Webユーザインターフェイスを使用したCatalyst 1300での認可変更の設定

目的

この記事の目的は、Webユーザインターフェイス(UI)を使用してCatalyst 1300スイッチで認可変更(CoA)を設定する方法を説明することです。

該当するデバイスとソフトウェアバージョン

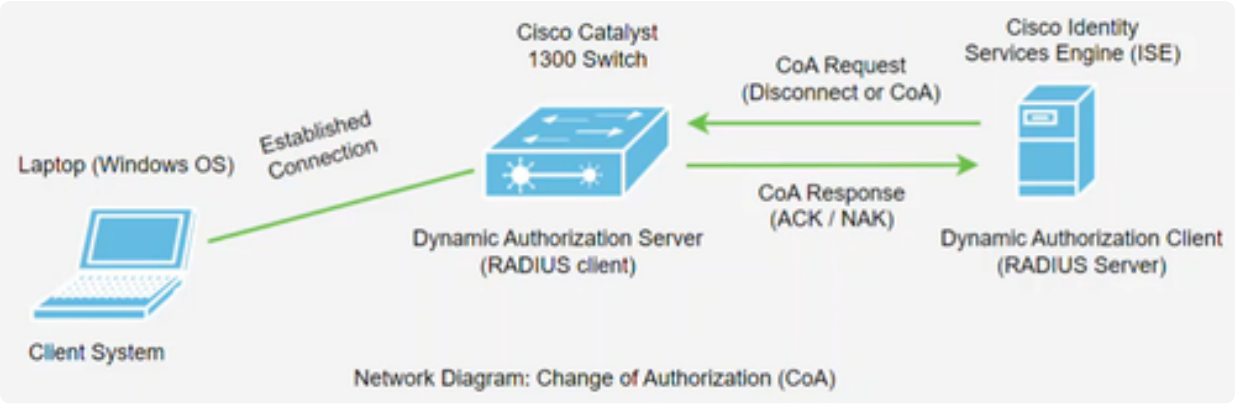
- Catalyst 1300スイッチ| 4.1.6.53

はじめに

認可変更(CoA)はRADIUSプロトコルの拡張機能であり、認証された後で認証、認可、アカウンティング(AAA)またはdot1xユーザセッションのプロパティを変更できます。AAA内のユーザまたはグループのポリシーが変更された場合、管理者はCisco Identity Services Engine(ISE)などのAAAサーバからRADIUS CoAパケットを送信して、認証を再初期化し、新しいポリシーを適用できます。

Cisco Identity Services Engine(ISE)は、完全な機能を備えたネットワークベースのアクセスコントロールおよびポリシー適用エンジンです。セキュリティの分析と適用、RADIUSおよびTACACSサービス、ポリシーの配布などを提供します。Cisco ISEは現在、Catalyst 1300スイッチ用にサポートされている唯一のCoAダイナミック認可クライアントです。詳細については、『ISE管理ガイド』を参照してください。

この機能には、Dynamic Authorization Client（RADIUSサーバ）とDynamic Authorization Server（Catalystスイッチ）間の通信が必要です。 次のネットワーク図に示すように、動的認可サーバは接続解除メッセージまたはCoAメッセージを動的認可サーバに送信し、スイッチが応答を返します。



CoAのサポートは、ファームウェアバージョン4.1.3.36でCatalyst 1300スイッチに追加されました。これには、ユーザの接続解除と、ユーザセッションに適用される認可の変更のサポートが含まれます。このデバイスは、次のCoAアクションをサポートしています。

- セッションの切断
- ホストポートのCoAコマンドを無効にする
- Bounce host port CoAコマンド
- Reauthenticate host CoAコマンド

コマンドラインインターフェイス(CLI)を使用してCoAを設定するには、『CLIを使用したCatalyst 1300スイッチでの認可変更の設定』を参照してください。

目次

ISEでのCatalyst 1300 RADIUSクライアントの設定

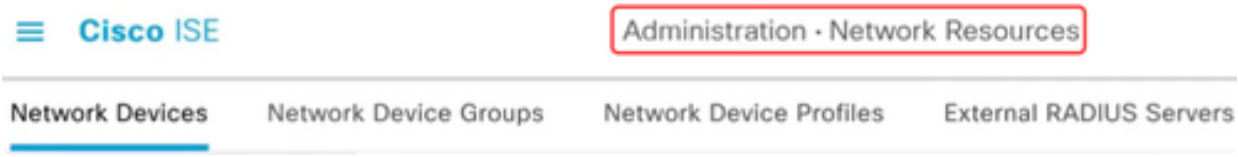
この例では、Cisco ISEサーババージョン3.2が使用されます。ISEの概要については、Cisco Identity Services Engineの製品ページを確認してください。

