Autorisierungsänderung in Catalyst 1300 über Web-Benutzeroberfläche konfigurieren

Ziel

In diesem Artikel wird erläutert, wie Sie die Autorisierungsänderung (Change of Authorization, CoA) in Catalyst 1300-Switches über die Web-Benutzeroberfläche (UI) konfigurieren.

Anwendbare Geräte und Softwareversion

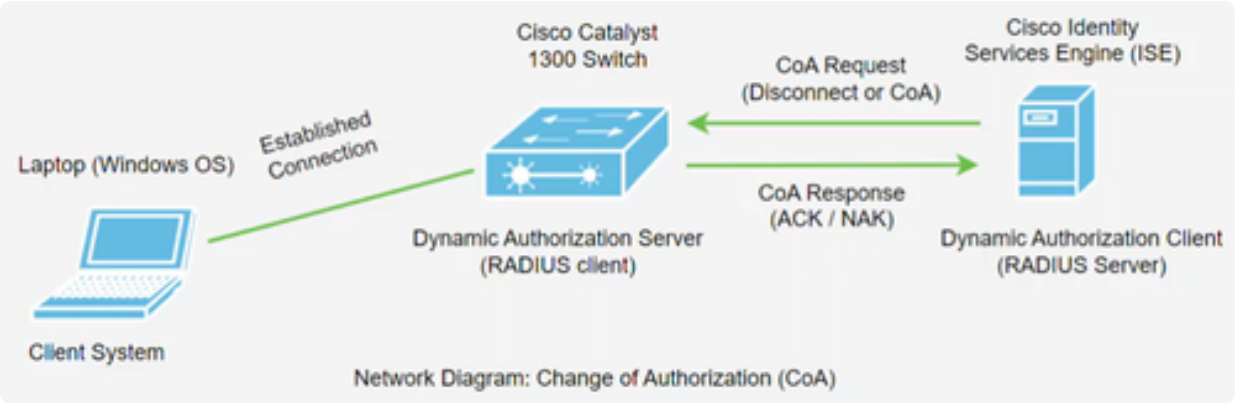
- Catalyst Switches der Serie 1300 | 4.1.6.53

Einleitung

Change of Authorization (CoA) ist eine Erweiterung des RADIUS-Protokolls, mit dem Sie die Eigenschaften einer AAA- (Authentication, Authorization, Accounting) oder dot1x-Benutzersitzung nach deren Authentifizierung ändern können. Wenn sich eine Richtlinie für einen Benutzer oder eine Gruppe in AAA ändert, können Administratoren RADIUS-CoA-Pakete vom AAA-Server, z. B. von der Cisco Identity Services Engine (ISE), übertragen, um die Authentifizierung neu zu initialisieren und die neue Richtlinie anzuwenden.

Die Cisco Identity Services Engine (oder ISE) ist eine Network Based Access Control and Policy Enforcement Engine mit vollem Funktionsumfang. Sie bietet Sicherheitsanalysen und -durchsetzung, RADIUS- und TACACS-Services, Richtlinienverteilung und vieles mehr. Die Cisco ISE ist derzeit der einzige unterstützte CoA Dynamic Authorization Client für Catalyst 1300-Switches. Weitere Informationen finden Sie im ISE-Administratorhandbuch.

Diese Funktion erfordert die Kommunikation zwischen dem Dynamic Authorization Client (RADIUS-Server) und dem Dynamic Authorization Server (Catalyst-Switch). Wie im folgenden Netzwerkdiagramm zu sehen ist, sendet der Dynamic Authorization Server eine Verbindungs- oder CoA-Meldung an den Dynamic Authorization Server, und der Switch antwortet.



Die CoA-Unterstützung wurde den Catalyst 1300-Switches in der Firmware-Version 4.1.3.36 hinzugefügt. Dazu gehört die Unterstützung für das Trennen von Benutzern und das Ändern von Berechtigungen für eine Benutzersitzung. Das Gerät unterstützt die folgenden CoA-Aktionen:

- Sitzung trennen
- Host-Port-CoA-Befehl deaktivieren
- CoA-Befehl für Bounce-Host-Port
- CoA-Befehl für Host erneut authentifizieren

Informationen zur Konfiguration von CoA über die Befehlszeilenschnittstelle (CLI) finden Sie unter Configuration of Change of Authorization in Catalyst 1300 Switch using CLI (Konfiguration der Autorisierungsänderung in Catalyst 1300 Switch unter Verwendung von CLI).

Inhalt

- Konfigurieren des Catalyst 1300 RADIUS-Clients auf der ISE
- Konfigurationen des Catalyst 1300 Switches
- CoA-Betrieb

Konfigurieren des Catalyst 1300 RADIUS-Clients auf der ISE

In diesem Beispiel wird Cisco ISE Server Version 3.2 verwendet. Einen Überblick über die ISE finden Sie auf der Produktseite zur Cisco Identity Services Engine.

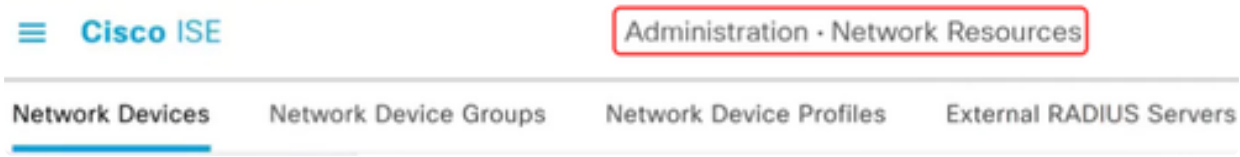
> **Note:**
> CoA wird von ISE Version 2.7 und höher unterstützt.

Melden Sie sich nach der Bereitstellung des Cisco ISE-Servers an, um auf die

Webbenutzeroberfläche zuzugreifen.

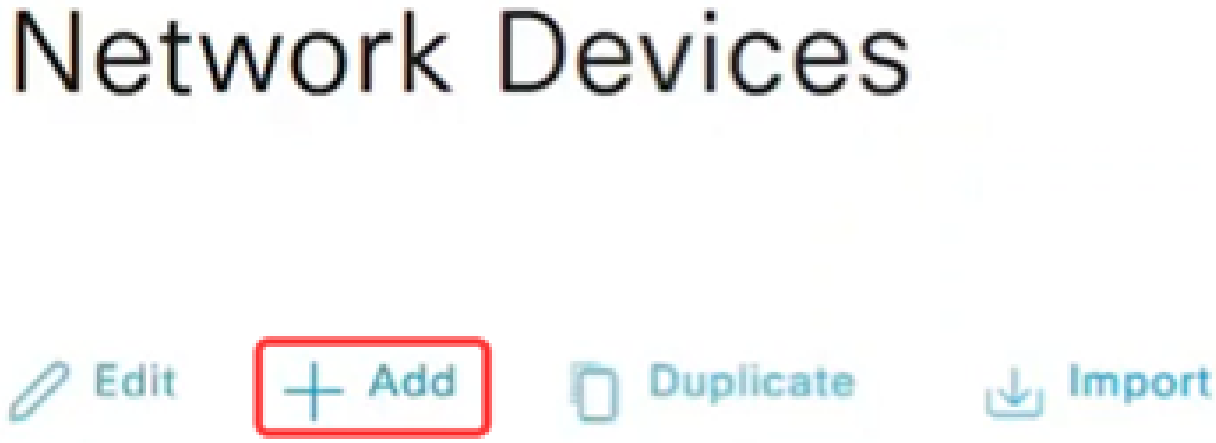
Schritt 1

Um Netzwerkgeräte hinzuzufügen, navigieren Sie zum Menü Administration > Network Resources (Verwaltung > Netzwerkressourcen).



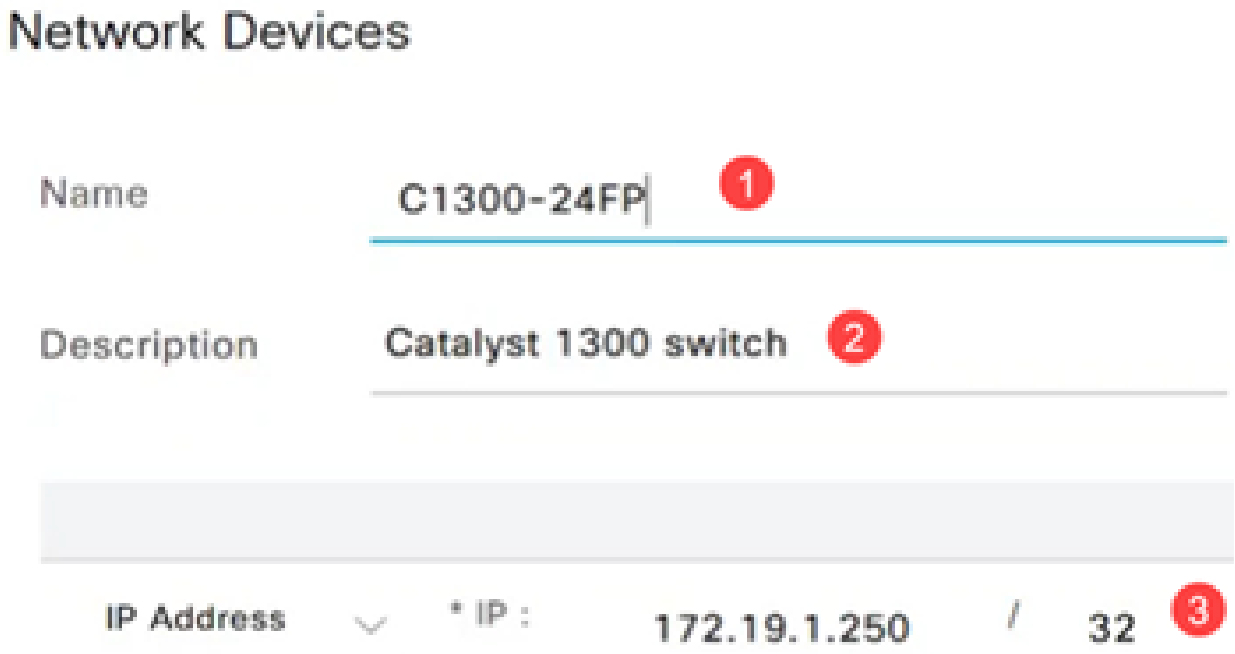
Schritt 2

Klicken Sie auf die Schaltfläche + Hinzufügen.



