Configuratie van wijziging van autorisatie in Catalyst 1300 met behulp van webgebruikersinterface

Doel

Het doel van dit artikel is om u te tonen hoe te om verandering van vergunning (CoA) in Catalyst 1300 switches te vormen die de gebruikersinterface van het Web (UI) gebruiken.

Toepasselijke apparaten en softwareversie

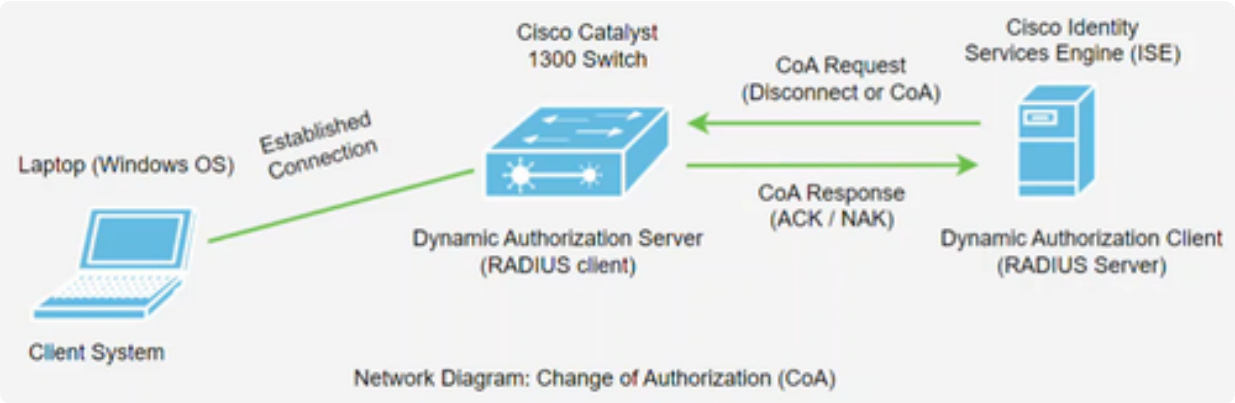
- Catalyst 1300 switches | 4.1.6.53

Inleiding

Wijziging van autorisatie (CoA) is een uitbreiding van het RADIUS-protocol, waarmee u de eigenschappen van een verificatie-, autorisatie- en accounting (AAA) of dot1x-gebruikerssessie kunt wijzigen nadat deze is geverifieerd. Wanneer een beleid voor een gebruiker of groep in AAA verandert, kunnen beheerders RADIUS CoA-pakketten verzenden vanaf de AAA-server, zoals een Cisco Identity Services Engine (ISE), om de verificatie opnieuw te initialiseren en het nieuwe beleid toe te passen.

De Cisco Identity Services Engine (of ISE) is een volledig uitgeruste, op netwerk gebaseerde engine voor toegangscontrole en beleidshandhaving. Het biedt veiligheidsanalyse en handhaving, RADIUS- en TACACS-diensten, beleidsdistributie, en meer. Cisco ISE is momenteel de enige ondersteunde CoA Dynamic Autorisation-client voor Catalyst 1300 switches. Raadpleeg de ISE-beheerhandleiding voor meer informatie.

Voor deze optie is communicatie tussen de Dynamic Authorisation Client (RADIUS-server) en de Dynamic Authorisation Server (Catalyst switch) vereist. Zoals in het netwerkdiagram hieronder wordt weergegeven, stuurt de Dynamic Authorisation Server een bericht over de verbinding verbroken of CoA naar de Dynamic Authorisation Server en de switch geeft een antwoord.



De CoA-ondersteuning is toegevoegd aan de Catalyst 1300-switches in firmware versie 4.1.3.36. Dit omvat ondersteuning voor het verbreken van gebruikers en het wijzigen van machtigingen die van toepassing zijn op een gebruikerssessie. Het apparaat ondersteunt de volgende CoA-acties:

- Sessie verbreken
- Uitschakelen van host-poort CoA-opdracht
- Bounce host-poort CoA-opdracht
- Opdracht Host CoA opnieuw verifiëren

Om CoA te configureren met behulp van een opdrachtregelinterface (CLI), raadpleegt u Configuration of Change of Authorisation in Catalyst 1300 Switch met behulp van CLI.

Inhoud

Catalyst 1300 RADIUS-client configureren op ISE

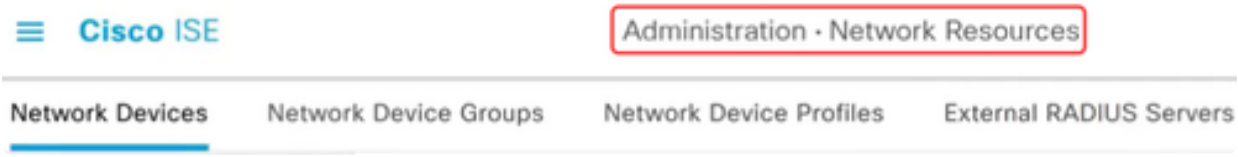
In dit voorbeeld wordt Cisco ISE-serverversie 3.2 gebruikt. Kijk voor een overzicht van ISE op de productpagina Cisco Identity Services Engine.

> **Note:**
> CoA wordt ondersteund op ISE versie 2.7 en hoger.

Na het implementeren van Cisco ISE-server inloggen om de web-UI te openen.

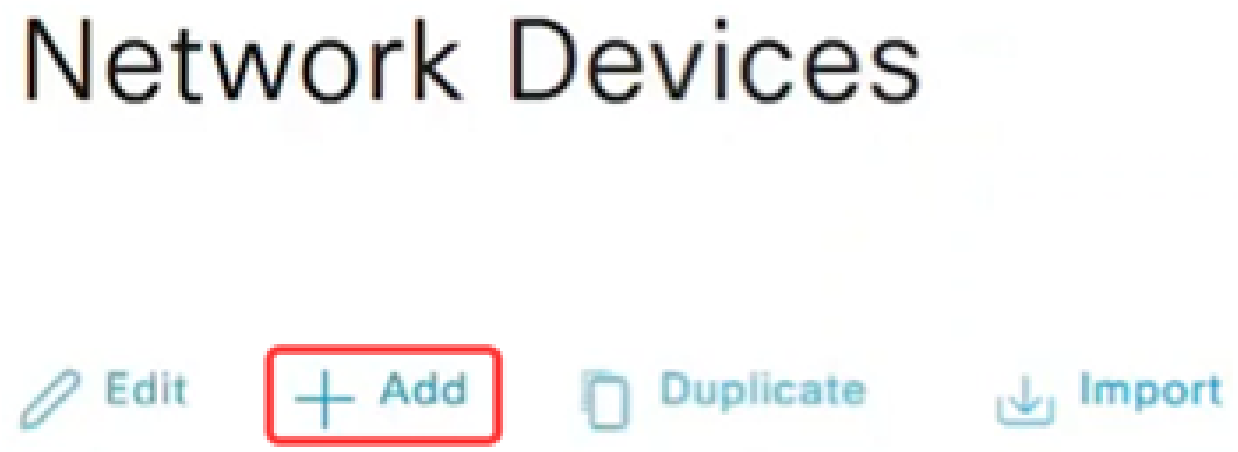
Stap 1

Als u netwerkapparaten wilt toevoegen, navigeert u naar het menu Beheer > Netwerkbronnen.



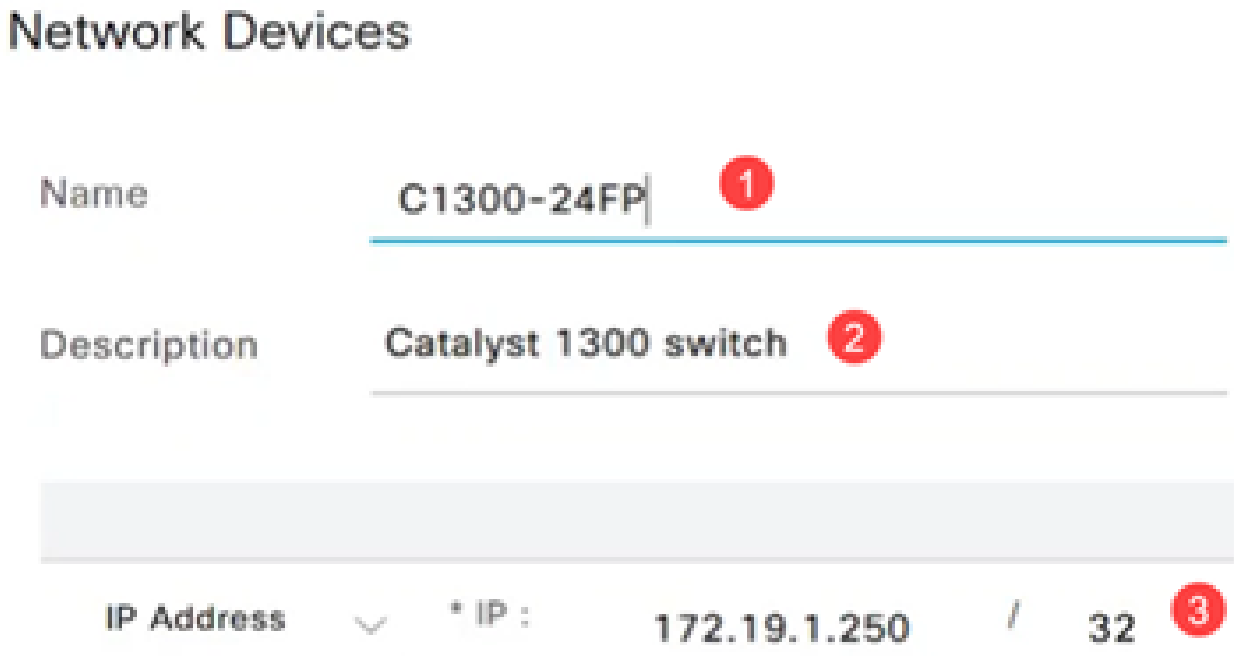
Stap 2

Klik op de knop Toevoegen.