> Note:
> CoAはISEバージョン2.7以降でサポートされています。

Cisco ISEサーバの導入後、ログインしてWeb UIにアクセスします。

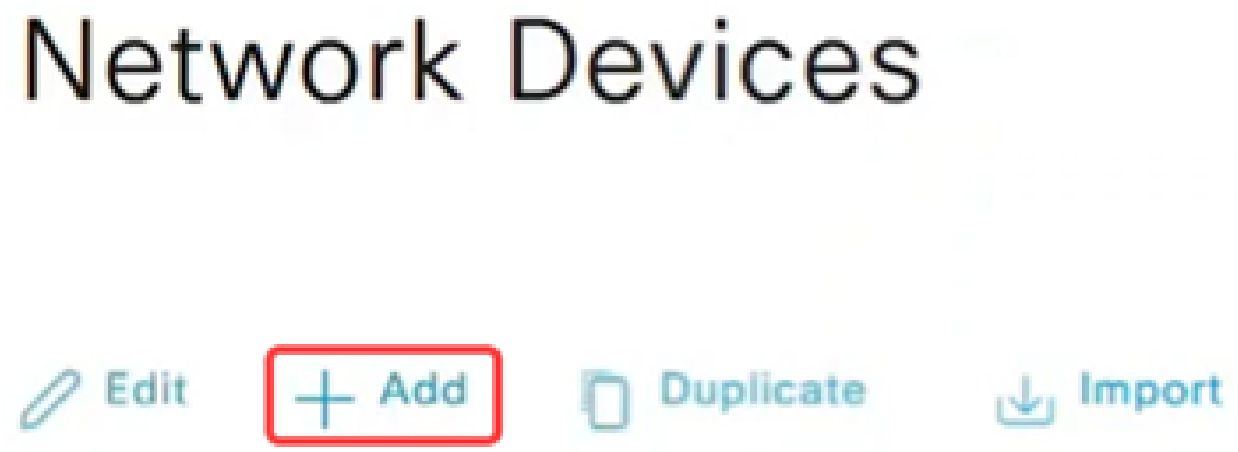
手順 1

ネットワークデバイスを追加するには、Administration > Network Resourcesメニューに移動します。



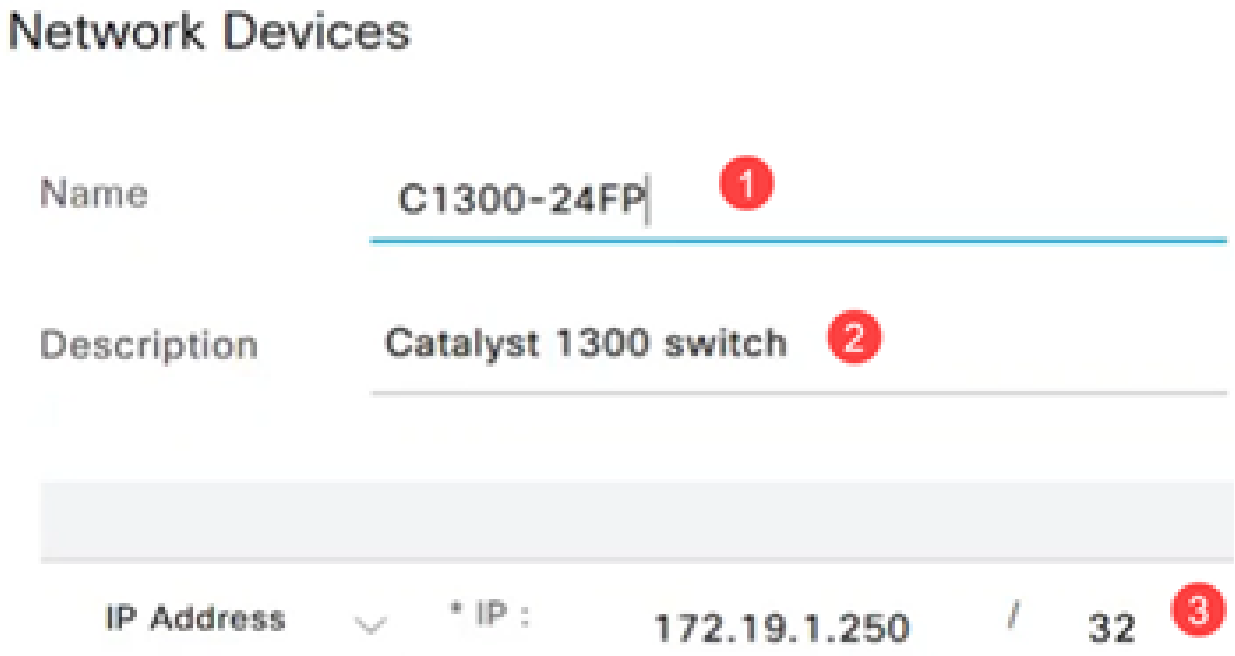
手順 2

+ Addボタンをクリックします。



手順 3

Catalystスイッチの名前、説明、およびIPアドレスを入力します。

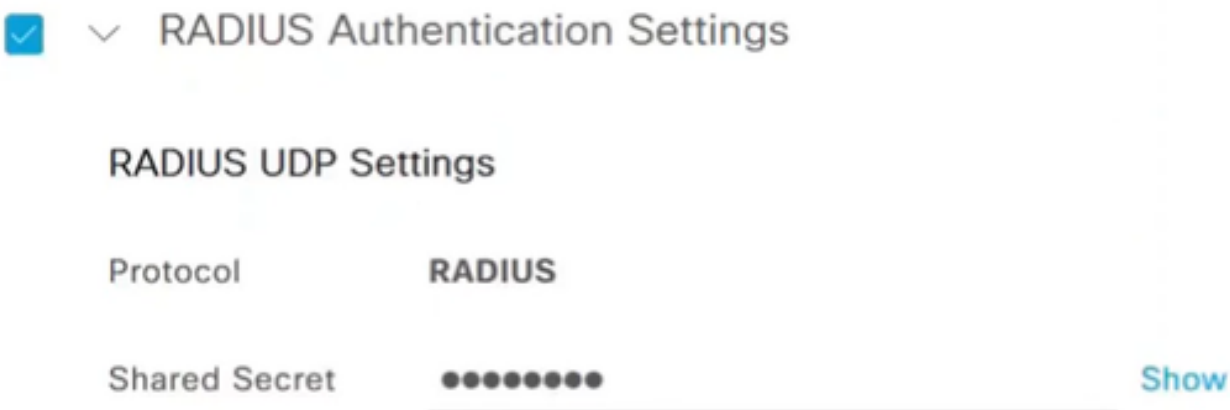


手順 4

Device Profileドロップダウンメニューから、Ciscoを選択します。

手順 5

共有秘密を入力して、RADIUS認証設定を設定します。



手順 6

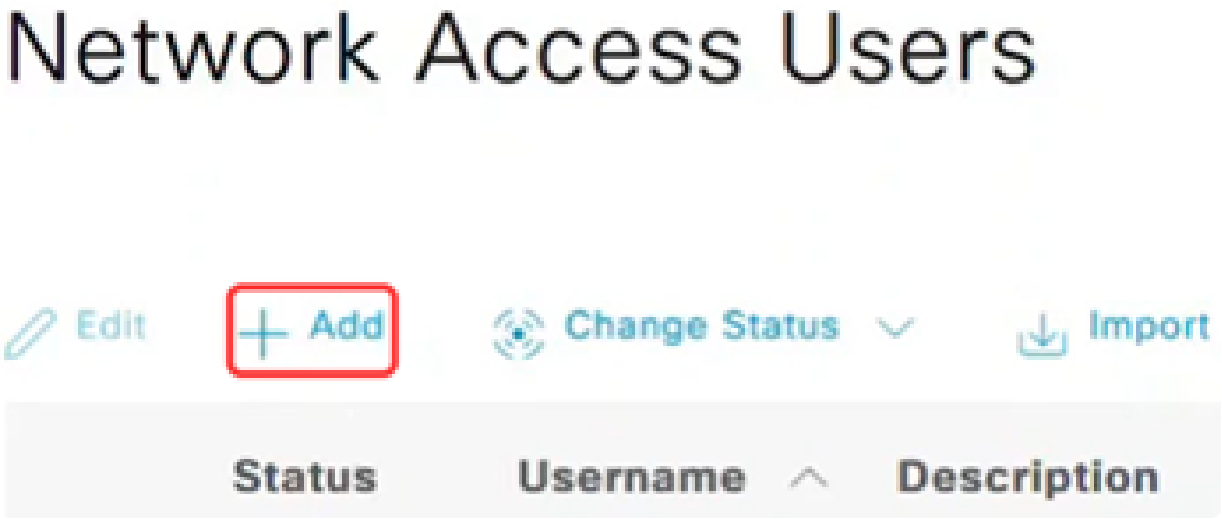
CoAポート番号を入力します。デフォルト ポートは 1700 です。

ステップ7

次に、Administration > Identity Managementの順に移動し、Network Access Usersを選択します。

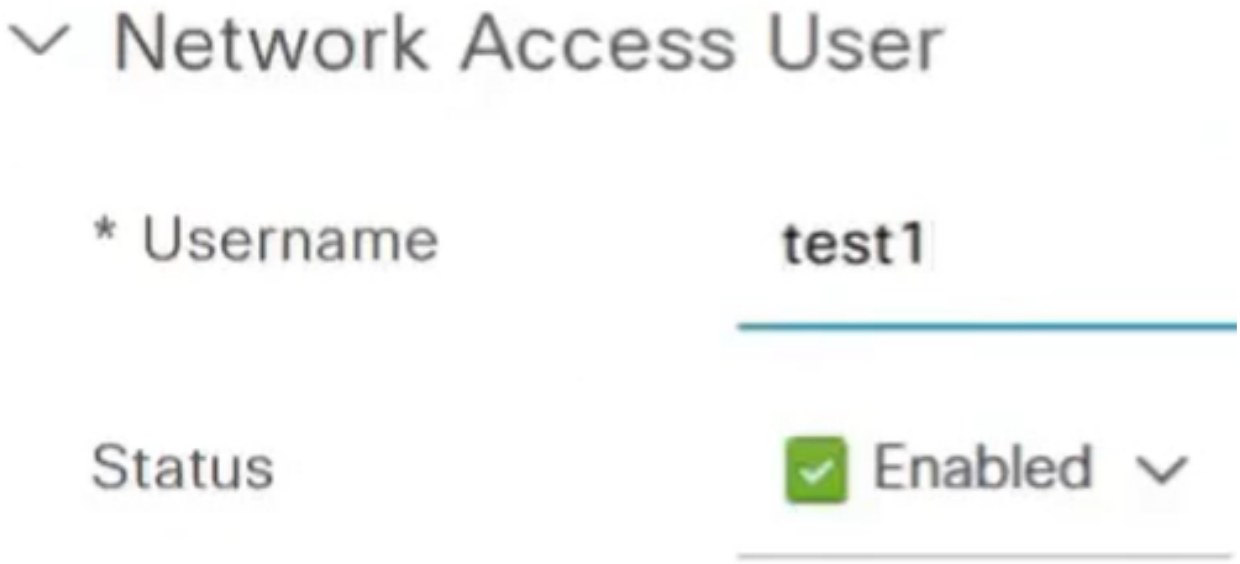
手順 8

ユーザ名とパスワードを定義するには、+Add記号をクリックします。



手順 9

ユーザ名とパスワードを入力し、ページの下部にあるSaveをクリックします。



