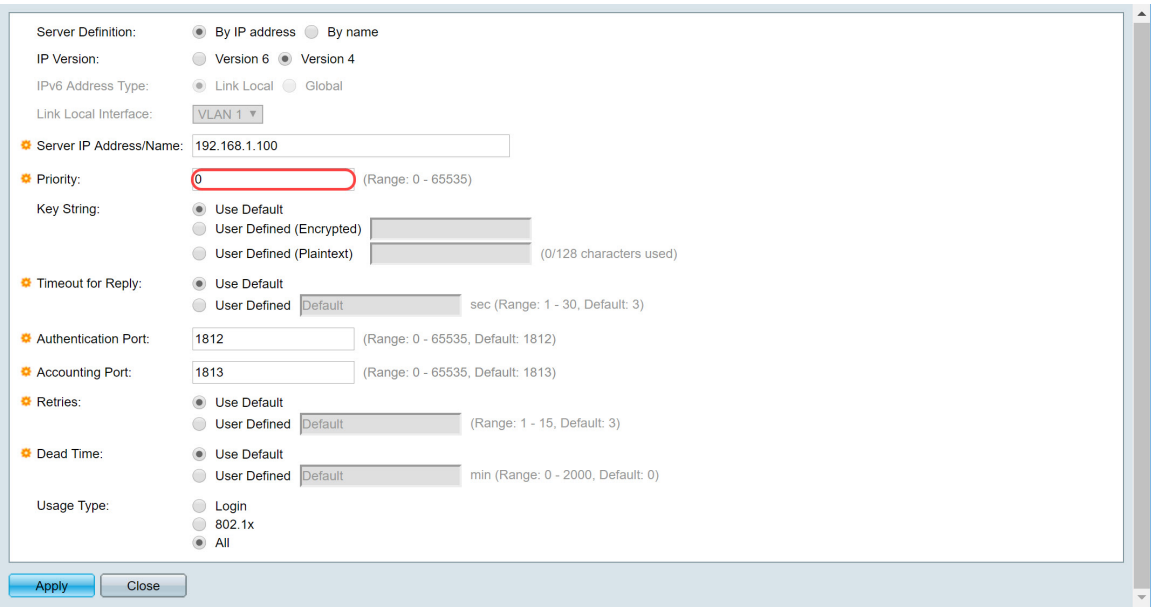
Passaggio 4. (Facoltativo) Selezionare la versione dell'indirizzo IP del server RADIUS nel campo *Versione IP*. Per questo esempio verrà mantenuta la selezione predefinita della **versione 4**.



Passaggio 5. Immettere nel server RADIUS l'indirizzo IP o il nome. Nel campo *Indirizzo IP/Nome server* verrà immesso l'indirizzo IP **192.168.1.100**.

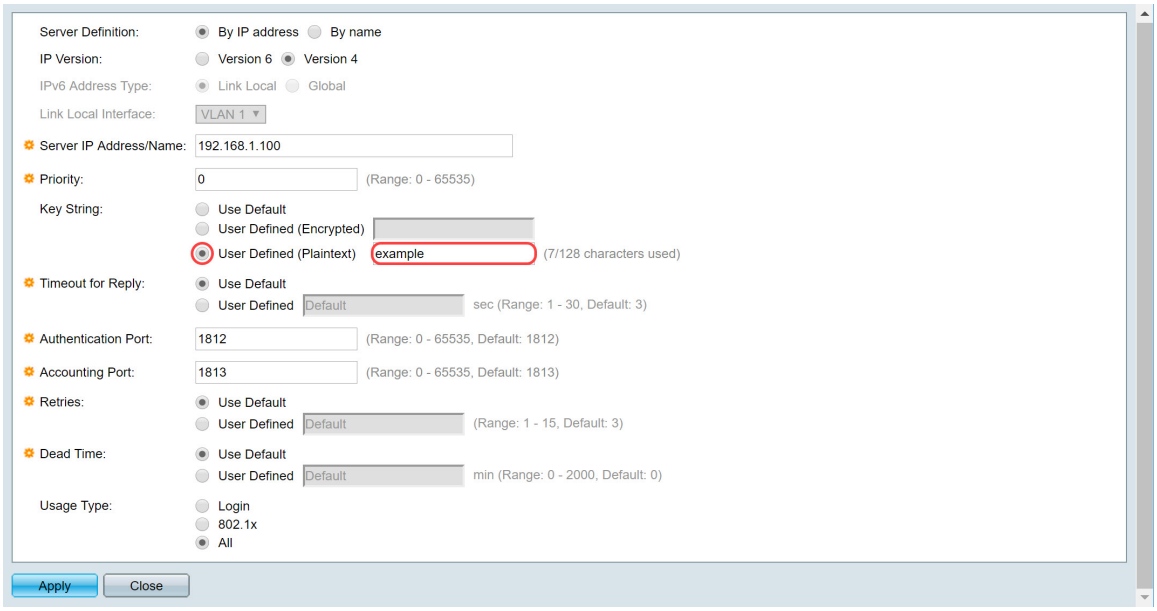


Passaggio 6. Immettere la priorità del server. La priorità determina l'ordine in cui il dispositivo tenta di contattare i server per autenticare un utente. Il dispositivo viene avviato con il server RADIUS con la priorità più alta. Zero è la priorità più alta.



Passaggio 7. Immettere la stringa di chiave utilizzata per autenticare e crittografare la comunicazione tra il dispositivo e il server RADIUS. Questa chiave deve corrispondere alla chiave configurata nel server RADIUS. Può essere immesso in formato **crittografato** o **non crittografato**. Se si seleziona **Utilizza predefinito**, il dispositivo tenta di eseguire l'autenticazione al server RADIUS utilizzando la stringa di chiave predefinita. Verrà utilizzato il **testo definito dall'utente (testo normale)** e verrà immesso l'**esempio** chiave.

Nota: Il resto della configurazione verrà mantenuto come predefinito. Se lo si desidera, è possibile configurarli.

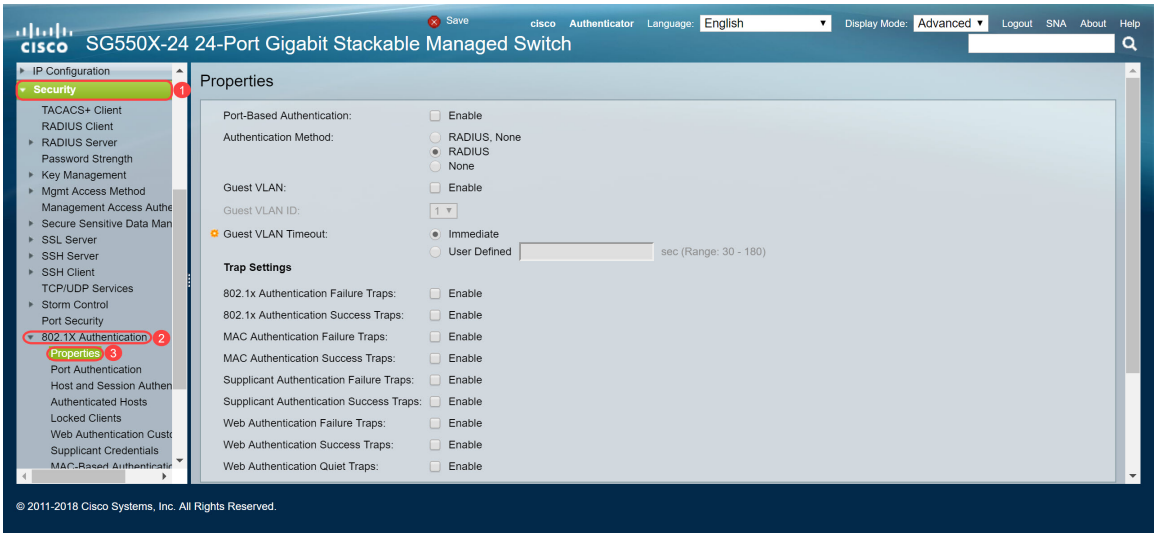


Passaggio 8. Fare clic su **Apply** per salvare la configurazione.