Stap 3

Voer de naam, beschrijving en IP-adres van de Catalyst switch in.

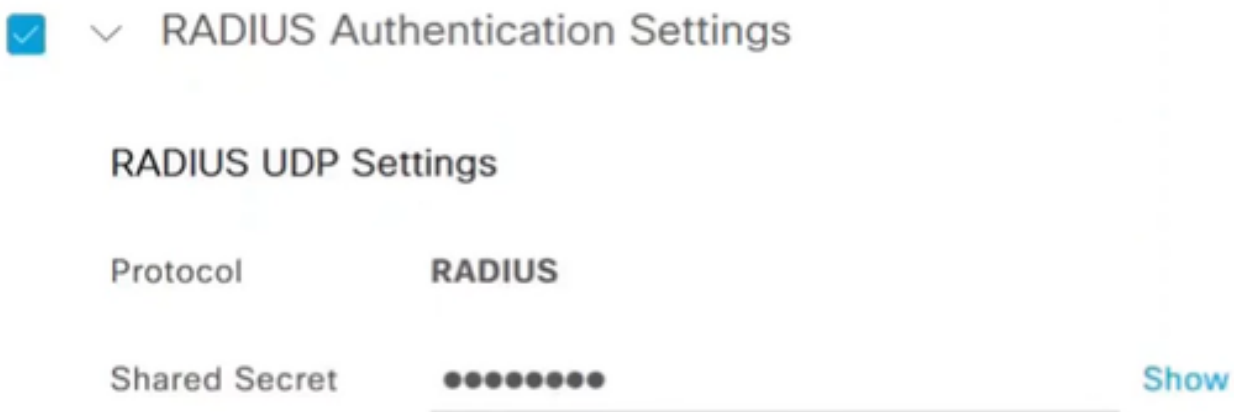


Stap 4

Selecteer Cisco in het vervolgkeuzemenu Apparaatprofiel.

Stap 5

Configureer de RADIUS-verificatie-instellingen door het gedeelde geheim in te voeren.



Stap 6

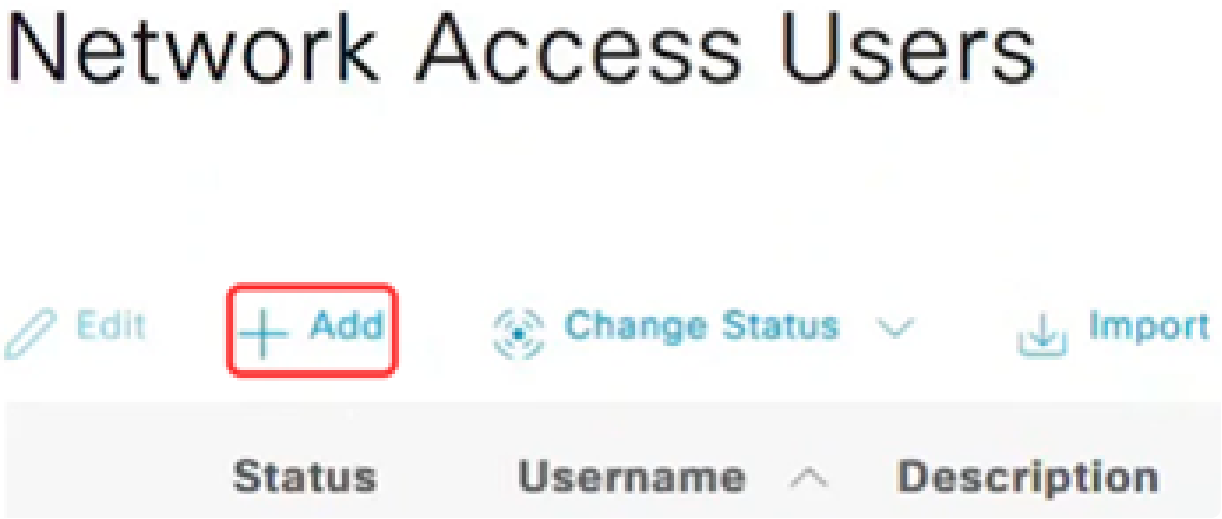
Voer het CoA-poortnummer in. De standaardpoort is 1700.

Stap 7

Navigeer vervolgens naar Beheer > Identity Management en selecteer Netwerktoegangsgebruikers.

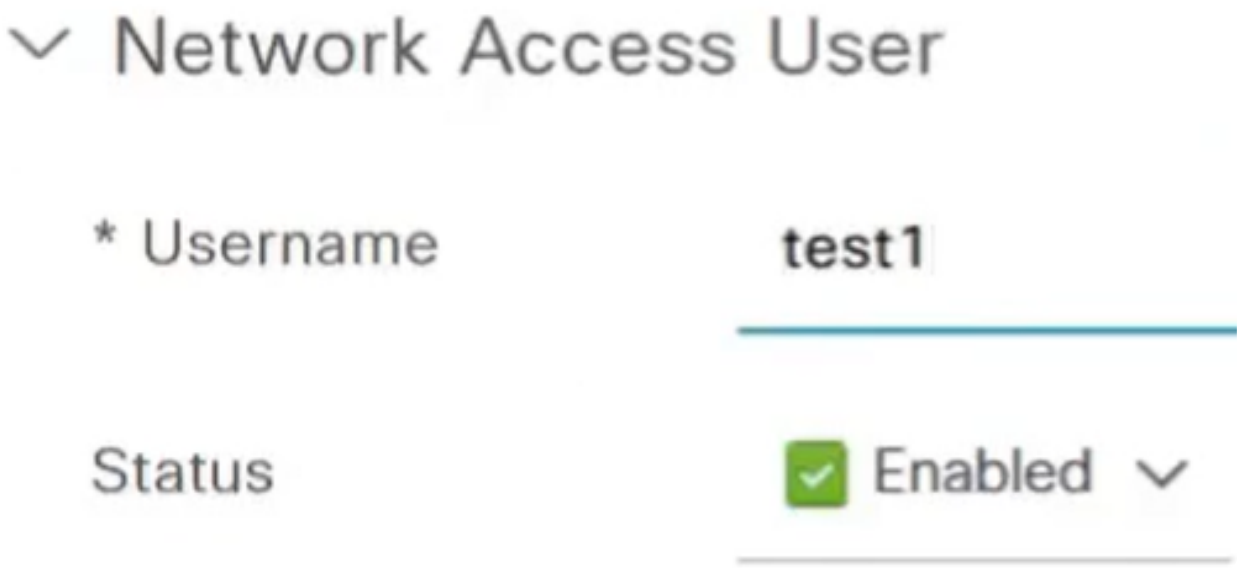
Stap 8

Om de gebruikersnaam en het wachtwoord te definiëren, klikt u op het symbool +Add.



Stap 9

Voer de gebruikersnaam en het wachtwoord in en klik op Opslaan onder aan de pagina.



Configuraties in Catalyst 1300 Switch

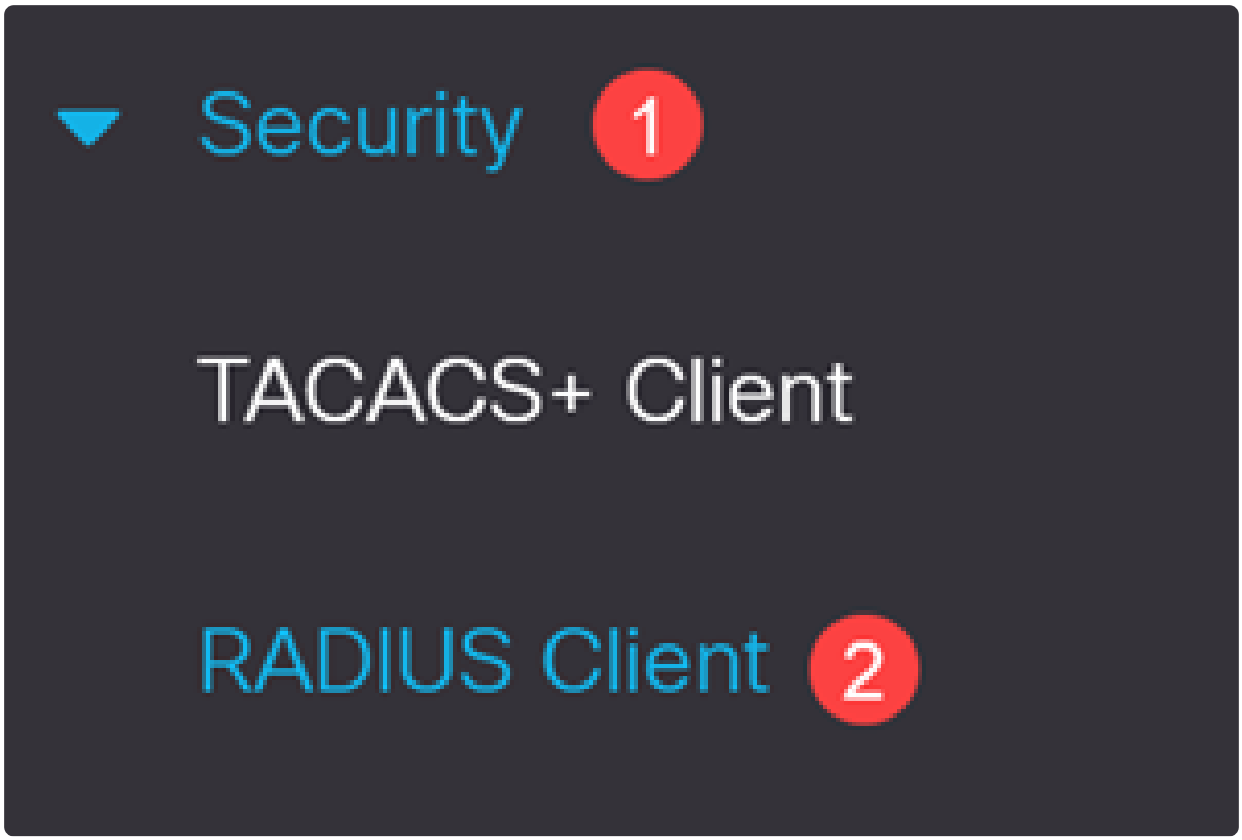
Stap 1

Meld u aan bij uw Catalyst 1300 switch en selecteer de geavanceerde modus. In dit voorbeeld wordt C1300-24FP-4X gebruikt.