Catalyst 1300スイッチでの設定

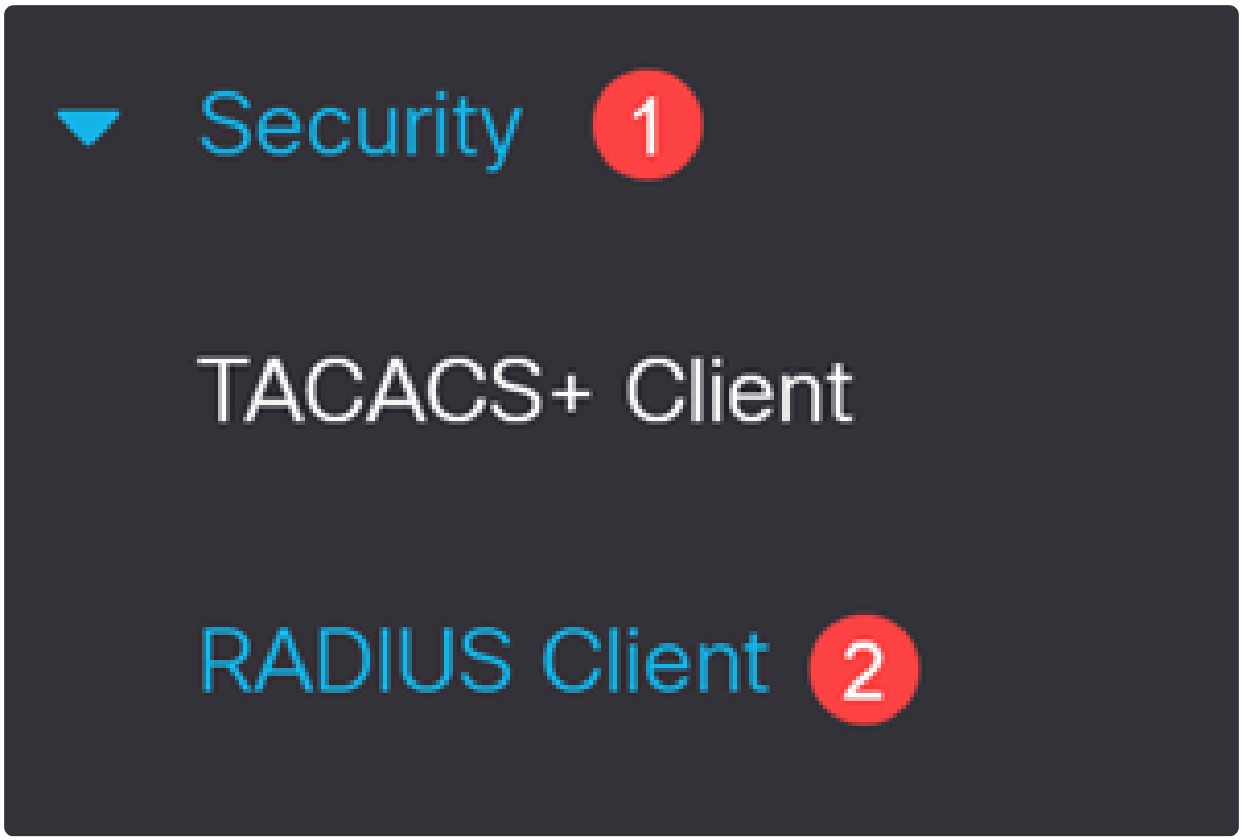
手順 1

Catalyst 1300スイッチにログインし、Advancedモードを選択します。この例では、C1300-24FP-4Xが使用されています。

> Note:
> CoAのサポートは、ファームウェアバージョン4.1.3.36でCatalyst 1300スイッチに追加されました。

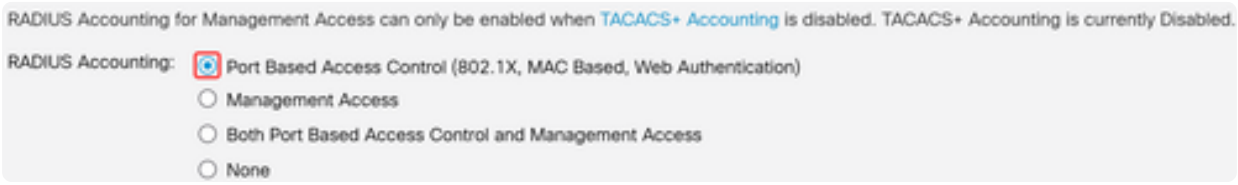
手順 2

ナビゲーションペインで、Security > RADIUS Clientの順に選択します。



手順 3

RADIUS AccountingをPort Based Access Controlに設定します。



手順 4

ISEサーバを追加するには、RADIUSテーブルまで下にスクロールし、プラス記号のアイコンをクリックします。

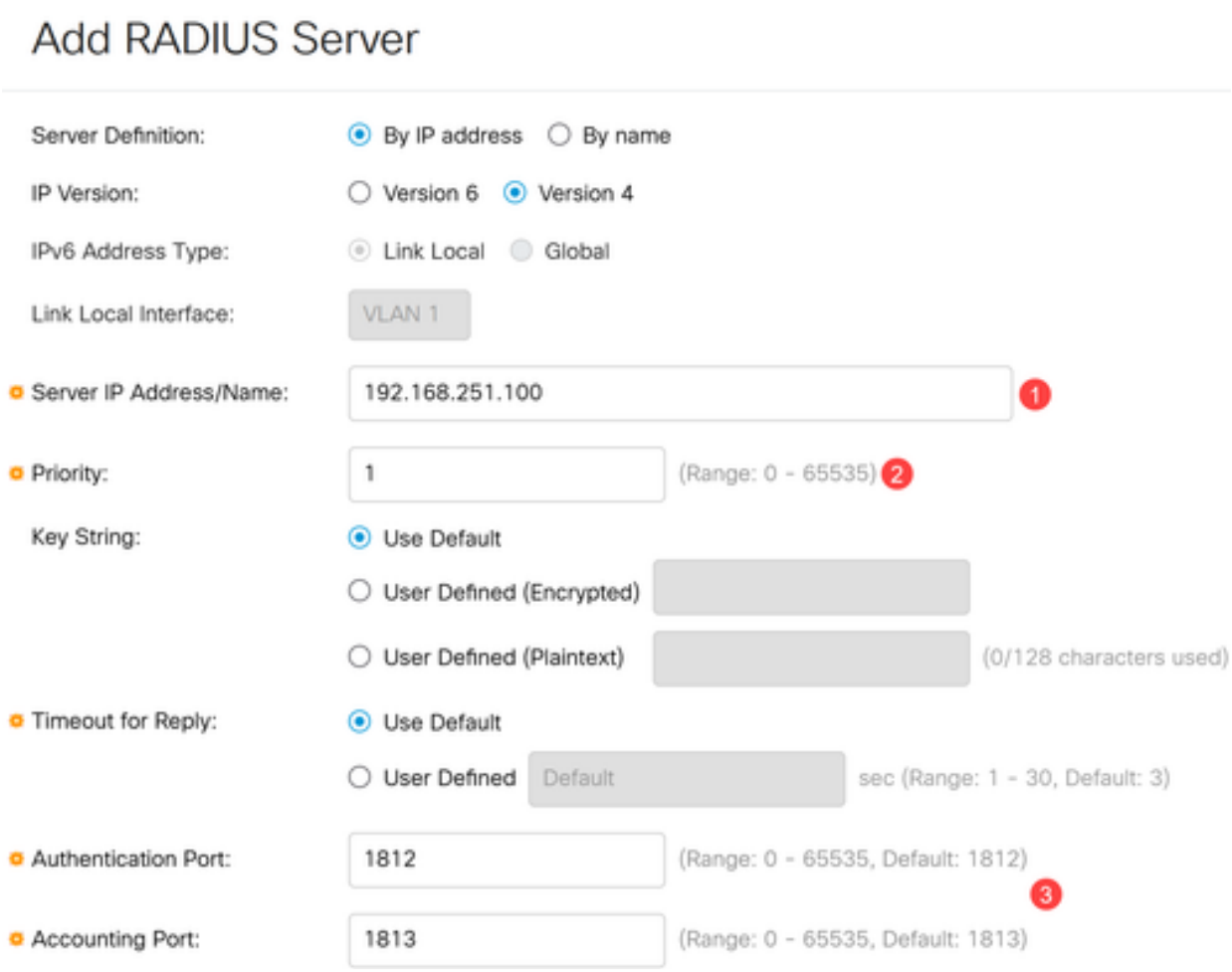
手順 5

RADIUSサーバの設定を行います。

- Server Definitionを選択します。この例では、By IP addressが選択されています。Server IP Address/NameフィールドにIPアドレスを入力します。
- RADIUSの優先度を設定します。

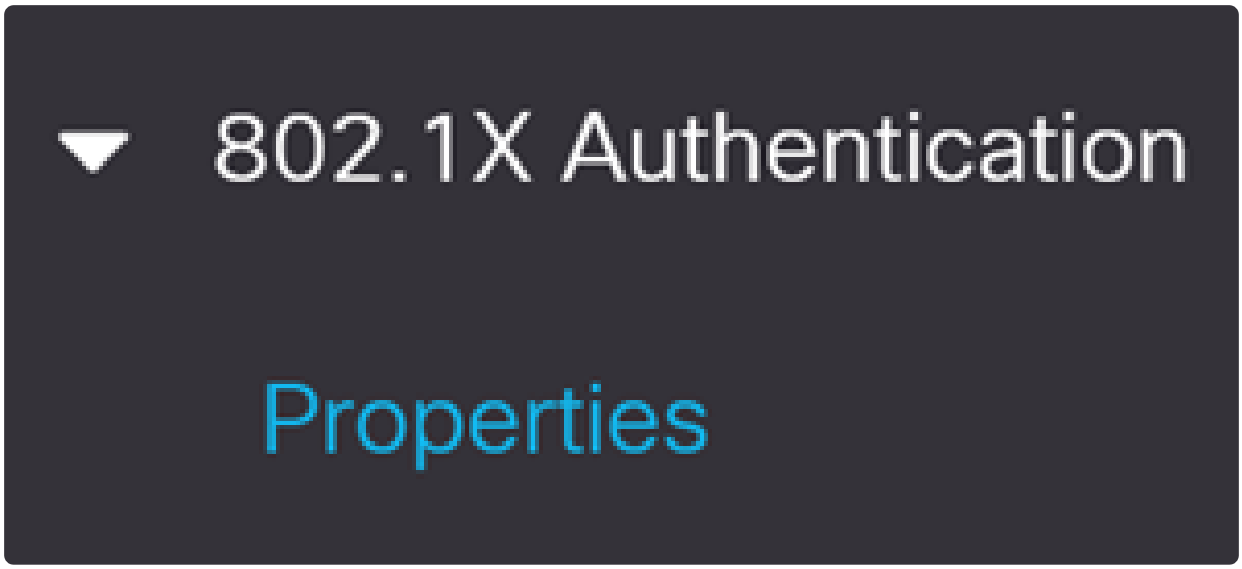
- 認証ポートとアカウンティングポートはデフォルトに設定されています。
- Usage Typeは802.1xです。