Schritt 3

Geben Sie den Namen, die Beschreibung und die IP-Adresse des Catalyst Switches ein.

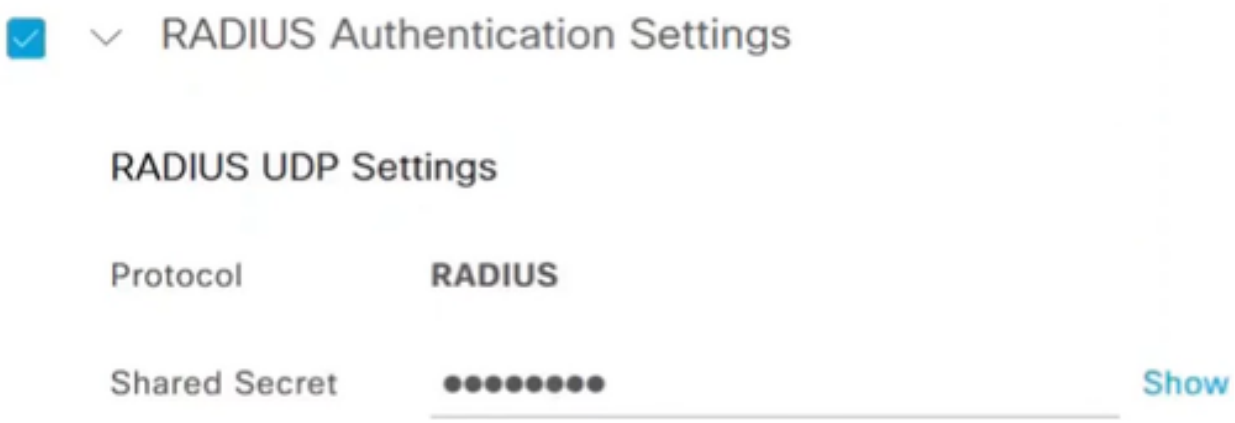


Schritt 4

Wählen Sie im Dropdown-Menü Geräteprofil die Option Cisco aus.

Schritt 5

Konfigurieren Sie die RADIUS-Authentifizierungseinstellungen, indem Sie den freigegebenen Schlüssel eingeben.



Schritt 6

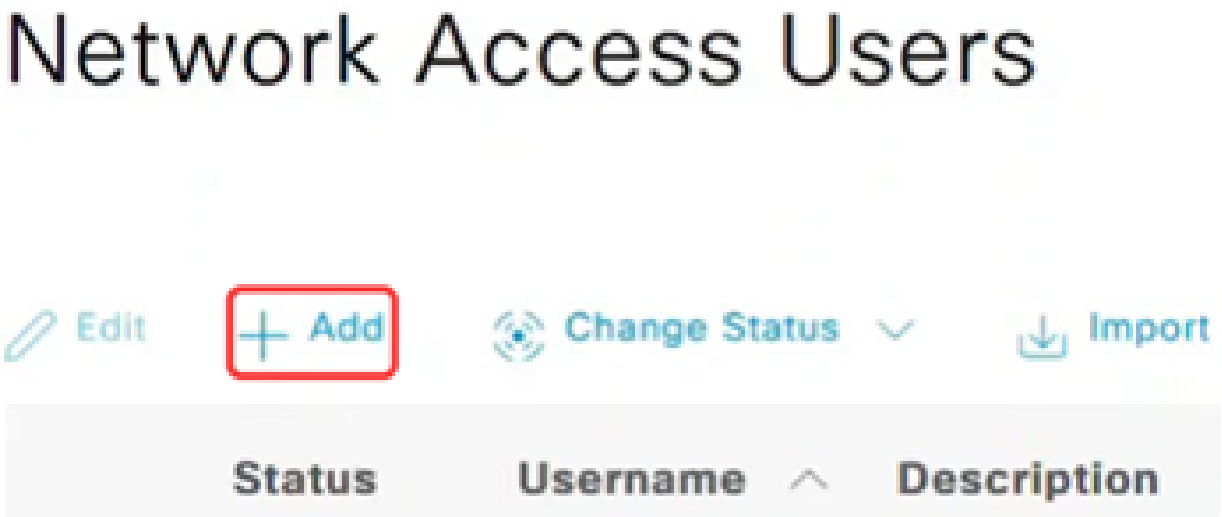
Geben Sie die CoA-Portnummer ein. Der Standardport ist 1700.

Schritt 7

Navigieren Sie anschließend zu Administration > Identity Management, und wählen Sie Network Access Users aus.

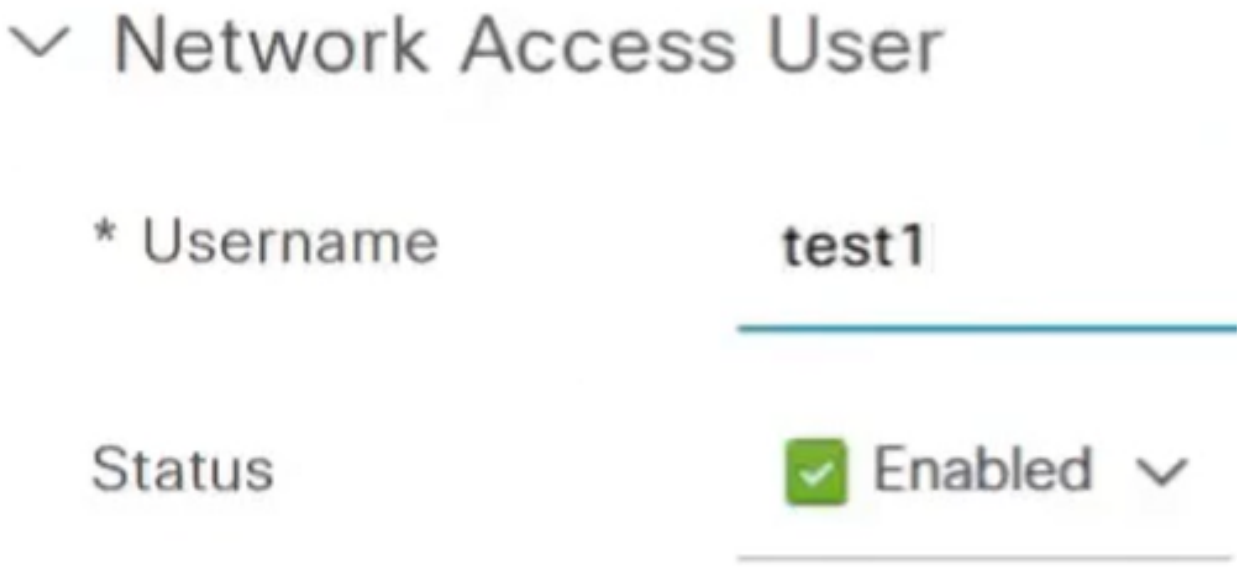
Schritt 8

Um Benutzername und Passwort zu definieren, klicken Sie auf das Symbol +Hinzufügen.



Schritt 9

Geben Sie den Benutzernamen und das Kennwort ein, und klicken Sie unten auf der Seite auf Speichern.



Konfigurationen des Catalyst 1300 Switches

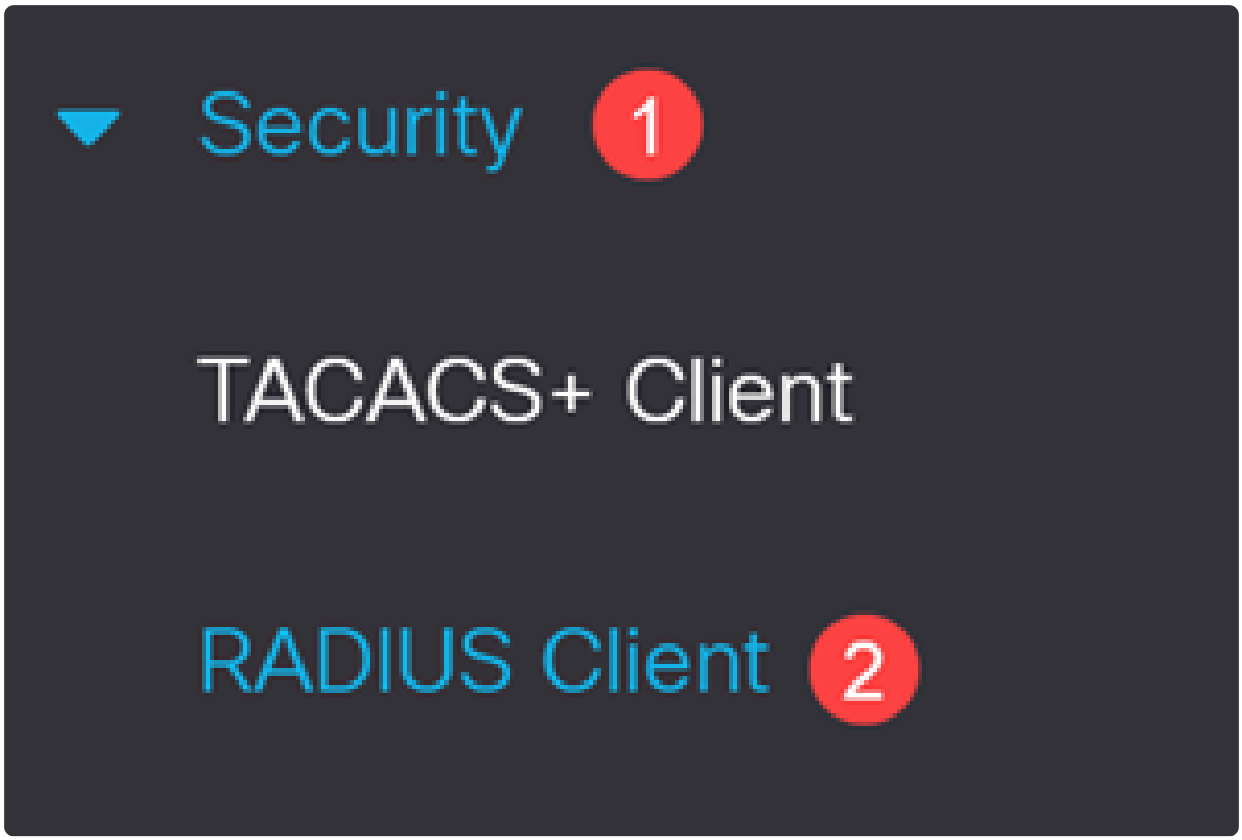
Schritt 1

Melden Sie sich bei Ihrem Catalyst 1300 Switch an, und wählen Sie den erweiterten Modus aus. In diesem Beispiel wird C1300-24FP-4X verwendet.