> **Note:**
> De CoA ondersteuning is toegevoegd aan Catalyst 1300 switches in firmware versie 4.1.3.36.

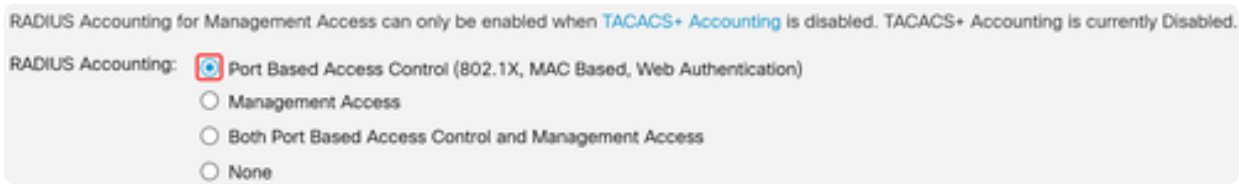
Stap 2

Navigeer naar de Security > RADIUS-client in het navigatiedeelvenster.



Stap 3

Stel RADIUS-accounting in op poortgebaseerde toegangscontrole.



Stap 4

Als u de ISE-server wilt toevoegen, scrolt u omlaag naar de RADIUS-tabel en klikt u op het plus-pictogram.

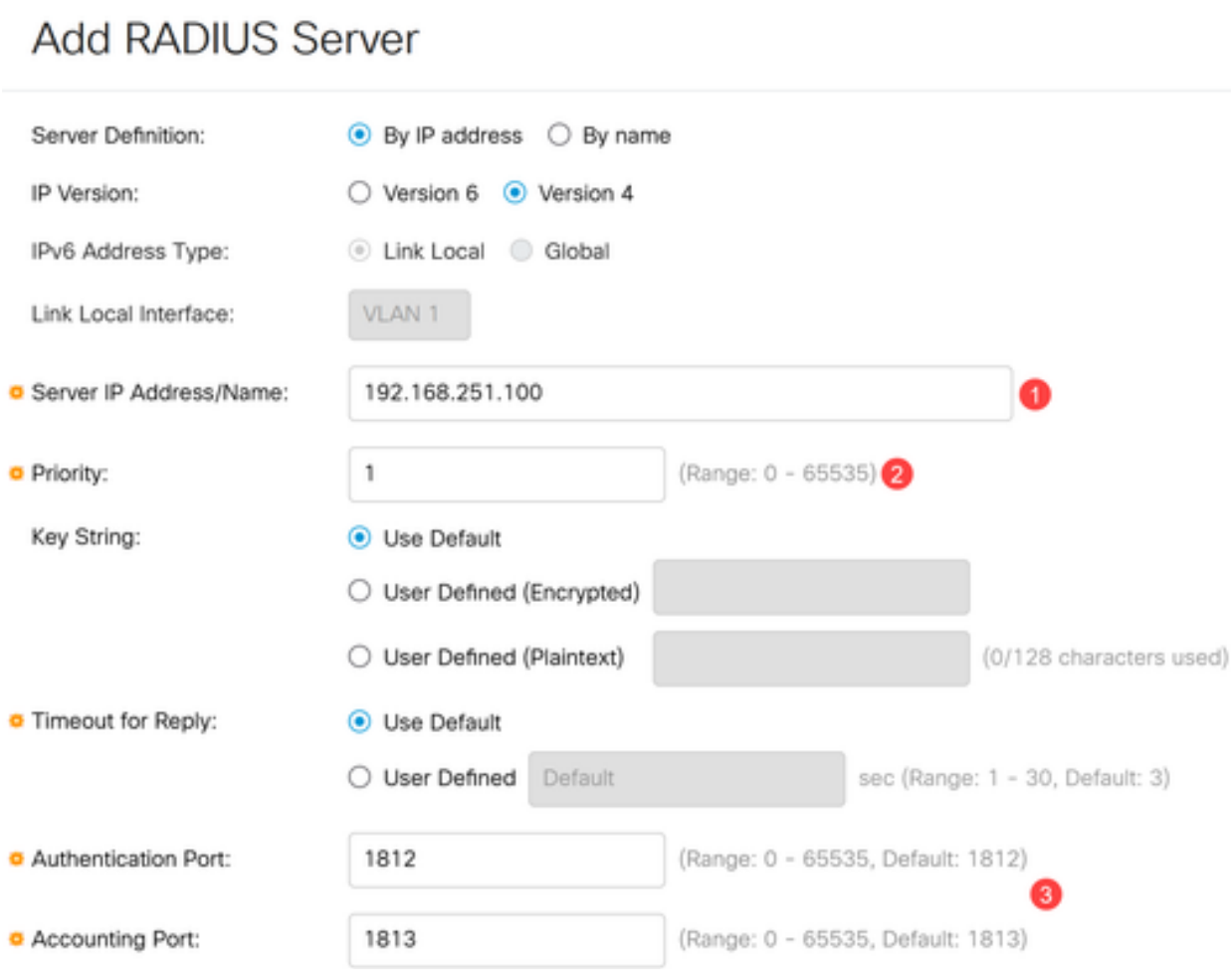
Stap 5

Configureer de RADIUS-serverinstellingen.

- Selecteer Serverdefinitie. In dit voorbeeld is IP-adres geselecteerd. Voer het IP-adres in in het veld IP-adres/naam van de server.
- Stel een RADIUS-prioriteit in.

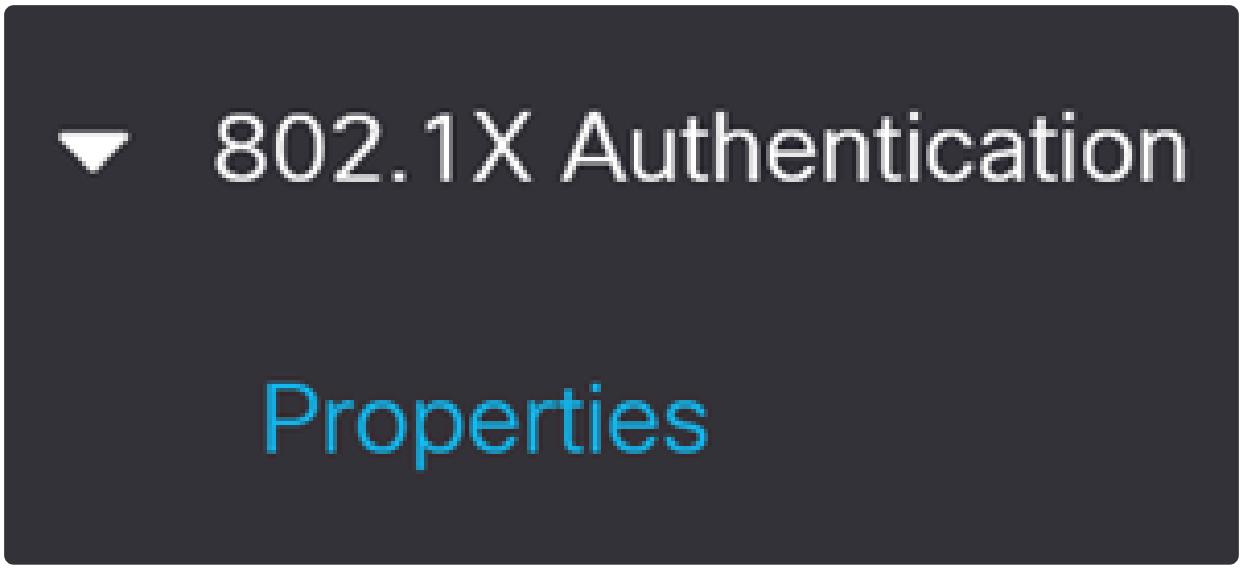
- De standaardinstelling is voor de verificatie- en accounting poorten.
- Het type gebruik is 802.1x.

Klik op Apply (Toepassen).



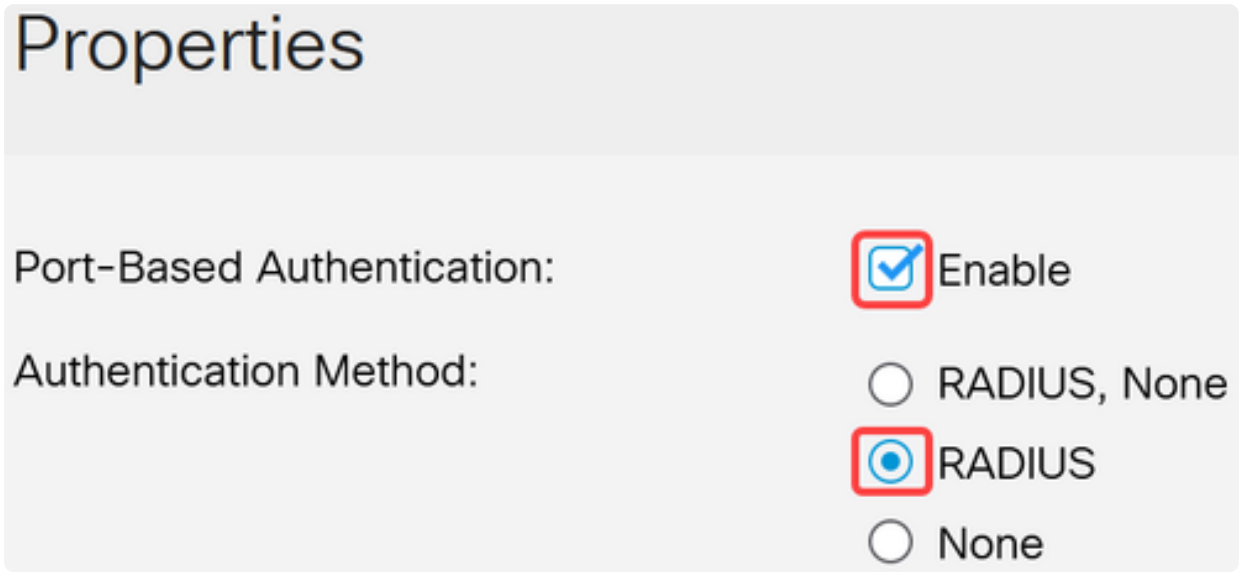
Stap 6

Voor het configureren van 802.1x-verificatie navigeer je naar Security > 802.1x-verificatie > Properties menu.