[APPLY] をクリックします。



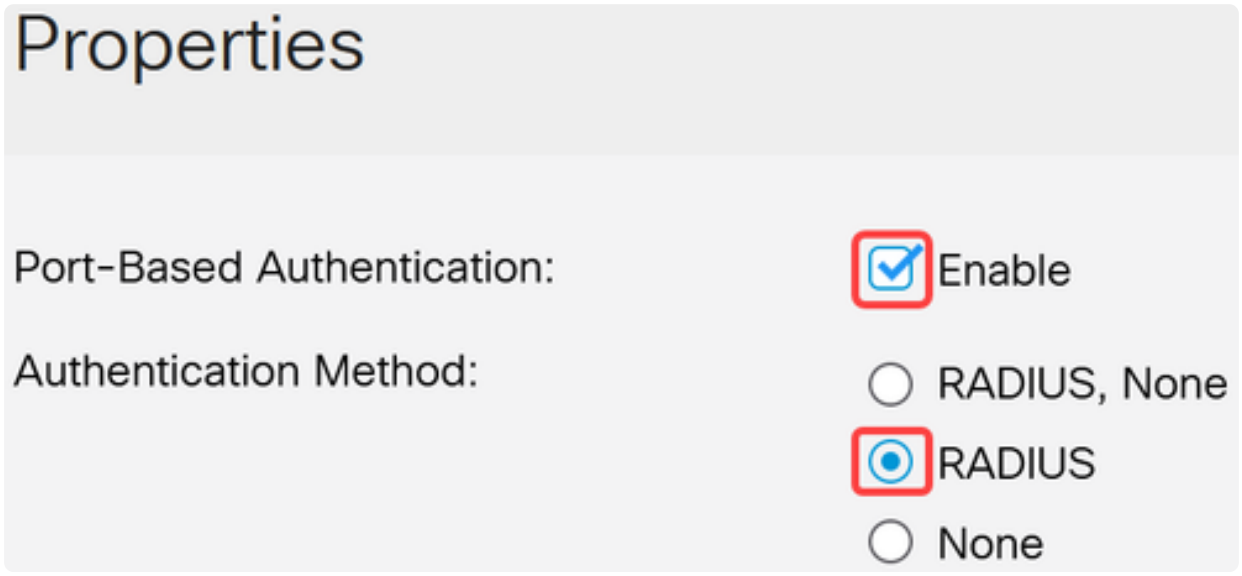
手順 6

802.1x認証を設定するには、Security > 802.1X Authentication > Propertiesメニューに移動します。



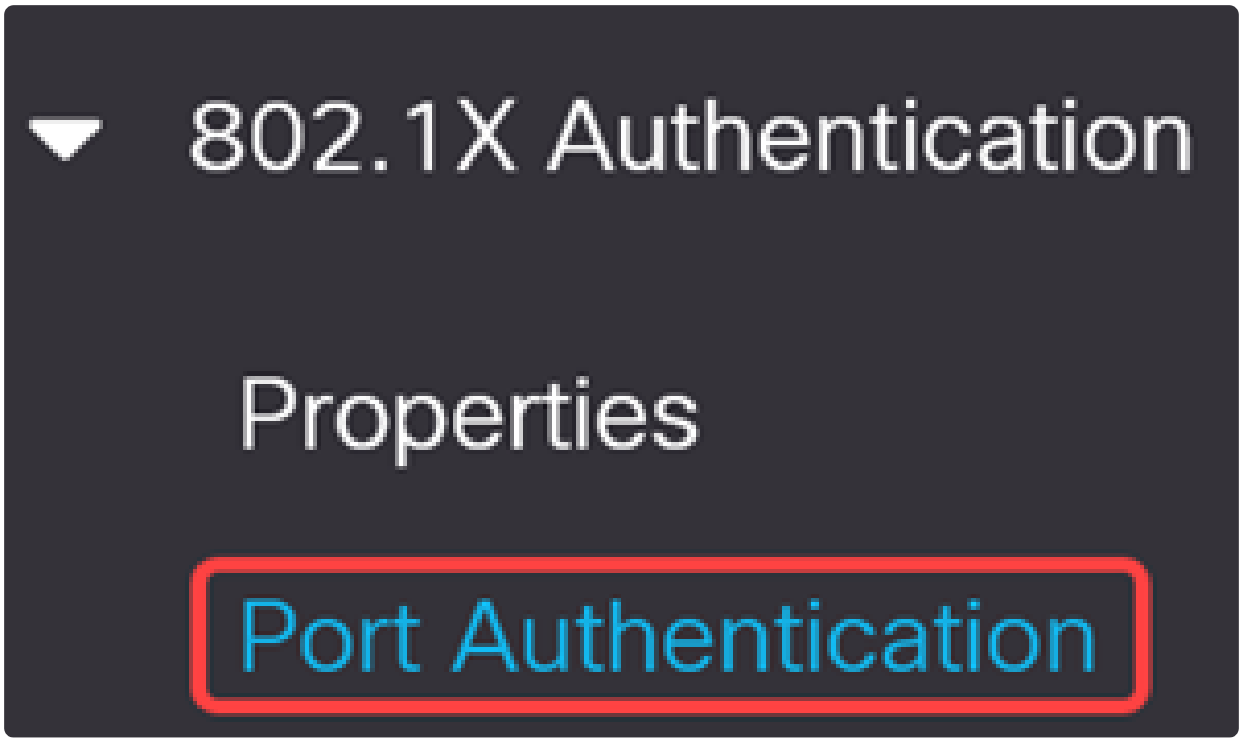
ステップ7

Port-Based Authenticationが有効で、Authentication MethodがRADIUSに設定されていることを確認します。



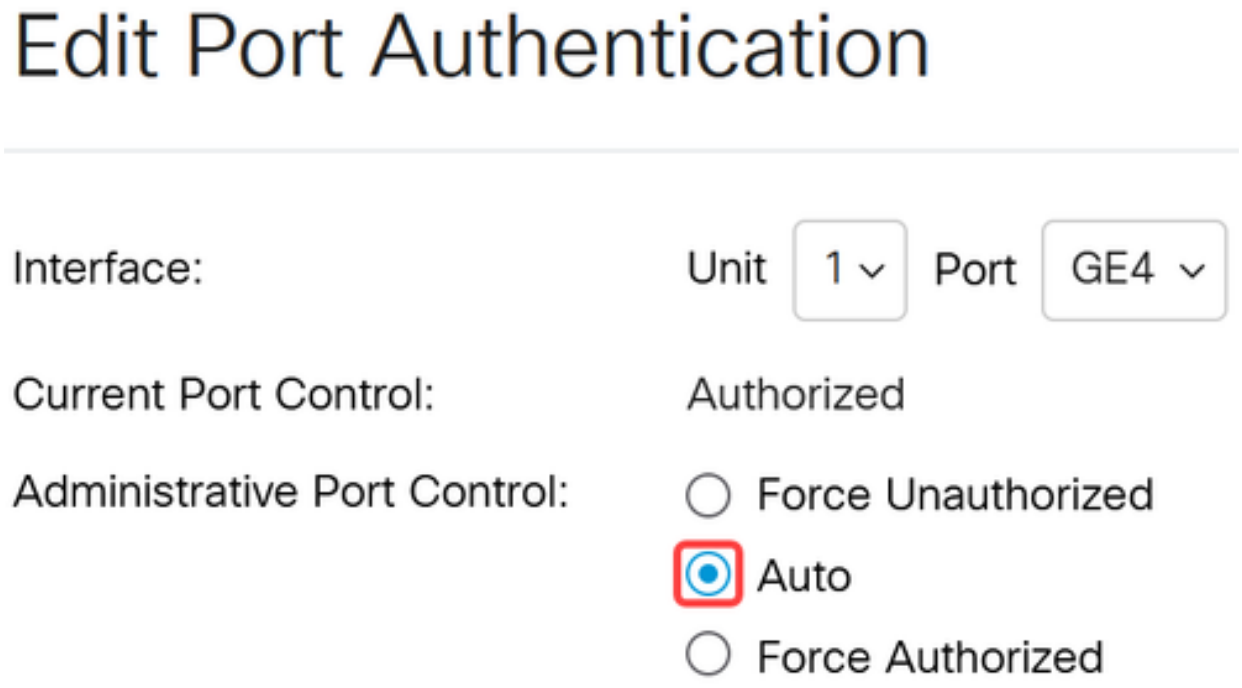
手順 8

Port Authenticationメニューに移動し、目的のポートを選択して、editをクリックします。



手順 9

Administrative Port Controlでは、Autoオプションを選択します。このオプションでは、RADIUS応答に基づいてポートが承認済みと未承認の状態を切り替えます。

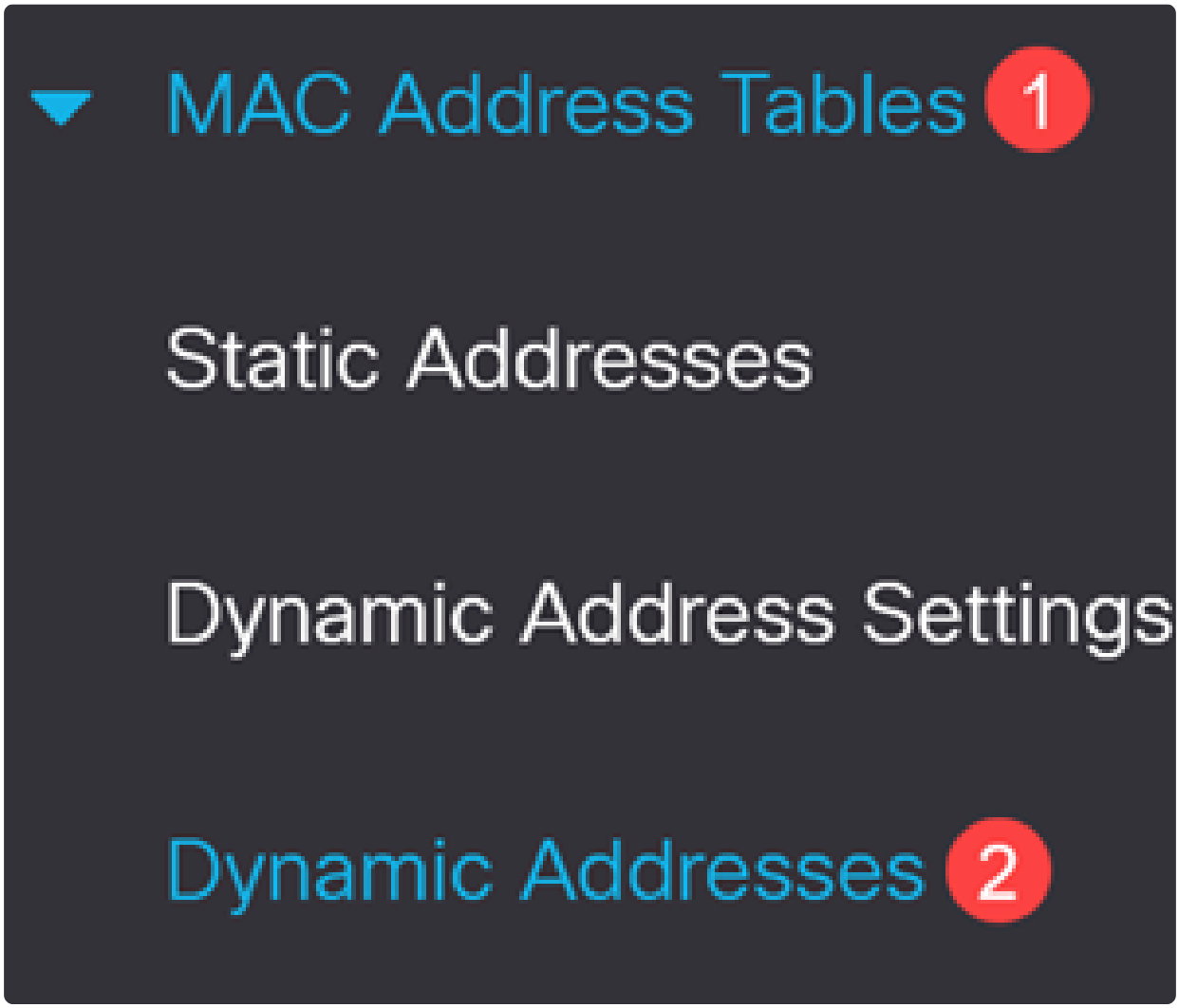


手順 10

802.1xベースの認証を有効にし、Applyをクリックします。

手順 11

ポート上のデバイスのMACアドレスが必要になります。ISEでのCoA操作は、そのMACアドレスに適用されます。この例では、ポート9です。これを取得するには、MAC Address Tables > Dynamic Addressesの順に移動します。

