Configuration du changement d'autorisation dans Catalyst 1300 à l'aide de l'interface utilisateur Web

Objectif

L'objectif de cet article est de vous montrer comment configurer la modification de l'autorisation (CoA) dans les commutateurs Catalyst 1300 à l'aide de l'interface utilisateur Web.

Périphériques et version du logiciel applicables

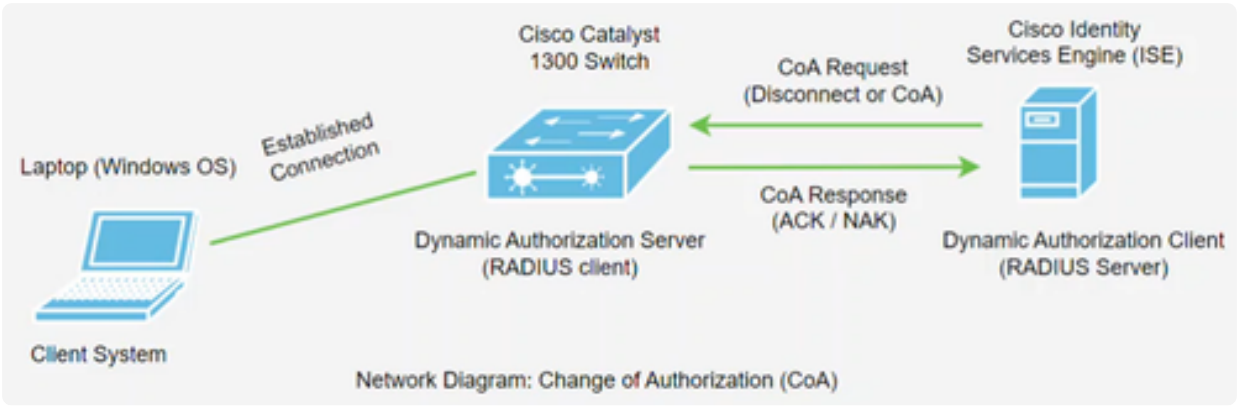
- commutateurs Catalyst 1300 |4.1.6.53

Introduction

Change of Authorization (CoA) est une extension du protocole RADIUS qui vous permet de modifier les propriétés d'une session utilisateur AAA (Authentication, Authorization, and Accounting) ou dot1x après son authentification. Lorsqu'une stratégie pour un utilisateur ou un groupe dans AAA change, les administrateurs peuvent transmettre des paquets RADIUS CoA à partir du serveur AAA, tel qu'un moteur Cisco Identity Services Engine (ISE), pour réinitialiser l'authentification et appliquer la nouvelle stratégie.

Cisco Identity Services Engine (ou ISE) est un moteur de contrôle d'accès basé sur le réseau et d'application des politiques doté de toutes les fonctionnalités. Il fournit des services d'analyse et d'application de la sécurité, RADIUS et TACACS, la distribution des politiques, etc. Cisco ISE est actuellement le seul client d'autorisation dynamique CoA pris en charge pour les commutateurs Catalyst 1300. Reportez-vous au guide d'administration ISE pour plus d'informations.

Cette fonctionnalité nécessite une communication entre le client d'autorisation dynamique (serveur RADIUS) et le serveur d'autorisation dynamique (commutateur Catalyst). Comme le montre le schéma de réseau ci-dessous, le serveur d'autorisation dynamique envoie un message de déconnexion ou de CoA au serveur d'autorisation dynamique et le commutateur fournit une réponse.



La prise en charge CoA a été ajoutée aux commutateurs Catalyst 1300 dans la version 4.1.3.36 du microprogramme. Elle inclut la prise en charge de la déconnexion des utilisateurs et de la modification des autorisations applicables à une session utilisateur. Le périphérique prend en charge les actions CoA suivantes :

- Déconnecter la session
- Commande Disable host port CoA
- Commande Bounce host port CoA
- Commande CoA de réauthentification hôte

Pour configurer la CoA à l'aide de l'interface de ligne de commande (CLI), référez-vous à Configuration de la modification d'autorisation dans le commutateur Catalyst 1300 à l'aide de la CLI.

Table des matières

Configuration du client RADIUS Catalyst 1300 sur ISE

Dans cet exemple, le serveur Cisco ISE version 3.2 est utilisé. Pour une présentation d'ISE, consultez la page produit Cisco Identity Services Engine.

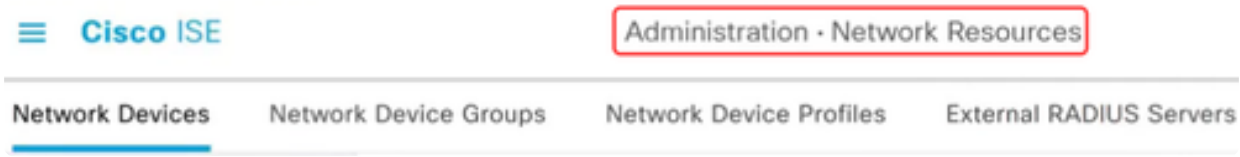
> **Note:**
> CoA est pris en charge sur ISE version 2.7 et ultérieure.

Après le déploiement du serveur Cisco ISE, connectez-vous pour accéder à l'interface

utilisateur Web.