> **Note:**
> Die CoA-Unterstützung wurde den Catalyst 1300-Switches in der Firmware-Version 4.1.3.36 hinzugefügt.

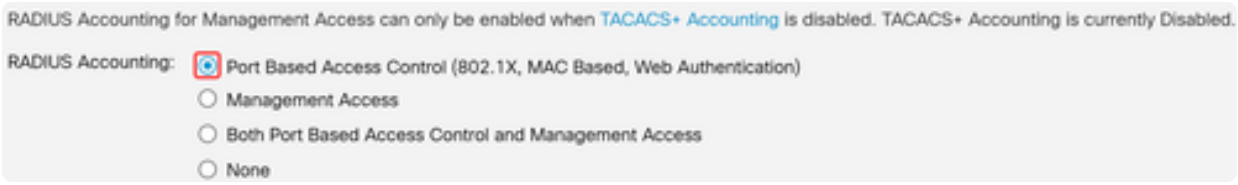
Schritt 2

Navigieren Sie im Navigationsbereich zu Security > RADIUS Client (Sicherheit > RADIUS-Client).



Schritt 3

Legen Sie RADIUS Accounting auf Port Based Access Control fest.



Schritt 4

Um den ISE-Server hinzuzufügen, scrollen Sie nach unten zur RADIUS-Tabelle, und klicken Sie auf das Pluszeichen.

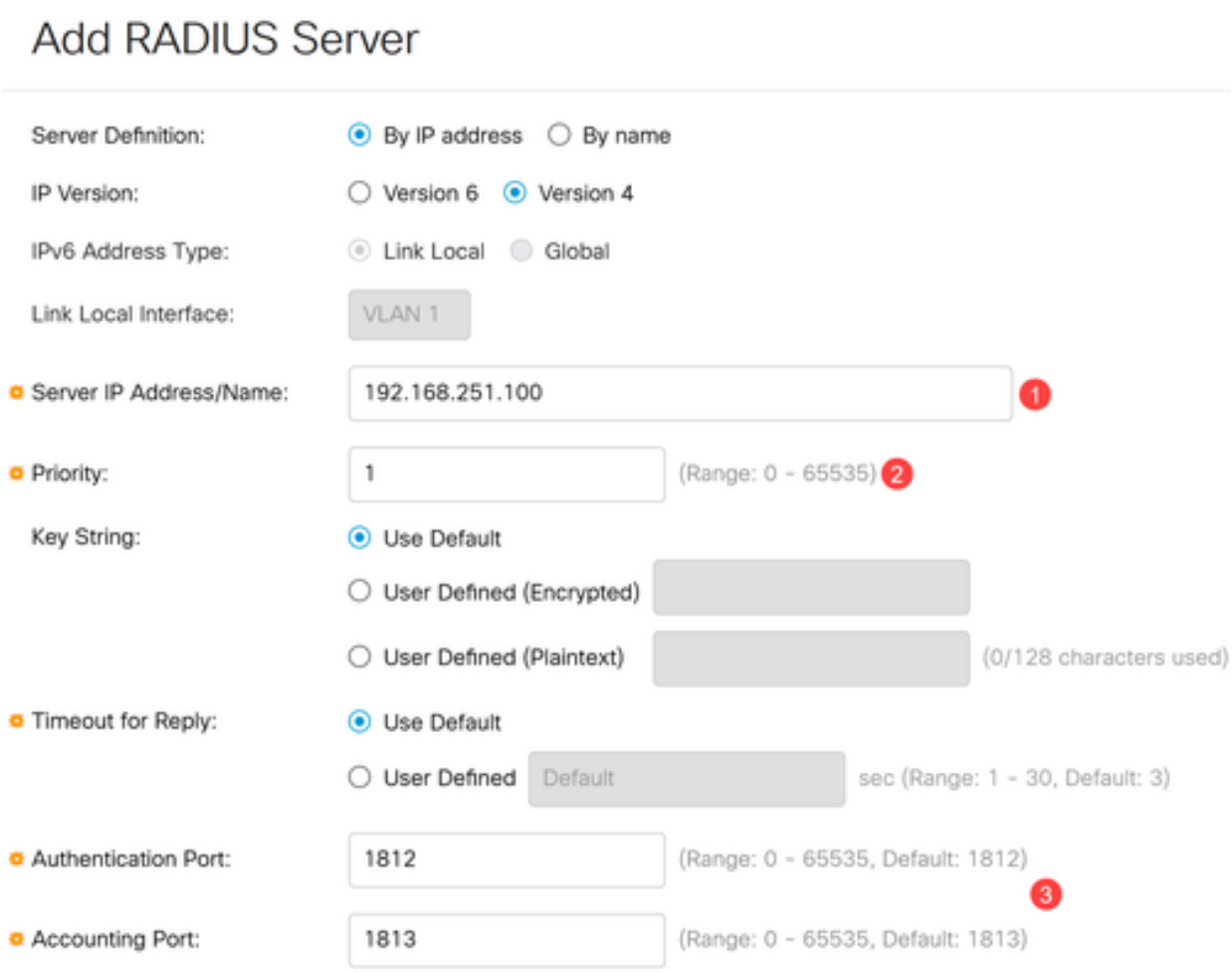
Schritt 5

Konfigurieren der RADIUS-Servereinstellungen

- Wählen Sie Serverdefinition aus. In diesem Beispiel ist Nach IP-Adresse ausgewählt. Geben Sie die IP-Adresse in das Feld Server-IP-Adresse/-Name ein.
- Legen Sie eine RADIUS-Priorität fest.

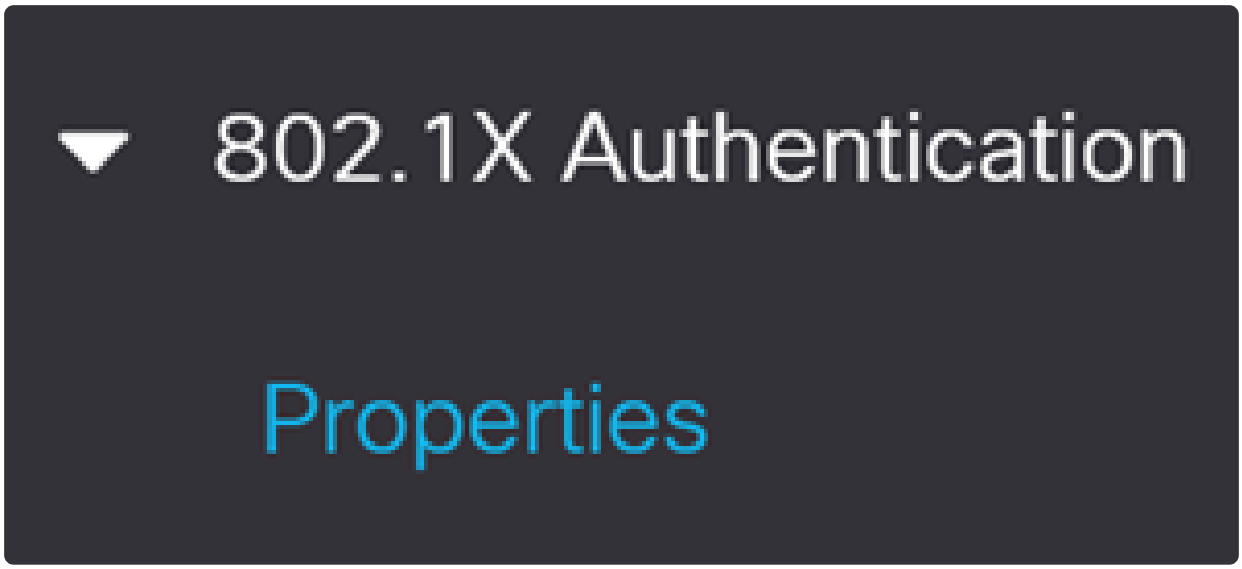
- Die Authentifizierungs- und Buchhaltungsports sind auf die Standardwerte gesetzt.
- Der Nutzungstyp ist 802.1x.

Klicken Sie auf Apply (Anwenden).



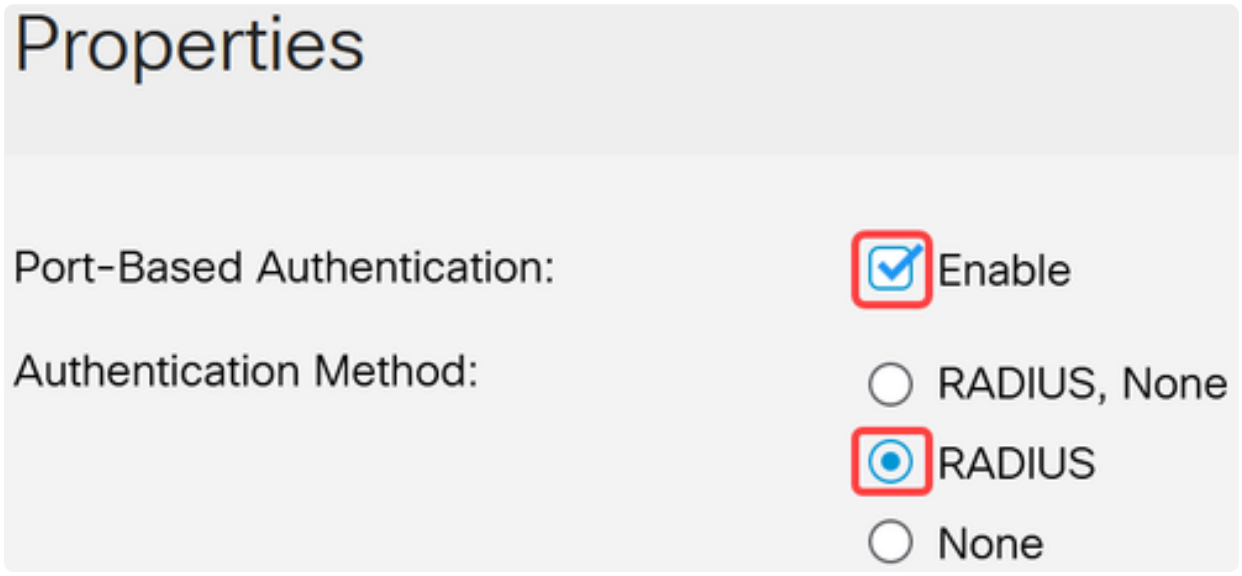
Schritt 6

Um die 802.1x-Authentifizierung zu konfigurieren, navigieren Sie zum Menü Security > 802.1x Authentication > Properties (Sicherheit > 802.1x-Authentifizierung > Eigenschaften).