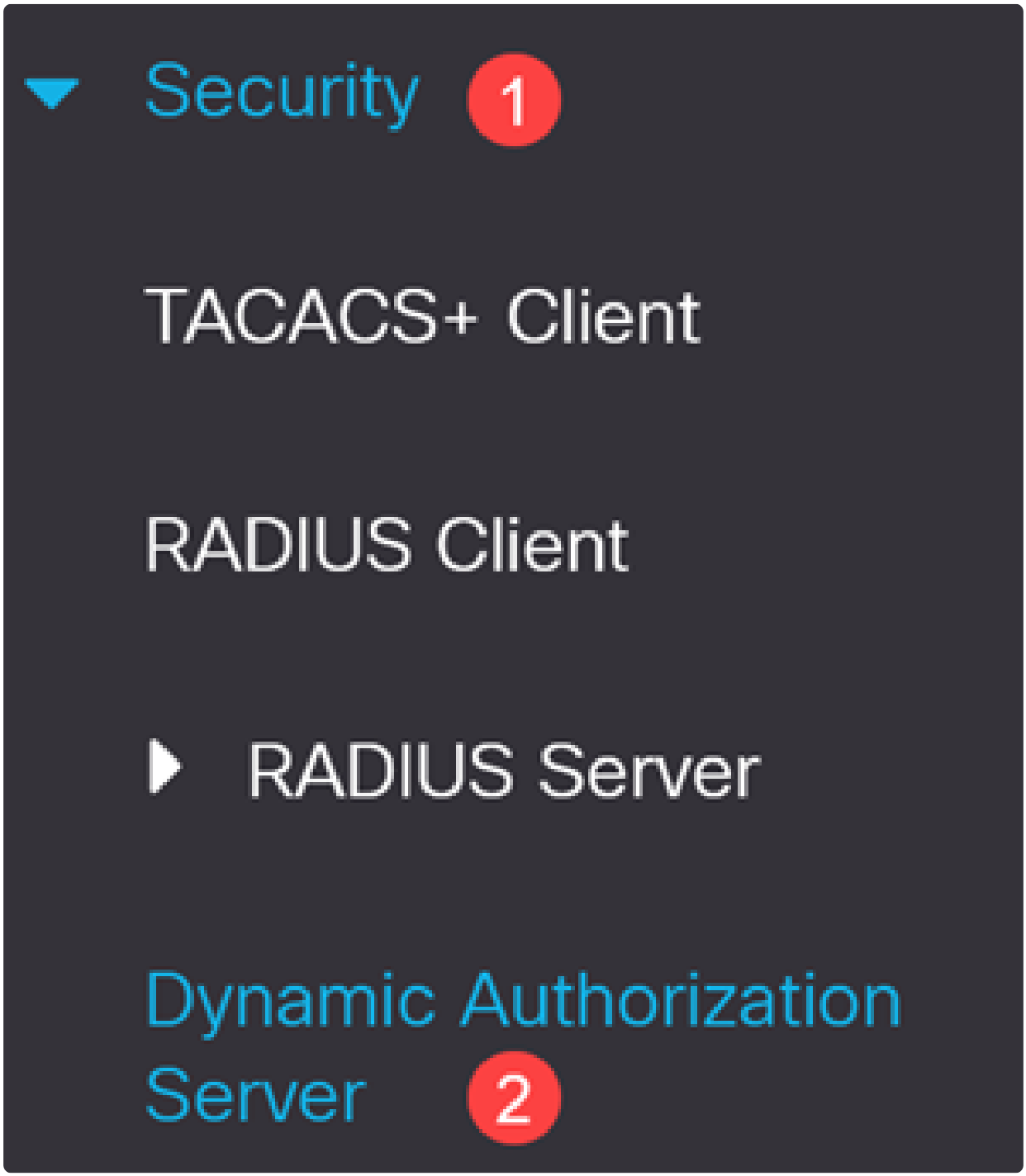


手順 12

ポートまでスクロールし、MACアドレスをメモします。

手順 13

Security > Dynamic Authorization Serverの順に移動します。

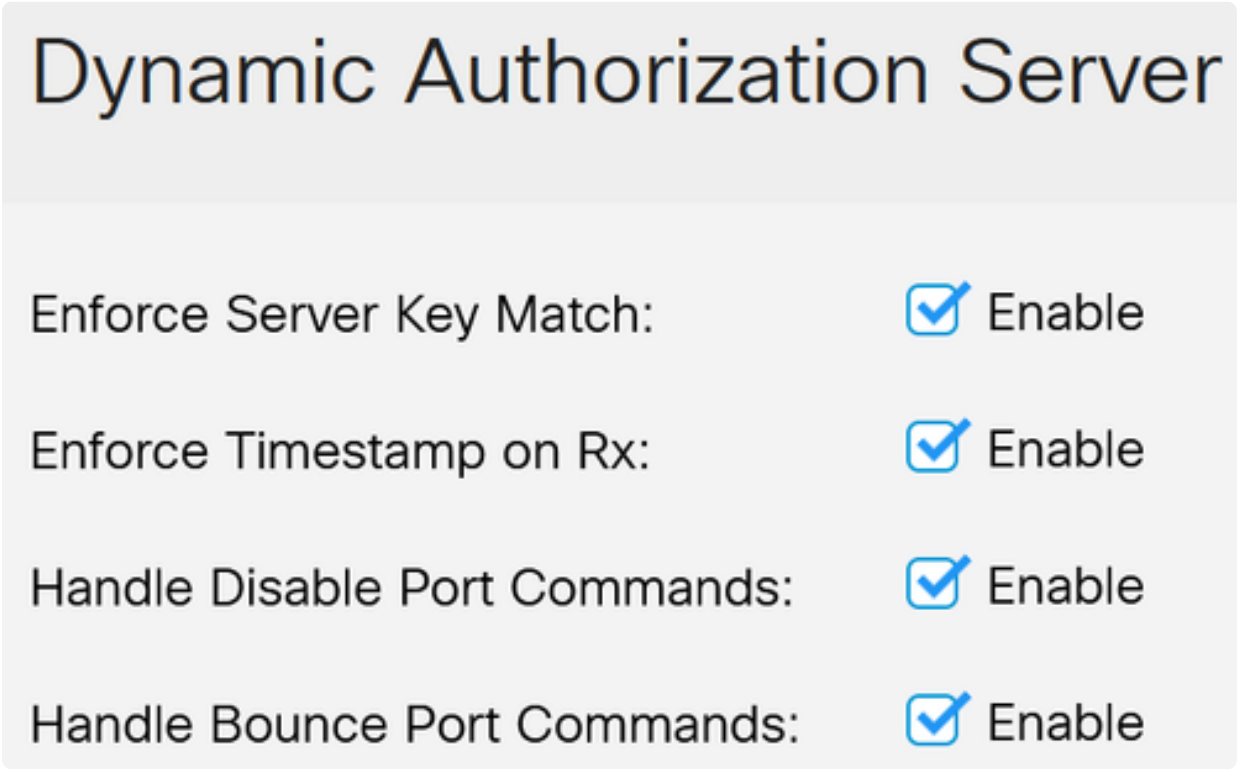


手順 14

次の機能を有効にします。

- サーバーキーの一致の強制

- Rxにタイムスタンプを適用
- Handle Disable Portコマンド
- バウンスポートコマンドの処理

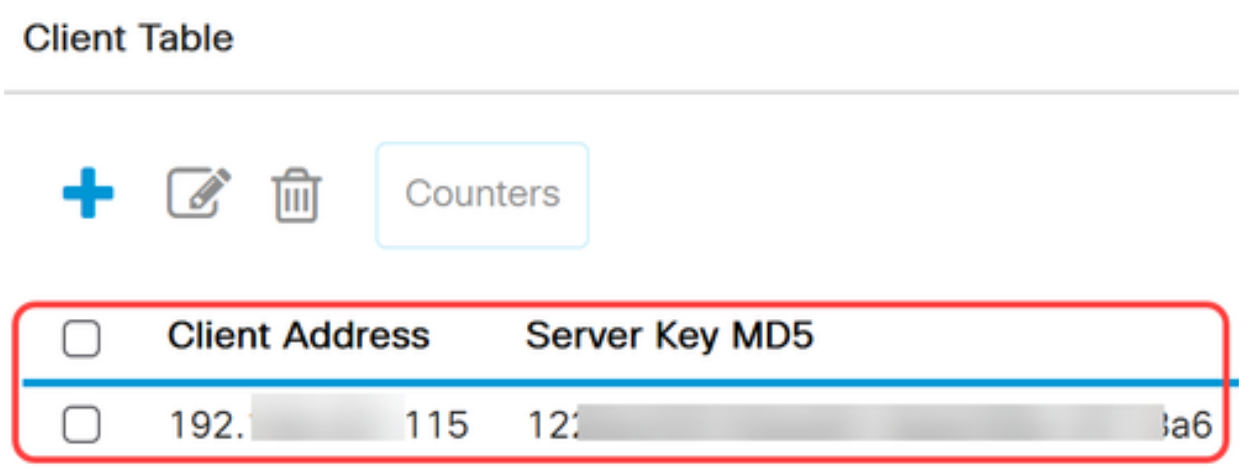


手順 15

UDP Portはデフォルト値の1700のままにしておきます。

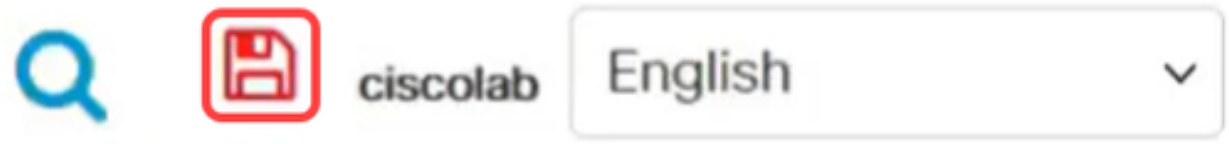
手順 16

Client Tableの下で、ISEサーバが正しいサーバキーで追加されていることを確認します。[APPLY] をクリックします。



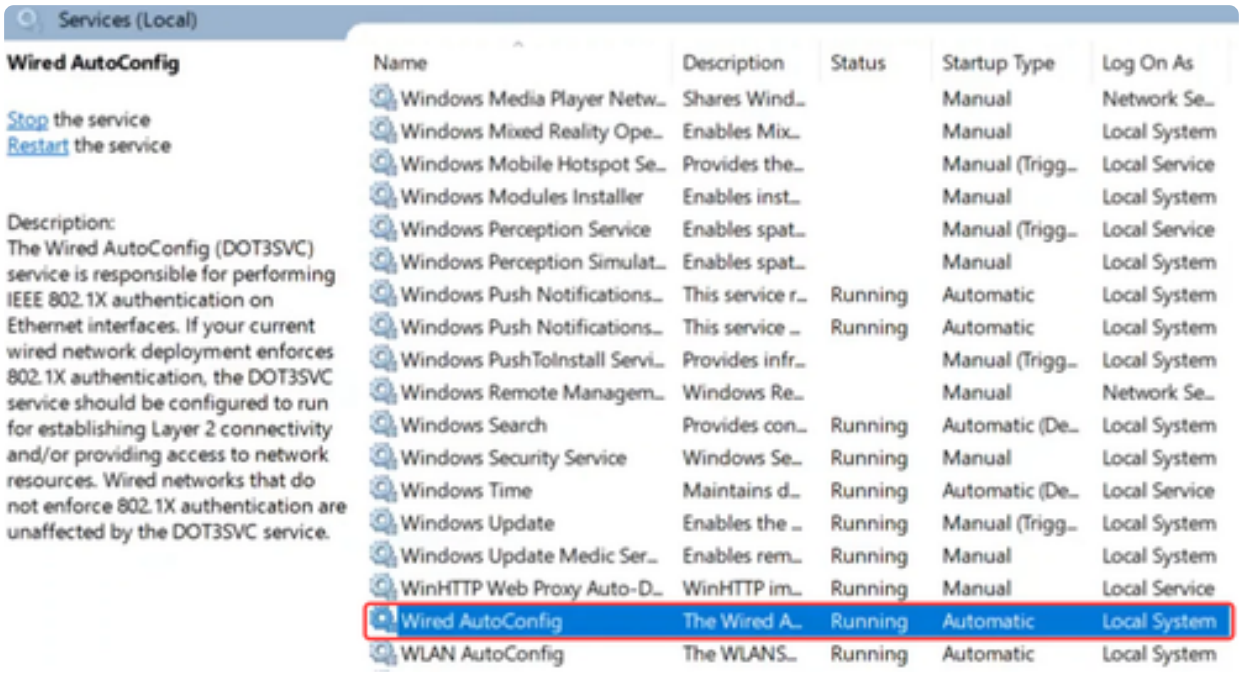
手順 17

赤色に点滅しているSaveアイコンをクリックして、設定を保存します。



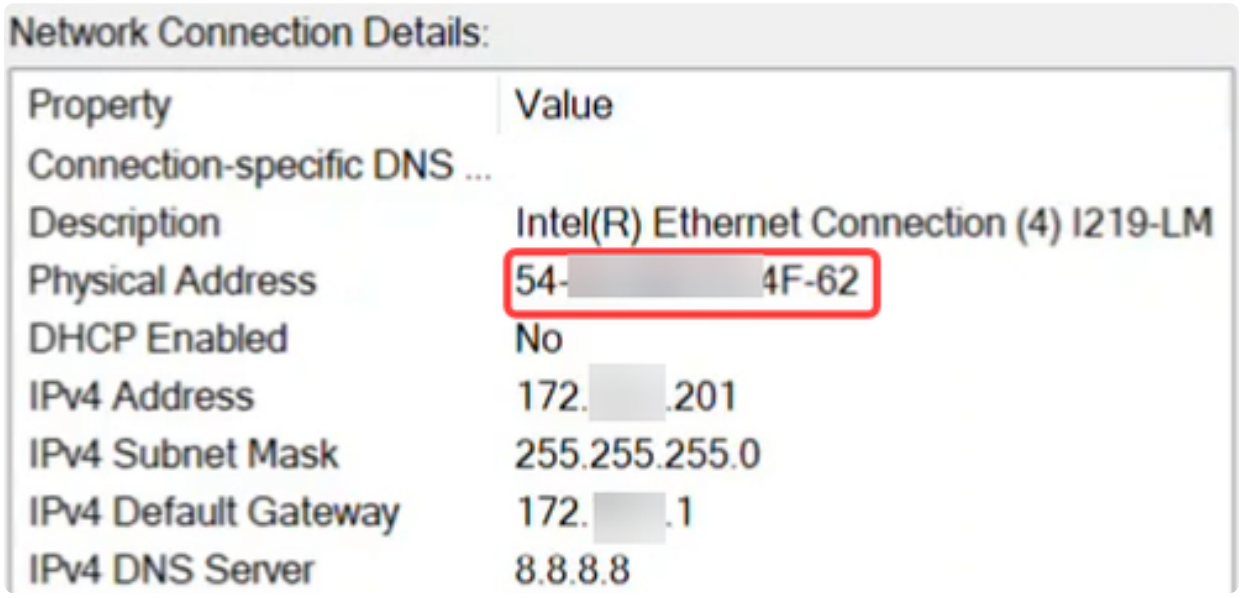