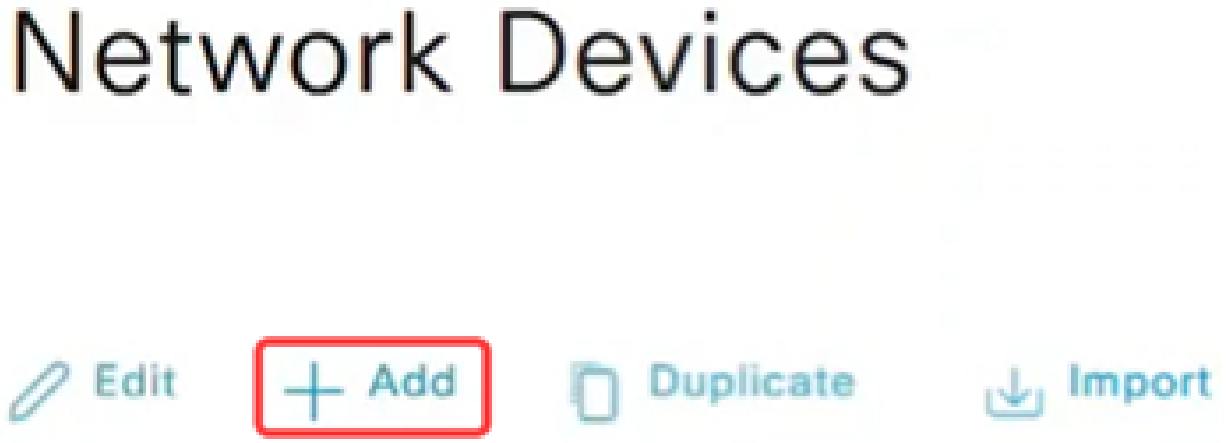
Étape 1

Pour ajouter des périphériques réseau, accédez au menu Administration > Ressources réseau.



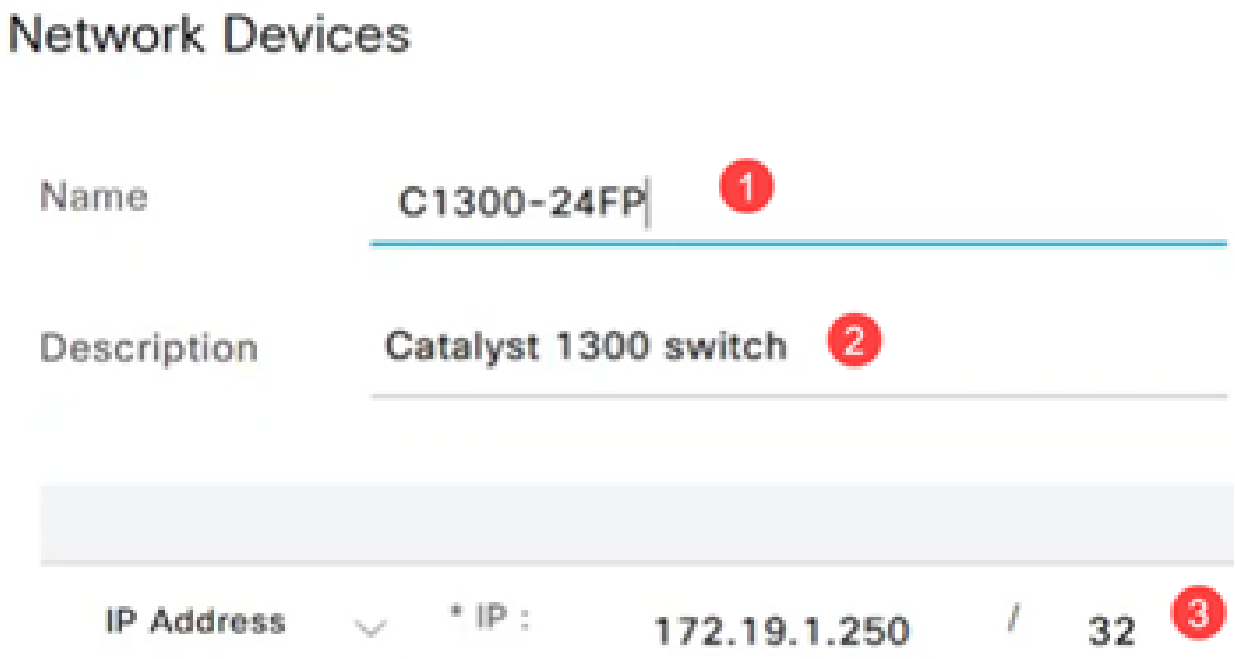
Étape 2

Cliquez sur le bouton + Add.



Étape 3

Saisissez le nom, la description et l'adresse IP du commutateur Catalyst.

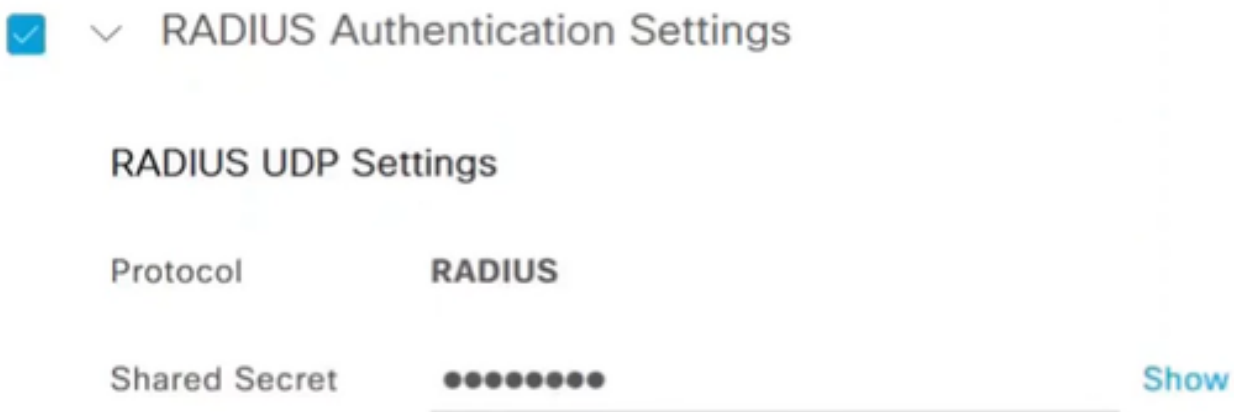


Étape 4

Dans le menu déroulant Device Profile, sélectionnez Cisco.

Étape 5

Configurez les paramètres d'authentification RADIUS en saisissant le secret partagé.