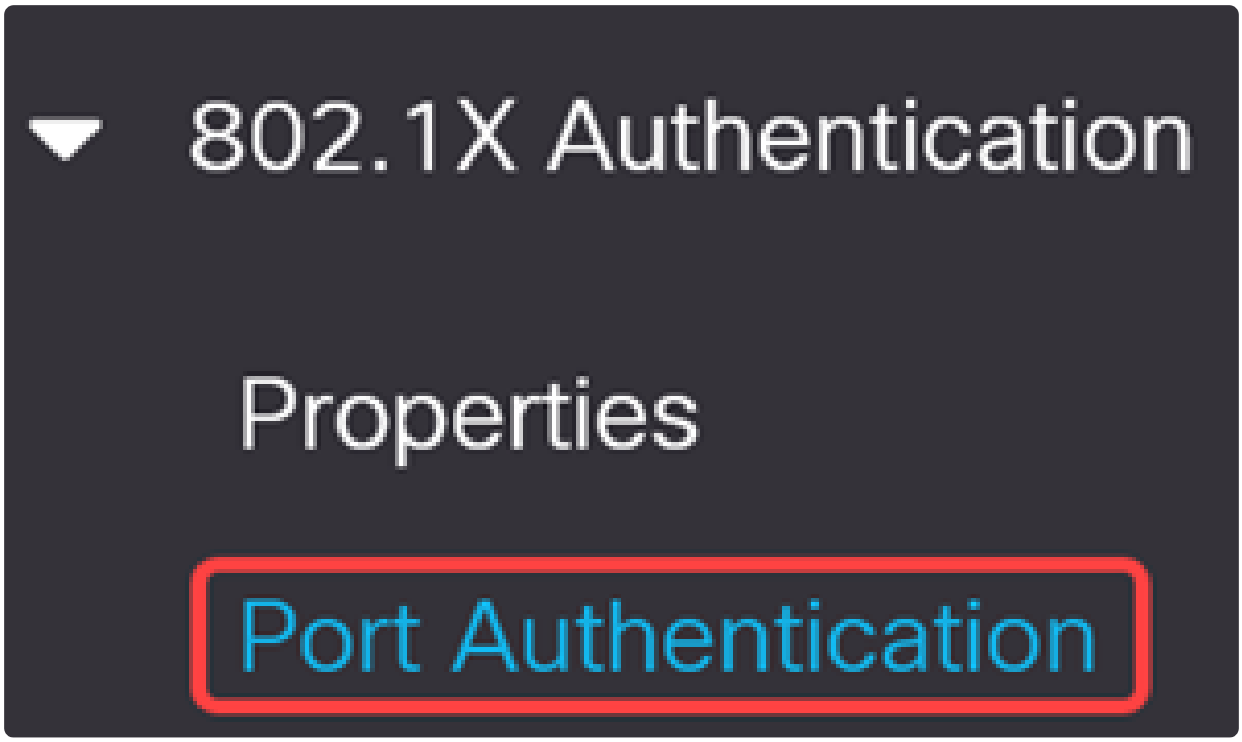
Schritt 7

Stellen Sie sicher, dass die portbasierte Authentifizierung aktiviert und die Authentifizierungsmethode auf RADIUS festgelegt ist.



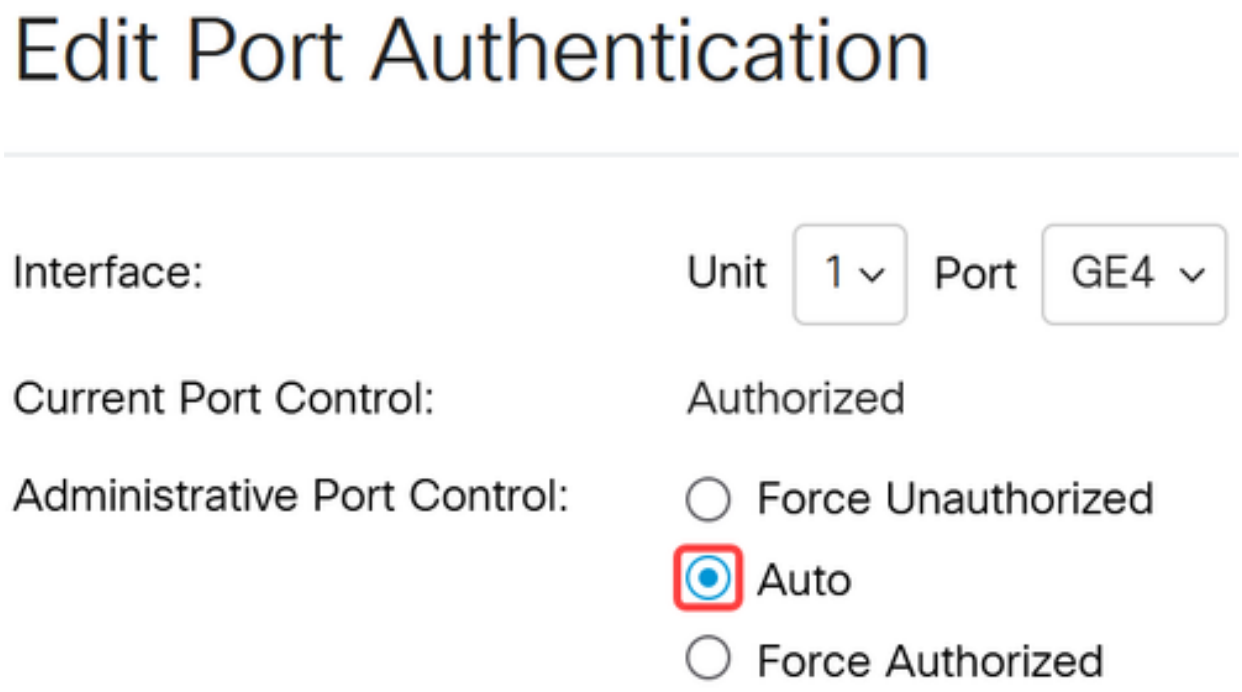
Schritt 8

Navigieren Sie zum Menü Port Authentication (Portauthentifizierung), wählen Sie den gewünschten Port aus, und klicken Sie auf Edit.



Schritt 9

Wählen Sie für die administrative Port-Steuerung die Option Auto (Automatisch) aus, mit der der Port auf Basis der RADIUS-Antwort zwischen dem autorisierten und dem nicht autorisierten Status umgeschaltet wird.

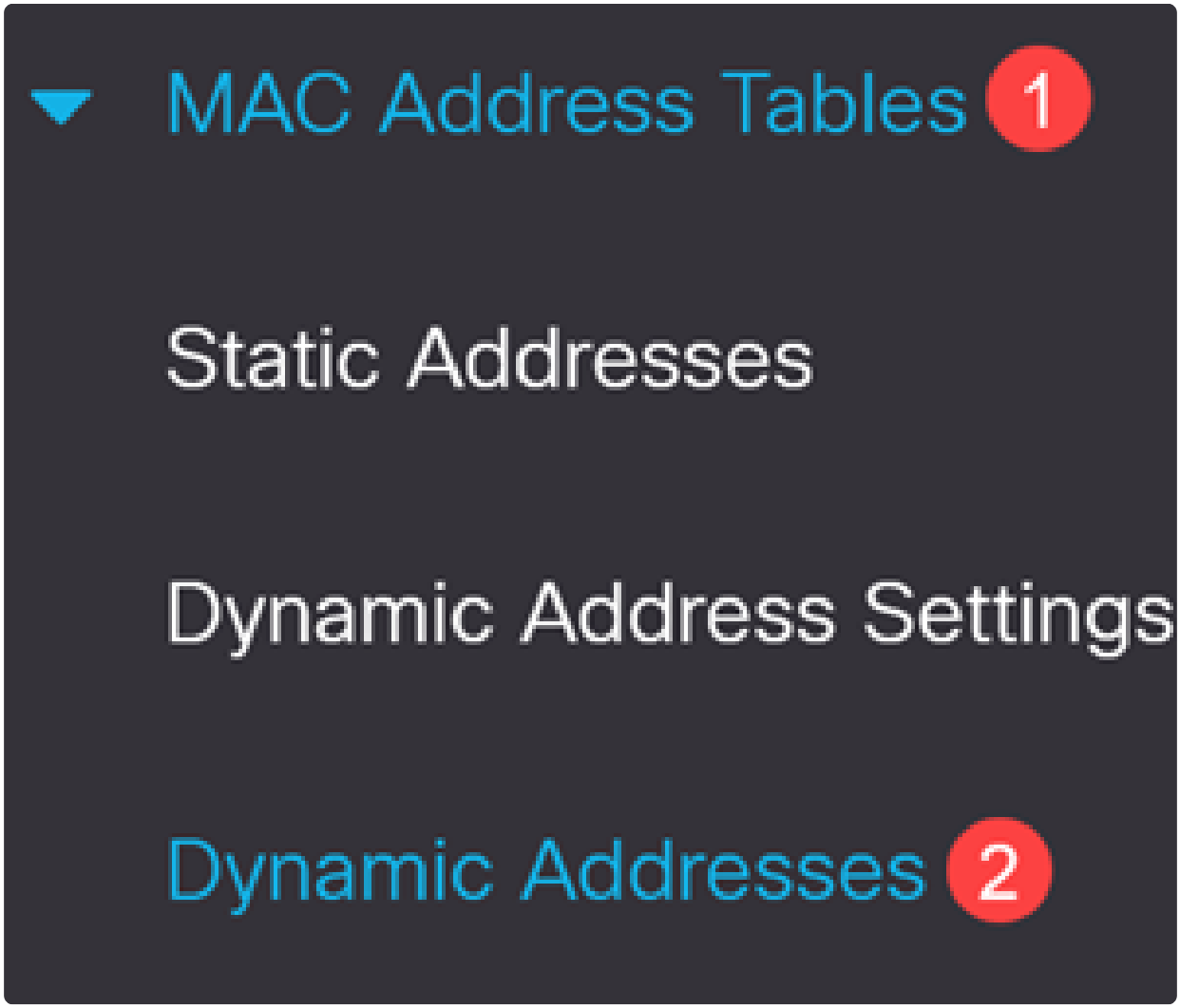


Schritt 10

Aktivieren Sie die 802.1x-basierte Authentifizierung, und klicken Sie auf Anwenden.