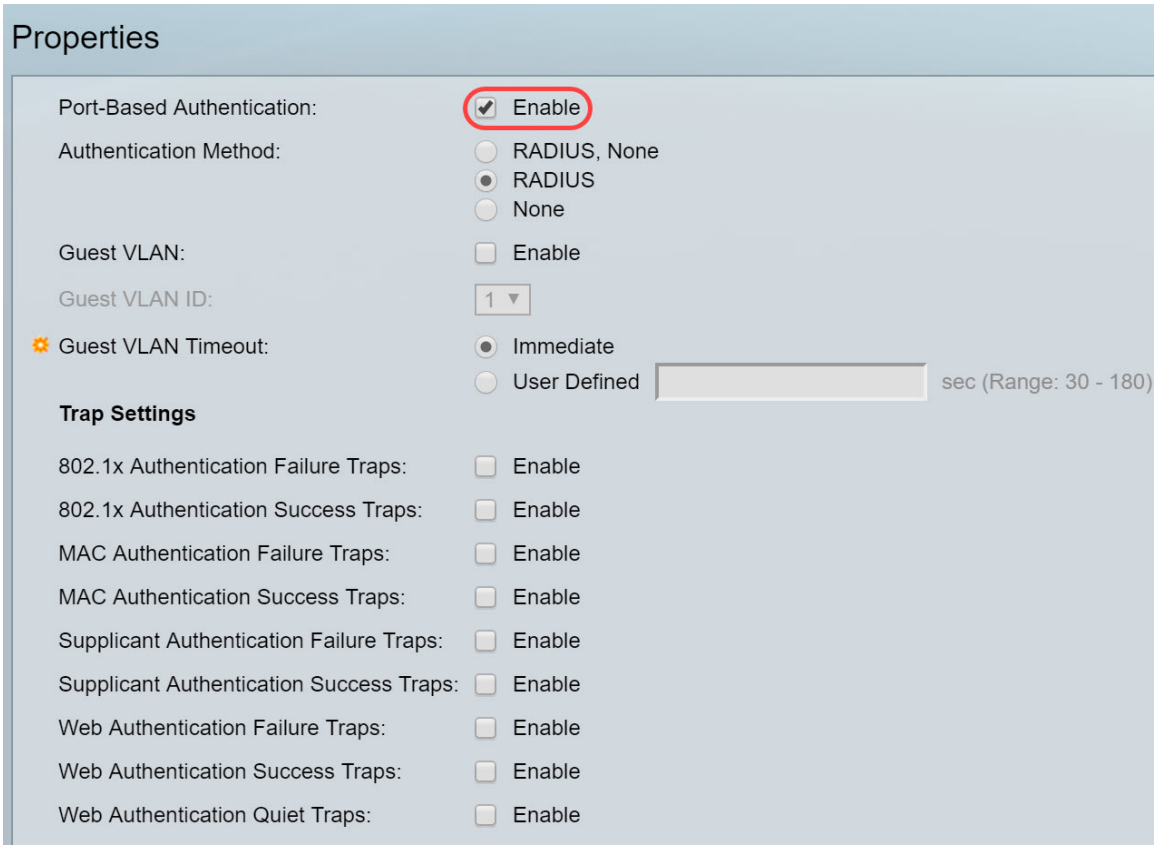
Proprietà autenticazione 802.1X

La pagina delle proprietà viene utilizzata per abilitare globalmente l'autenticazione della porta o del dispositivo. per funzionare, l'autenticazione deve essere attivata sia globalmente che singolarmente su ciascuna porta.

Passaggio 1. Passare a **Protezione > Autenticazione 802.1X > Proprietà**.

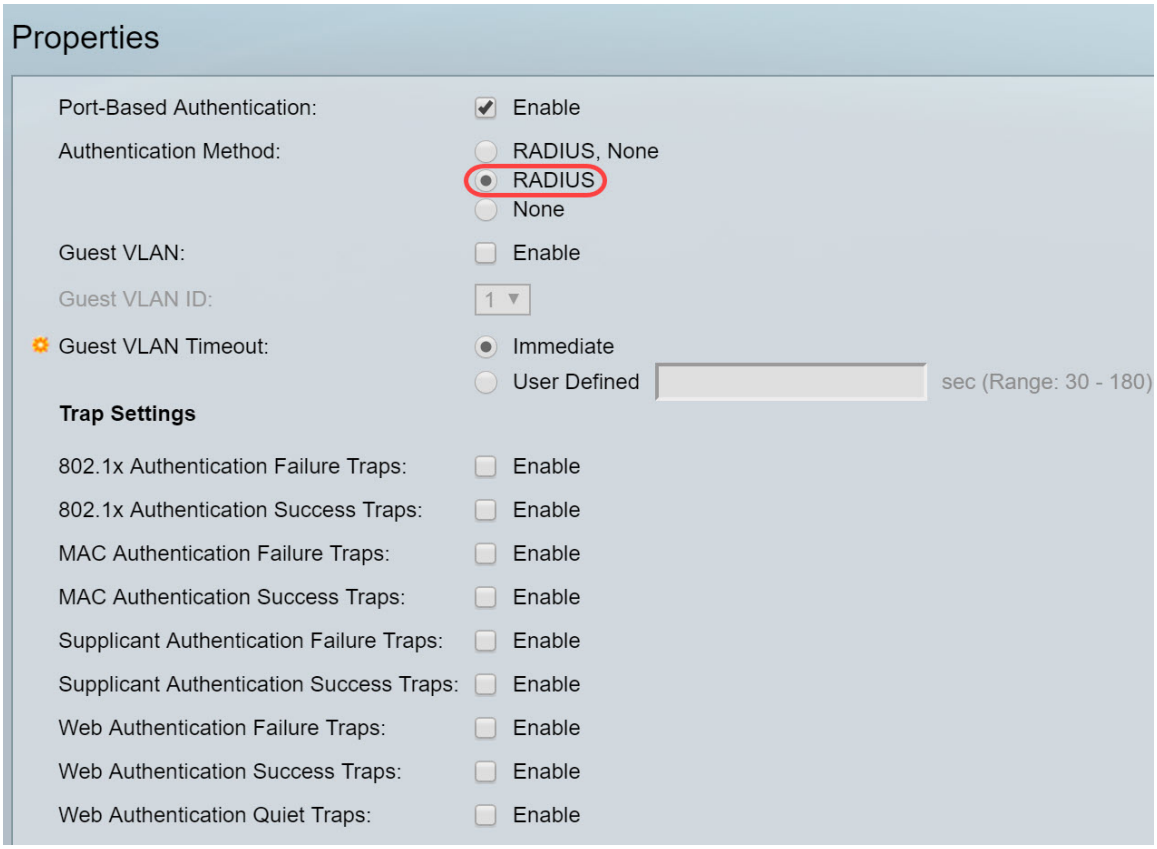


Passaggio 2. Selezionare la casella di controllo **Abilita** per abilitare l'autenticazione basata sulla porta.

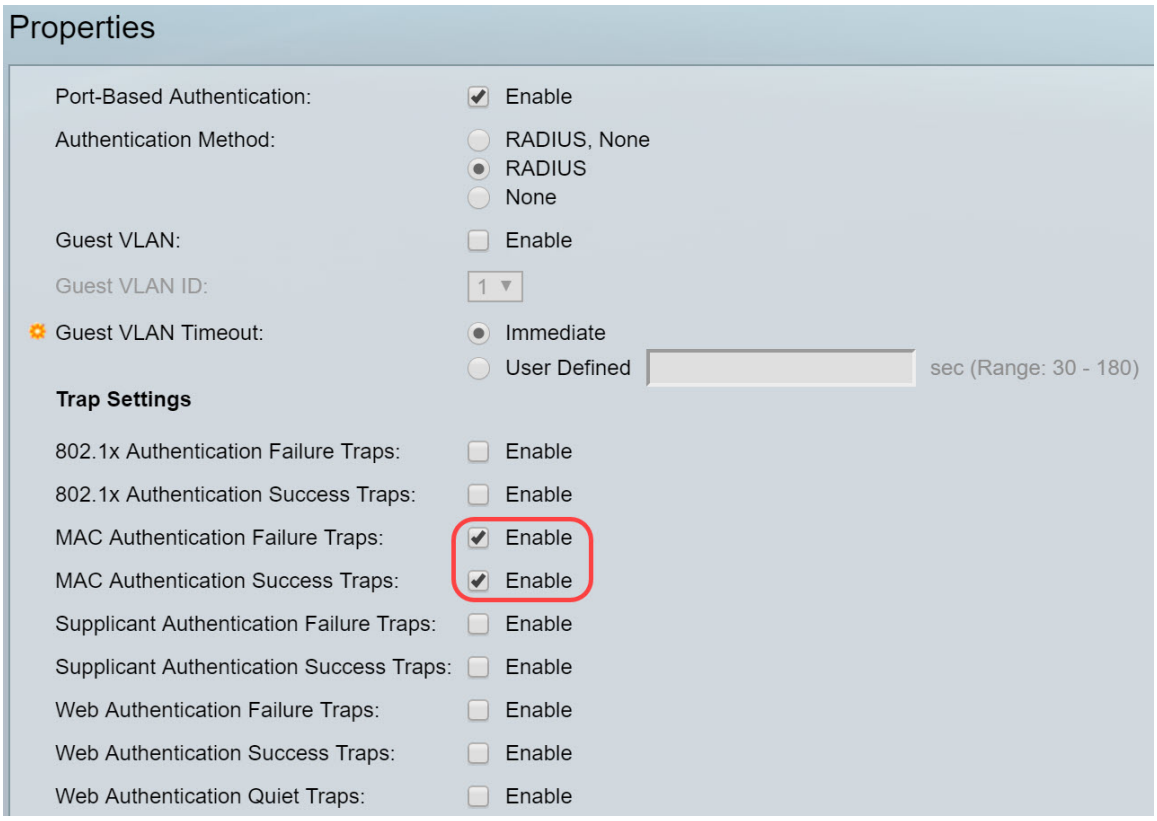


Passaggio 3. Selezionare i metodi di autenticazione utente. Verrà scelto RADIUS come metodo di autenticazione. Le opzioni seguenti sono:

- RADIUS, Nessuno — esegue prima l'autenticazione delle porte utilizzando il server RADIUS. Se non si riceve alcuna risposta da RADIUS (ad esempio se il server non è attivo), non viene eseguita alcuna autenticazione e la sessione è consentita. Se il server è disponibile ma le credenziali utente non sono corrette, l'accesso viene negato e la sessione viene terminata.
- RADIUS — autentica l'utente sul server RADIUS. Se non viene eseguita alcuna autenticazione, la sessione non è consentita.
- Nessuno - Non autentica l'utente. Consentire la sessione.



Passaggio 4. (Facoltativo) Selezionare la casella di controllo **Abilita** per *Registrazioni errori autenticazione MAC* e Registrazioni *errori autenticazione MAC*. Se l'autenticazione MAC ha esito negativo o positivo, verrà generata una trap. In questo esempio, verranno abilitati sia i *trap degli errori di autenticazione MAC* che i *trap degli errori di autenticazione MAC*.

