Configurazione della modifica delle autorizzazioni in Catalyst 1300 con l'interfaccia utente Web

Obiettivo

In questo articolo viene spiegato come configurare la modifica dell'autorizzazione (CoA) sugli switch Catalyst 1300 con l'interfaccia utente Web.

Dispositivi e versione software interessati

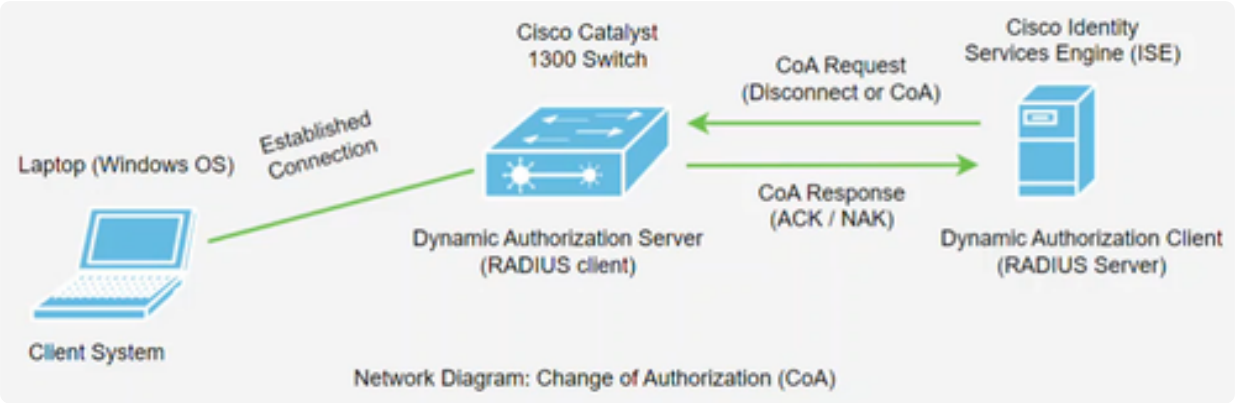
- Catalyst 1300 switch |4.1.6.53

Introduzione

Change of Authorization (CoA) è un'estensione del protocollo RADIUS che consente di modificare le proprietà di un'autenticazione, autorizzazione e accounting (AAA) o di una sessione utente dot1x dopo l'autenticazione. Quando viene modificato un criterio per un utente o un gruppo in AAA, gli amministratori possono trasmettere pacchetti RADIUS CoA dal server AAA, ad esempio Cisco Identity Services Engine (ISE), per reinizializzare l'autenticazione e applicare il nuovo criterio.

Cisco Identity Services Engine (o ISE) è un motore di controllo dell'accesso e applicazione delle policy basato sulla rete completo di tutte le funzionalità. Fornisce analisi e applicazione della sicurezza, servizi RADIUS e TACACS, distribuzione delle policy e altro ancora. Cisco ISE è attualmente l'unico client di autorizzazione dinamica CoA supportato per gli switch Catalyst 1300. Per ulteriori informazioni, consultare la guida per l'amministratore di ISE.

Questa funzionalità richiede la comunicazione tra il client di autorizzazione dinamica (server RADIUS) e il server di autorizzazione dinamica (switch Catalyst). Come illustrato nel diagramma di rete riportato di seguito, il server di autorizzazione dinamica invia un messaggio di disconnessione o CoA al server di autorizzazione dinamica e lo switch fornisce una risposta.



Network Diagram: Change of Authorization (CoA)

Il supporto CoA è stato aggiunto agli switch Catalyst 1300 nella versione firmware 4.1.3.36. Include il supporto per la disconnessione degli utenti e la modifica delle autorizzazioni applicabili a una sessione utente. Il dispositivo supporta le seguenti azioni CoA:

- Disconnetti sessione
- Disabilita comando CoA porta host
- Comando CoA della porta host di rimbalzo
- Riautentica comando CoA host

Per configurare la CLI con l'interfaccia della riga di comando (CLI), consultare il documento sulla configurazione della modifica dell'autorizzazione nello switch Catalyst 1300 con CLI.

Sommario

- Configurazione del client Catalyst 1300 RADIUS su ISE
- Configurazioni in Catalyst 1300 Switch
- CoA

Configurazione del client Catalyst 1300 RADIUS su ISE

Nell'esempio, viene usato Cisco ISE server versione 3.2. Per una panoramica su ISE, vedere la pagina dei prodotti Cisco Identity Services Engine.

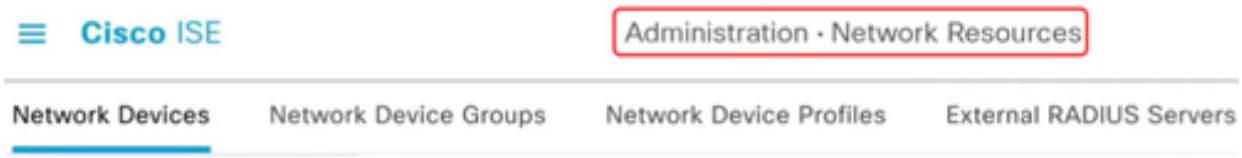
> **Note:**
> CoA è supportato su ISE versione 2.7 e successive.

Dopo aver distribuito il server Cisco ISE, accedere per accedere all'interfaccia utente

Web.

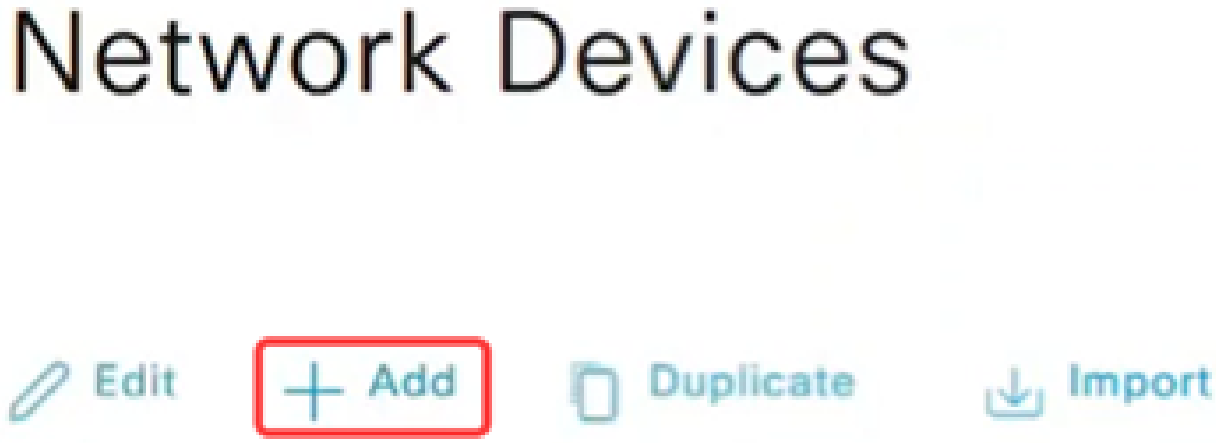
Passaggio 1

Per aggiungere dispositivi di rete, passare al menu Amministrazione > Risorse di rete.



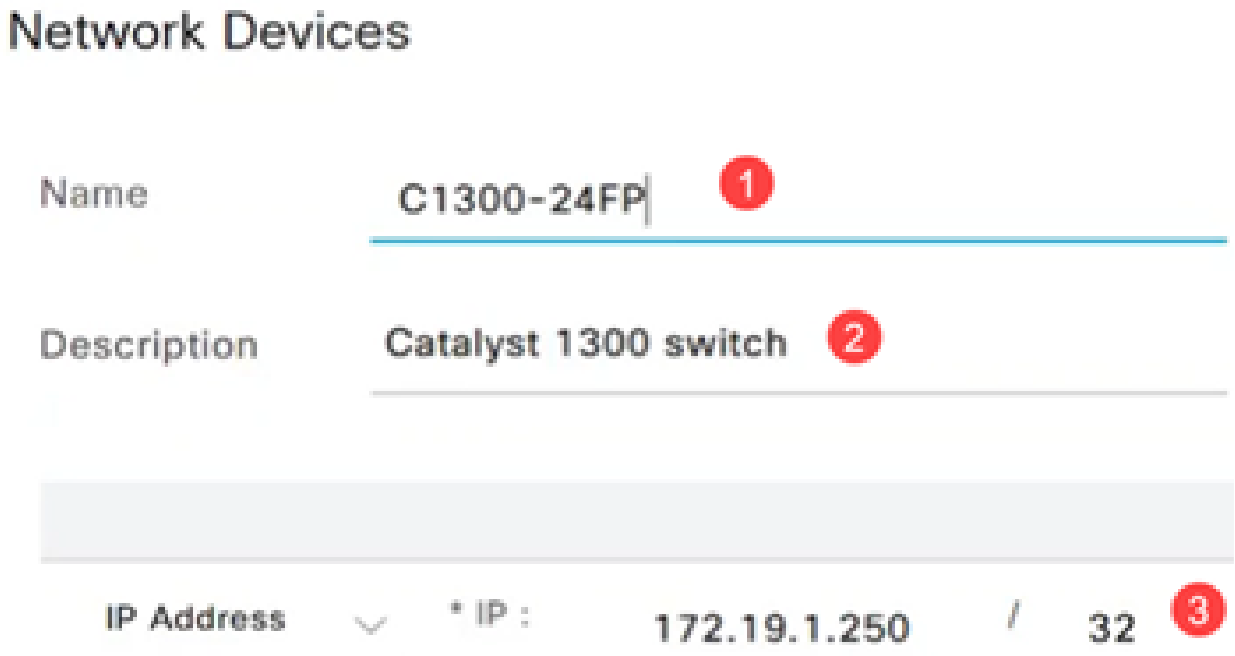
Passaggio 2

Fare clic sul pulsante + Aggiungi.



Passaggio 3

Immettere il nome, la descrizione e l'indirizzo IP dello switch Catalyst.