Étape 6

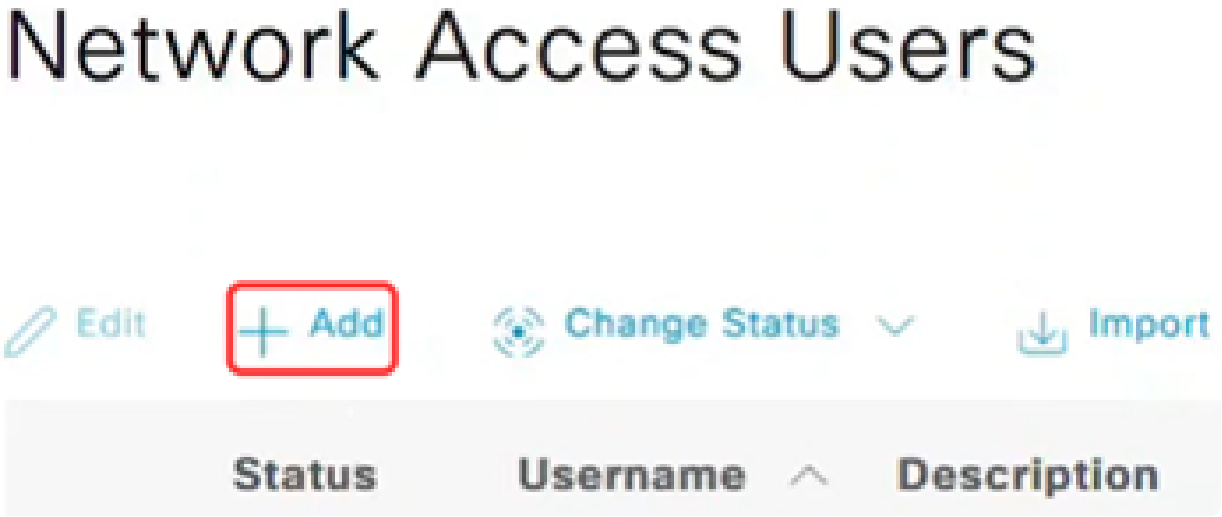
Saisissez le numéro de port CoA. Le port par défaut est 1700.

Étape 7

Accédez ensuite à Administration > Identity Management et sélectionnez Network Access Users.

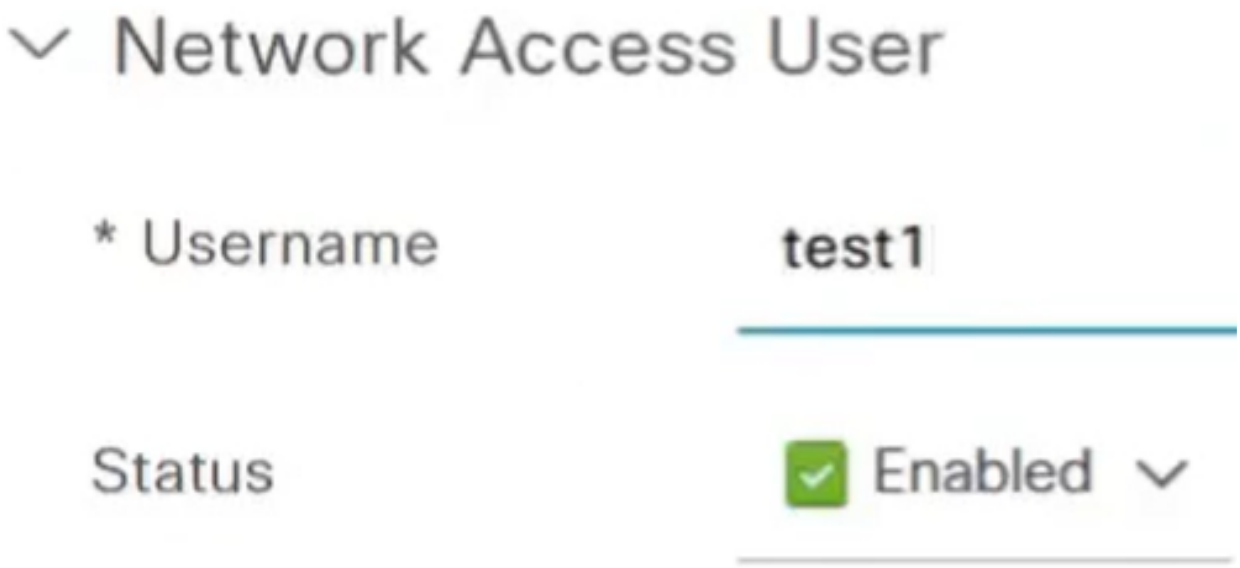
Étape 8

Pour définir le nom d'utilisateur et le mot de passe, cliquez sur le symbole +Add.



Étape 9

Saisissez le nom d'utilisateur et le mot de passe, puis cliquez sur Save au bas de la page.