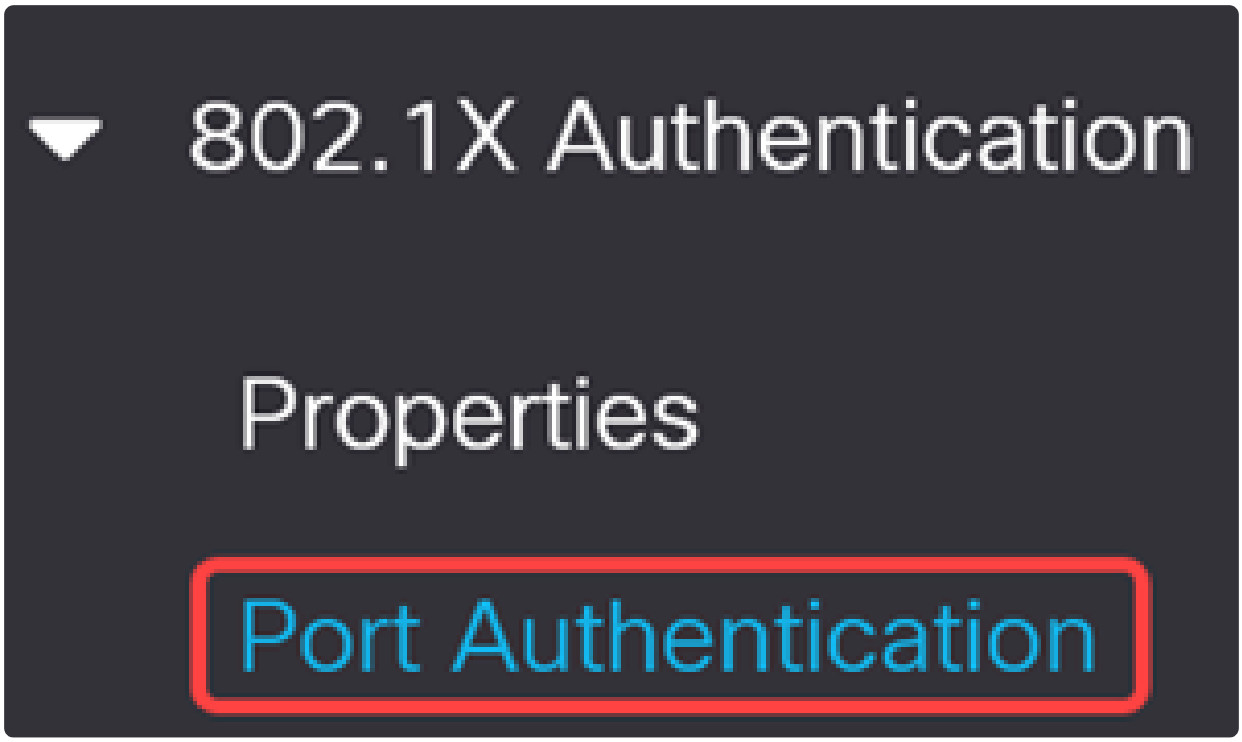
Stap 7

Zorg ervoor dat poortgebaseerde verificatie is ingeschakeld en dat de verificatiemethode is ingesteld op RADIUS.



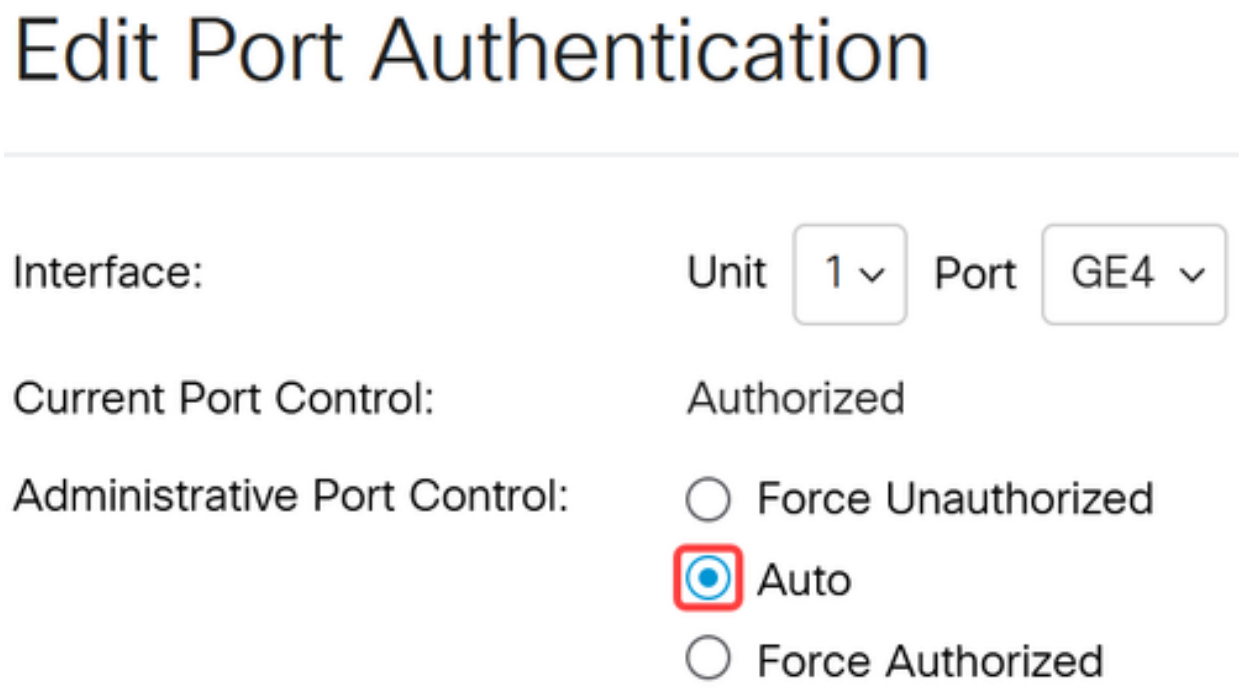
Stap 8

Navigeer naar het menu Poortverificatie, selecteer de gewenste poort en klik op Bewerken.



Stap 9

Voor Administratieve Poortcontrole, selecteer Auto-optie die de poort tussen geautoriseerde en niet-geautoriseerde status zal switches op basis van de RADIUS-respons.

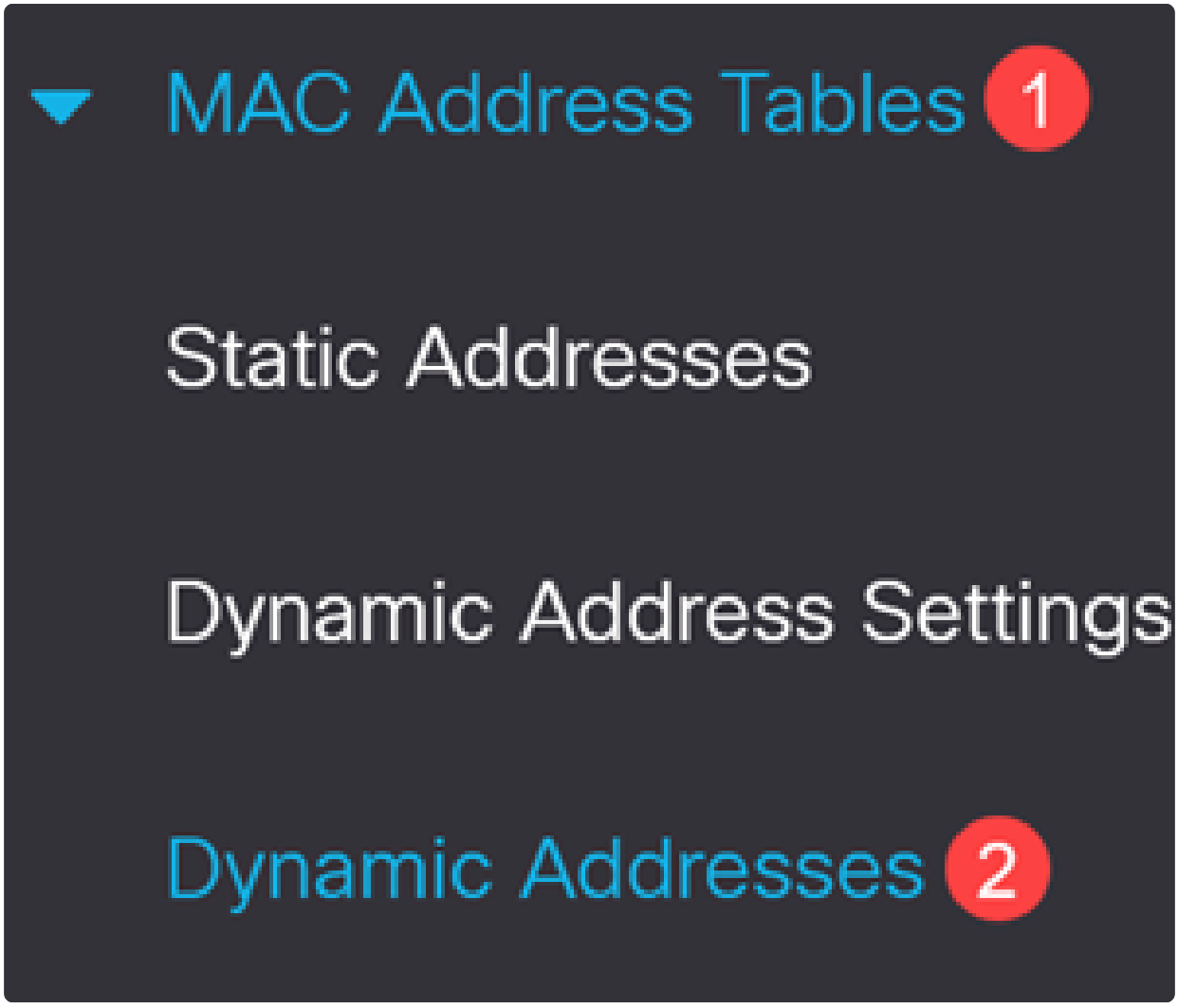


Stap 10

Schakel 802.1x-gebaseerde verificatie in en klik op Toepassen.