手順 18

ポート9に接続されているクライアントラップトップで、Wired AutoConfigサービスが802.1 X認証に対して有効になっていることを確認します。



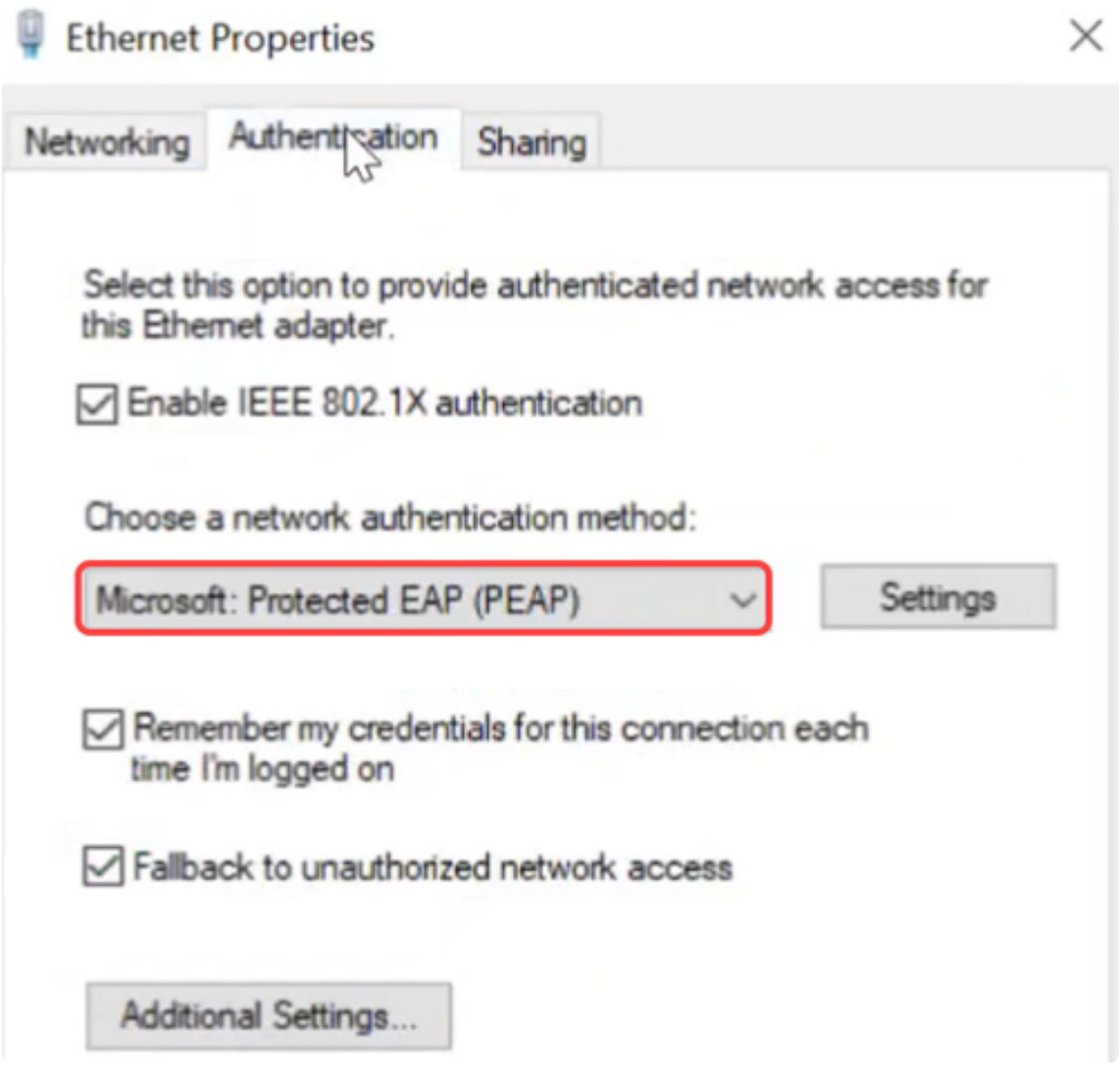
手順 19

イーサネットアダプタの設定で、MACアドレスが一致していることを確認します。



手順 20

Ethernet settingsの下にあるPropertiesボタンをクリックし、Authenticationタブでチェックボックスが有効になっていることを確認します。また、認証方式がProtected EAP(PEAP)であることを確認します。



ステップ 21

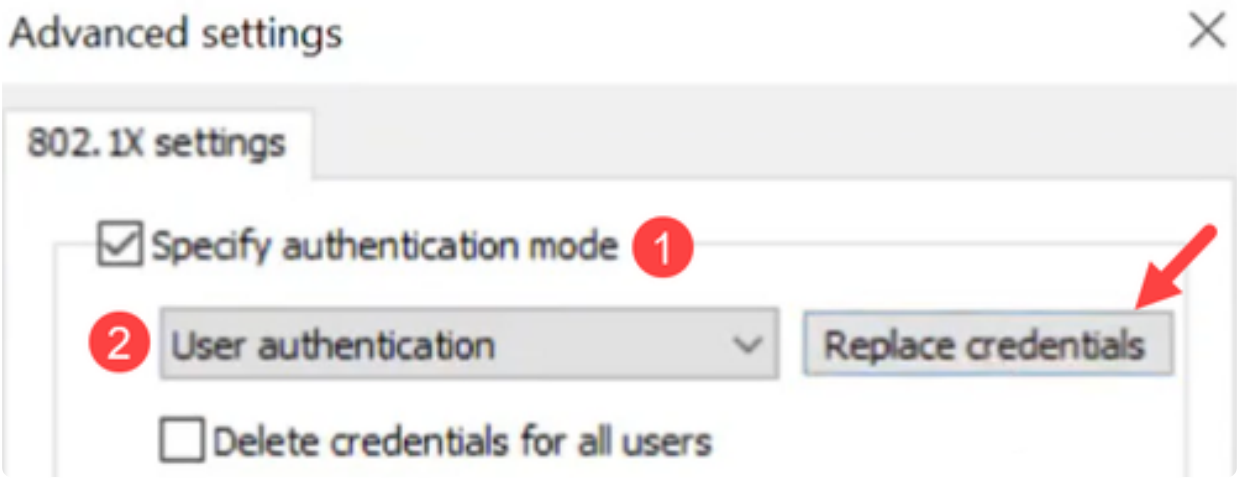
Settingsボタンをクリックし、Verify the server's identity by validating the certificateの横にあるチェックボックスがオフになっていることを確認します。

ステップ 22

Enable Fast Reconnectボックスにチェックマークを入れる必要があります。

ステップ 23