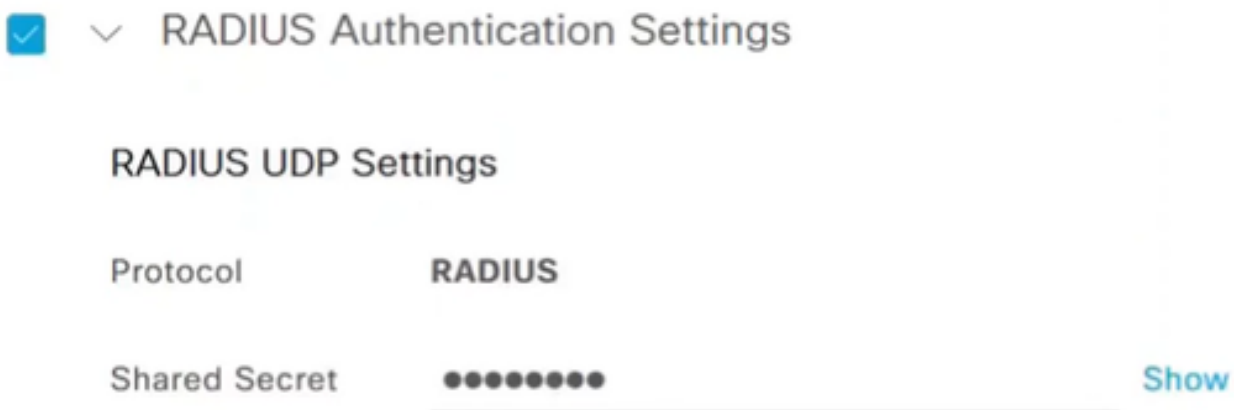


Passaggio 4

Dal menu a discesa Device Profile, selezionare Cisco.

Passaggio 5

Configurare le impostazioni di autenticazione RADIUS immettendo il segreto condiviso.



Passaggio 6

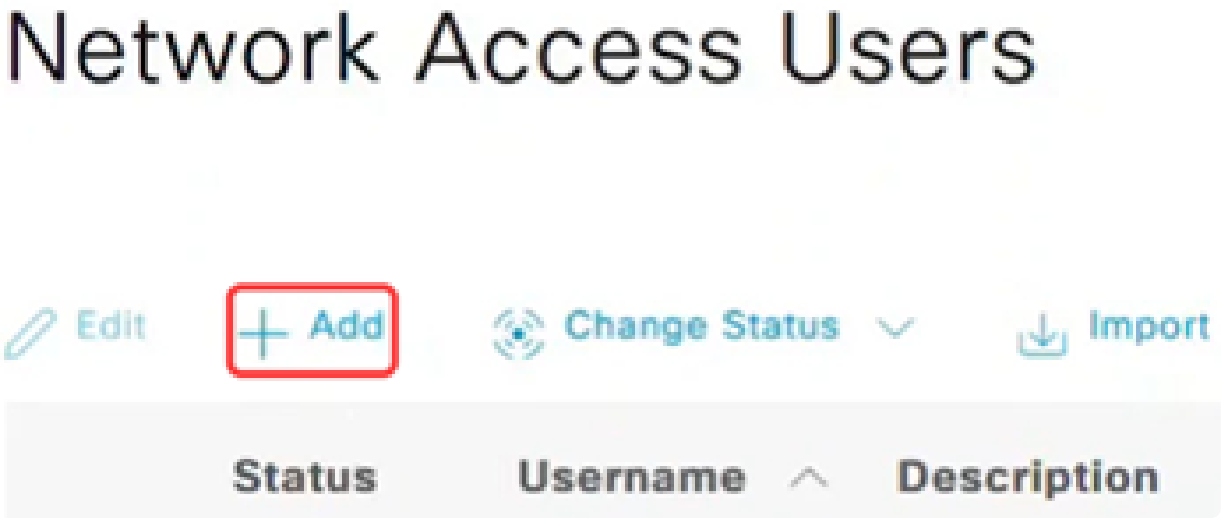
Immettere il numero della porta CoA. La porta predefinita è 1700.

Passaggio 7

Passare quindi a Amministrazione > Gestione delle identità e selezionare Utenti accesso alla rete.

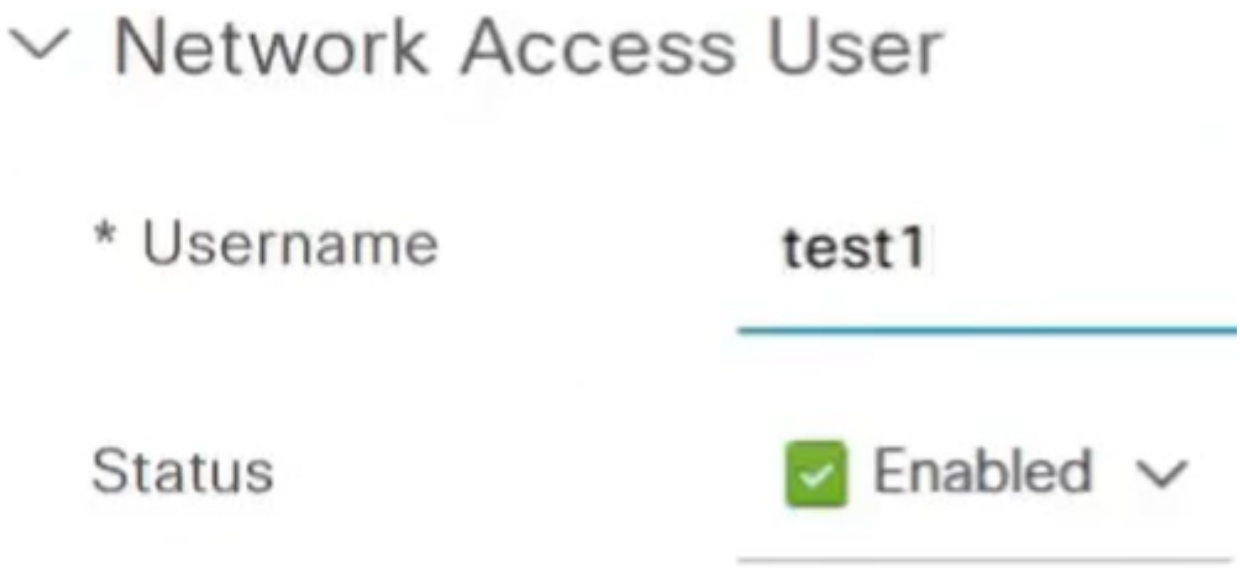
Passaggio 8

Per definire il nome utente e la password, fare clic sul simbolo +Add.



Passaggio 9

Immettere il nome utente e la password e fare clic su Salva nella parte inferiore della pagina.



Configurazioni in Catalyst 1300 Switch

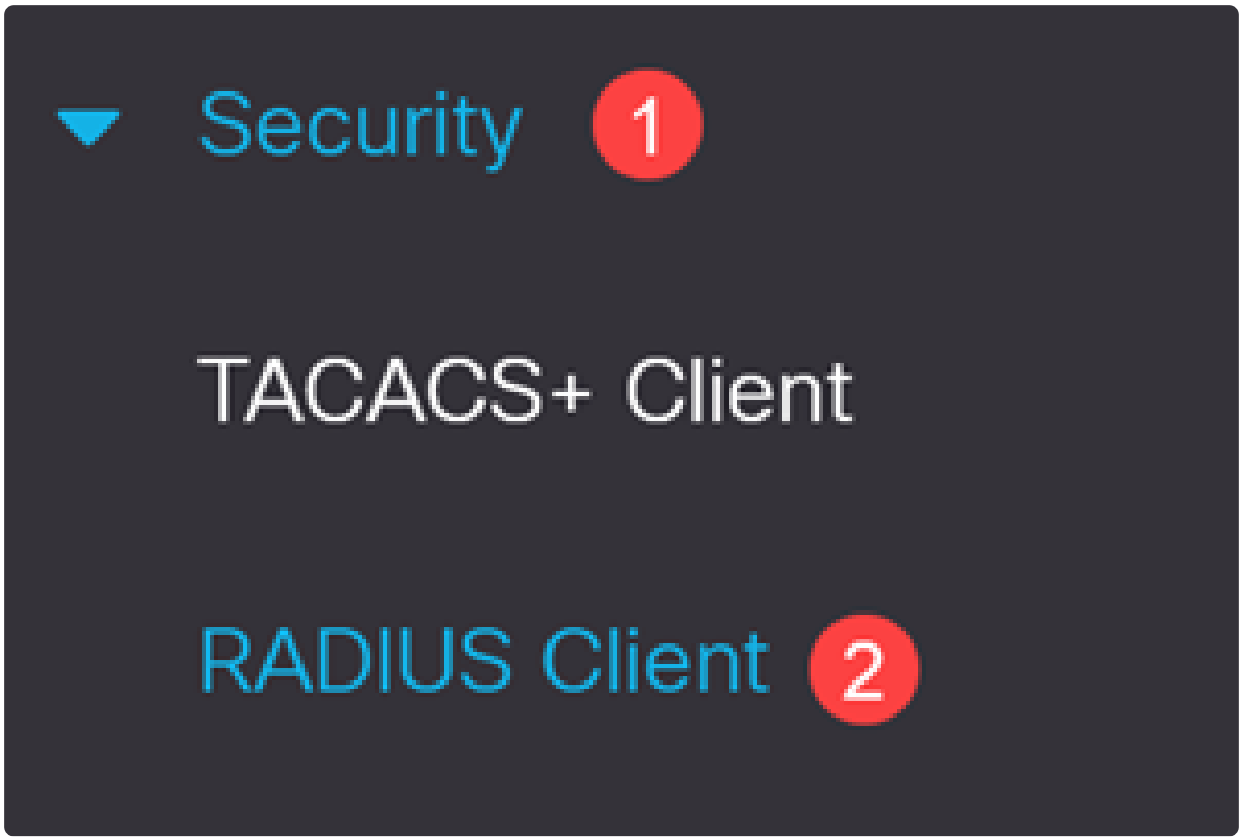
Passaggio 1

Accedere allo switch Catalyst 1300 e selezionare la modalità avanzata. Nell'esempio viene utilizzato il C1300-24FP-4X.