Stap 11

U hebt het MAC-adres nodig voor het apparaat op de poort. De CoA-operatie op ISE wordt toegepast op dat MAC-adres. In dit voorbeeld, is het poort 9. Om het te krijgen, navigeer naar MAC-adrestabellen > Dynamische adressen.

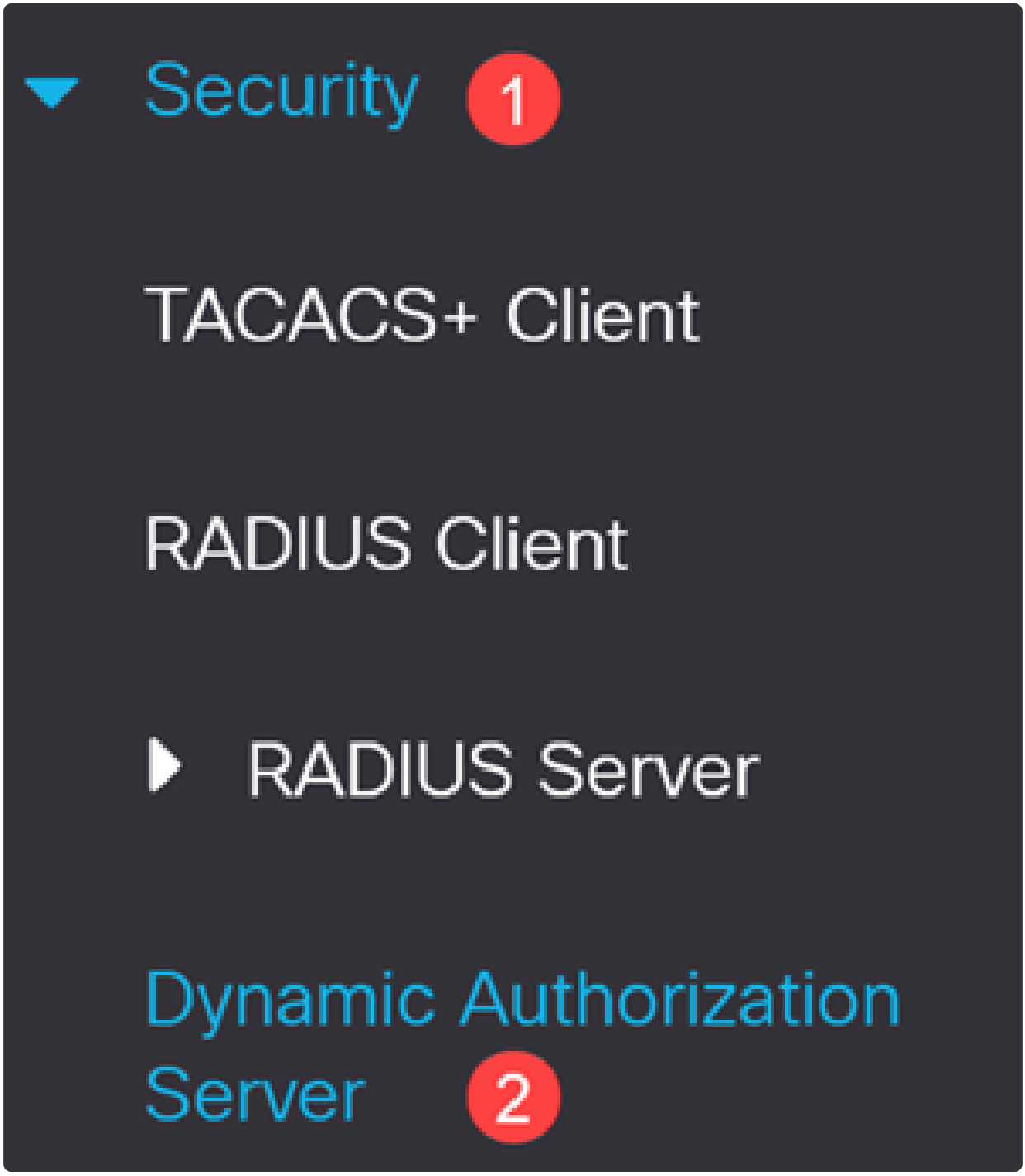


Stap 12

Scroll naar beneden naar de poort en noteer het MAC-adres.

Stap 13

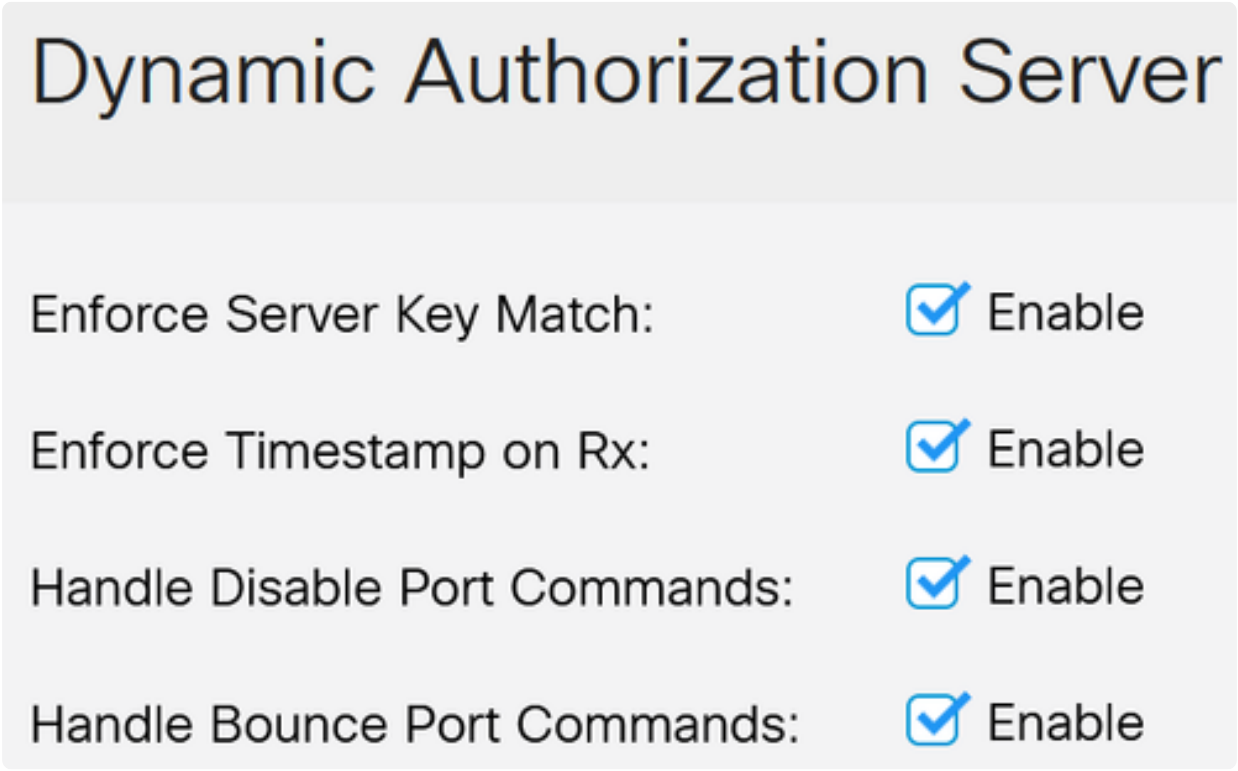
Ga naar Security > Dynamic Authorisation Server.



Stap 14

Schakel het volgende in:

- Toetsenovereenkomst voor afdwingen van server
- Tijdstempel op RX afdwingen
- Handle - Poortopdrachten uitschakelen
- Opdrachten voor terugkaatsen van handgrepen

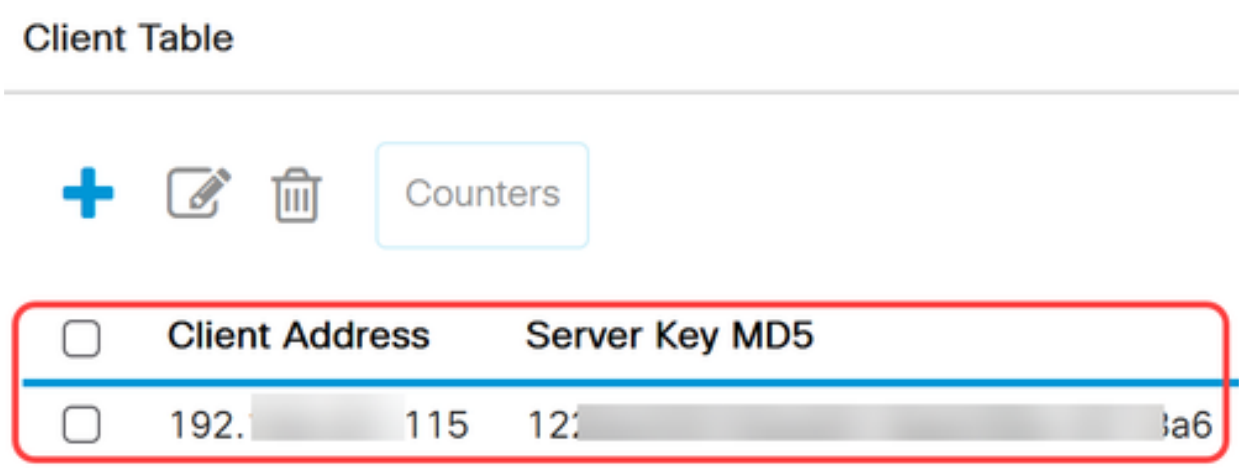


Stap 15

Verlaat de UDP-poort op de standaardwaarde van 1700.