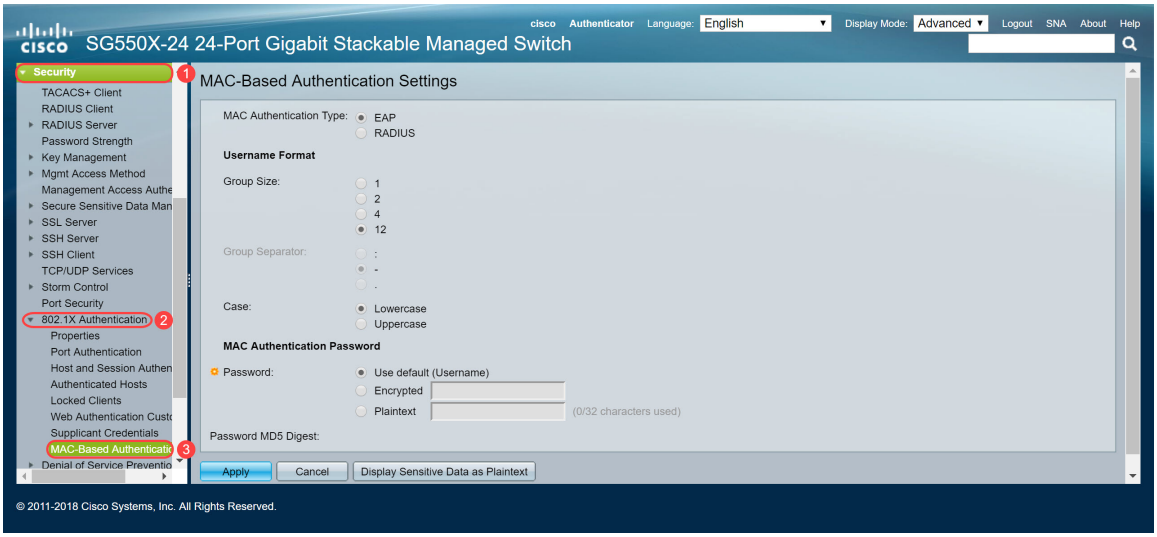


Passaggio 5. Fare clic su **Applica**.

Impostazioni di autenticazione basata su MAC per l'autenticazione 802.1X

Questa pagina consente di configurare varie impostazioni applicabili all'autenticazione basata su MAC.

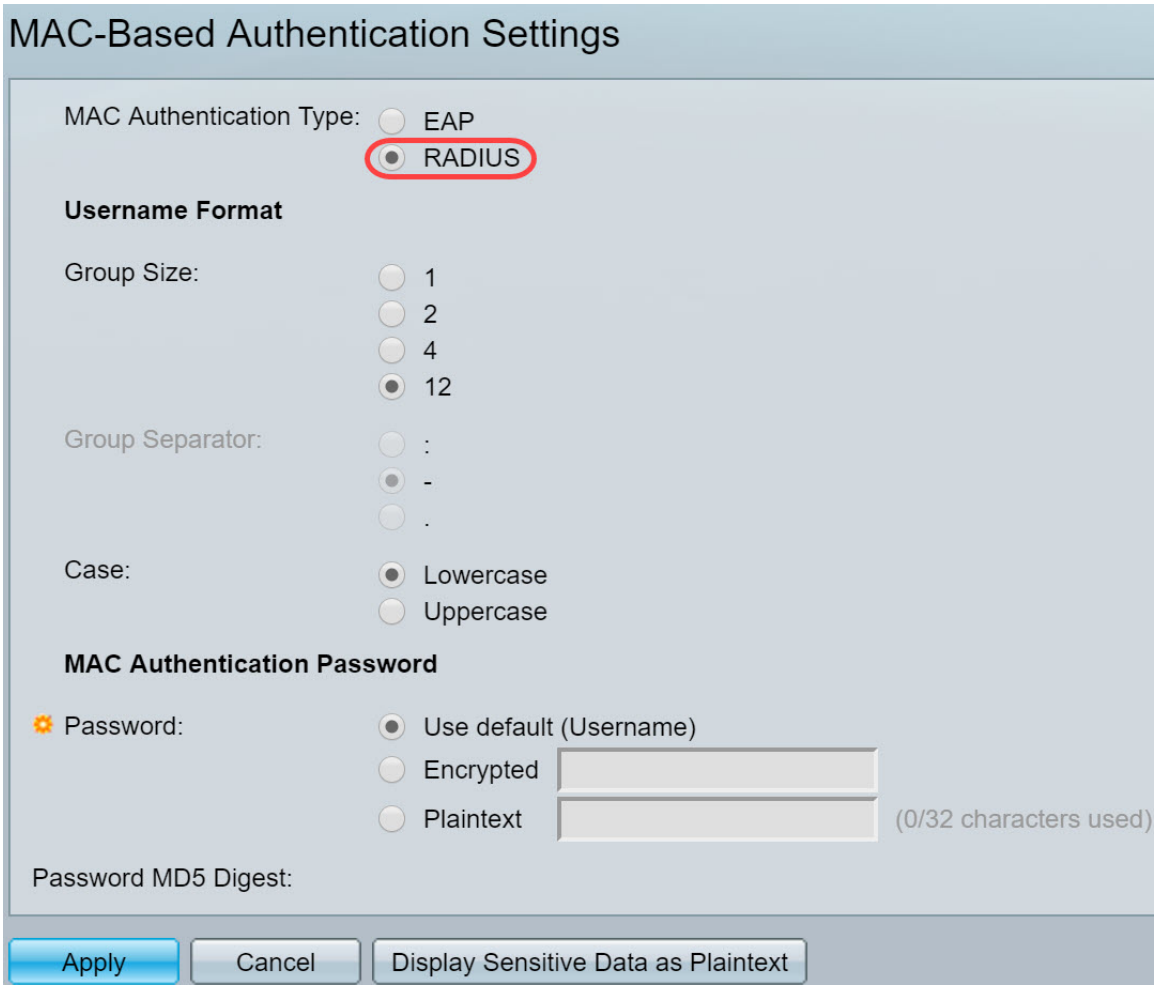
Passaggio 1. Passare a **Sicurezza > Autenticazione 802.1X > Impostazioni di autenticazione basate su MAC**.



Passaggio 2. Nel campo *Tipo di autenticazione MAC*, selezionare una delle seguenti opzioni:

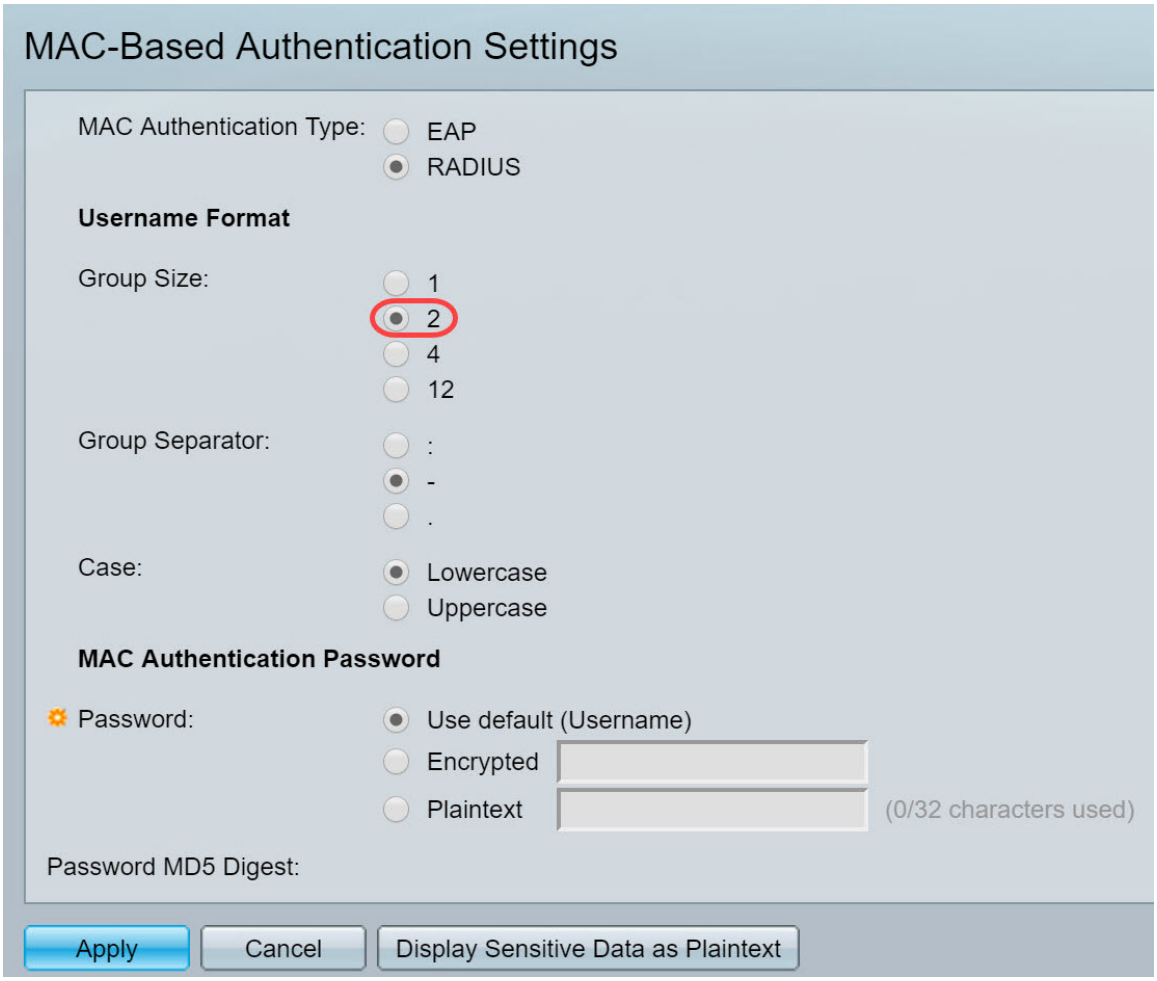
- EAP: utilizzare RADIUS con incapsulamento EAP per il traffico tra lo switch (client RADIUS) e il server RADIUS, che autentica un supplicant basato su MAC.
- RADIUS: utilizza RADIUS senza incapsulamento EAP per il traffico tra lo switch (client RADIUS) e il server RADIUS, che autentica un supplicant basato su MAC.

In questo esempio verrà scelto RADIUS come tipo di autenticazione MAC.