Schritt 11

Sie benötigen die MAC-Adresse für das Gerät am Port. Der CoA-Vorgang für die ISE wird auf diese MAC-Adresse angewendet. In diesem Beispiel ist dies Port 9. Navigieren Sie zu MAC Address Tables > Dynamic Addresses, um die Adresse abzurufen.

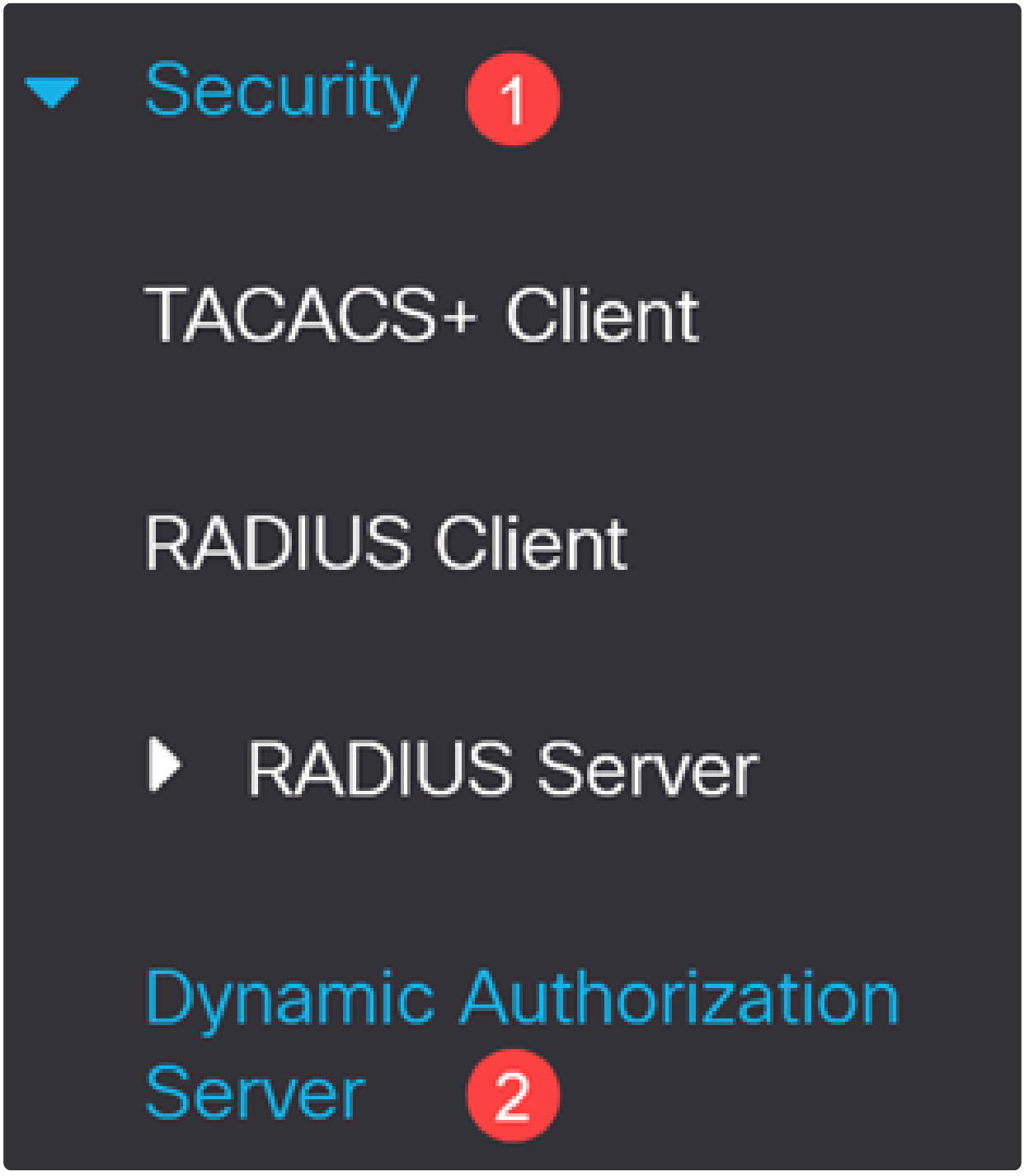


Schritt 12

Blättern Sie nach unten zum Port, und notieren Sie sich die MAC-Adresse.

Schritt 13

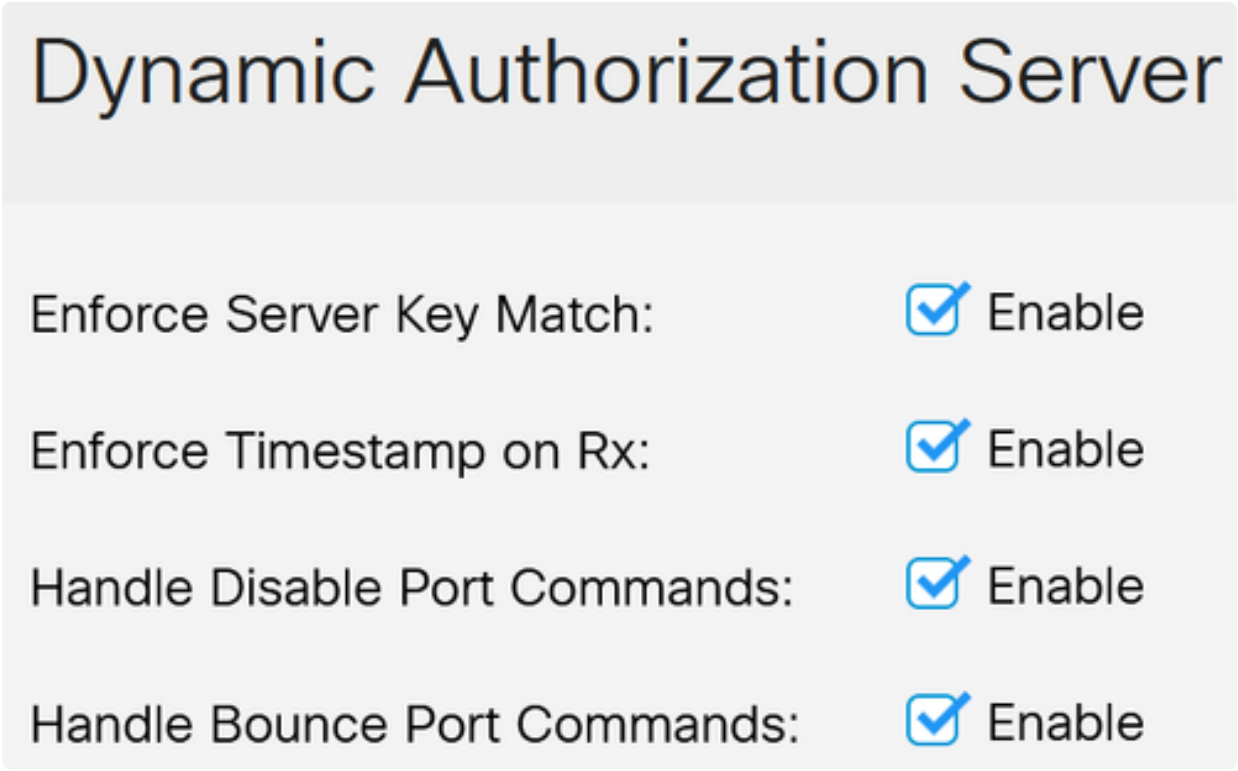
Navigieren Sie zu Sicherheit > Dynamic Authorization Server.



Schritt 14

Aktivieren Sie Folgendes:

- Serverschlüsselzuordnung erzwingen
- Zeitstempel auf Rx erzwingen
- Umgang mit Befehlen zum Deaktivieren von Ports
- Befehle des Bounce-Ports behandeln

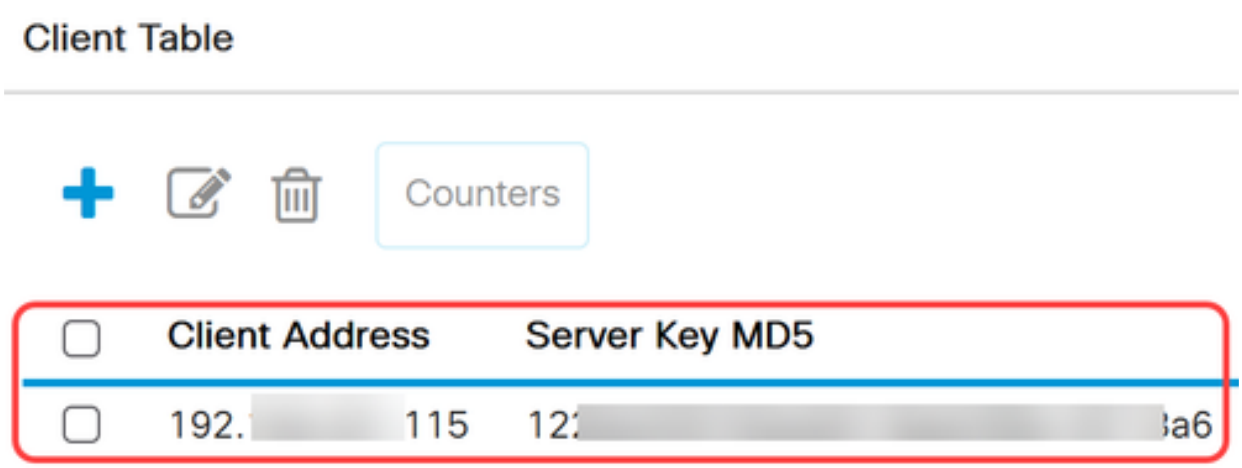


Schritt 15

Lassen Sie den UDP-Port auf dem Standardwert von 1700.