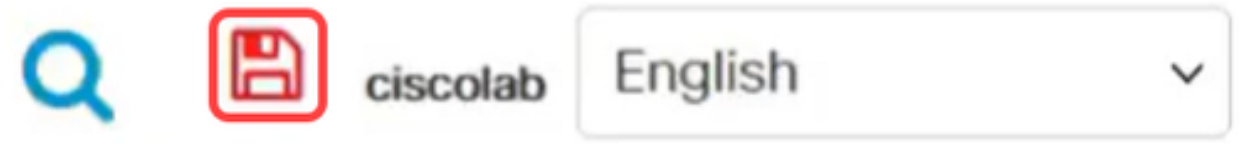
Stap 16

Controleer onder Clienttabel of de ISE-server is toegevoegd met de juiste servertoets. Klik op Apply (Toepassen).



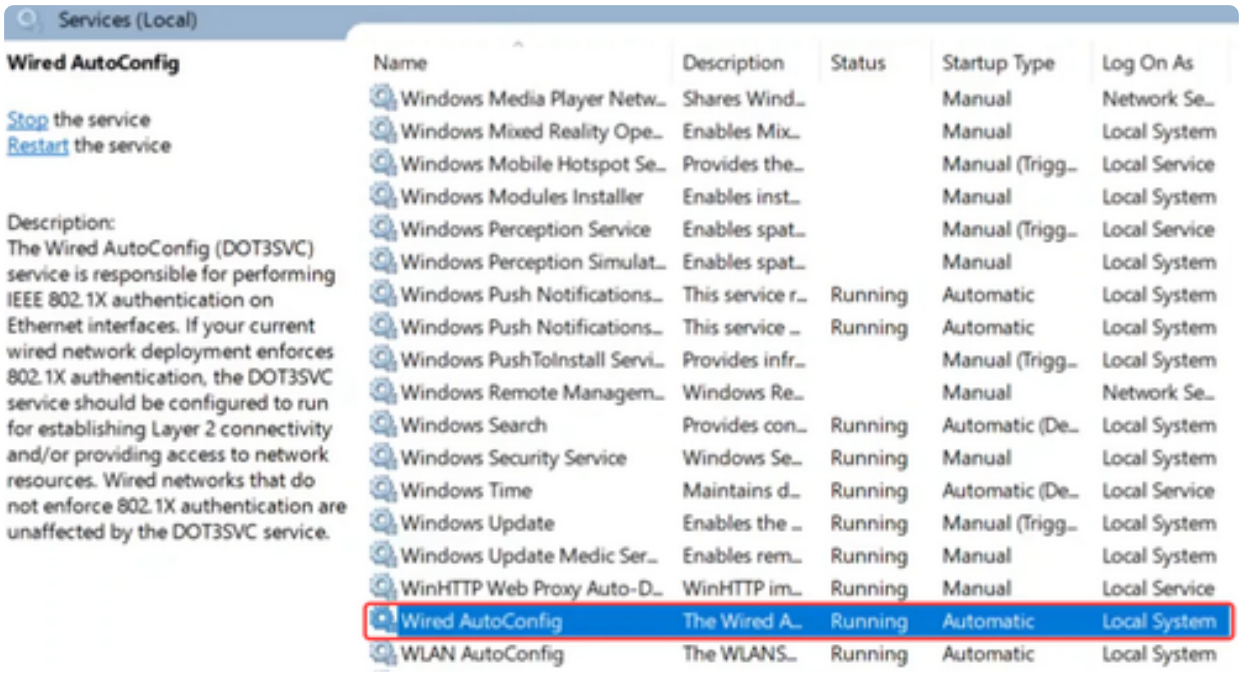
Stap 17

Klik op het rode knipperende pictogram Opslaan om de configuraties op te slaan.



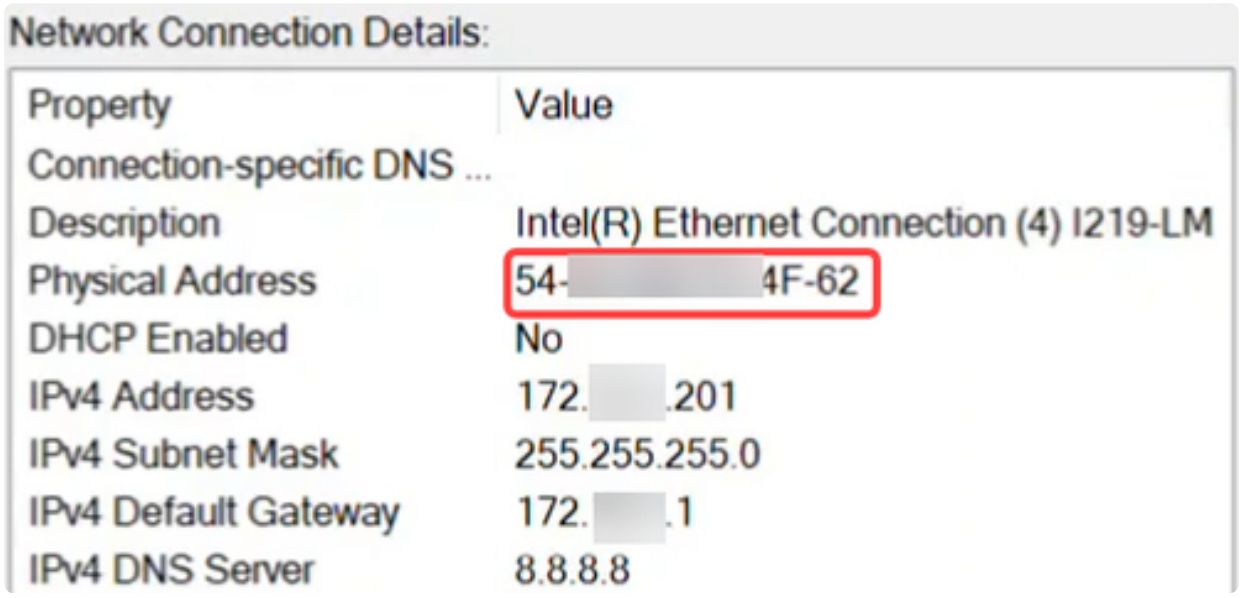
Stap 18

Controleer of op de laptop van de client die is aangesloten op poort 9 de Wired AutoConfig-service is ingeschakeld voor 802.1 X-verificatie.