> Note:
> Il supporto CoA è stato aggiunto agli switch Catalyst 1300 nella versione firmware 4.1.3.36.

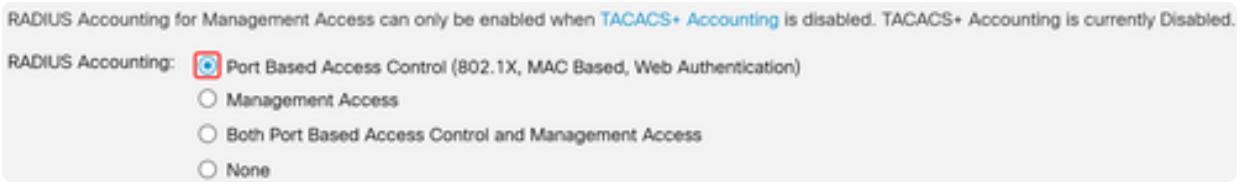
Passaggio 2

Passare a Protezione > Client RADIUS nel riquadro di navigazione.



Passaggio 3

Impostare Accounting RADIUS su Controllo degli accessi basato sulle porte.



Passaggio 4

Per aggiungere il server ISE, scorrere verso il basso fino alla tabella RADIUS e fare clic sull'icona più.

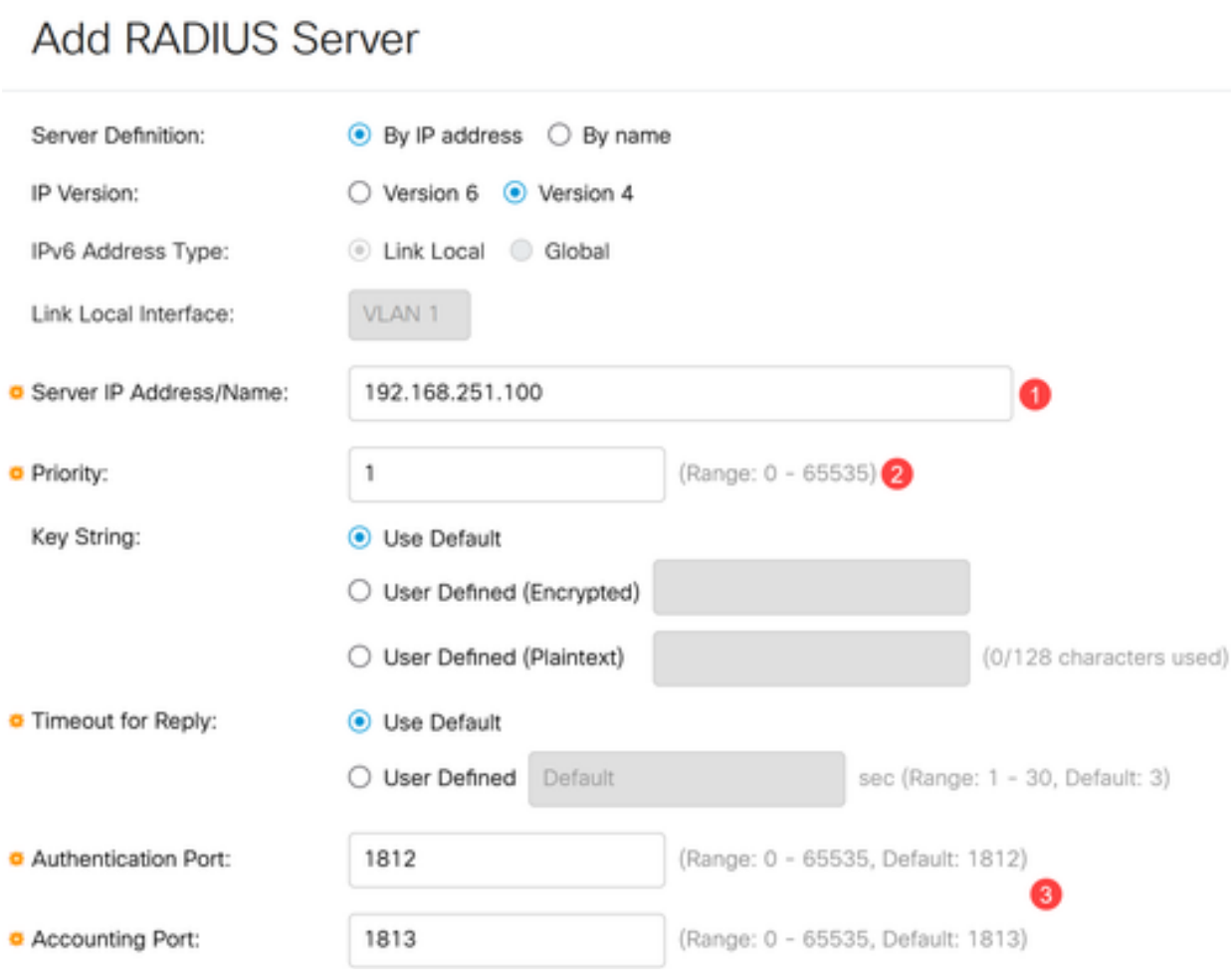
Passaggio 5

Configurare le impostazioni del server RADIUS.

- Selezionare Definizione server. Nell'esempio, è selezionato By IP address. Immettere l'indirizzo IP nel campo Server IP Address/Name (Indirizzo IP/Nome server).
- Impostate una priorità RADIUS.

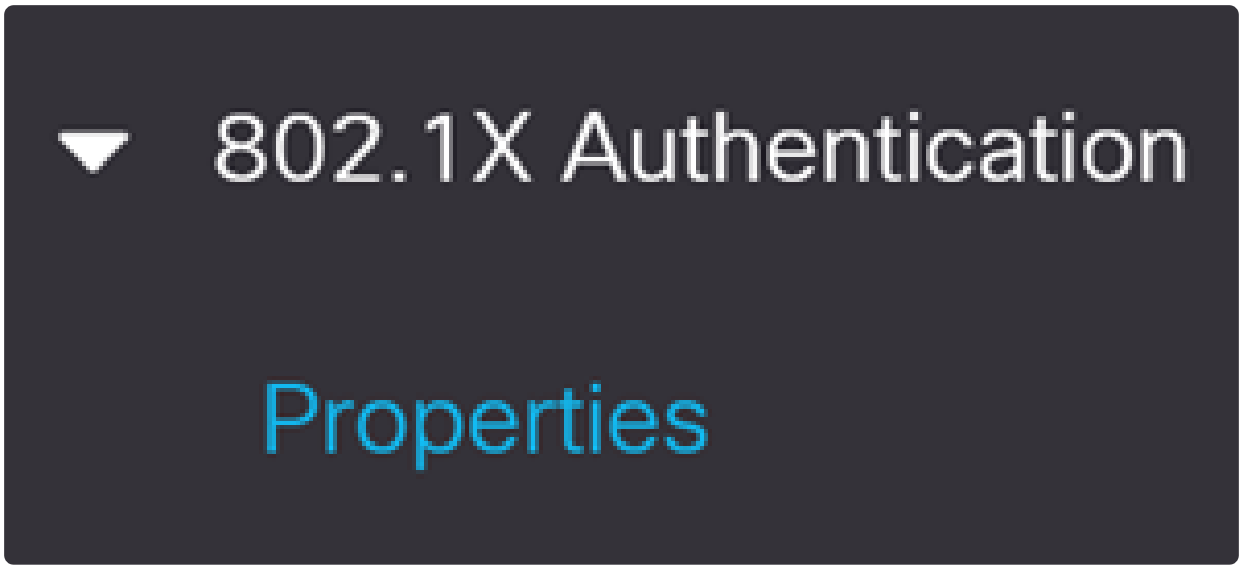
- Le porte di autenticazione e accounting sono impostate sul valore predefinito.
- Il tipo di utilizzo è 802.1x.

Fare clic su Apply (Applica).



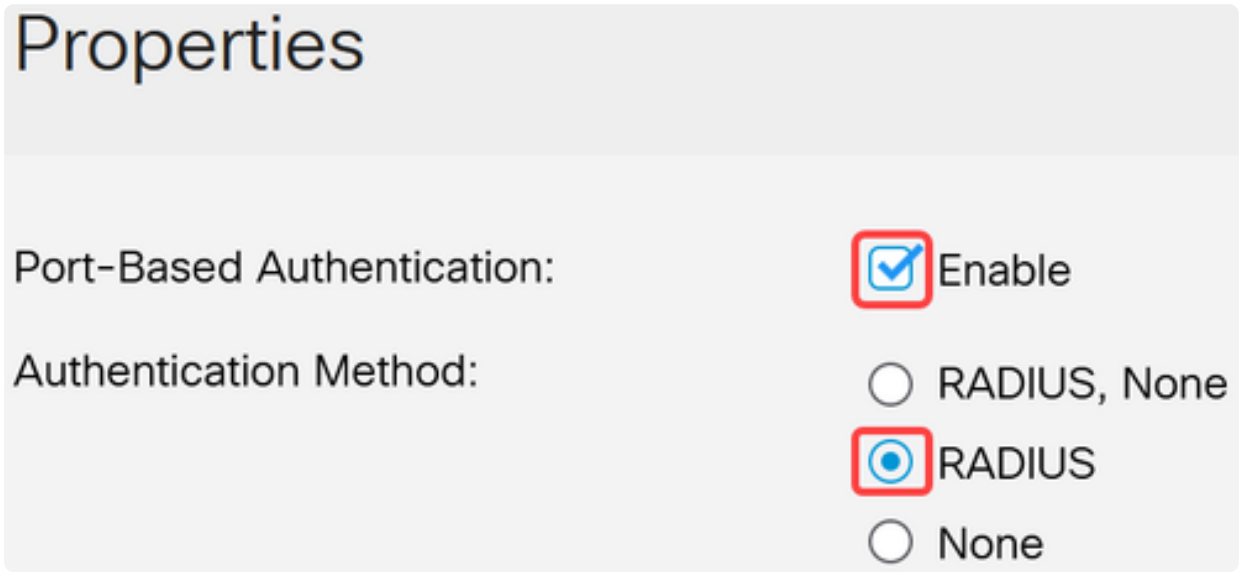
Passaggio 6

Per configurare l'autenticazione 802.1x, passare al menu Protezione > Autenticazione 802.1X >Proprietà.