Configurations dans le commutateur Catalyst 1300

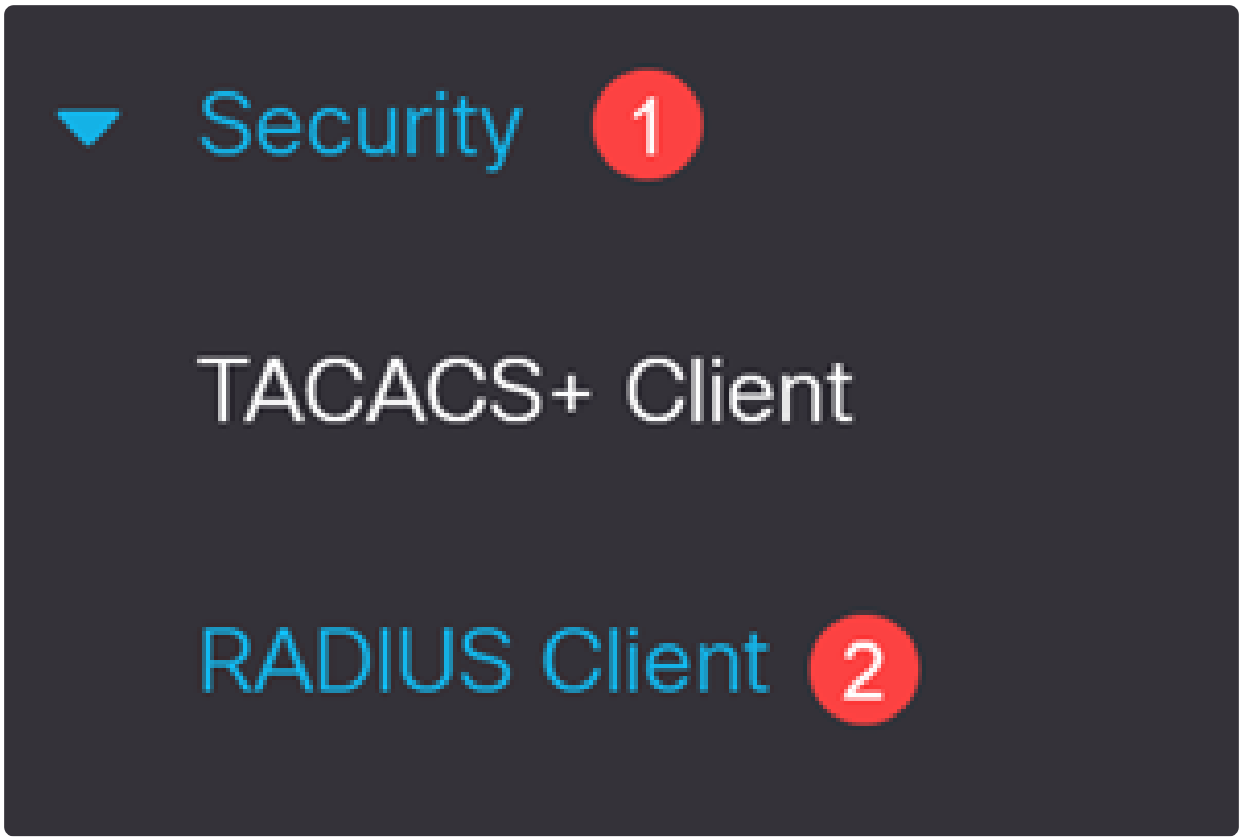
Étape 1

Connectez-vous à votre commutateur Catalyst 1300 et sélectionnez le mode avancé. Dans cet exemple, C1300-24FP-4X est utilisé.

> Note:
> La prise en charge CoA a été ajoutée aux commutateurs Catalyst 1300 dans la version 4.1.3.36 du microprogramme.

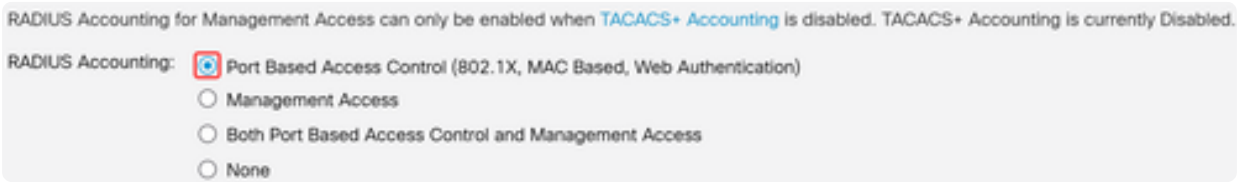
Étape 2

Accédez à Security > RADIUS Client dans le volet de navigation.



Étape 3

Définissez la comptabilité RADIUS sur Port Based Access Control.



Étape 4

Pour ajouter le serveur ISE, faites défiler jusqu'au tableau RADIUS et cliquez sur l'icône plus.