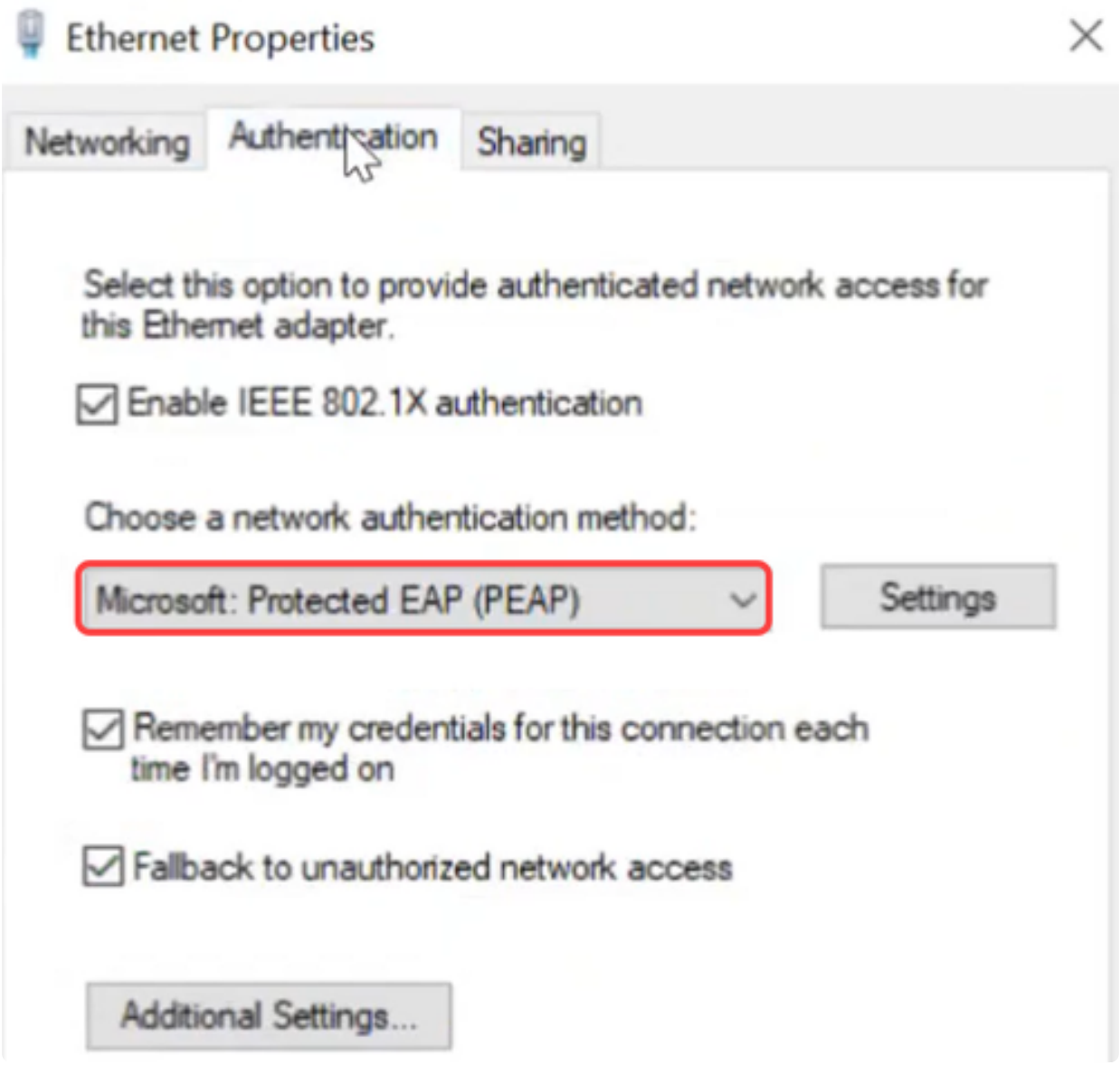
Stap 19

Controleer in de instellingen van de Ethernet-adapter of het MAC-adres overeenkomt.



Stap 20

Klik op de knop Properties onder Ethernet-instellingen en controleer of de selectievakjes ingeschakeld zijn onder het tabblad Verificatie. Controleer ook of de verificatiemethode is beveiligd met EAP (PEAP).



Stap 21

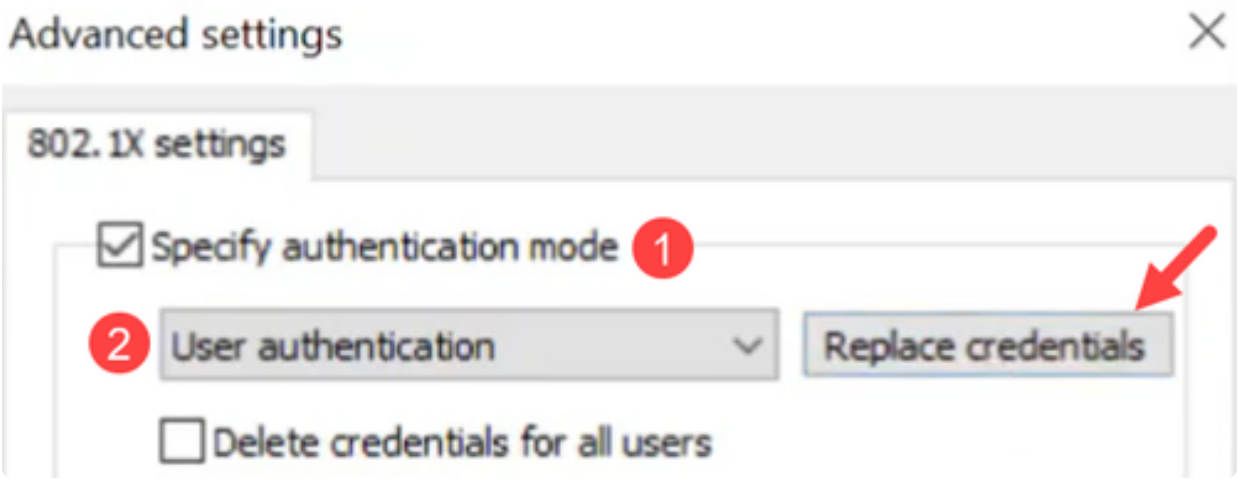
Klik op de knop Instellingen om ervoor te zorgen dat het aankruisvakje naast Verifiëren van de identiteit van de server door te bevestigen dat het certificaat onaangevinkt is.

Stap 22

Schakel het vakje Fast Recconnect in.

Stap 23

Zorg er onder Extra instellingen voor dat de verificatiemodus is ingeschakeld en dat Gebruikersverificatie is geselecteerd in het vervolgkeuzemenu. U kunt de referenties die op ISE zijn gemaakt, opslaan of vervangen met de knop Credentials vervangen.



Samenwerking

Alvorens een CoA-bewerking te starten, dient u pakketopname op de switch in te schakelen.

Stap 1

Meld u op PuTTY aan bij uw Catalyst-switch en specificeer de buffergrootte en de opnamemodus met behulp van de opdrachtmonitor Capture cap1 buffergrootte 20 cirkelvormig.

Stap 2

Specificeer het bedieningsvlak als beide door gebruik van de opdrachtmonitor Capture cap1 control-plane beide.

Stap 3

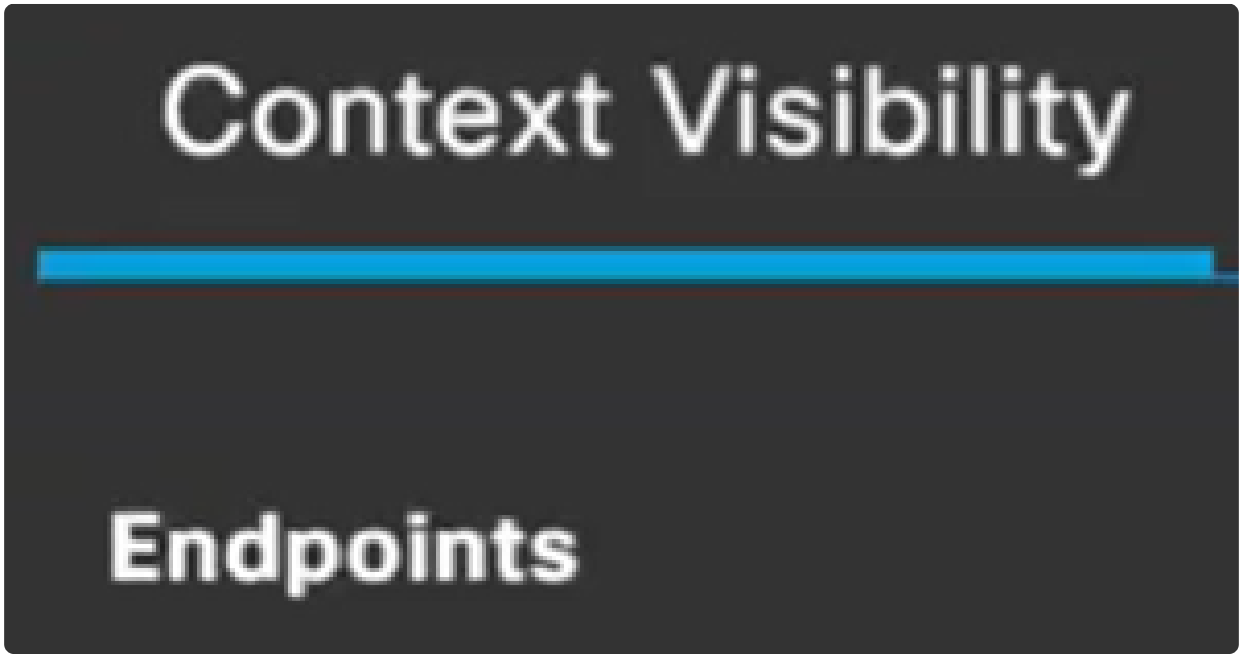
Voer de matchcriteria in zoals ze zijn. De opdracht hiervoor is monitor Capture cap1 match any.

Stap 4

Start de pakketopname.

Stap 5

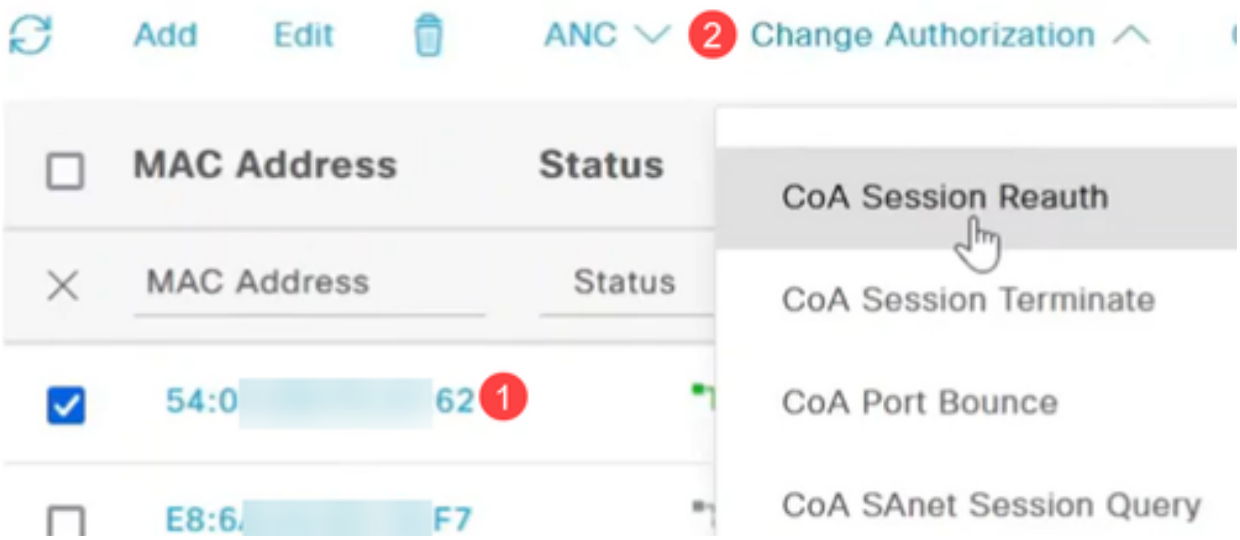
Navigeer op de ISE-interface naar de optie Endpoints onder Context Visibility.