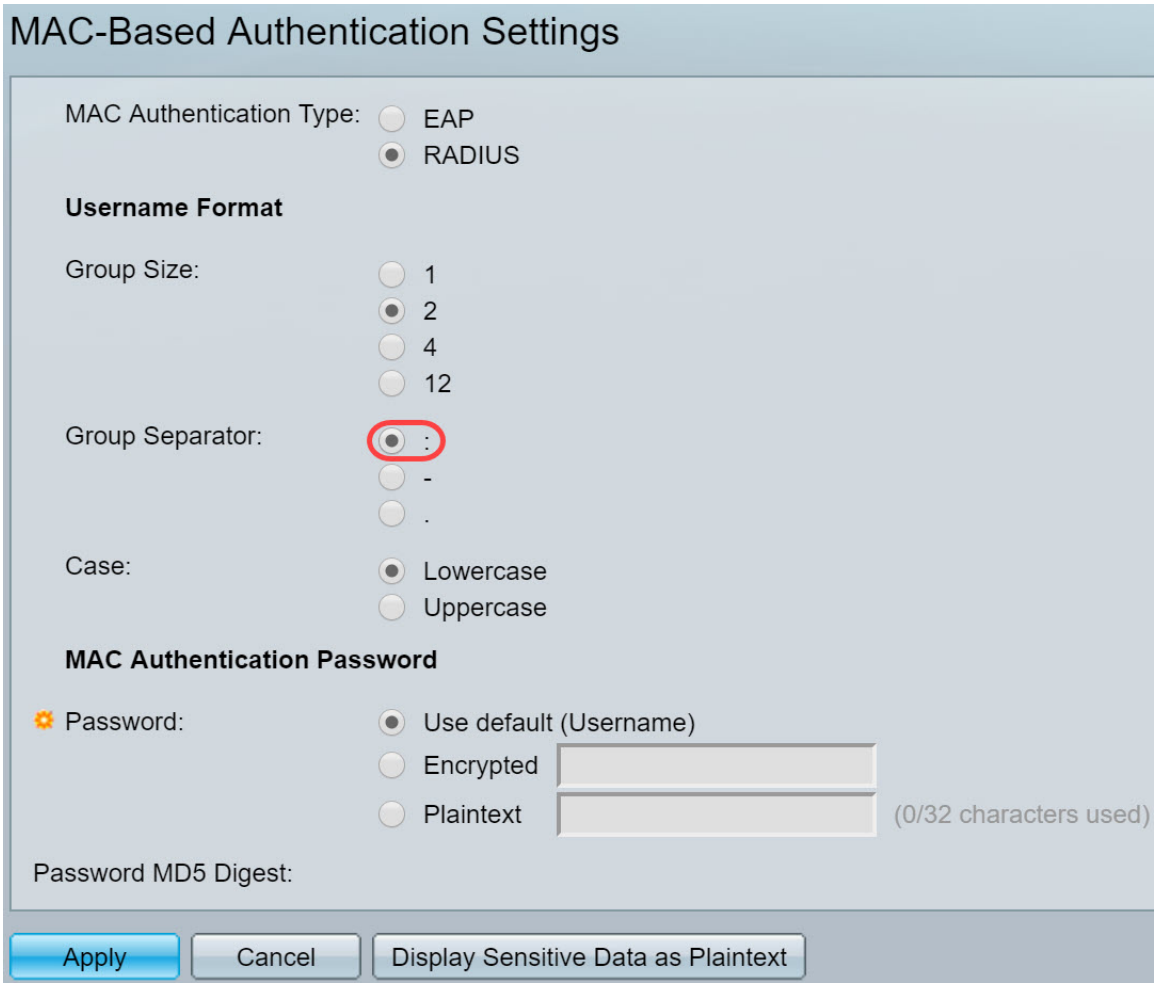


Passaggio 3. In *Formato nome utente*, selezionare il numero di caratteri ASCII tra i delimitatori dell'indirizzo MAC inviato come nome utente. In questo caso, sceglieremo 2 come dimensione del nostro gruppo.

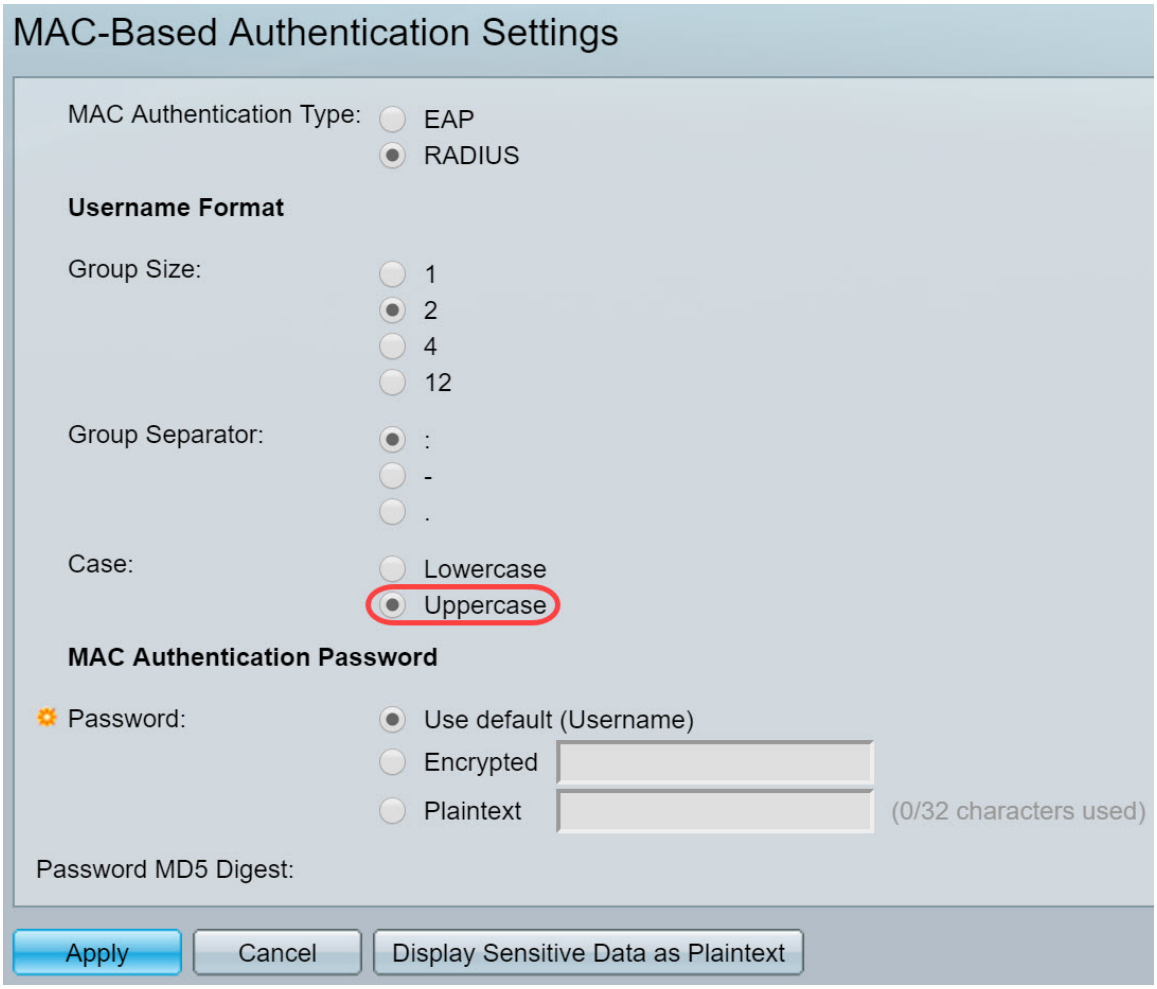
Nota: Verificare che il formato del nome utente sia lo stesso utilizzato per l'immissione dell'indirizzo MAC nella sezione *Utenti server Radius*.



Passaggio 4. Selezionare il carattere utilizzato come delimitatore tra i gruppi definiti di caratteri nell'indirizzo MAC. In questo esempio verranno selezionati **:** come separatore di gruppo.