Additional settingsの下で、Specify authentication modeが有効になっており、ドロップダウンメニューからUser authenticationが選択されていることを確認します。ISEで作成したクレデンシャルを保存するか、Replace credentialsボタンを使用して置き換えることができます。



CoAオペレーション

CoA処理を開始する前に、スイッチでパケットキャプチャを有効にします。

手順 1

PuTTYで、Catalystスイッチにログインし、コマンドmonitor capture cap1 buffer size 20 circularを使用して、バッファサイズとキャプチャモードを指定します。

手順 2

monitor capture cap1 control-plane bothコマンドを使用して、コントロールプレーンをbothとして指定します。

手順 3

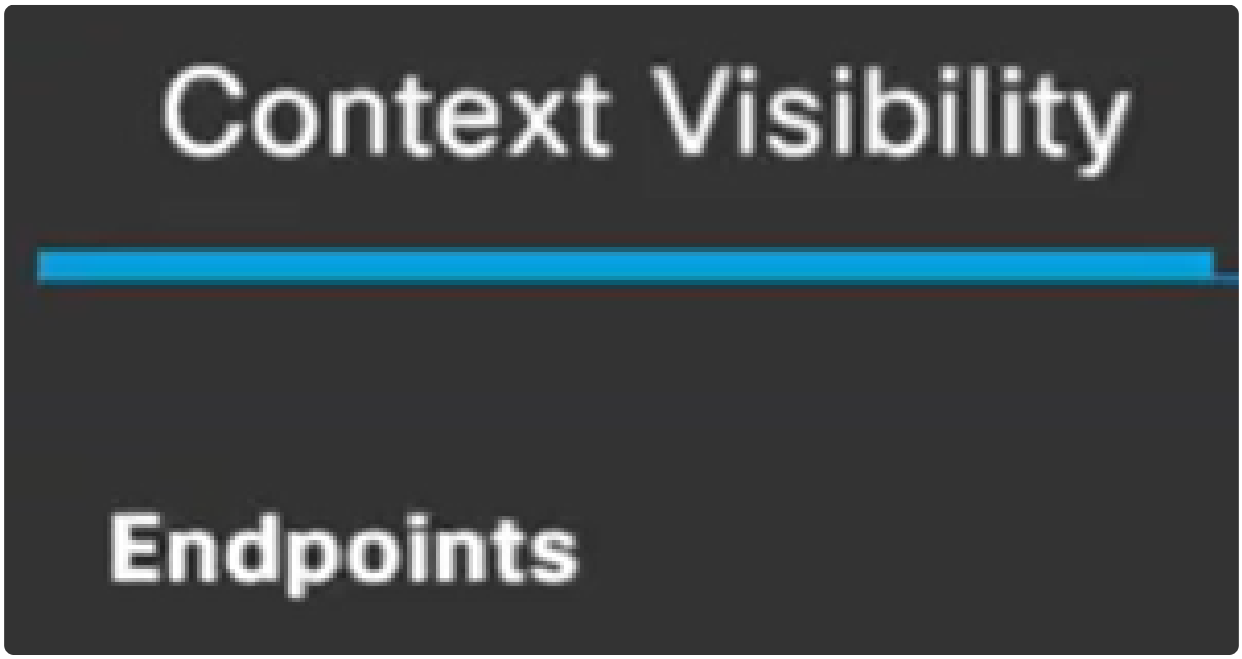
一致基準を入力します。このためのコマンドは、monitor capture cap1 match anyです。

手順 4

パケットキャプチャを開始します。

手順 5

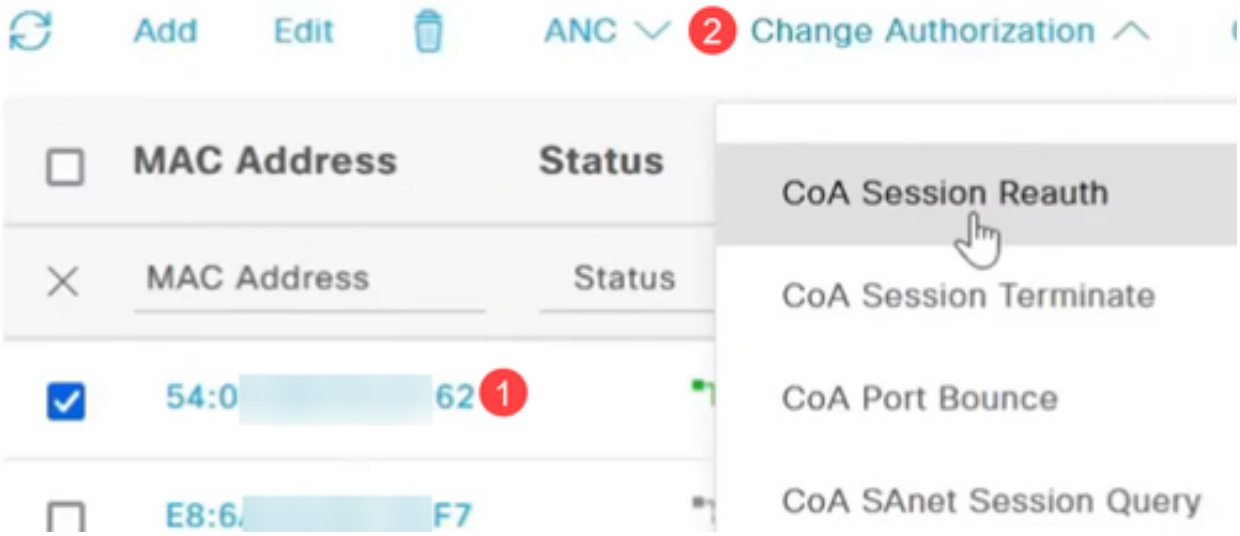
ISEインターフェイスで、Context Visibilityの下のEndpointsオプションに移動します。