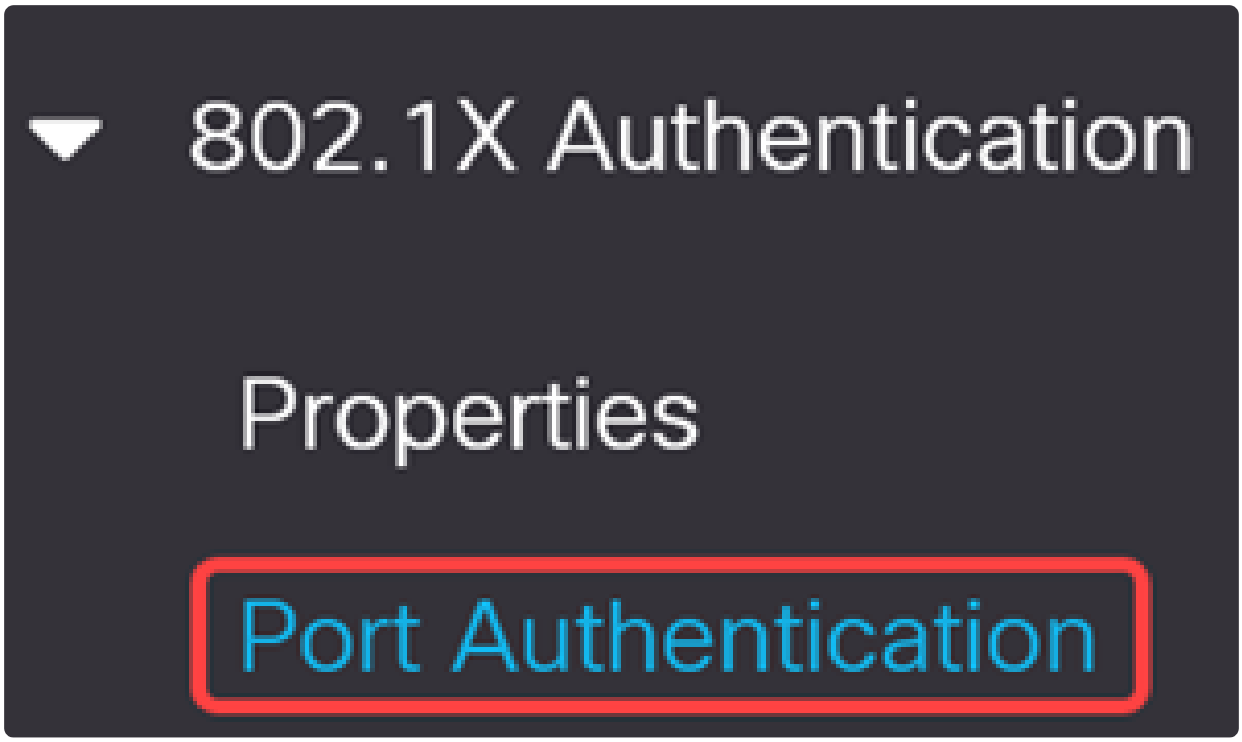
Passaggio 7

Verificare che l'autenticazione basata sulla porta sia abilitata e che il metodo di autenticazione sia impostato su RADIUS.



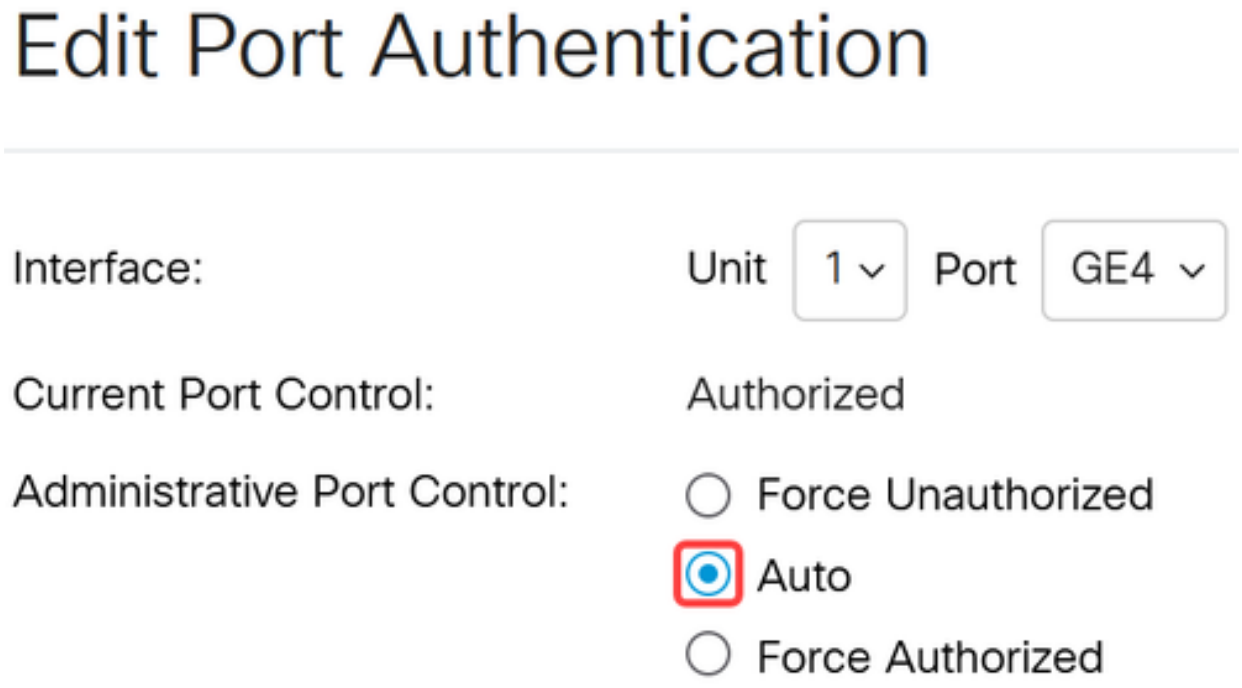
Passaggio 8

Passare al menu Port Authentication (Autenticazione porta), selezionare la porta desiderata e fare clic su edit (Modifica).



Passaggio 9

Per Controllo porta amministrativa, selezionare l'opzione Auto per commutare la porta tra stato autorizzato e non autorizzato in base alla risposta RADIUS.

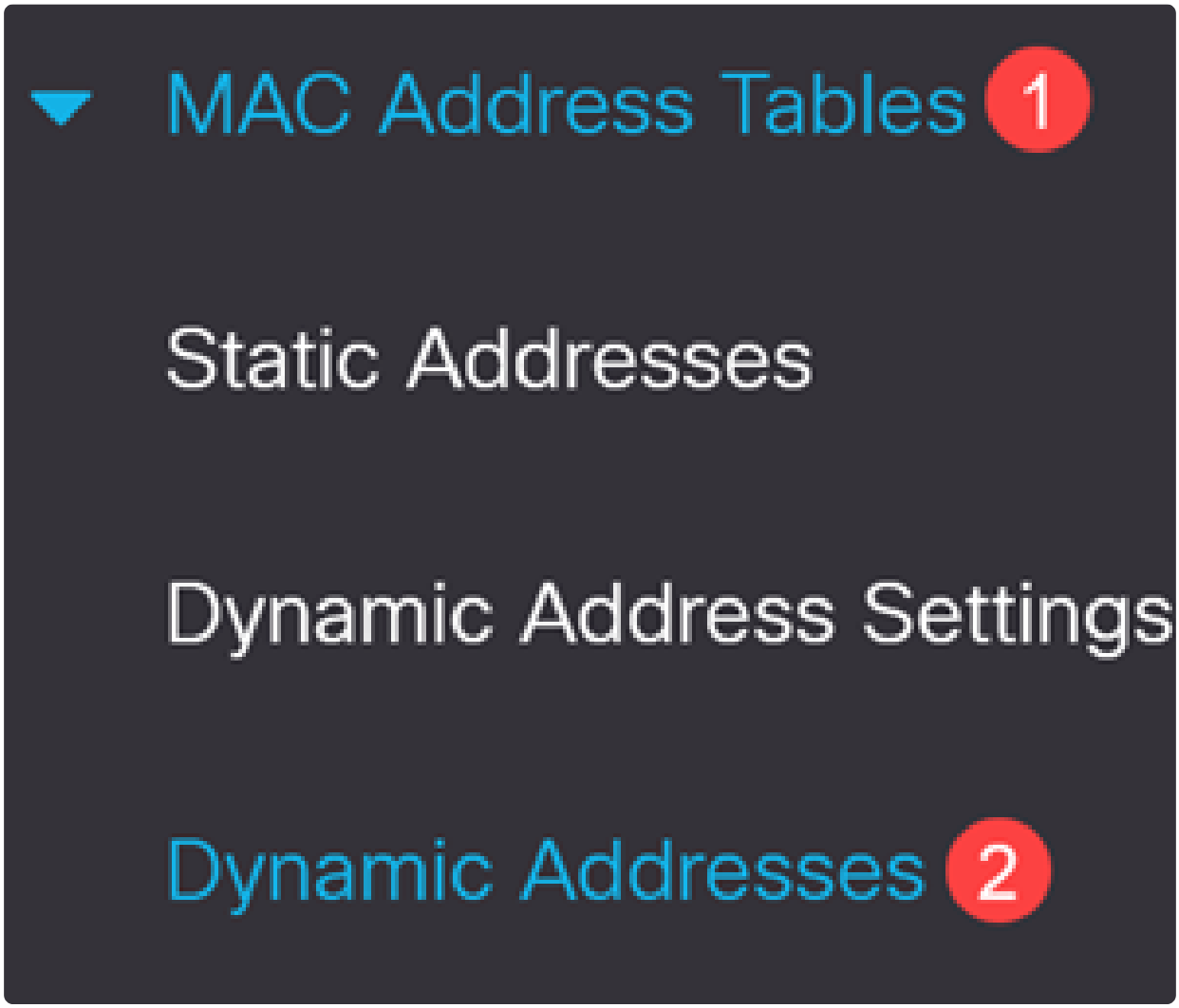


Passaggio 10

Abilitare l'autenticazione basata su 802.1x e fare clic su Applica.