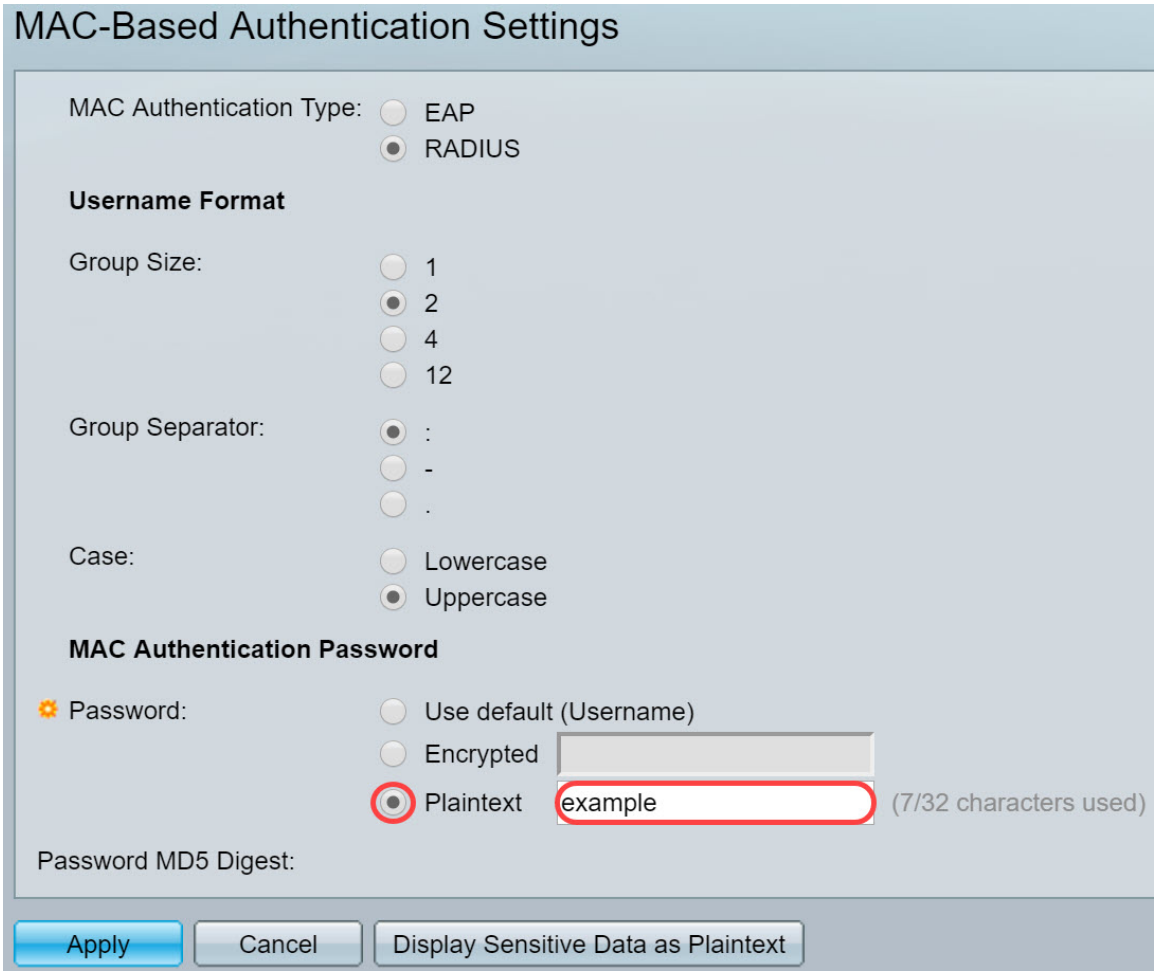


Passaggio 5. Nel campo *Case*, selezionare **Minuscolo** o **Maiuscolo** per inviare il nome utente in lettere minuscole o maiuscole.



Passaggio 6. La password definisce la modalità di autenticazione dello switch tramite il server RADIUS. Selezionate una delle seguenti opzioni:

- Usa default (Username) - Selezionare questa opzione per utilizzare il nome utente definito come password.
- Crittografata — Definire una password in formato crittografato.
- Testo normale — definire una password in formato testo normale.



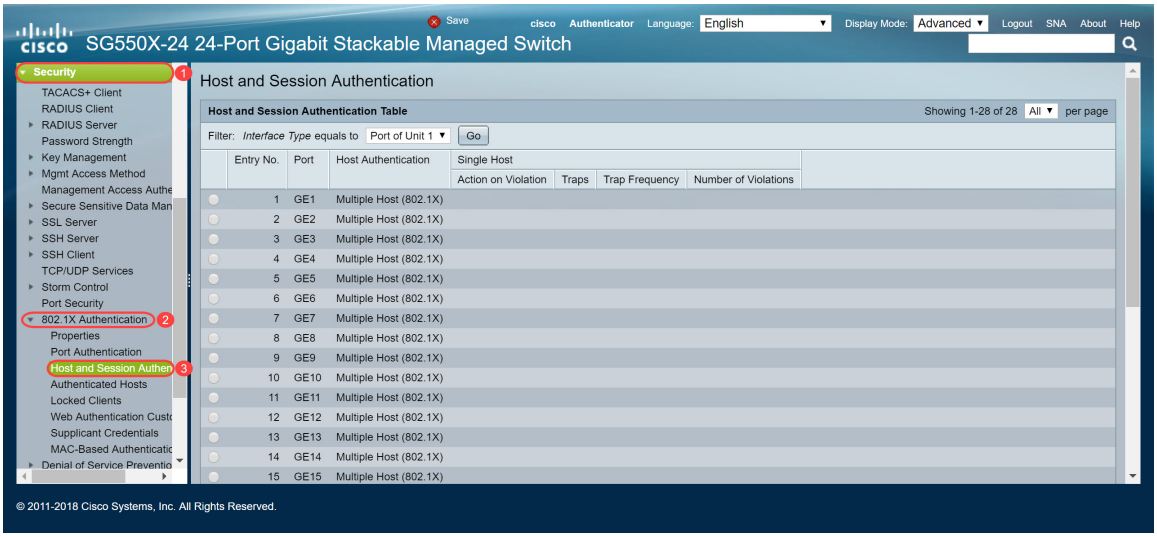
Nota: *Password Message-Digest Algorithm 5 (MD5) Digest* visualizza la password MD5 Digest. MD5 è una funzione hash crittografica che accetta un dato e crea un output esadecimale univoco che in genere non è riproducibile. MD5 utilizza un valore hash a 128 bit.

Passaggio 7. Fare clic su **Apply** (Applica) per salvare le impostazioni nel file della configurazione corrente.

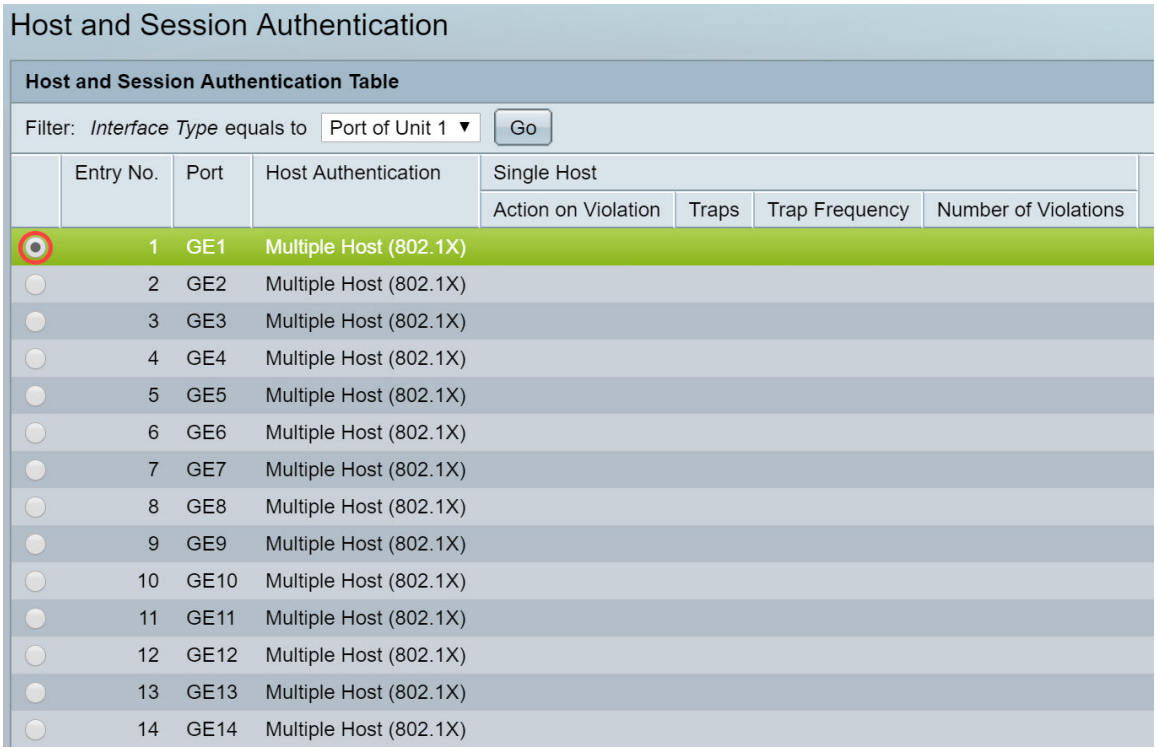
Autenticazione 802.1X Autenticazione host e sessione

La pagina *Autenticazione host e sessione* consente di definire la modalità di funzionamento di 802.1X sulla porta e l'azione da eseguire se viene rilevata una violazione.

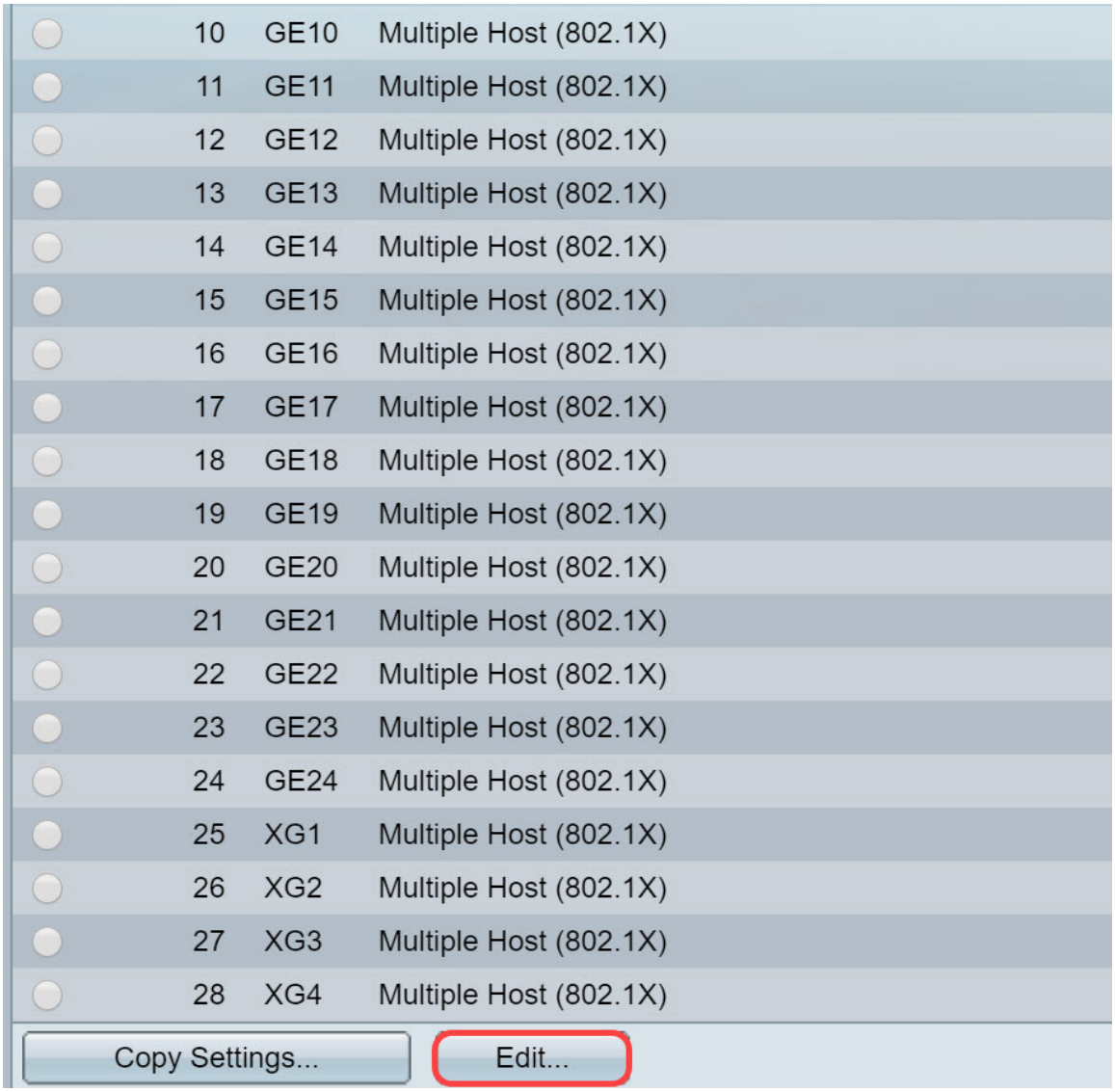
Passaggio 1. Passare a **Sicurezza > Autenticazione 802.1X > Autenticazione host e sessione**.