Stap 6

Kies het MAC-adres en selecteer de CoA-bewerking in het vervolgkeuzemenu Wijzigen van autorisatie. In dit voorbeeld is CoA Session Reauth geselecteerd. Dit

dwingt re-authenticatie op de poort door het verzenden van een CoA pakket met een reauthenticate opdracht.



Stap 7

Ga terug naar de PuTTY-terminal om te controleren of de CoA-bewerking succesvol was.

```
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"
```

Stap 8

Als u CoA Session Terminate selecteert, zal het een verzoek om loskoppeling verzenden met een beëindigingsbevel dat op een administratief verzoek wordt gebaseerd.

```
Cat1300-1#04-Jul-2024 20:50:02 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 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 gi1/0/9 is Authorized
```

Stap 9

CoA Port Bounce zal een CoA-verzoekpakket verzenden met een bounce host-

poortopdracht, waardoor de poort op de switch wordt uitgeschakeld en opnieuw wordt ingeschakeld. De netwerkadapter gaat 10 seconden offline en wordt niet-geautoriseerd. Het zal de comeback online, wordt geautoriseerd en kan pakketten doorsturen.

```
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
```

Stap 10

CoA-sessiebeëindiging met poortbounce zal de bestaande sessie beëindigen, de poort 10 seconden stuiteren, en onbevoegd worden. Het komt dan online terug, wordt geautoriseerd en kan pakketten doorsturen.

```
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
```

Stap 11

CoA sessie beëindiging met port shutdown zal de sessie beëindigen en administratief afsluiten van de poort.

```
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
```

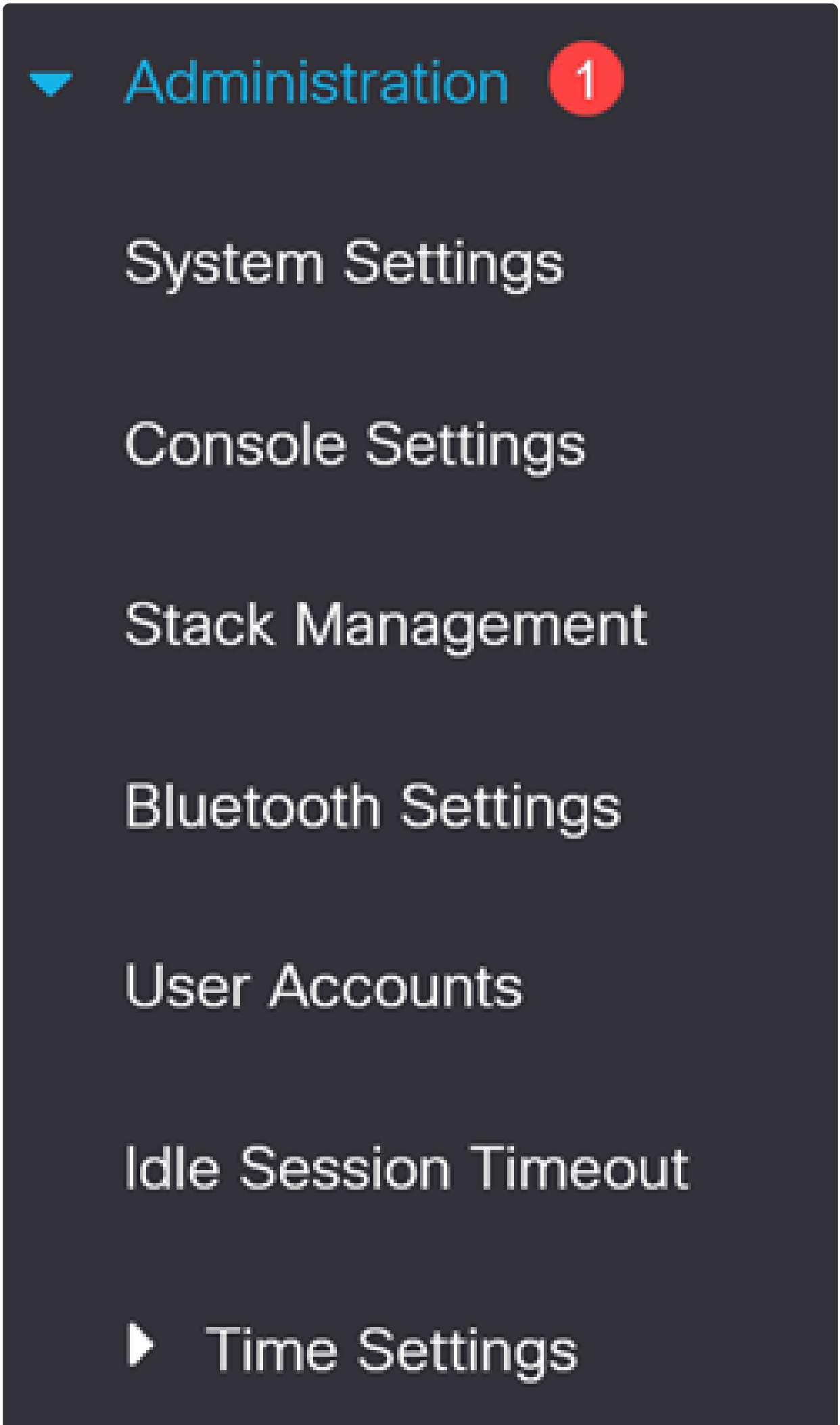
Stap 12

Om het pakket tegen te houden vang, gebruik de bevelmonitor vangen cap1 stop.

Stap 13

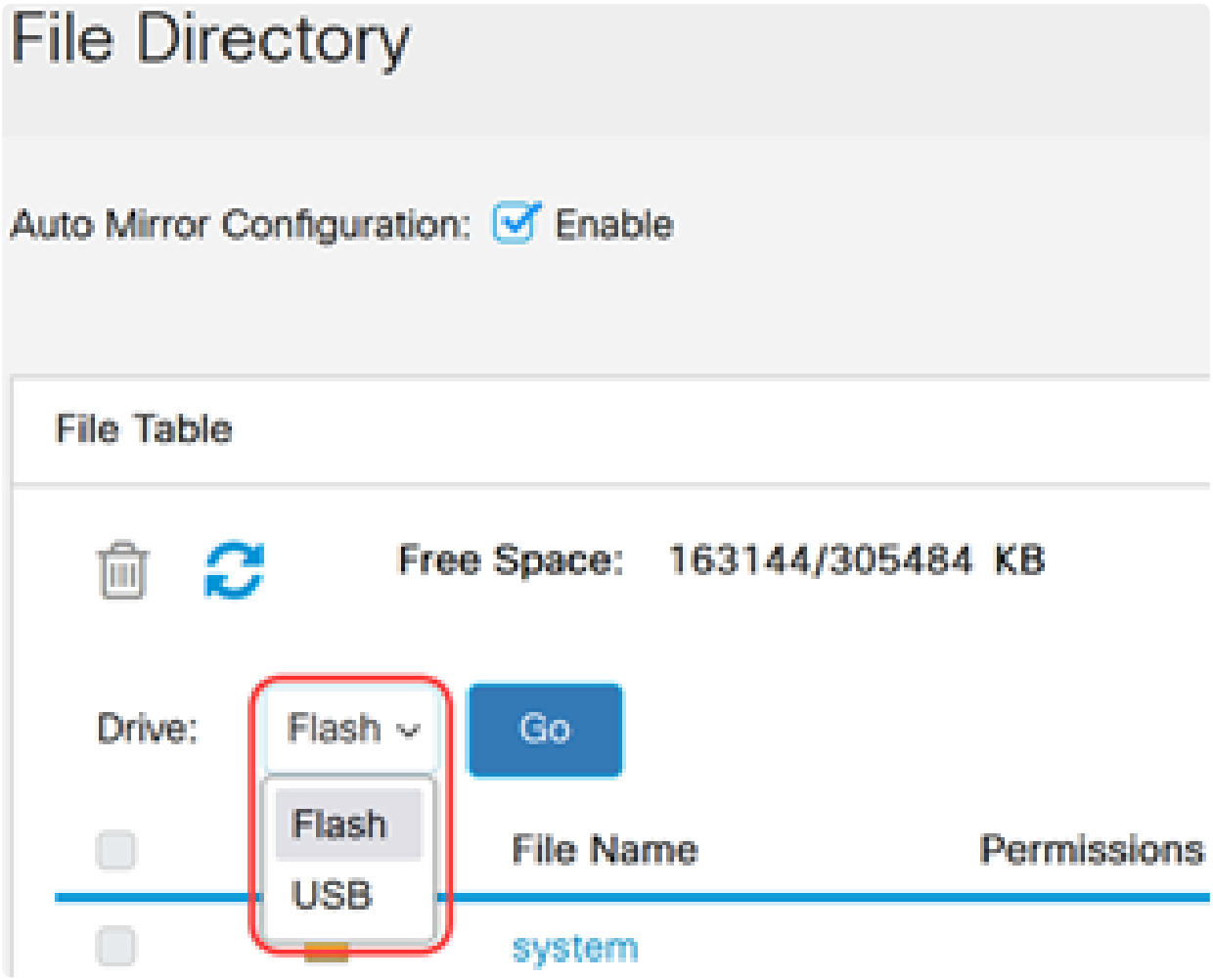
Als u de bestanden wilt kopiëren, navigeert u naar Beheer > Bestandsbeheer >

Bestandsmap.


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

Stap 14

De standaard Flash is beschikbaar. U kunt ook USB selecteren in het vervolgkeuzemenu Drive.



Conclusie

Nu weet u alles over ISE en hoe u CoA kunt configureren in de Catalyst 1300 Series switches.

Kijk voor meer informatie op de video hieronder.

Bekijk een video gerelateerd aan dit artikel ...

Klik hier om nog meer Tech Talks van Cisco te bekijken

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.