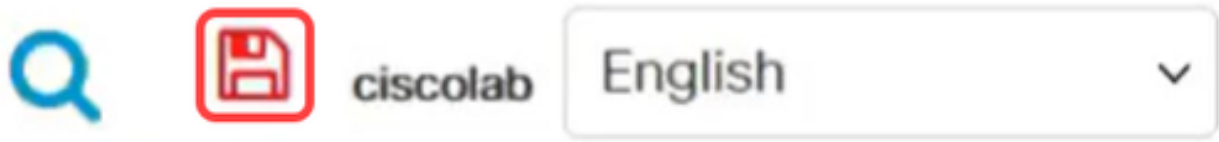
Schritt 16

Vergewissern Sie sich unter Client Table, dass der ISE-Server mit dem richtigen Serverschlüssel hinzugefügt wurde. Klicken Sie auf Apply (Anwenden).



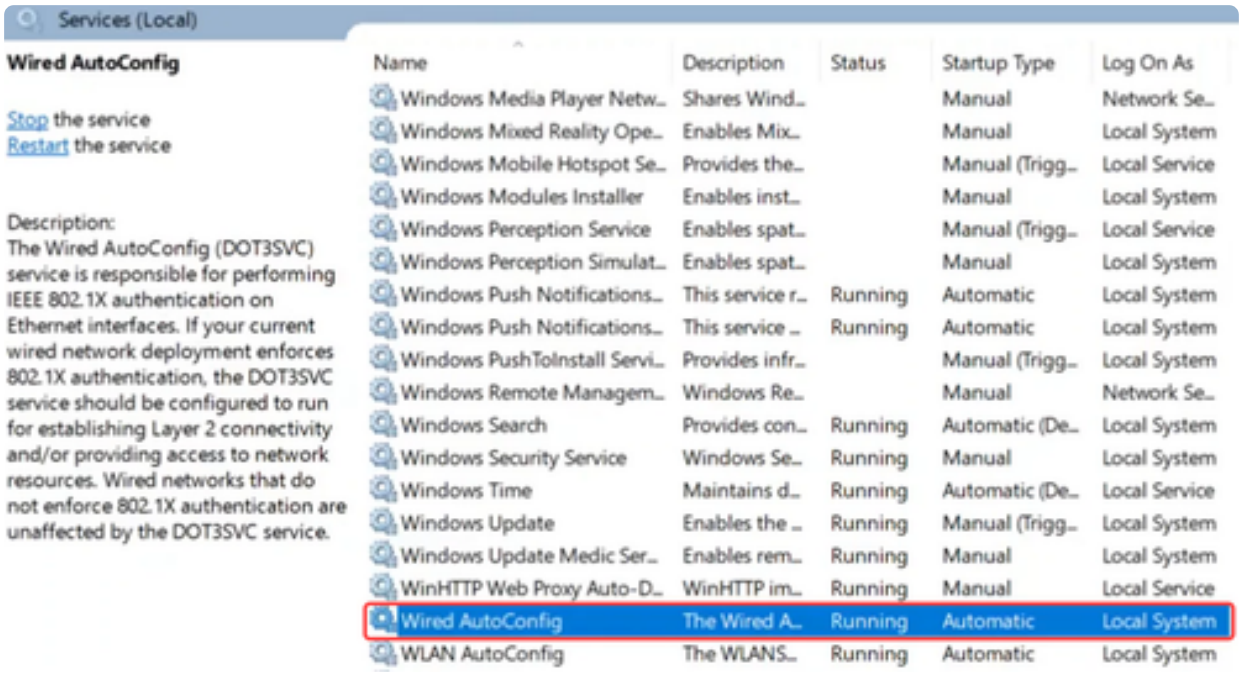
Schritt 17

Klicken Sie auf das rot blinkende Symbol Speichern, um die Konfigurationen zu speichern.



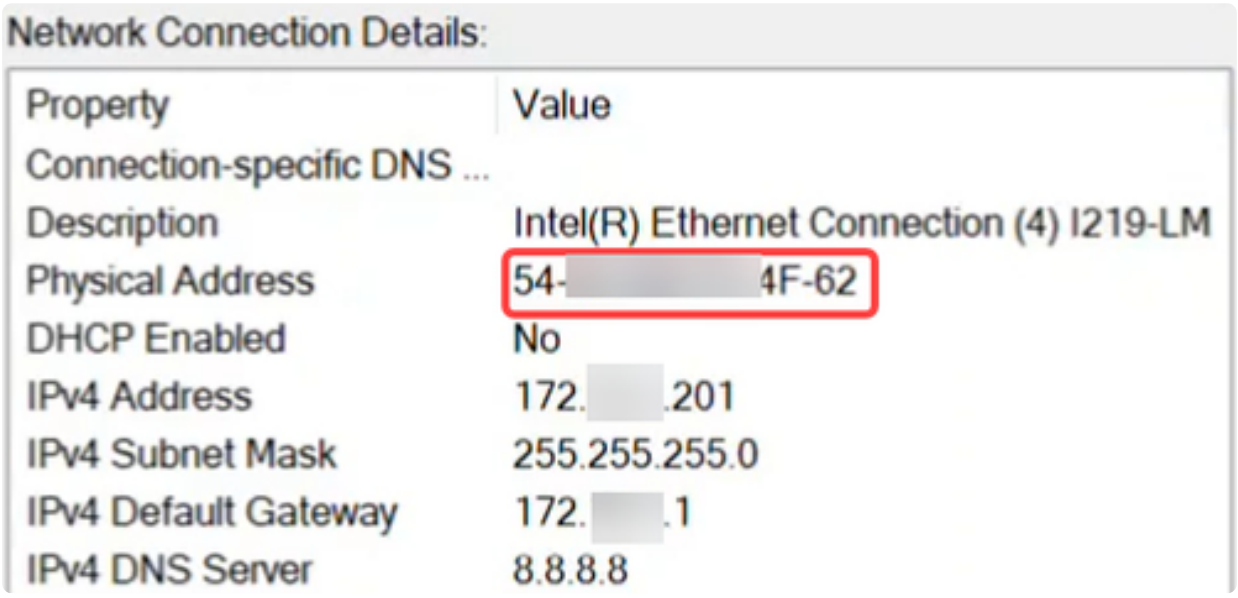
Schritt 18

Überprüfen Sie auf dem Client-Laptop, der mit Port 9 verbunden ist, ob der Wired AutoConfig-Service für die 802.1 X-Authentifizierung aktiviert ist.



Schritt 19

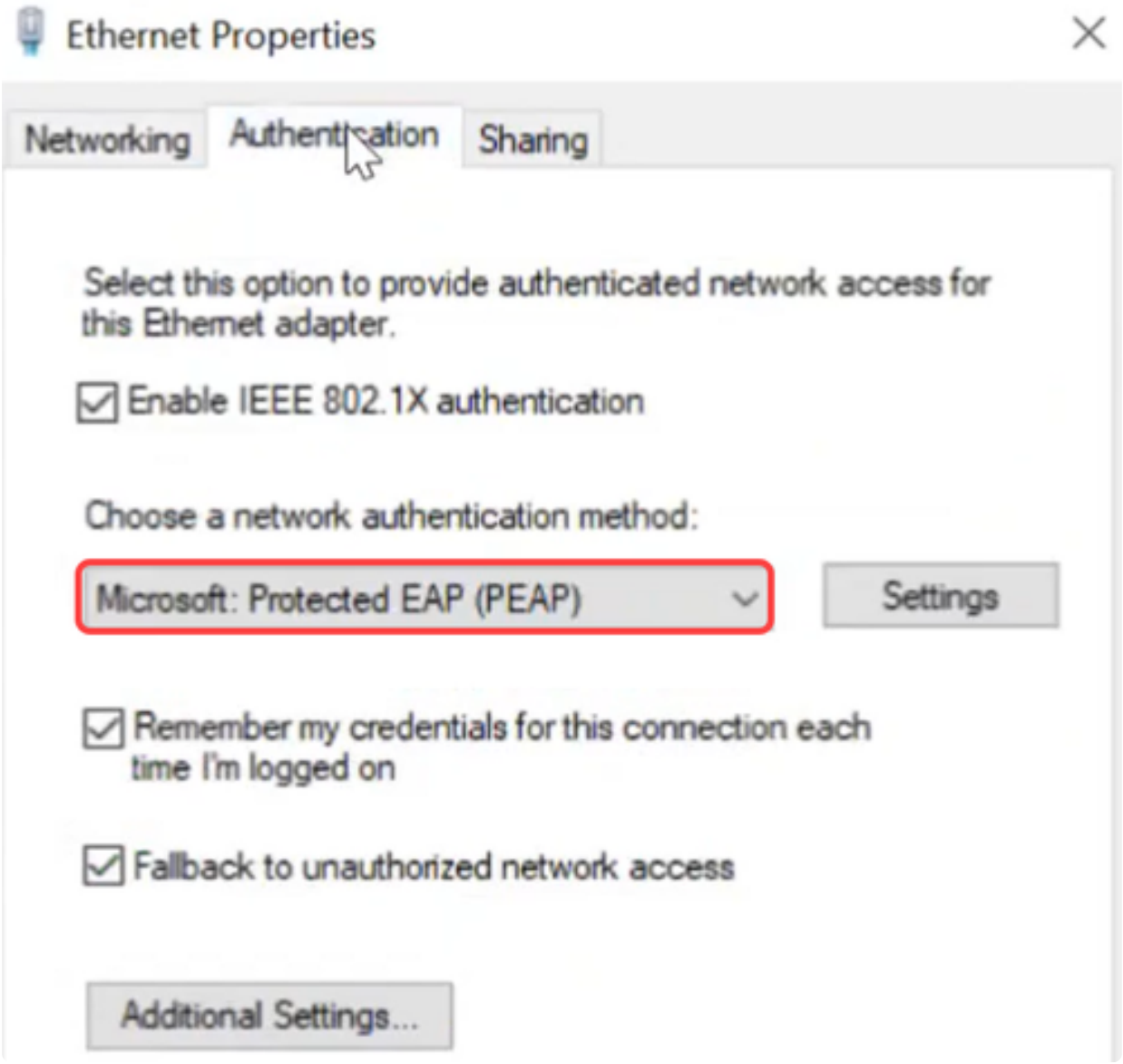
Überprüfen Sie in den Ethernet-Adaptereinstellungen, ob die MAC-Adresse übereinstimmt.