Passaggio 11

È necessario l'indirizzo MAC del dispositivo sulla porta. La cooperazione su ISE sarà applicata a quell'indirizzo MAC. In questo esempio, la porta è 9. Per ottenerla, selezionare Tabelle indirizzi MAC > Indirizzi dinamici.

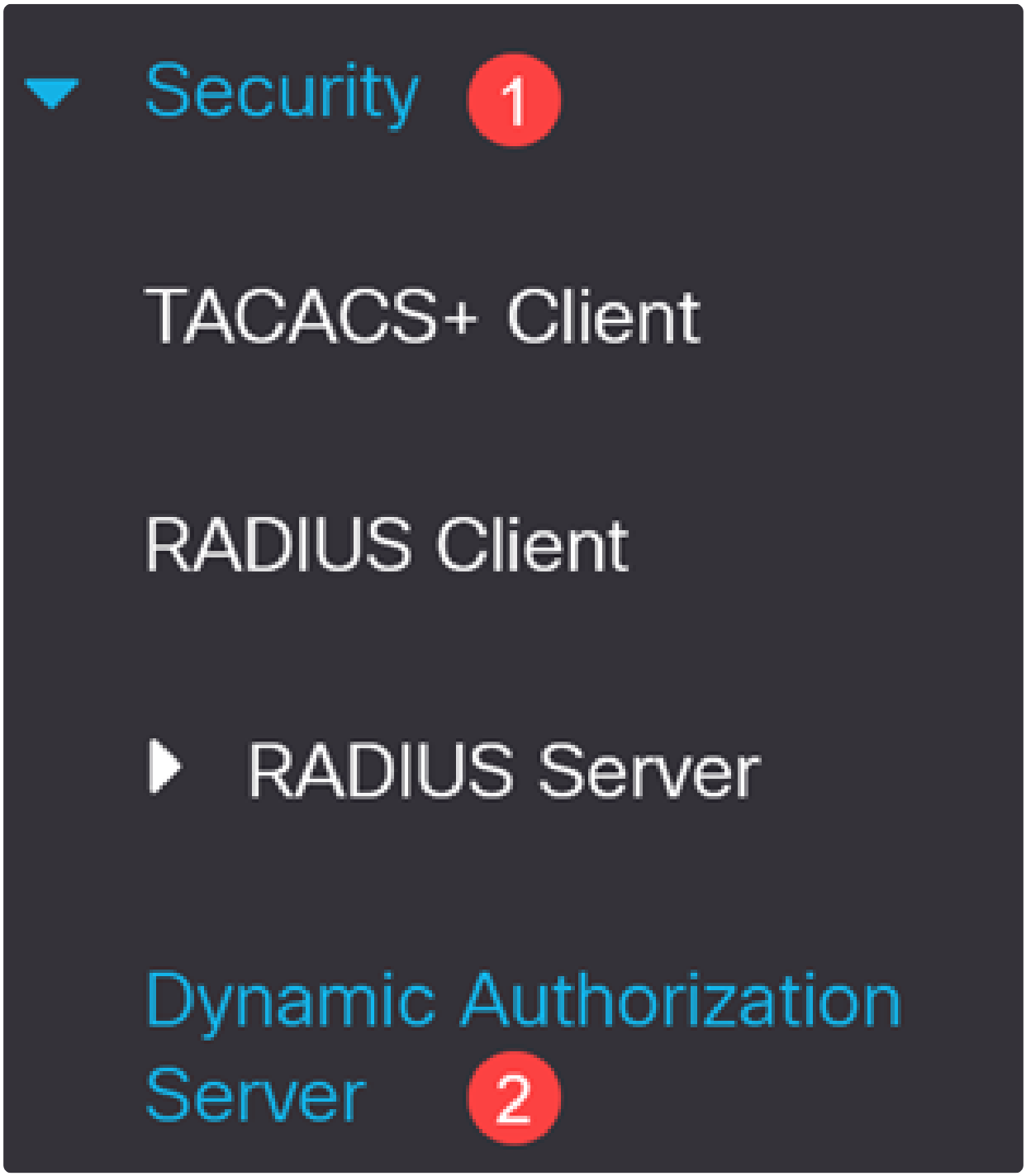


Passaggio 12

Scorrere fino alla porta e annotare l'indirizzo MAC.

Passaggio 13

Passare a Sicurezza > Server di autorizzazione dinamica.

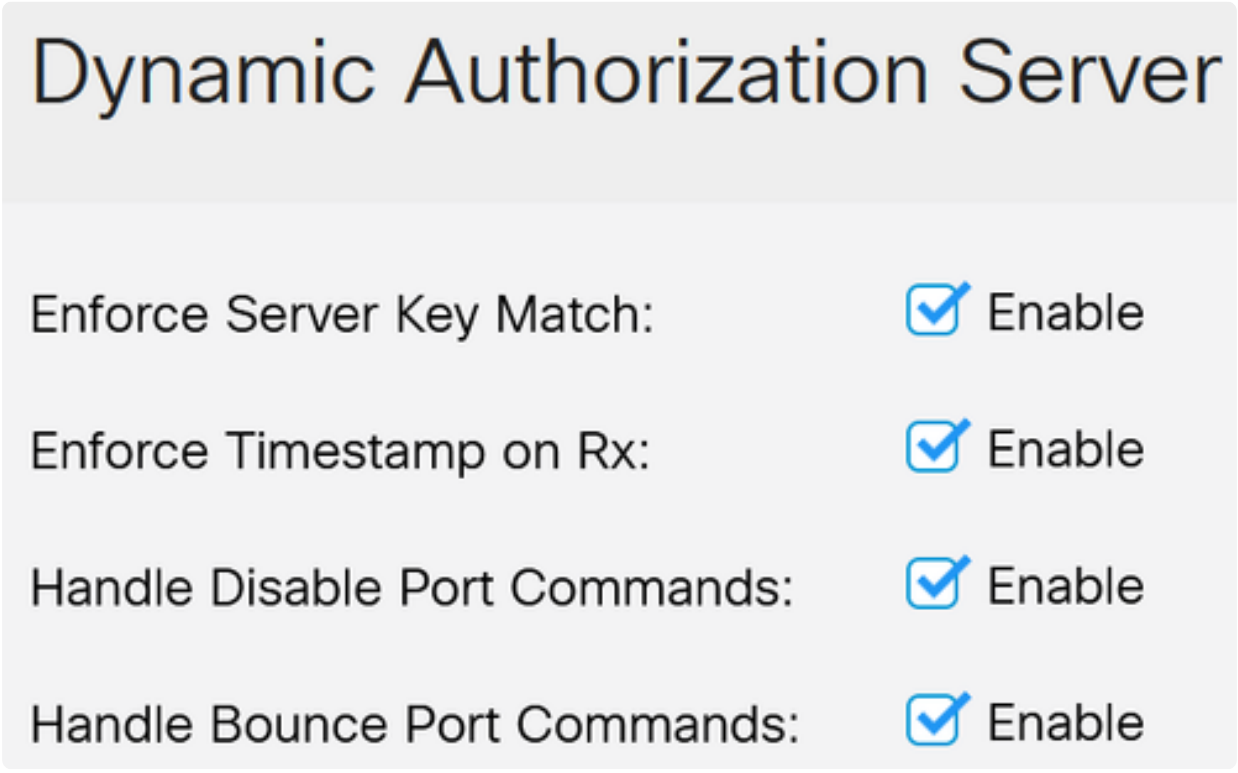


Passaggio 14

Abilitare quanto segue:

- Imponi corrispondenza chiave server

- Imponi timestamp su Rx
- Gestisci Comandi Porta Disabilita
- Gestisci comandi porta di rimbalzo

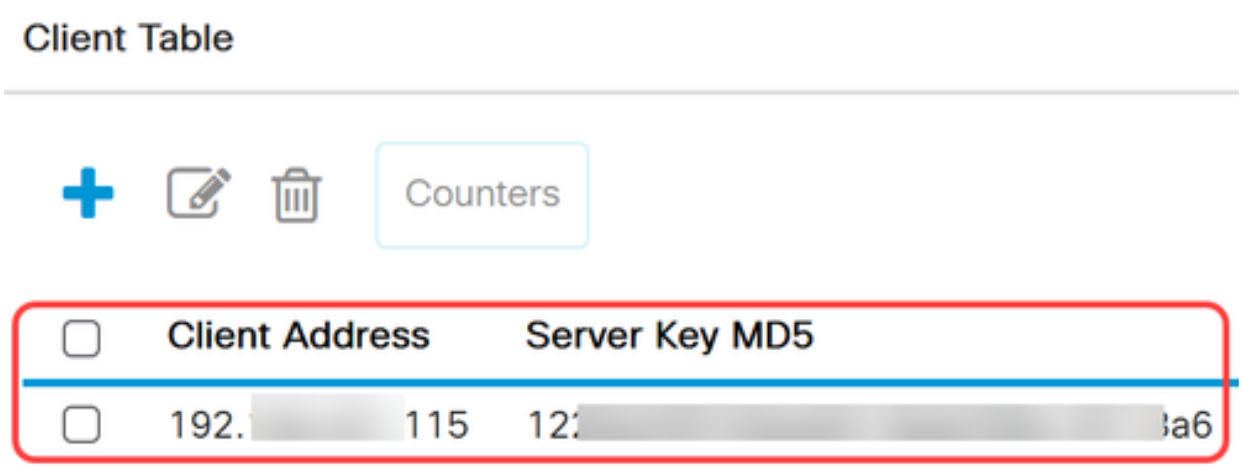


Passaggio 15

Lasciare la porta UDP sul valore predefinito di 1700.