Passaggio 2. Selezionare la porta per cui si desidera configurare l'autenticazione host. In questo esempio, verrà configurata la connessione di GE1 a un host finale.



Passaggio 3. Fare clic su **Modifica...** per configurare la porta.

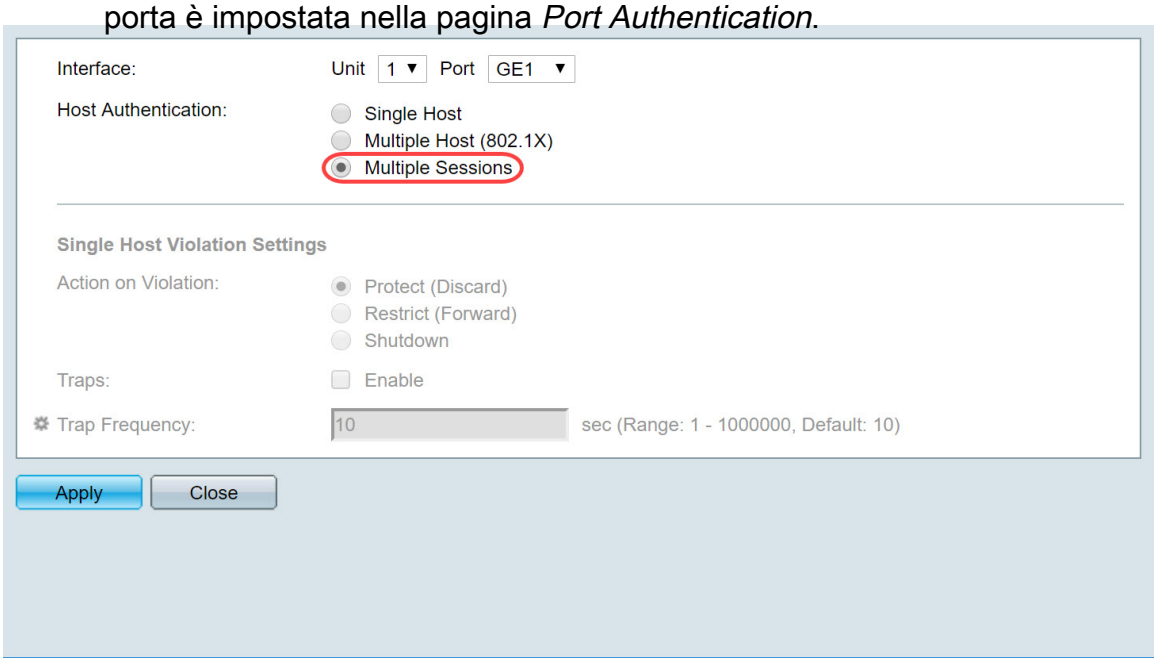


Passaggio 4. Nel campo *Autenticazione host*, selezionare una delle seguenti opzioni:

1. Modalità host singolo
   - Una porta è autorizzata se esiste un client autorizzato. Su una porta è possibile autorizzare un solo host.
   - Quando una porta non è autorizzata e la VLAN guest è abilitata, il traffico senza tag viene mappato nuovamente sulla VLAN guest. Il traffico con tag viene interrotto a meno che non appartenga alla VLAN guest o a una VLAN non autenticata. Se una VLAN guest non è abilitata sulla porta, viene eseguito il bridging solo del traffico con tag appartenente alle VLAN non autenticate.
   - Quando una porta è autorizzata, il traffico non contrassegnato e contrassegnato proveniente dall'host autorizzato viene bloccato in base alla configurazione della porta di appartenenza della VLAN statica. Il traffico proveniente da altri host viene scartato.
   - Un utente può specificare che il traffico senza tag proveniente dall'host autorizzato venga mappato nuovamente su una VLAN assegnata da un server RADIUS durante il processo di autenticazione. Il traffico contrassegnato viene interrotto a meno che non appartenga alla VLAN assegnata da RADIUS o alle VLAN non autenticate. L'assegnazione di VLAN Radius su una porta è impostata nella pagina *Port Authentication* (Autenticazione porta).
2. Modalità multi-host
   - Una porta è autorizzata se esiste almeno un client autorizzato.
   - Quando una porta non è autorizzata e una VLAN guest è abilitata, il traffico senza tag viene mappato nuovamente sulla VLAN guest. Il traffico con tag viene interrotto a meno

che non appartenga alla VLAN guest o a una VLAN non autenticata. Se la VLAN guest non è abilitata su una porta, viene eseguito il bridging solo del traffico con tag appartenente alle VLAN non autenticate.
- Quando una porta è autorizzata, il traffico senza tag e con tag da tutti gli host connessi alla porta viene sottoposto a bridging in base alla configurazione della porta di appartenenza della VLAN statica.
- Èpossibile specificare che il traffico senza tag proveniente dalla porta autorizzata venga mappato nuovamente su una VLAN assegnata da un server RADIUS durante il processo di autenticazione. Il traffico con tag viene interrotto a meno che non appartenga alla VLAN assegnata da RADIUS o a VLAN non autenticate. L'assegnazione di VLAN Radius su una porta è impostata nella pagina *Port Authentication* (Autenticazione porta).

3. Modalità multisessione
   - A differenza delle modalità host singolo e host multiplo, le porte in modalità multisessione non hanno uno stato di autenticazione. Questo stato viene assegnato a ciascun client connesso alla porta.
   - Il traffico contrassegnato appartenente a una VLAN non autenticata viene sempre indirizzato, indipendentemente dal fatto che l'host sia autorizzato o meno.
   - Il traffico contrassegnato e non contrassegnato proveniente da host non autorizzati che non appartengono a una VLAN non autenticata viene mappato nuovamente alla VLAN guest se è definita e abilitata sulla VLAN, oppure viene scartato se la VLAN guest non è abilitata sulla porta.
   - Èpossibile specificare che il traffico senza tag proveniente dalla porta autorizzata venga mappato nuovamente su una VLAN assegnata da un server RADIUS durante il processo di autenticazione. Il traffico con tag viene interrotto a meno che non appartenga alla VLAN assegnata da RADIUS o a VLAN non autenticate. L'assegnazione di VLAN Radius a una porta è impostata nella pagina *Port Authentication*.



Passaggio 5. Fare clic su **Apply** per salvare la configurazione.

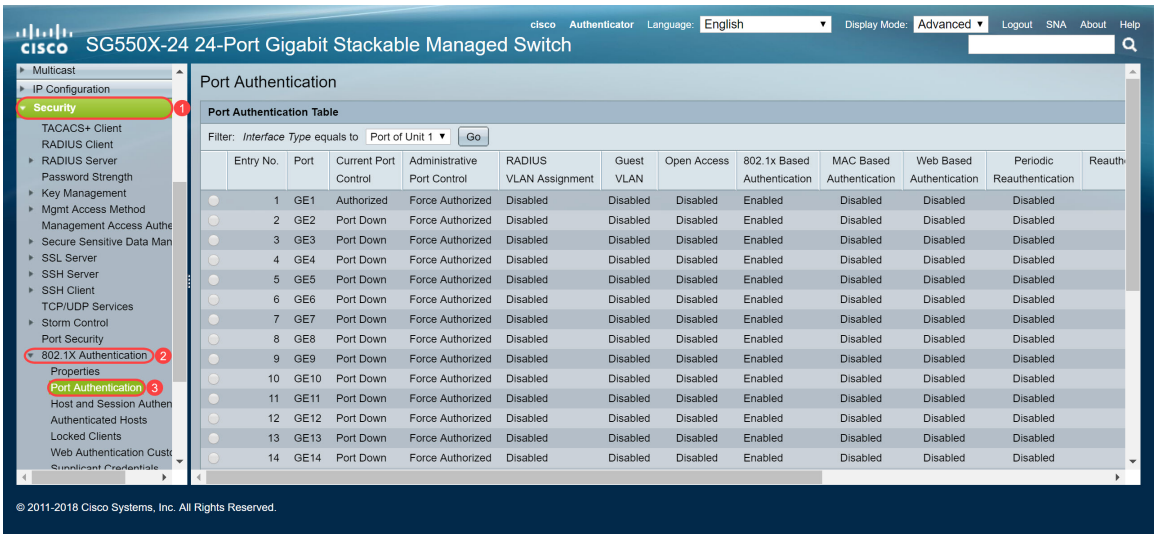
Nota: Usa *impostazioni copia...* per applicare la stessa configurazione di GE1 a più porte. Lasciare la porta collegata al server RADIUS come *Host multiplo (802.1X)*.