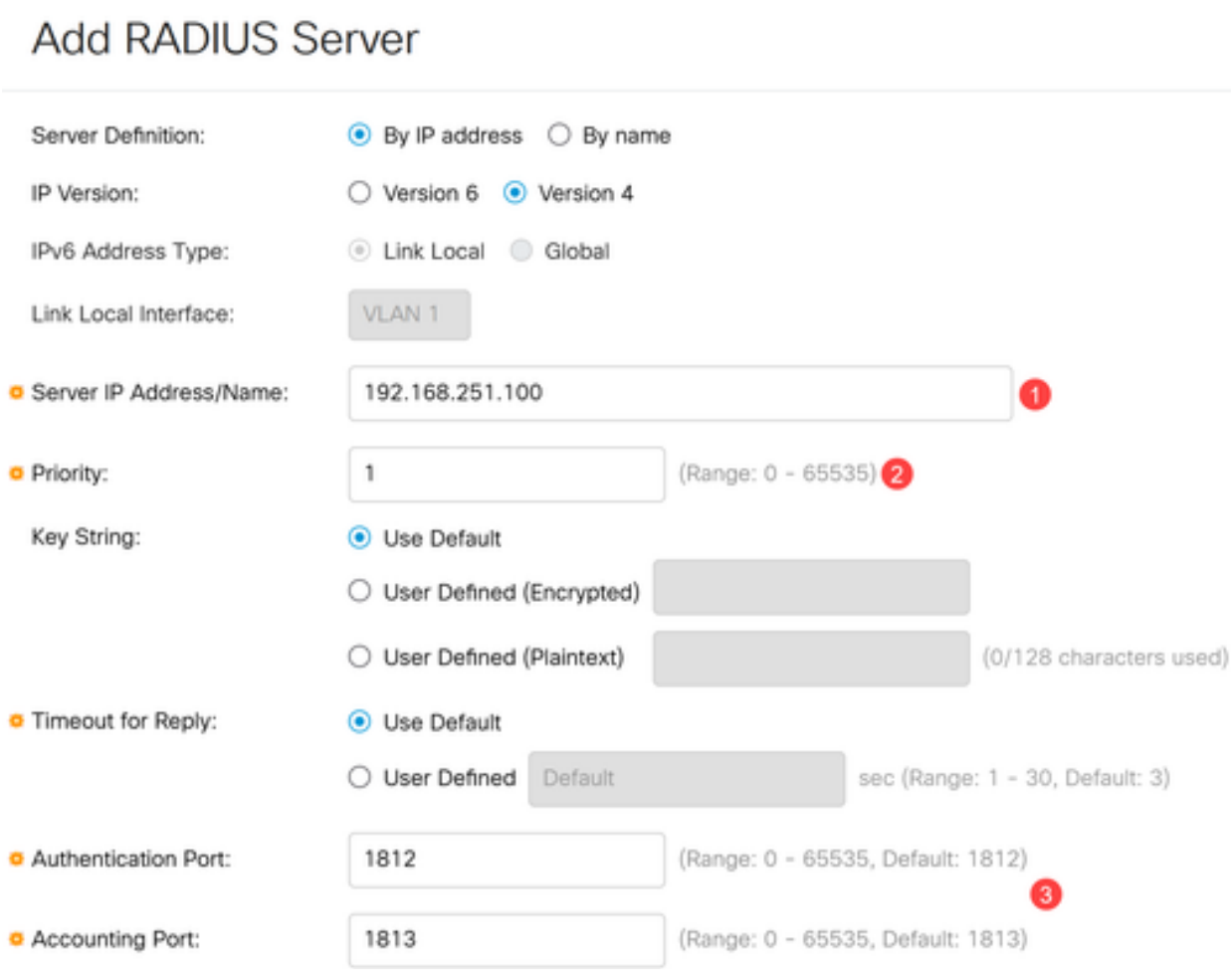
Étape 5

Configurer les paramètres du serveur RADIUS.

- Sélectionnez Définition du serveur. Dans cet exemple, By IP address est sélectionné. Saisissez l'adresse IP dans le champ Server IP Address/Name.
- Définissez une priorité RADIUS.

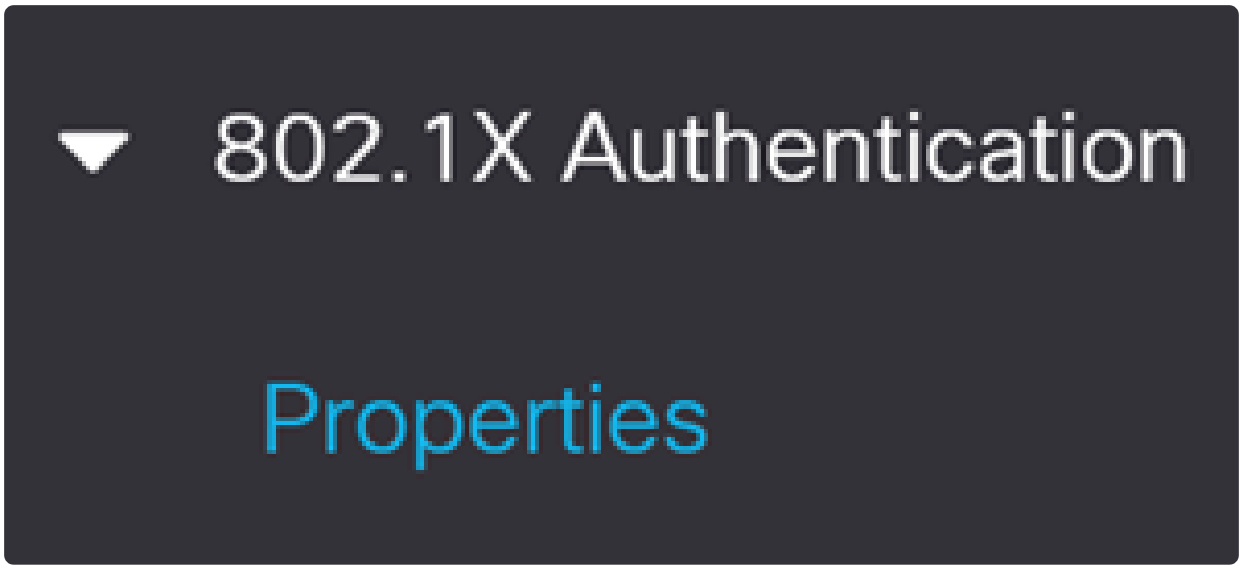
- Les ports d'authentification et de gestion des comptes sont définis par défaut.
- Le type d'utilisation est 802.1x.

Cliquez sur Apply.



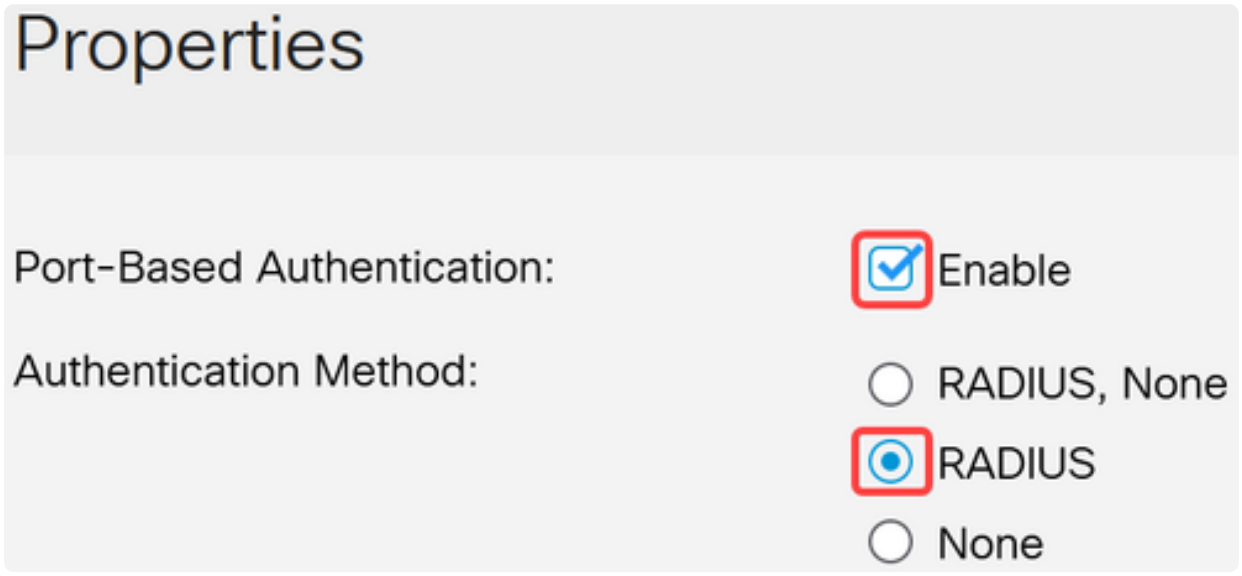
Étape 6

Pour configurer l'authentification 802.1x, accédez au menu Security > 802.1X Authentication > Properties.