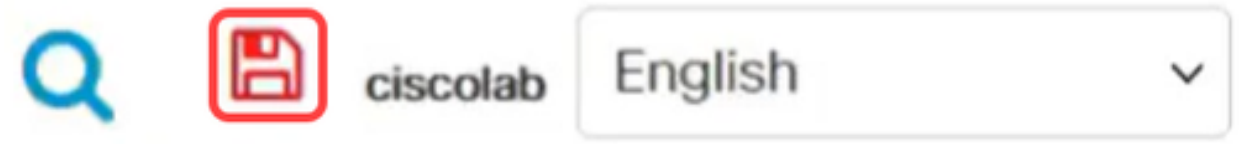
Passaggio 16

In Tabella client, verificare che il server ISE sia stato aggiunto con la chiave corretta del server. Fare clic su Apply (Applica).



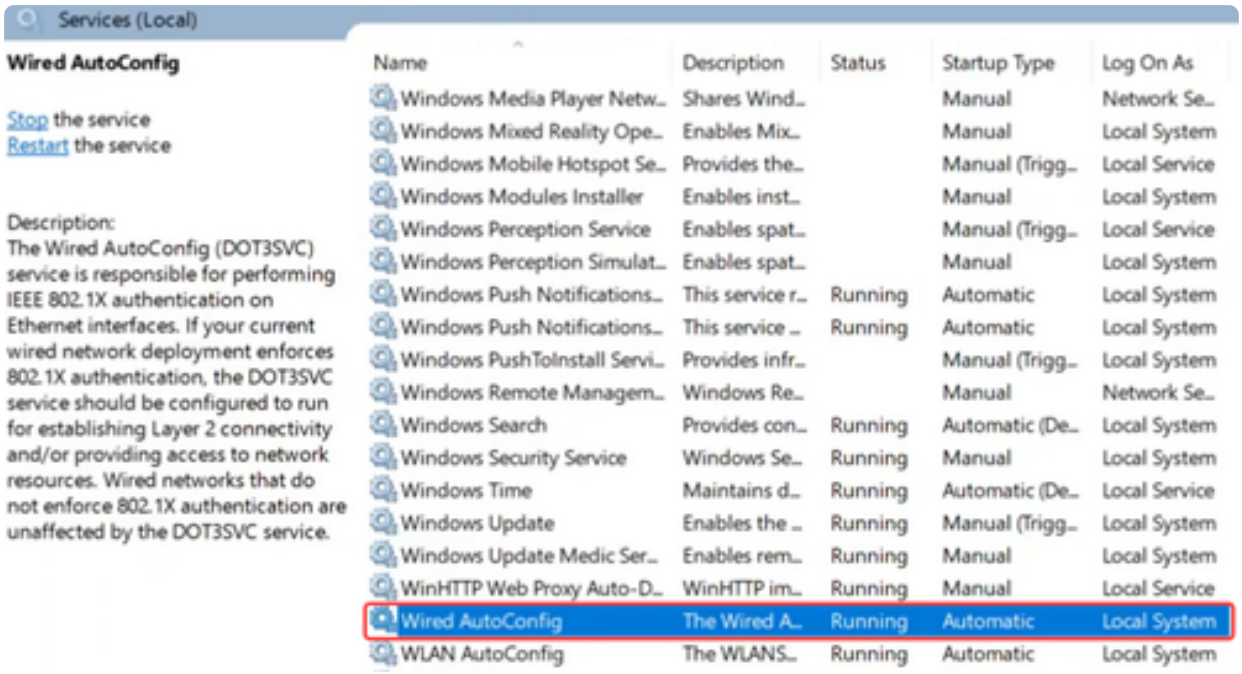
Passaggio 17

Fare clic sull'icona rossa lampeggiante Save per salvare le configurazioni.



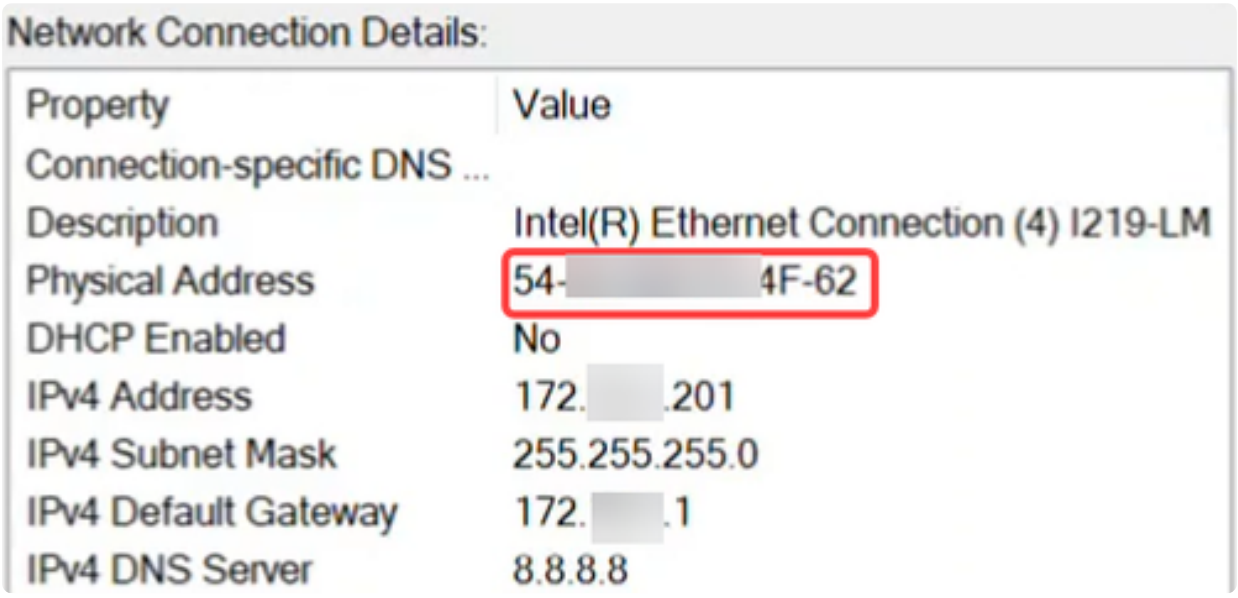
Passaggio 18

Sul laptop client collegato alla porta 9, verificare che il servizio Wired AutoConfig sia abilitato per l'autenticazione 802.1 X.



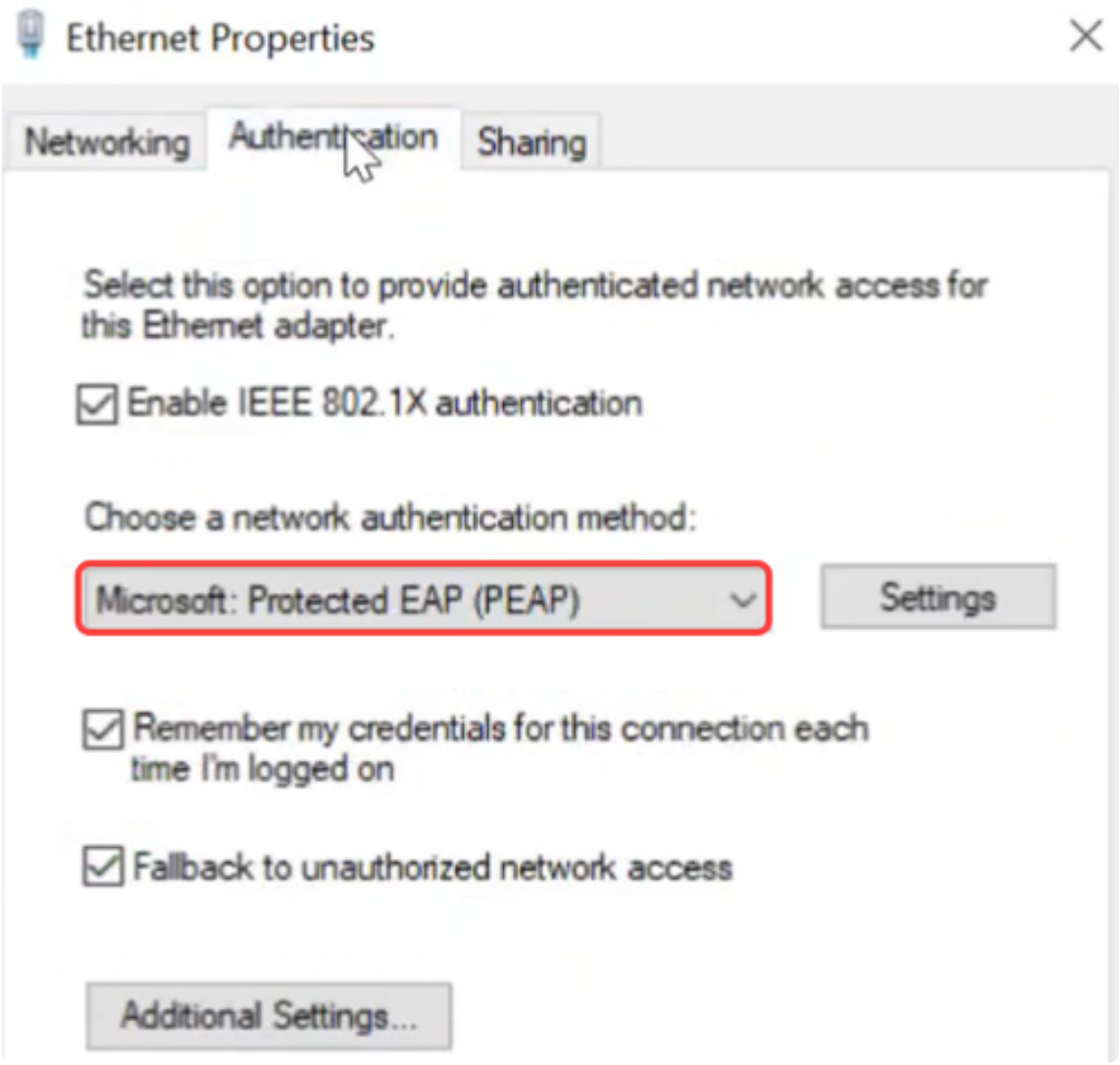
Passaggio 19

Verificare che l'indirizzo MAC corrisponda alle impostazioni della scheda di rete Ethernet.