手順 6

MACアドレスを選択し、Change of Authorizationドロップダウンメニューから CoA操作を選択します。この例では、CoA Session Reauthが選択されています。これにより、reauthenticateコマンドを使用してCoAパケットを送信することで、ポートで再認証

が強制されます。



ステップ7

PuTTY端末に戻り、CoA処理が成功したかどうかを確認します。

```
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"
```

手順 8

CoA Session Terminateを選択すると、管理要求に基づいてterminateコマンドで切断要求が送信されます。

```
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
```

手順 9

CoAポートバウンスオプションは、bounce host portコマンドを使用してCoA要求パケットを送信し、スイッチ上のポートを無効にしてから再度有効にします。ネットワークアダプタが10秒間オフラインになり、認証されなくなります。オンラインで復帰し、承認され、パケットを転送できます。

```
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
```

手順 10

ポートバウンスを使用したCoAセッションの終了では、既存のセッションが終了し、ポートが10秒間バウンスした後、不正なセッションになります。その後、再びオンラインになり、認証されてパケットを転送できます。

```
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
```

手順 11

ポートシャットダウンによるCoAセッションの終了は、セッションを終了し、ポートを管理上シャットダウンします。

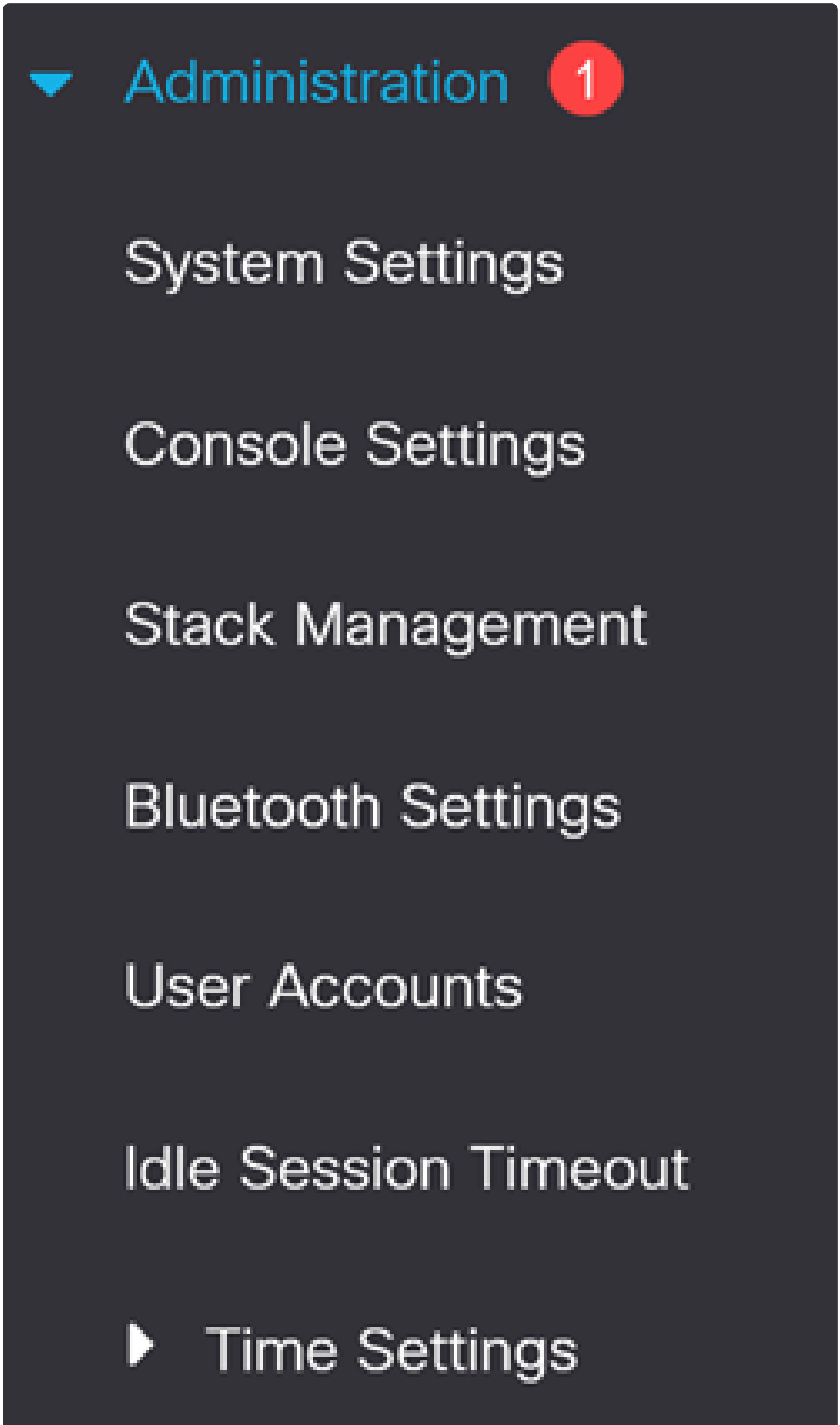
```
Cat1300-1#04-Jul-2024 20:51:47 %SEC-W-COADISPORT: Interface gi1/0/9 suspended by CoA Request "disab
le host port" for host 54:          :62
04-Jul-2024 20:51:47 %LINK-W-Down:  gi1/0/9
```

手順 12

パケットキャプチャを停止するには、monitor capture cap1 stopコマンドを使用します。

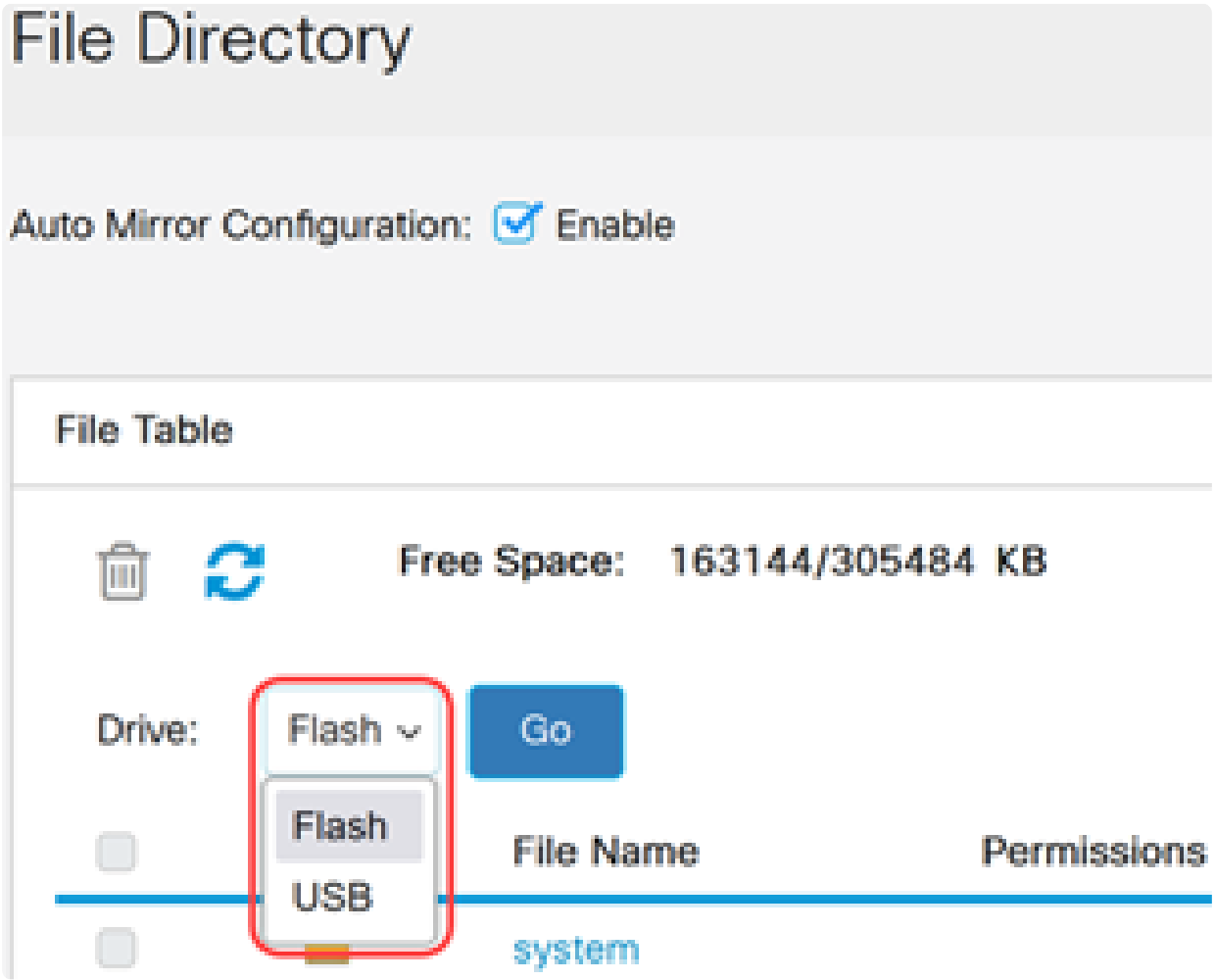
手順 13

ファイルをコピーするには、Administration > File Management > File Directoryの順に選択します。


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

手順 14

デフォルトのフラッシュが使用可能です。または、Driveドロップダウンメニューから USBを選択することもできます。



結論

これで、ISEに関するすべての情報と、Catalyst 1300シリーズスイッチでのCoAの設定方法を理解できました。

詳細については、以下のビデオをご覧ください。

この記事の関連ビデオを見る...

シスコの他のテクニカルトークを表示するには、こちらをクリックしてください

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。