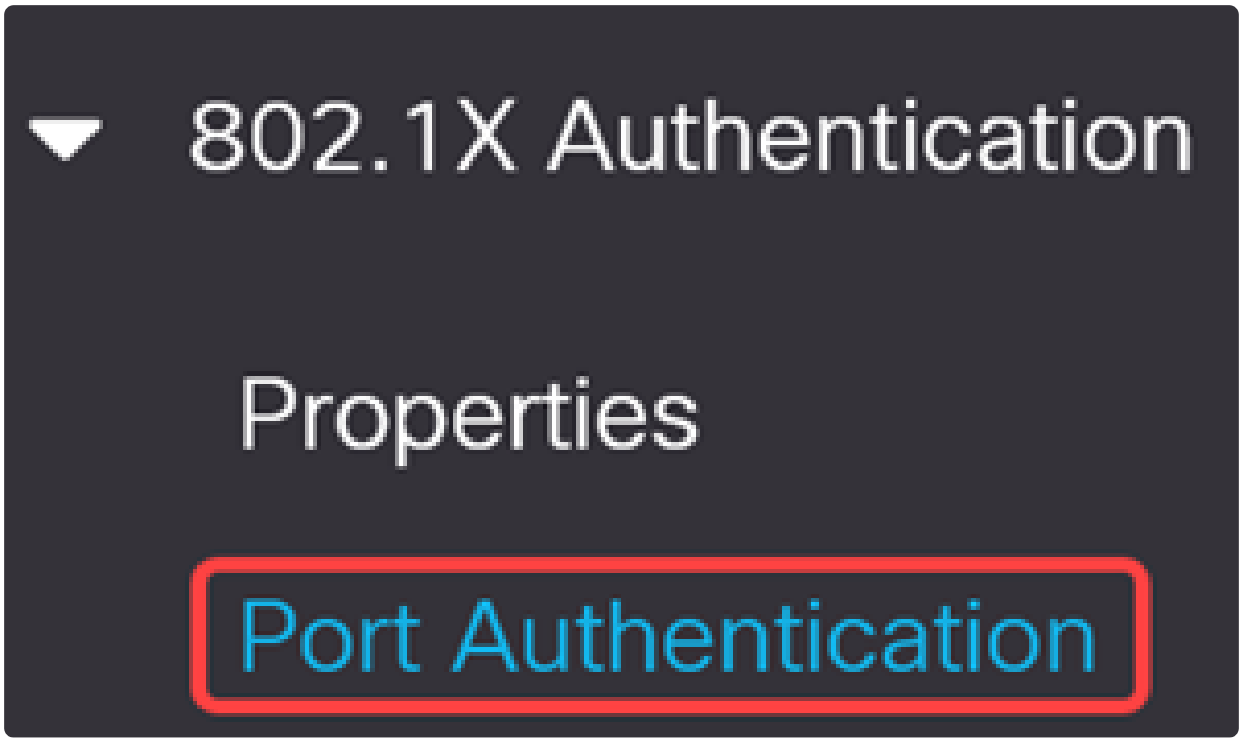
Étape 7

Vérifiez que l'authentification basée sur les ports est activée et que la méthode d'authentification est définie sur RADIUS.



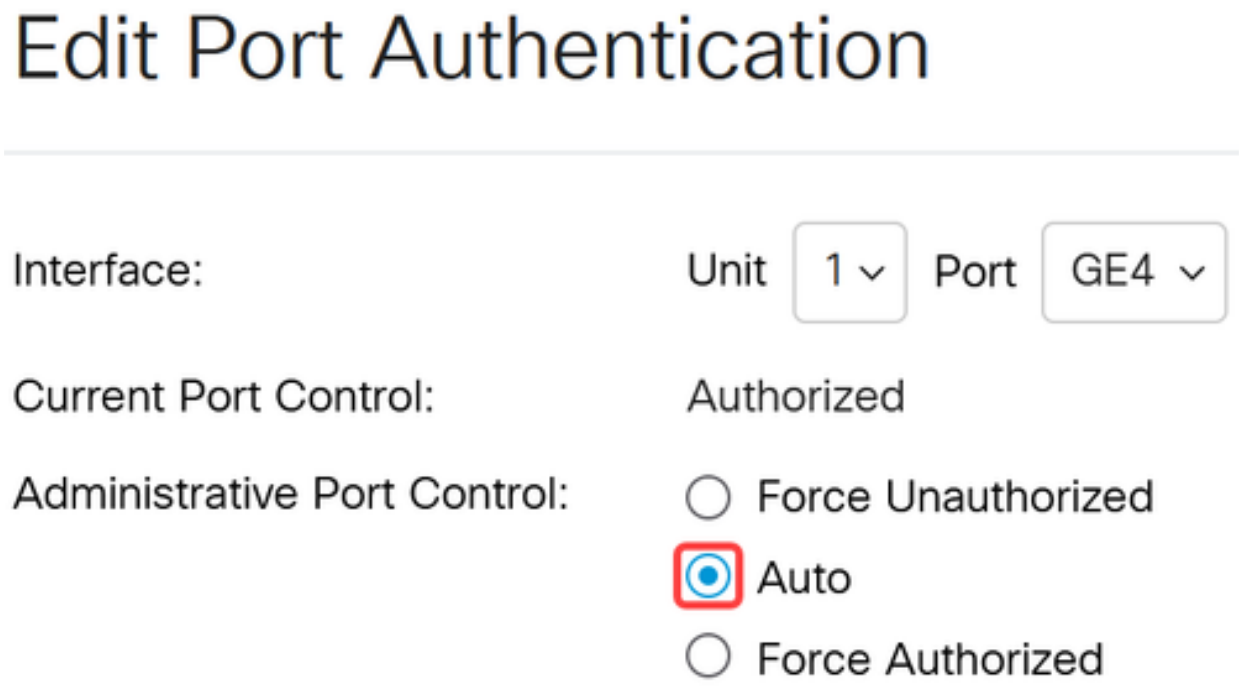
Étape 8

Accédez au menu Port Authentication, sélectionnez le port souhaité, puis cliquez sur edit.