Passaggio 20

Fare clic sul pulsante Proprietà in Impostazioni Ethernet e nella scheda Autenticazione verificare che le caselle di controllo siano attivate. Verificare inoltre che il metodo di autenticazione sia PEAP (Protected EAP).



Passaggio 21

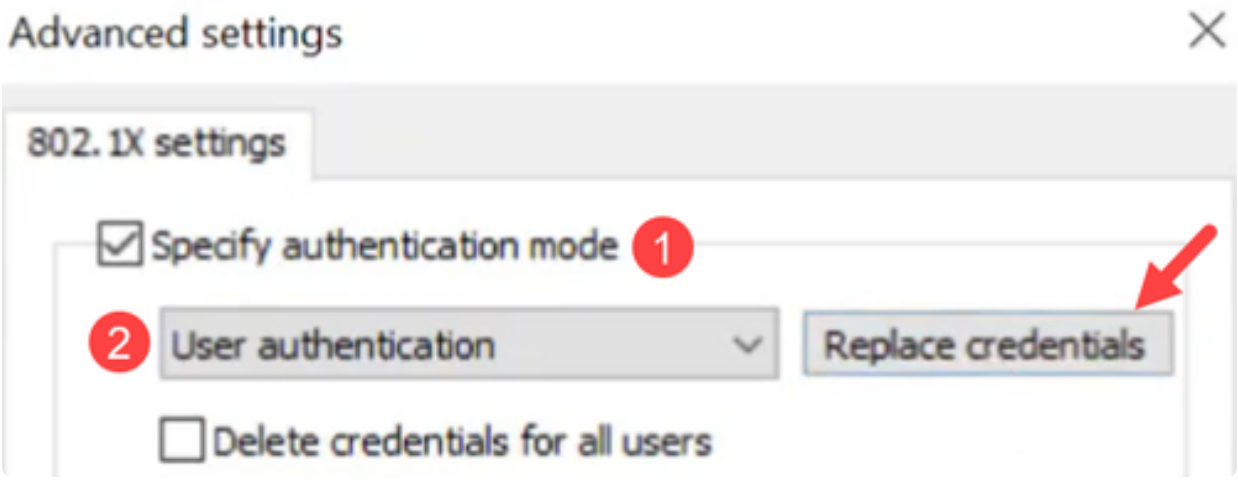
Fare clic sul pulsante Impostazioni per verificare che la casella di controllo accanto a Verifica dell'identità del server tramite la convalida del certificato sia deselezionata.

Passaggio 22

Selezionare la casella di controllo Abilita riconnessione rapida.

Passaggio 23

In Impostazioni aggiuntive verificare che Specifica modalità di autenticazione sia attivato e che Autenticazione utente sia selezionato dal menu a discesa. È possibile salvare le credenziali create su ISE o sostituirle utilizzando il pulsante Sostituisci credenziali.



CoA

Prima di avviare l'operazione CoA, abilitare l'acquisizione dei pacchetti sullo switch.

Passaggio 1

Su PuTTy, accedere allo switch Catalyst e specificare le dimensioni del buffer e la modalità di acquisizione usando il comando monitor capture cap1 buffer size 20 circle.

Passaggio 2

Specificare il piano di controllo come entrambi utilizzando il comando monitor capture cap1 control-plane both.

Passaggio 3

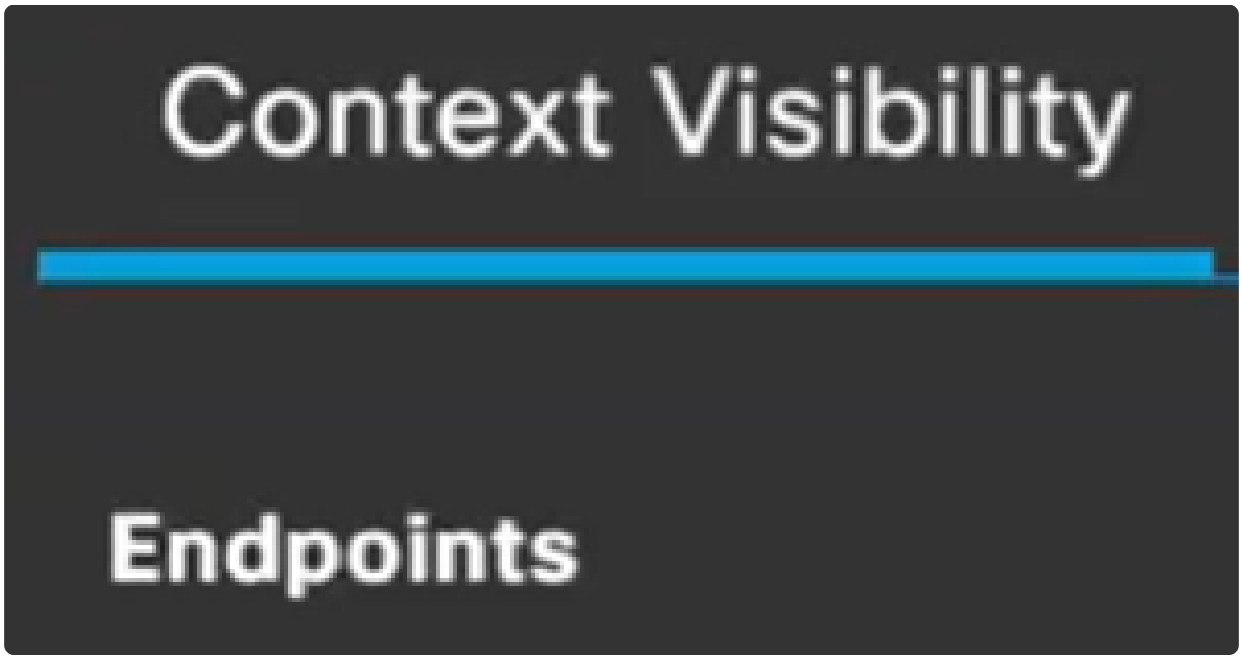
Inserire i criteri di corrispondenza come qualsiasi. Il comando per questa operazione sarà monitor capture cap1 match any.

Passaggio 4

Avviare l'acquisizione dei pacchetti.

Passaggio 5

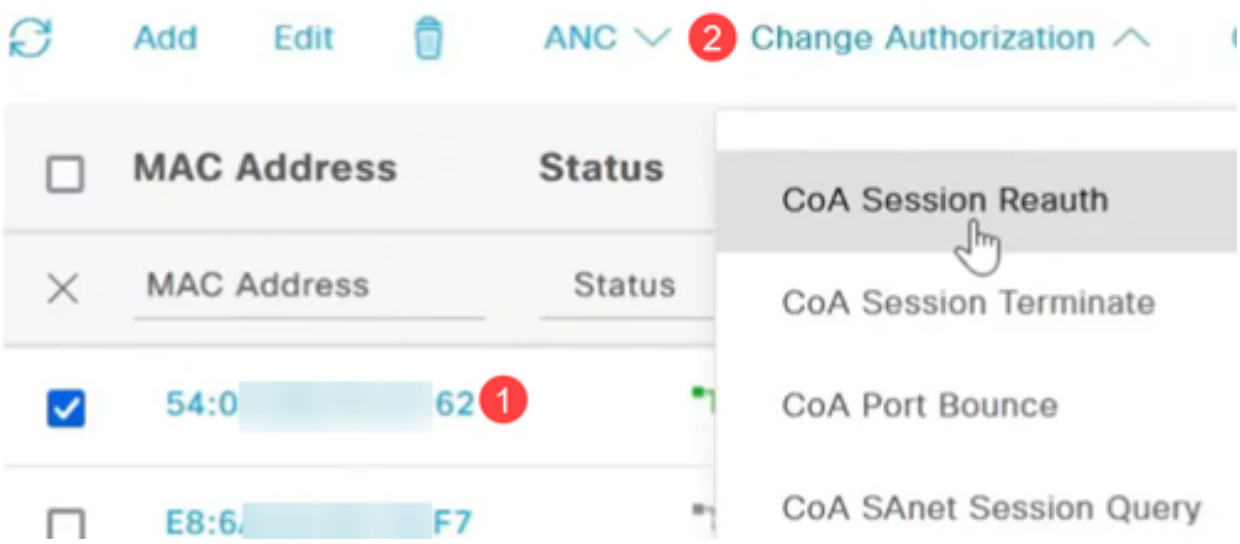
Sull'interfaccia ISE, selezionare l'opzione Endpoints in Context Visibility.



Passaggio 6

Scegliere l'indirizzo MAC e selezionare l'operazione CoA dal menu a discesa Modifica autorizzazione. Nell'esempio, è selezionata l'opzione CoA Session Reauth. In questo modo viene forzata la riautenticazione sulla porta tramite l'invio di un pacchetto CoA

con un comando reauthentication.