Autenticazione porta 802.1X

La pagina *Port Authentication* (Autenticazione porta) consente di configurare i parametri di ciascuna porta. Poiché alcune modifiche della configurazione sono possibili solo quando la porta è in stato Force Authorized, ad esempio l'autenticazione host, è consigliabile modificare il controllo della porta in Force Authorized prima di apportare modifiche. Al termine della configurazione, ripristinare lo stato precedente del controllo della porta.

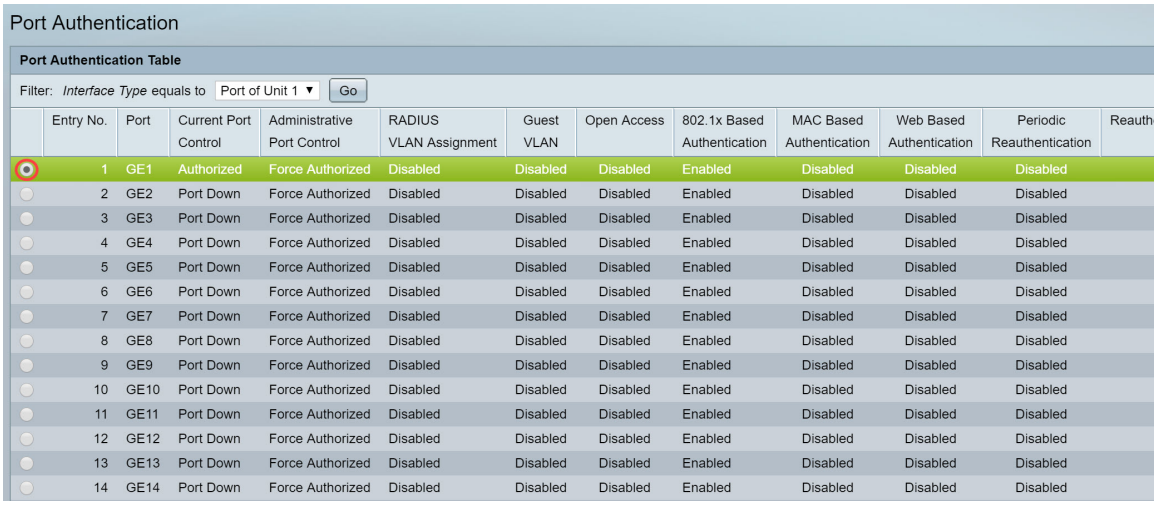
Nota: Verranno configurate solo le impostazioni necessarie per l'autenticazione basata su MAC. Il resto della configurazione verrà lasciato come predefinito.

Passaggio 1. Passare a **Sicurezza > Autenticazione 802.1X > Autenticazione porta**.

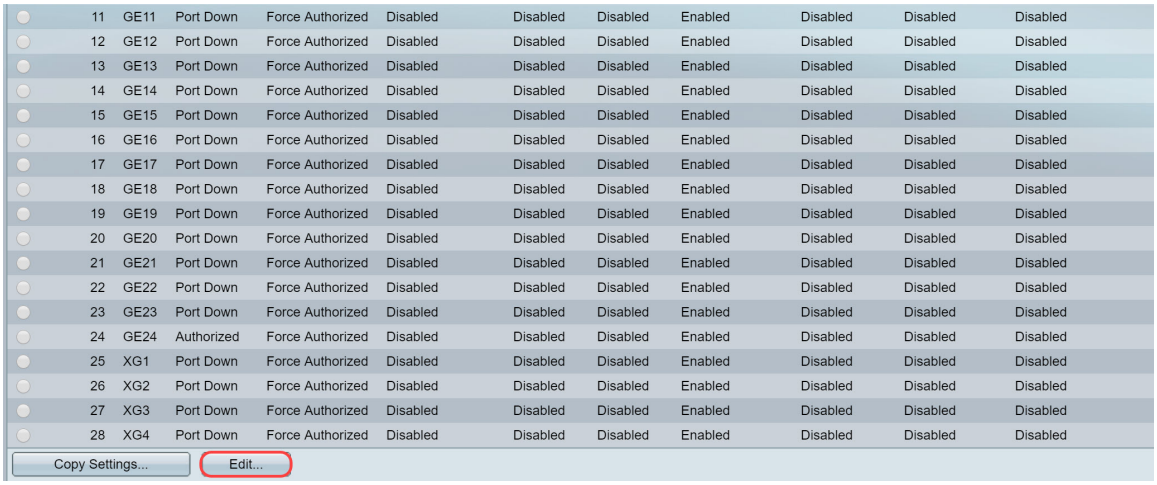


Passaggio 2. Selezionare la porta che si desidera configurare per l'autorizzazione della porta.

Nota: Non configurare la porta a cui è connesso lo switch. Poiché lo switch è un dispositivo attendibile, lasciare la porta *autorizzata* come *forzata*.



Passaggio 3. Scorrere quindi verso il basso e fare clic su **Modifica...** per configurare la porta.

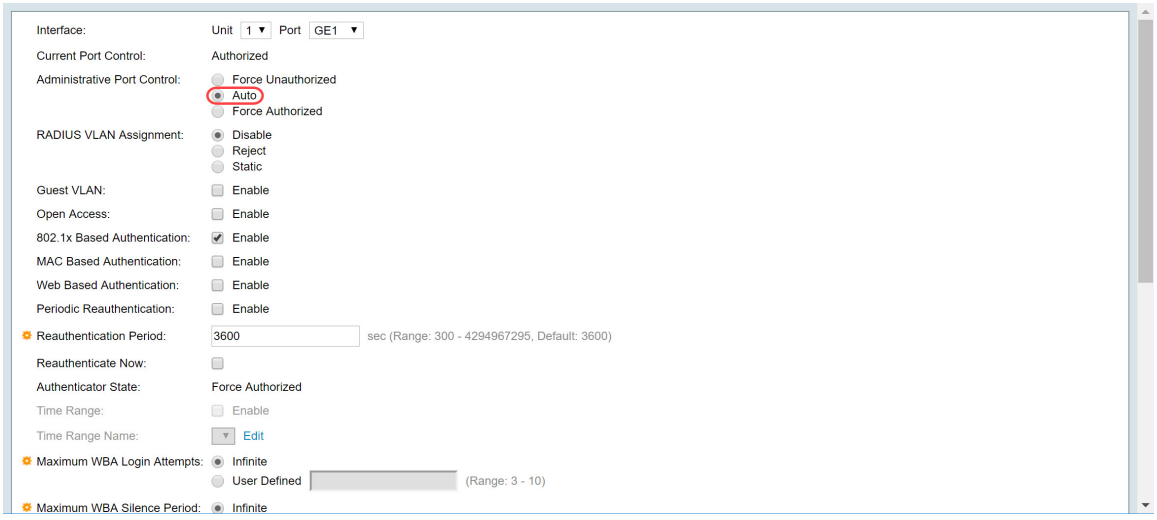


Nella pagina *Modifica autenticazione porta*, il campo *Controllo porta corrente* visualizza lo stato di autorizzazione della porta corrente. Se lo stato è *Authorized*, la porta è autenticata oppure *Administrative Port Control* è *Force Authorized* (Forzatura autorizzata). Al contrario, se lo stato è *Unauthorized* (Non autorizzato), la porta non è autenticata oppure il comando *Administrative Port Control* (Controllo porta amministrativa) è *Force Unauthorized* (Forza non autorizzato). Se supplicant è abilitato su un'interfaccia, il controllo della porta corrente sarà Supplicant.

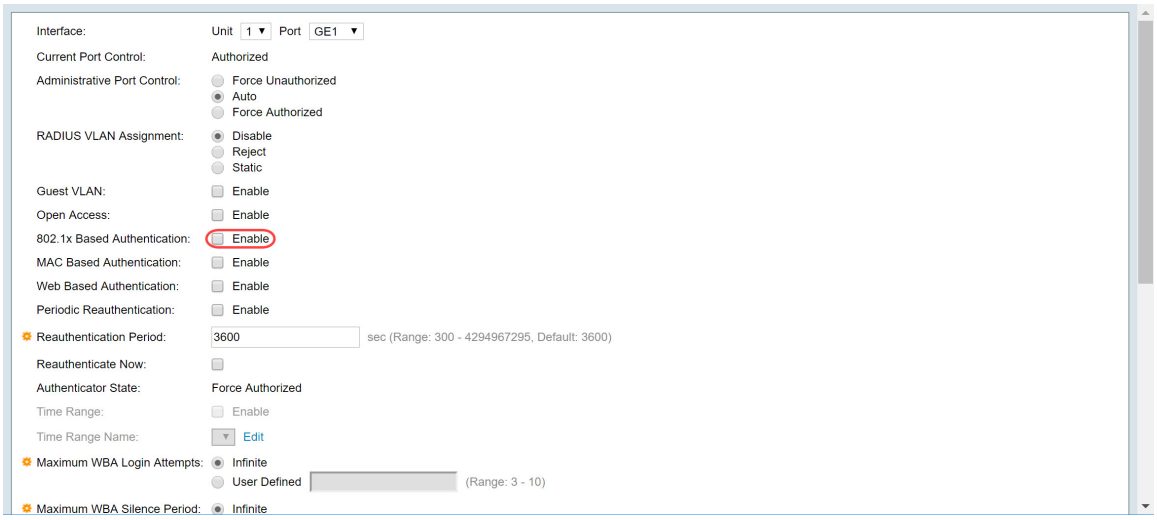
Passaggio 4. Selezionare lo stato di autorizzazione della porta amministrativa. Configurare la porta su **Auto**. Le opzioni disponibili sono:

- Non autorizzato - Nega l'accesso all'interfaccia attivando lo stato non autorizzato dell'interfaccia. Il dispositivo non fornisce servizi di autenticazione al client tramite l'interfaccia.
- Auto — attiva l'autenticazione e l'autorizzazione basate sulle porte sul dispositivo. L'interfaccia si sposta tra uno stato autorizzato e uno non autorizzato in base allo scambio di autenticazione tra il dispositivo e il client.
- Forced Authorized: autorizza l'interfaccia senza autenticazione.