Étape 9

Pour Administrative Port Control, sélectionnez l'option Auto qui commute le port entre l'état autorisé et non autorisé en fonction de la réponse RADIUS.

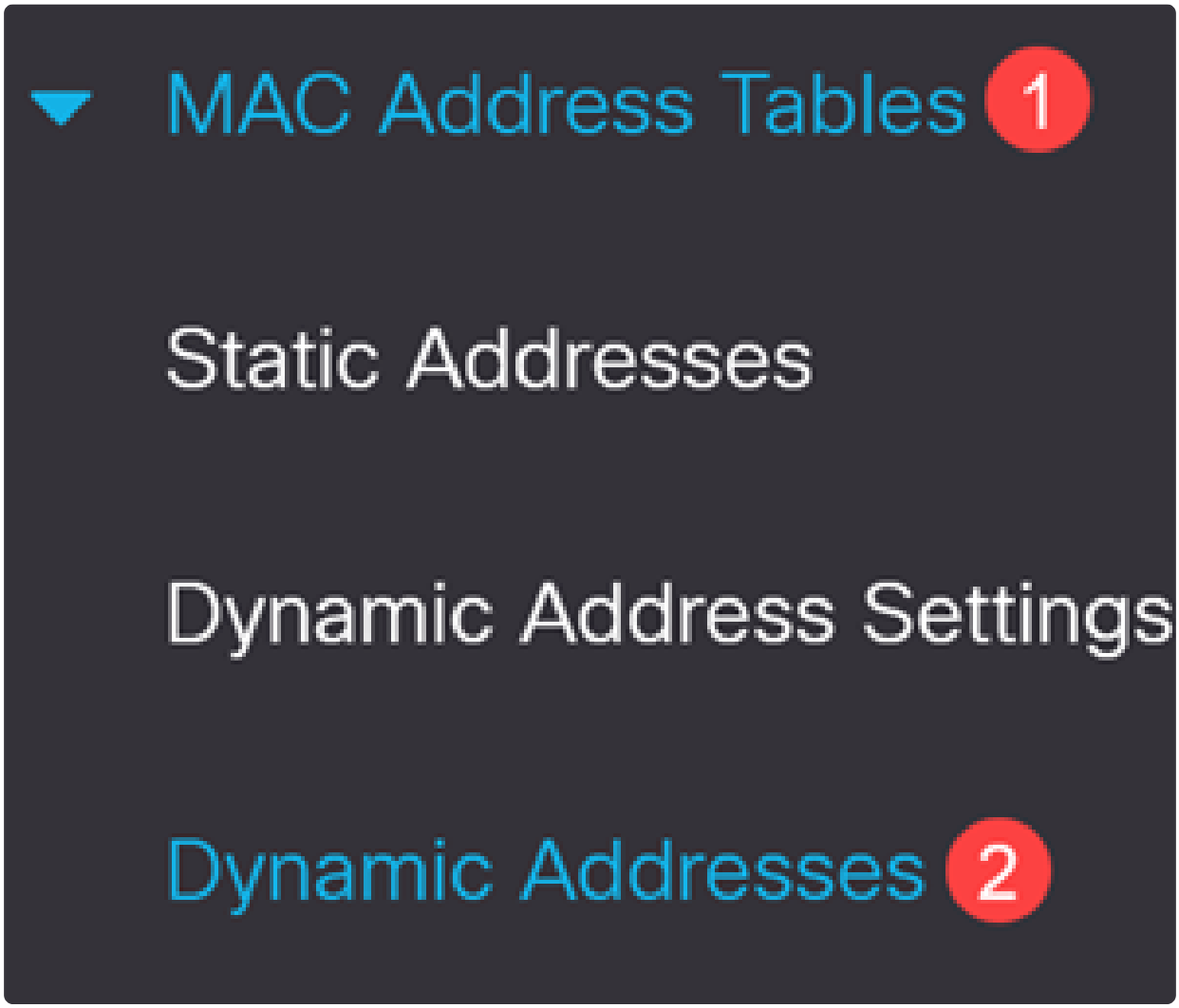


Étape 10

Activez l'authentification basée sur 802.1x et cliquez sur Apply.

Étape 11

Vous aurez besoin de l'adresse MAC du périphérique sur le port. L'opération CoA sur ISE sera appliquée à cette adresse MAC. Dans cet exemple, il s'agit du port 9. Pour l'obtenir, accédez à MAC Address Tables > Dynamic Addresses.