Schritt 20

Klicken Sie unter Ethernet-Einstellungen auf die Schaltfläche Eigenschaften, und stellen Sie auf der Registerkarte Authentifizierung sicher, dass die Kontrollkästchen aktiviert sind. Stellen Sie außerdem sicher, dass die Authentifizierungsmethode PEAP

(Protected EAP) ist.

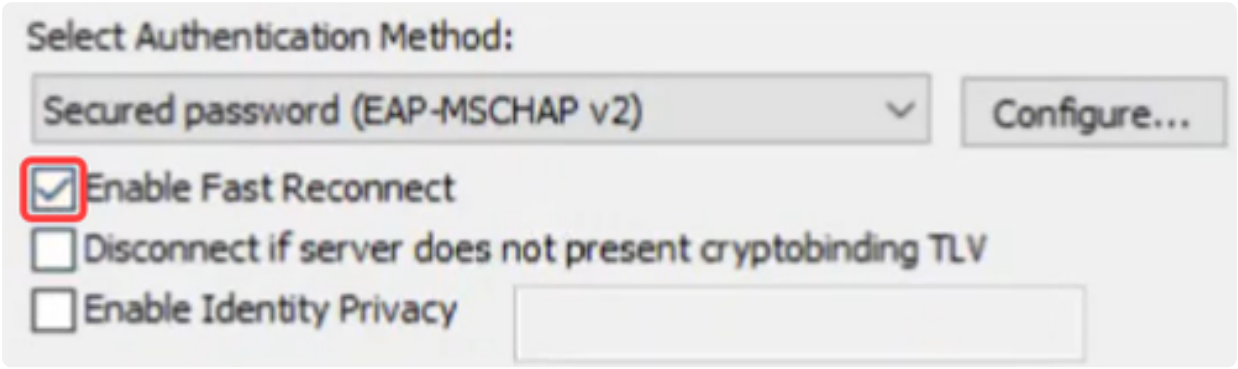


Schritt 21

Klicken Sie auf die Schaltfläche Einstellungen, um sicherzustellen, dass das Kontrollkästchen neben Identität des Servers durch Validierung des Zertifikats überprüfen deaktiviert ist.

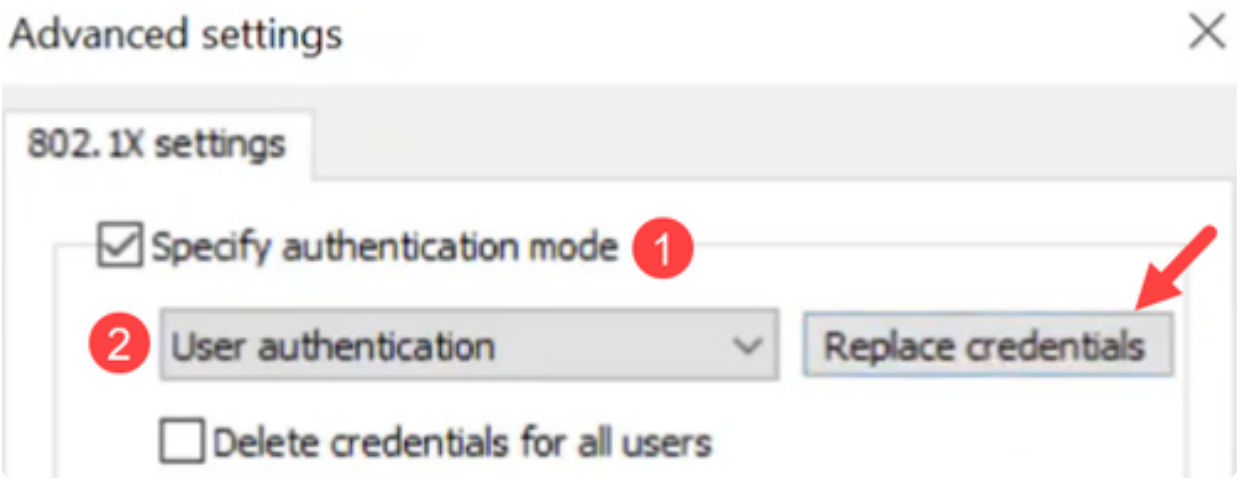
Schritt 22

Aktivieren Sie das Kontrollkästchen "Fast Reconnect".



Schritt 23

Vergewissern Sie sich unter Zusätzliche Einstellungen, dass der Authentifizierungsmodus angeben aktiviert ist und dass im Dropdown-Menü die Option Benutzerauthentifizierung ausgewählt ist. Sie können die auf der ISE erstellten Anmeldeinformationen speichern oder durch die Schaltfläche Anmeldeinformationen ersetzen.



CoA-Betrieb

Aktivieren Sie vor dem Initiieren des CoA-Vorgangs die Paketerfassung auf dem Switch.

Schritt 1

Melden Sie sich auf PuTTY bei Ihrem Catalyst Switch an, und geben Sie die Puffergröße und den Erfassungsmodus mithilfe des Befehls monitor capture cap1 buffer size 20 circle an.

Schritt 2

Legen Sie die Kontrollebene als beides fest, indem Sie den Befehl monitor capture cap1 control-plane both verwenden.

Schritt 3

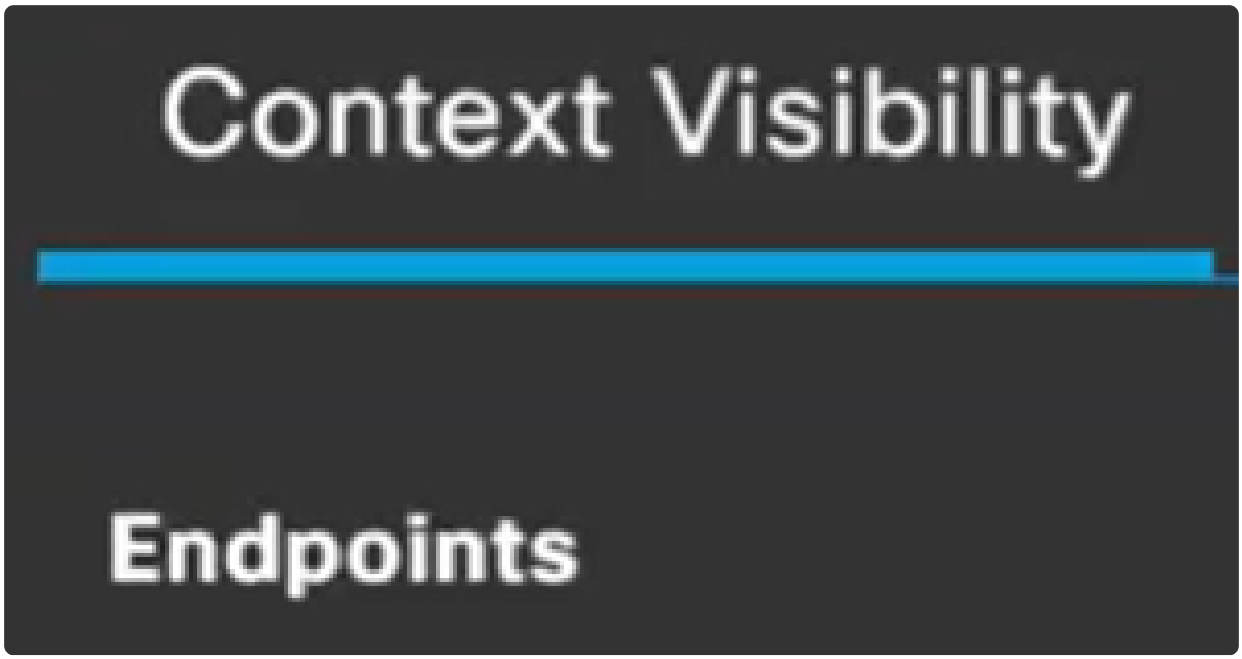
Geben Sie die Abgleichskriterien ein. Der Befehl hierfür lautet monitor capture cap1 match any.

Schritt 4

Starten der Paketerfassung

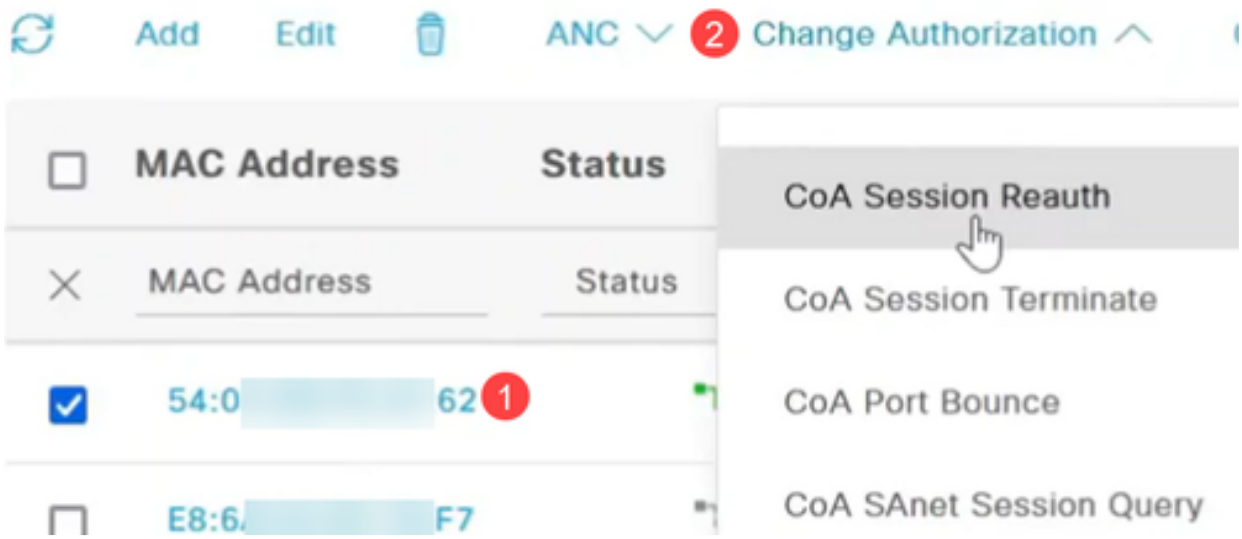
Schritt 5

Navigieren Sie auf der ISE-Schnittstelle unter "Context Visibility" zur Option Endgeräte.