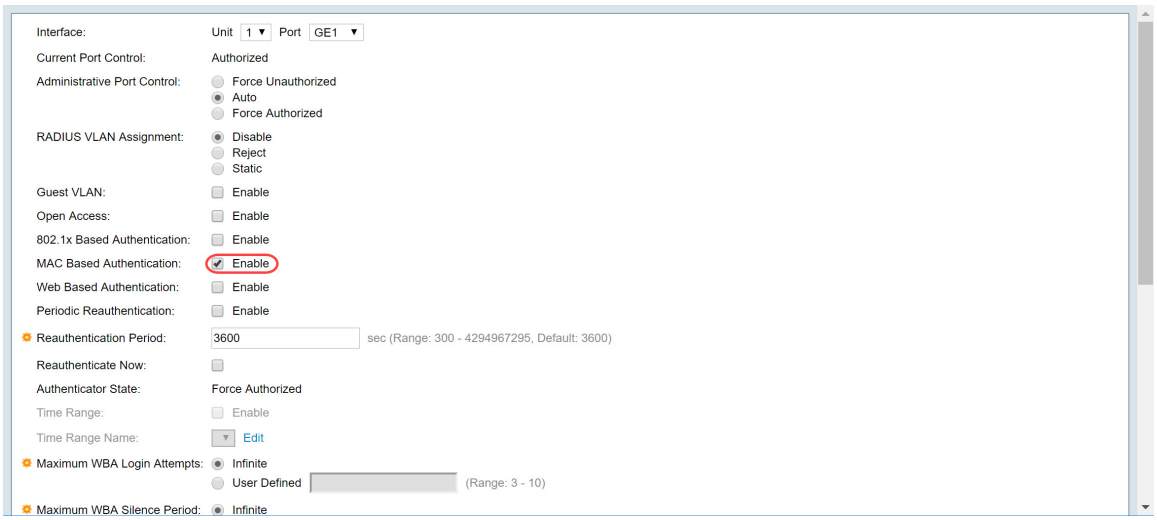
Nota: *Forced Authorized* è il valore predefinito.



Passaggio 5. Nel campo *Autenticazione basata su 802.1X*, deselezionare la casella di controllo **Abilita** in quanto non verrà utilizzato 802.1X come autenticazione. Il valore predefinito dell' *autenticazione basata su 802.1x* è abilitato.



Passaggio 6. Selezionare la casella di controllo **Abilita** autenticazione basata su *MAC* per abilitare l'autenticazione della porta in base all'indirizzo MAC del richiedente. Sulla porta è possibile usare solo 8 autenticazioni basate su MAC.



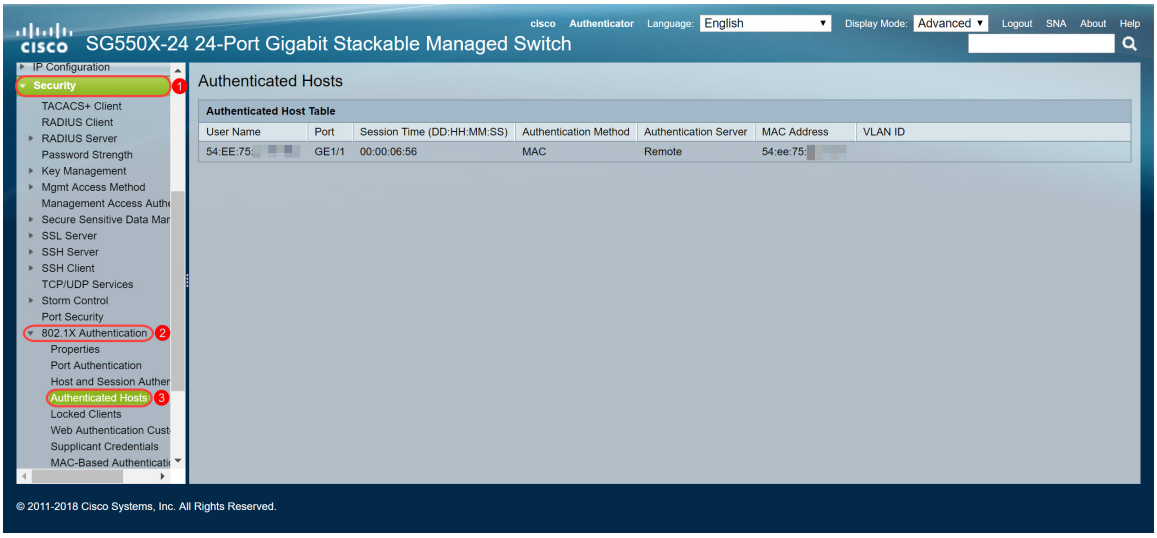
Passaggio 7. Fare clic su **Apply** (Applica) per salvare le modifiche.

Per salvare la configurazione, fare clic sul pulsante **Save** (Salva) nella parte superiore dello schermo.

Conclusioni

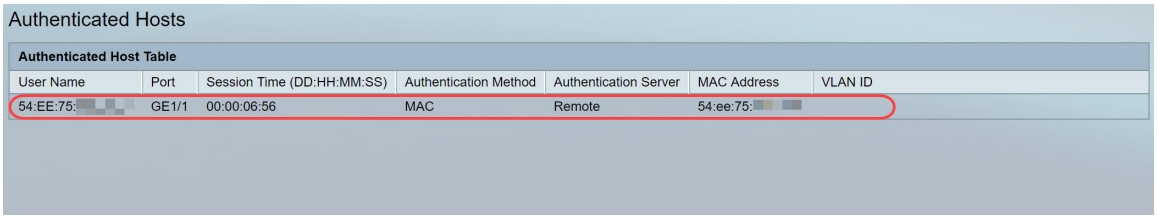
L'autenticazione basata su MAC è stata configurata correttamente sullo switch. Per verificare il funzionamento dell'autenticazione basata su MAC, procedere come segue.

Passaggio 1. Passare a **Sicurezza > Autenticazione 802.1X > Host autenticati** per visualizzare i dettagli sugli utenti autenticati.

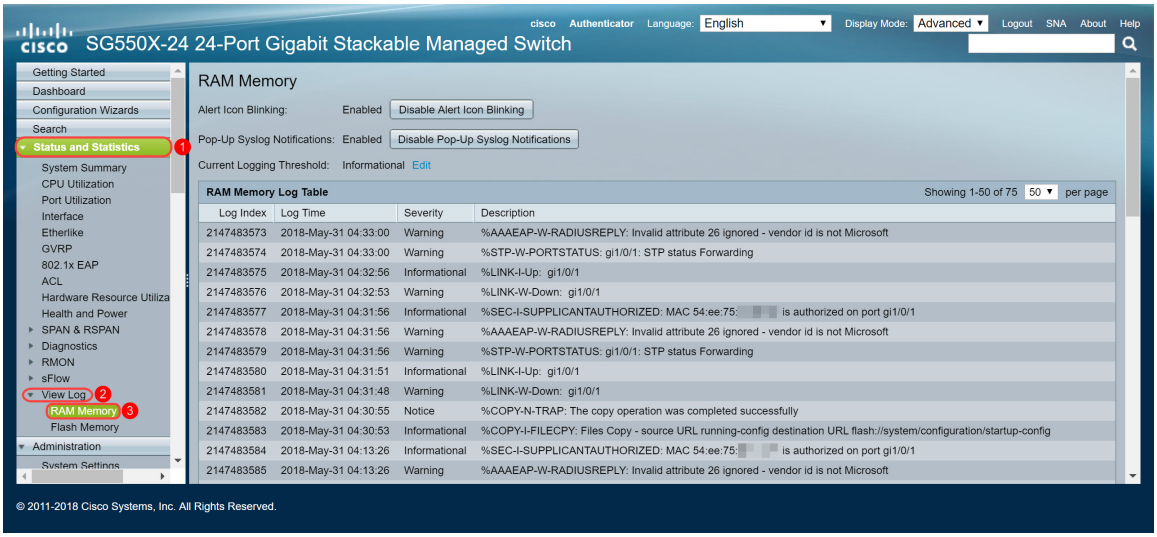


Passaggio 2. In questo esempio, è possibile vedere il nostro indirizzo MAC Ethernet è stato autenticato nella *tabella Authenticated Host*. I campi seguenti definiscono:

- Nome utente — nomi dei supplicant autenticati su ciascuna porta.
- Porta: numero della porta.
- Session Time (DD:HH:MM:SS): quantità di tempo per cui il richiedente è stato autenticato e autorizzato ad accedere alla porta.
- Metodo di autenticazione: il metodo con cui è stata autenticata l'ultima sessione.
- Server autenticato: server RADIUS.
- Indirizzo MAC — visualizza l'indirizzo MAC supplicant.
- ID VLAN: VLAN della porta.



Passaggio 3. (Facoltativo) Passare a **Stato e statistiche > Visualizza log > Memoria RAM**. Nella pagina *Memoria RAM* vengono visualizzati tutti i messaggi salvati nella RAM (cache) in ordine cronologico. Le voci vengono memorizzate nel log RAM in base alla configurazione nella pagina *Log Settings*.



Passaggio 4. Nella *RAM Memory Log Table*, dovrebbe essere visualizzato un messaggio di log informativo che indica che l'indirizzo MAC è autorizzato sulla porta gi1/0/1.

Nota: Parte dell'indirizzo MAC è sfocata.

Visualizza la versione video di questo articolo...

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