Passaggio 7

Tornare al terminale PuTTY per verificare se l'operazione CoA ha avuto esito positivo.

```
Started capture point : capl
Cat1300-1#04-Jul-2024 20:49:45 %SEC-W-COAREAUTHSESSN: 802.1x re-authentication initiated for host 5
4:  62 by CoA Request "reauthenticate"
```

Passaggio 8

Se si seleziona Termina sessione CoA, viene inviata una richiesta di disconnessione con un comando di terminazione basato su una richiesta amministrativa.

```
Cat1300-1#04-Jul-2024 20:50:02 %SEC-W-PORTUNAUTHORIZED: Port gil/0/9 is unAuthorized
04-Jul-2024 20:50:02 %SEC-W-COADISCSESSN: 802.1x session for host 54:  :62 on interface gi
1/0/9 has been terminated by Disconnect-Request. Authenticator state on the Interface will be re-in
itialized
04-Jul-2024 20:50:02 %SEC-I-PORTAUTHORIZED: Port gil/0/9 is Authorized
```

Passaggio 9

L'opzione CoA Port Bounce invia un pacchetto di richiesta CoA con un comando bounce host port, disabilitando e riabilitando la porta sullo switch. La scheda di rete rimane offline per 10 secondi e diventa non autorizzata. Il ritorno online, l'autorizzazione e l'inoltro dei pacchetti.

```
Cat1300-1#04-Jul-2024 20:50:21 %SEC-W-COABNCEPORT: Interface gi1/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54:          :62
04-Jul-2024 20:50:21 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:50:34 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:50:34 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:50:36 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:50:39 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:50:39 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized

Cat1300-1#04-Jul-2024 20:50:45 %STP-W-PORTSTATUS: gi1/0/9: STP status Forwarding
```

Passaggio 10

La terminazione di una sessione CoA con il rimbalzo della porta terminerà la sessione esistente, farà rimbalzare la porta per 10 secondi e non sarà più autorizzata. Torna online, viene autorizzato e può inoltrare i pacchetti.

```
Cat1300-1#04-Jul-2024 20:51:04 %SEC-W-COABNCEPORT: Interface gi1/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54:          :62
04-Jul-2024 20:51:04 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:51:22 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:51:22 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:51:22 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized
04-Jul-2024 20:51:29 %STP-W-PORTSTATUS: gi1/0/9: STP status Forwarding
```

Passaggio 11

La chiusura della sessione CoA con la chiusura della porta terminerà la sessione e la porta verrà chiusa a livello amministrativo.

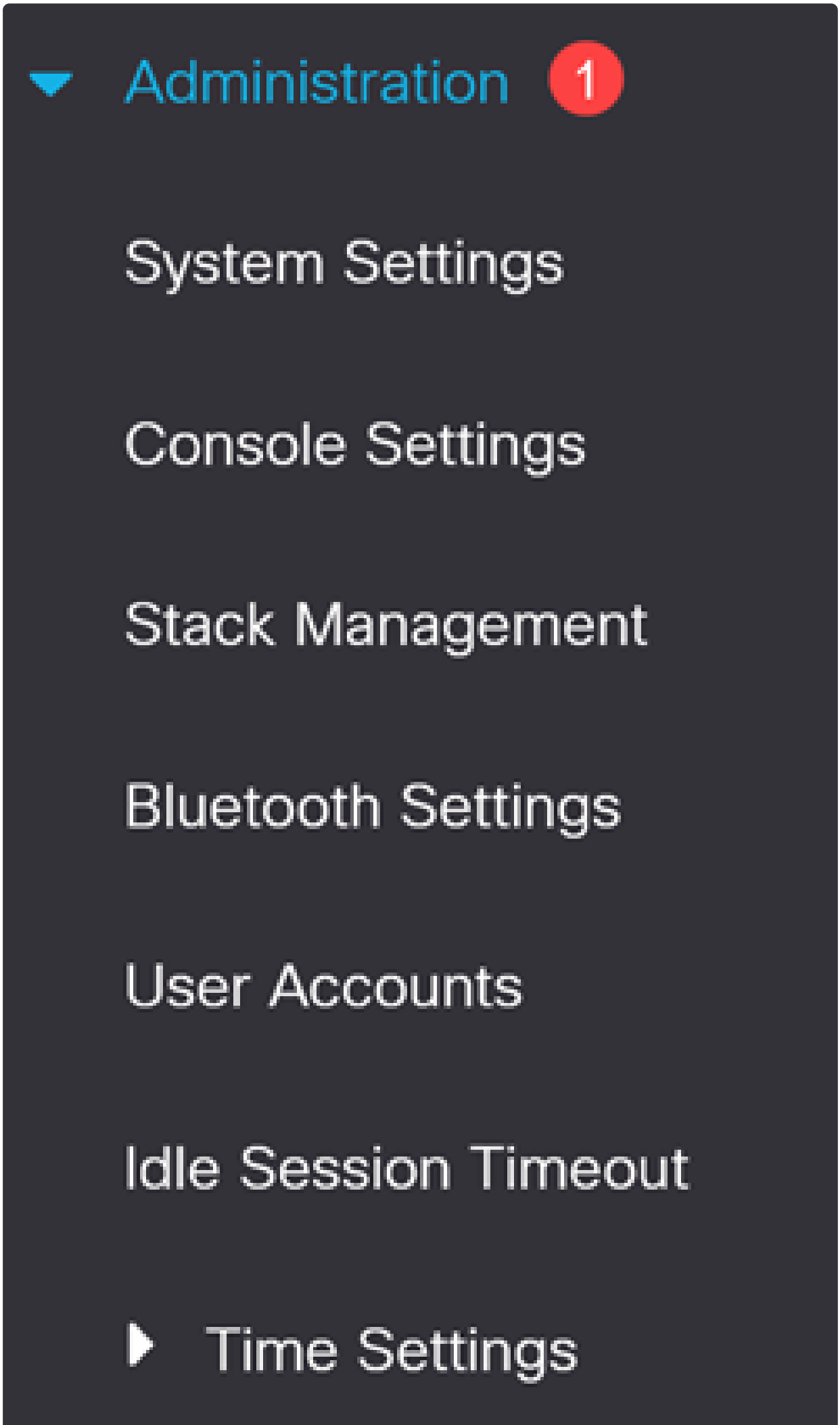
```
Cat1300-1#04-Jul-2024 20:51:47 %SEC-W-COADISPORT: Interface gi1/0/9 suspended by CoA Request "disab
le host port" for host 54:          :62
04-Jul-2024 20:51:47 %LINK-W-Down:  gi1/0/9
```

Passaggio 12

Per interrompere l'acquisizione del pacchetto, usare il comando monitor capture cap1 stop.

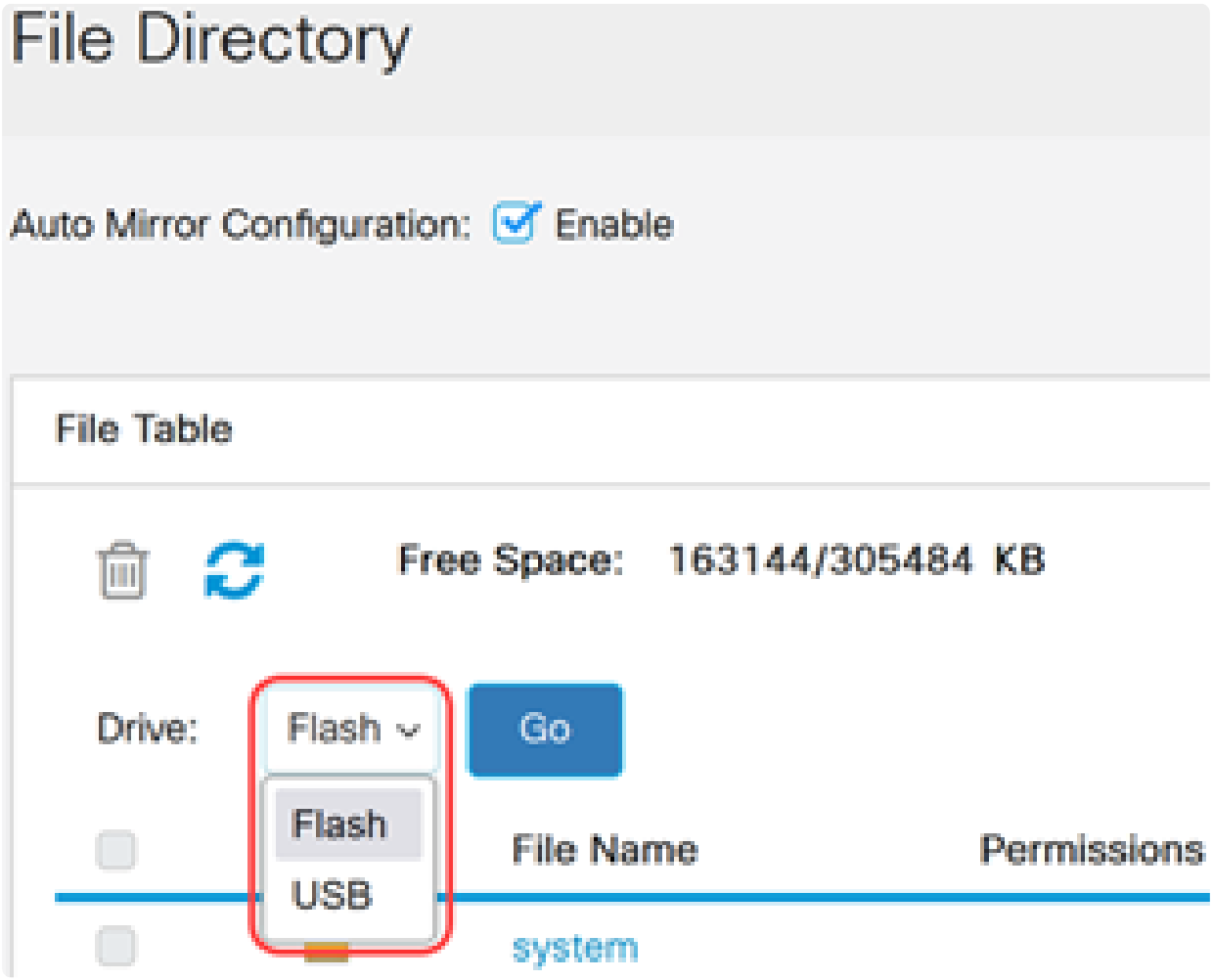
Passaggio 13

Per copiare i file, selezionare Amministrazione > Gestione file > Directory file.


Administration
1
System Settings
Console Settings
Stack Management
Bluetooth Settings
User Accounts
Idle Session Timeout
Time Settings

Passaggio 14

È disponibile il flash predefinito. In alternativa, è possibile selezionare USB (USB) dal menu a discesa Drive (Unità).



Conclusioni

Ora puoi sapere tutto su ISE e su come configurare la licenza CoA sugli switch Catalyst serie 1300.

Per maggiori informazioni, guarda il video qui sotto.

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

Fare clic qui per visualizzare altre Tech Talks di Cisco

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).