Schritt 6

Wählen Sie die MAC-Adresse aus, und wählen Sie im Dropdown-Menü Change of Authorization (Autorisierungsänderung) die CoA-Operation aus. In diesem Beispiel ist CoA Session Reauth ausgewählt. Dadurch wird eine erneute Authentifizierung am Port erzwungen, indem ein CoA-Paket mit dem Befehl reAuthenticate gesendet wird.



Schritt 7

Wechseln Sie zurück zum PuTTY-Terminal, um zu überprüfen, ob der CoA-Vorgang erfolgreich war.

```
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"
```

Schritt 8

Wenn Sie CoA Session Terminate (CoA-Sitzung beenden) auswählen, wird auf Basis einer Verwaltungsanfrage eine Verbindungstrennungsanfrage mit dem Befehl terminate gesendet.

```
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
```

Schritt 9

Die CoA-Port-Bounce-Option sendet ein CoA-Anforderungspaket mit einem Bounce-Host-Port-Befehl, wobei der Port am Switch deaktiviert und erneut aktiviert wird. Der Netzwerkadapter ist 10 Sekunden lang offline und wird nicht autorisiert. Es wird das Comeback online, wird autorisiert und kann Pakete weiterleiten.

```
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
```

Schritt 10

Bei Beendigung der CoA-Sitzung mit Port-Bounce wird die vorhandene Sitzung beendet, der Port wird für 10 Sekunden zurückgewiesen, und die Autorisierung wird aufgehoben. Anschließend ist er wieder online, wird autorisiert und kann Pakete weiterleiten.

```
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
```

Schritt 11

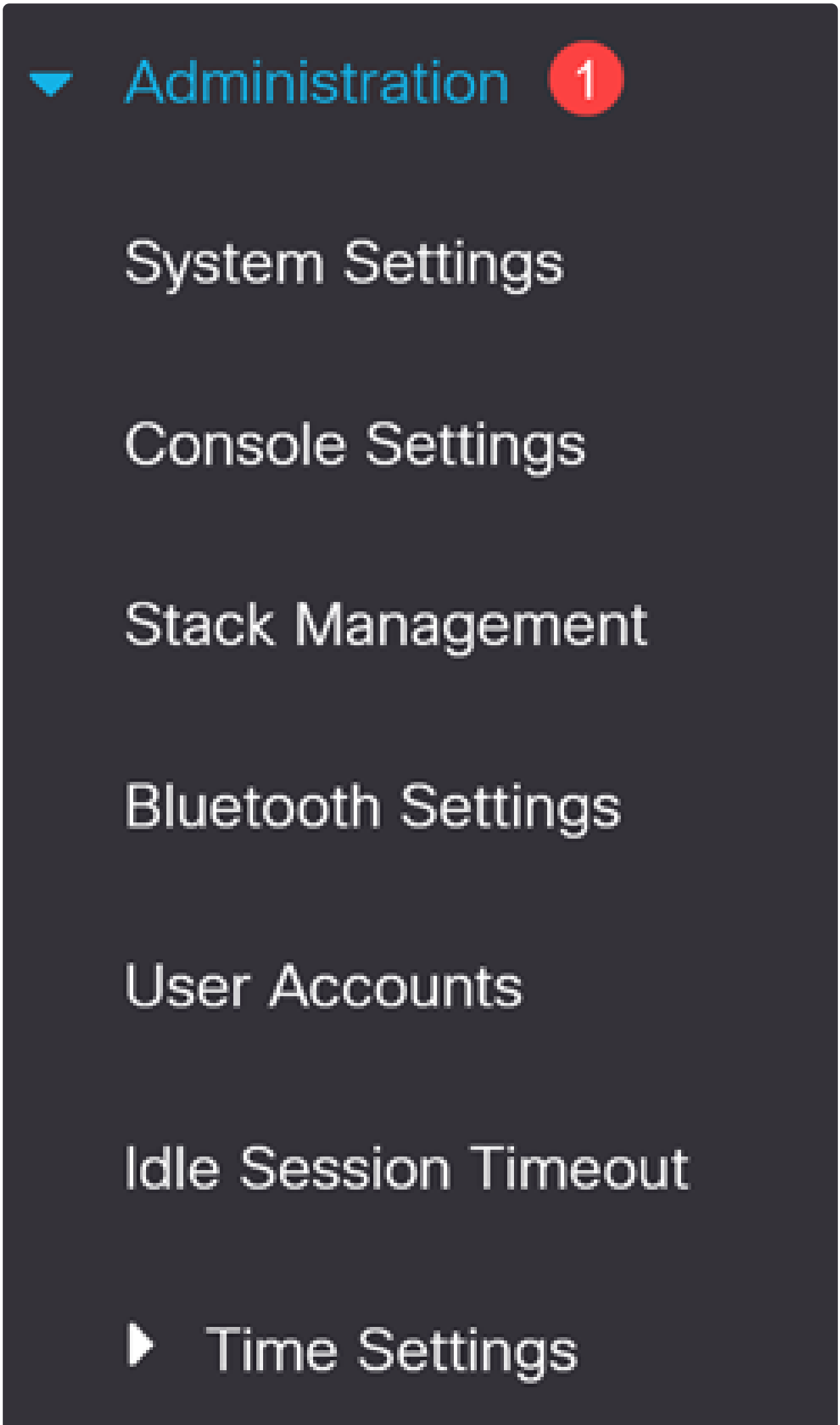
Bei Beendigung einer CoA-Sitzung mit deaktiviertem Port wird die Sitzung beendet und der Port vom Administrator deaktiviert.

Schritt 12

Um die Paketerfassung zu beenden, verwenden Sie den Befehl monitor capture cap1 stop.

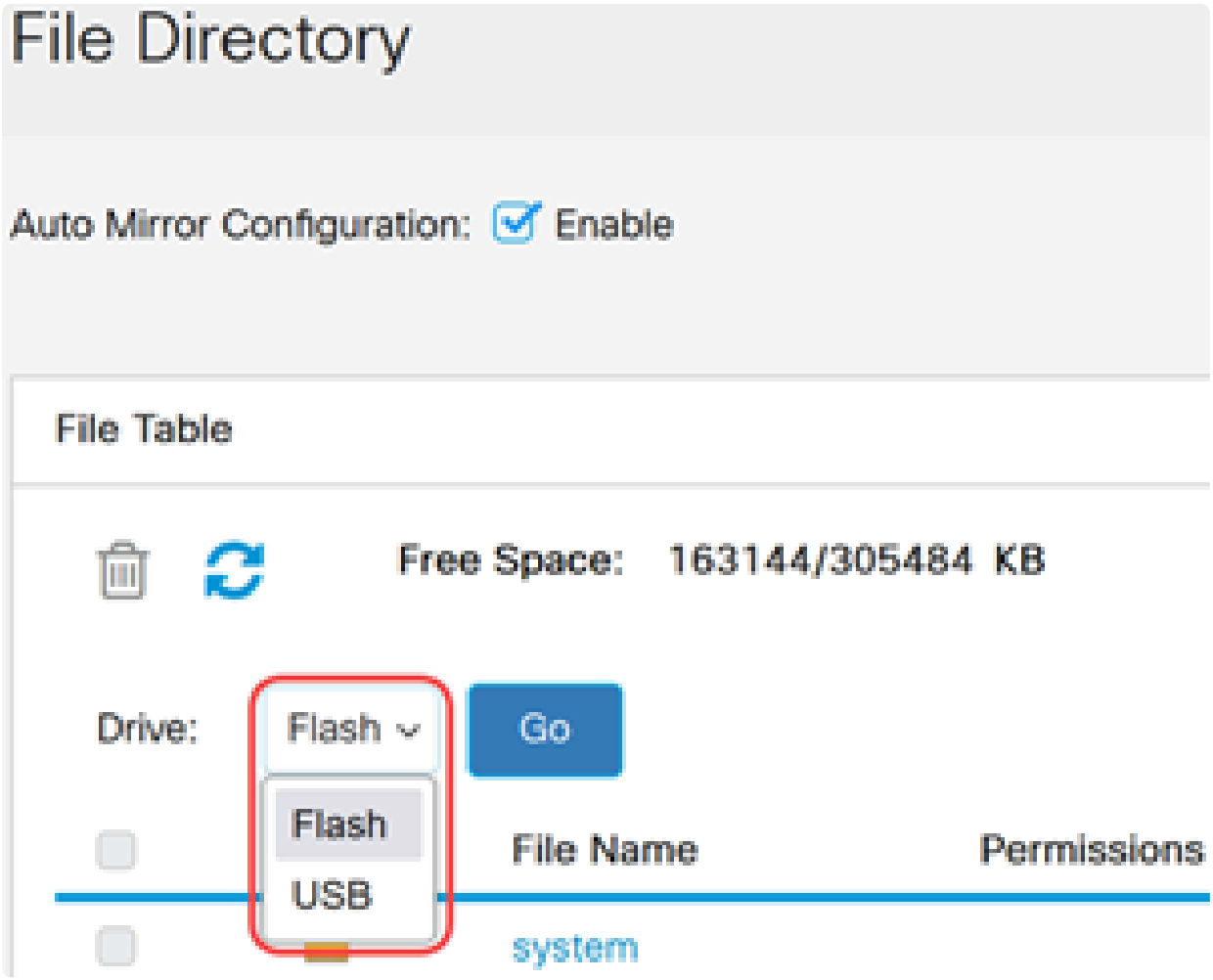
Schritt 13

Um die Dateien zu kopieren, navigieren Sie zu Administration > File Management > File Directory.


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

Schritt 14

Der Standard-Flash ist verfügbar. Alternativ können Sie USB aus dem Dropdown-Menü Drive (Laufwerk) auswählen.



Schlussfolgerung

Jetzt wissen Sie alles über die ISE und wie Sie CoA in den Catalyst Switches der Serie 1300 konfigurieren.

Weitere Informationen finden Sie im Video unten.

Video zu diesem Artikel anzeigen ...

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.