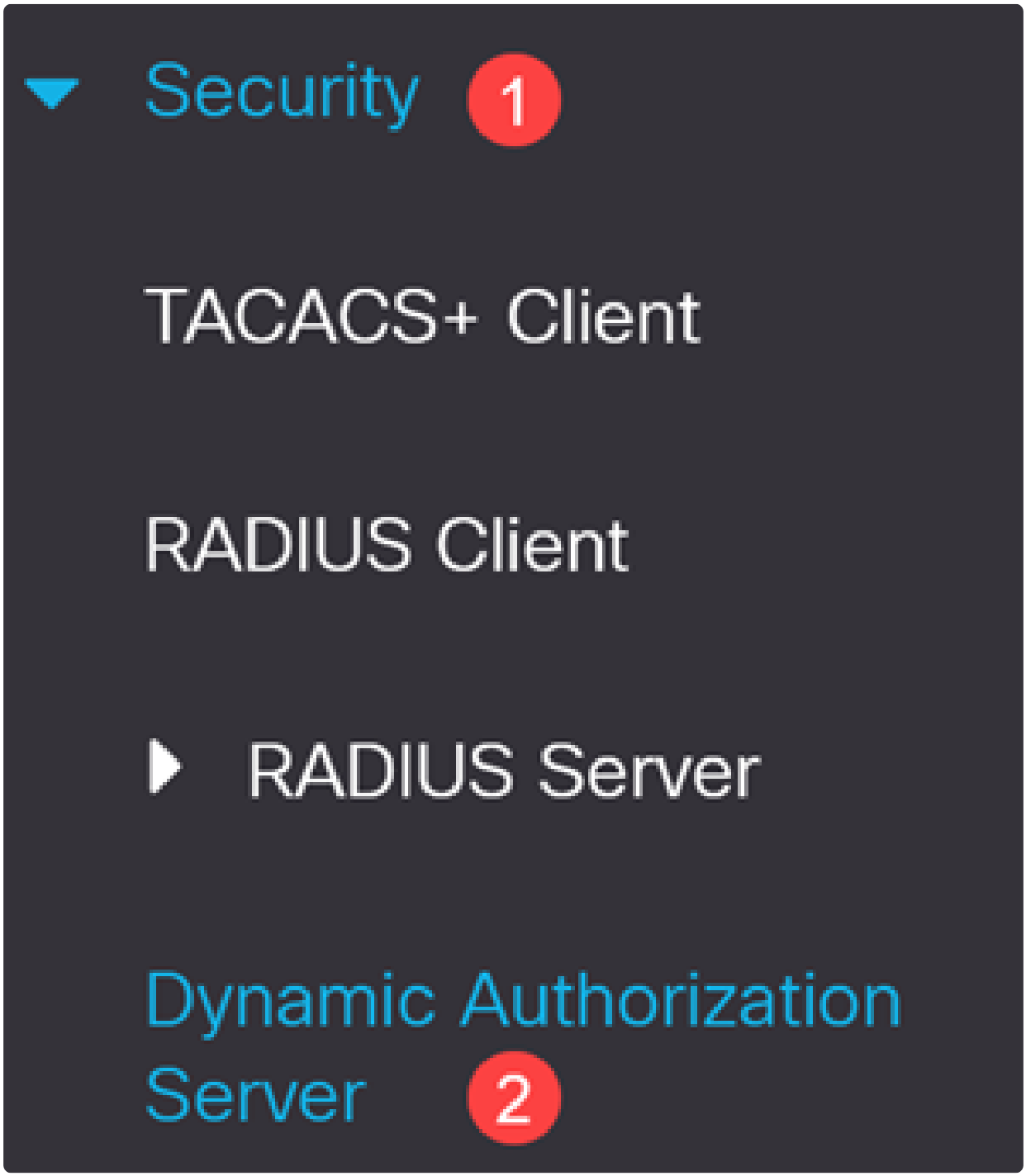


Étape 12

Faites défiler jusqu'au port et notez l'adresse MAC.

Étape 13

Accédez à Security > Dynamic Authorization Server.

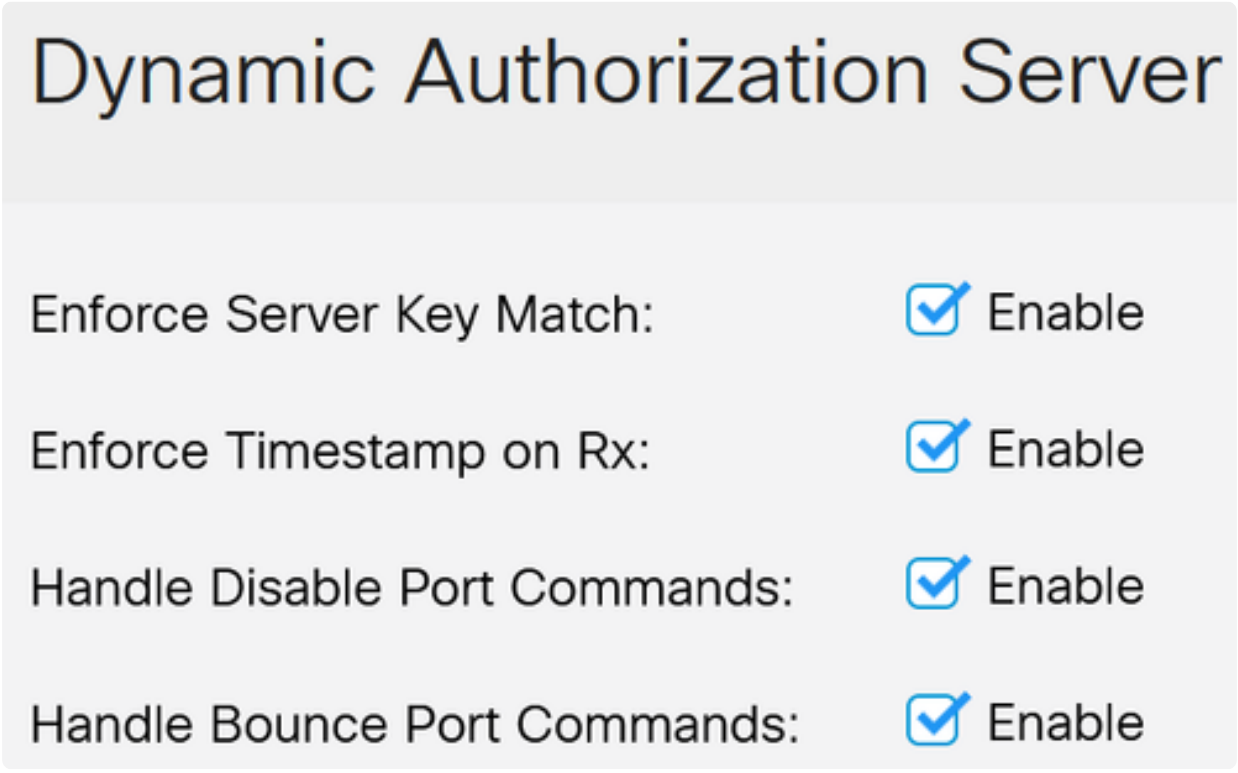


Étape 14

Activez les options suivantes :

- Appliquer la correspondance des clés du serveur

- Appliquer l'horodatage sur Rx
- Commandes Handle Disable Port
- Commandes de port de renvoi

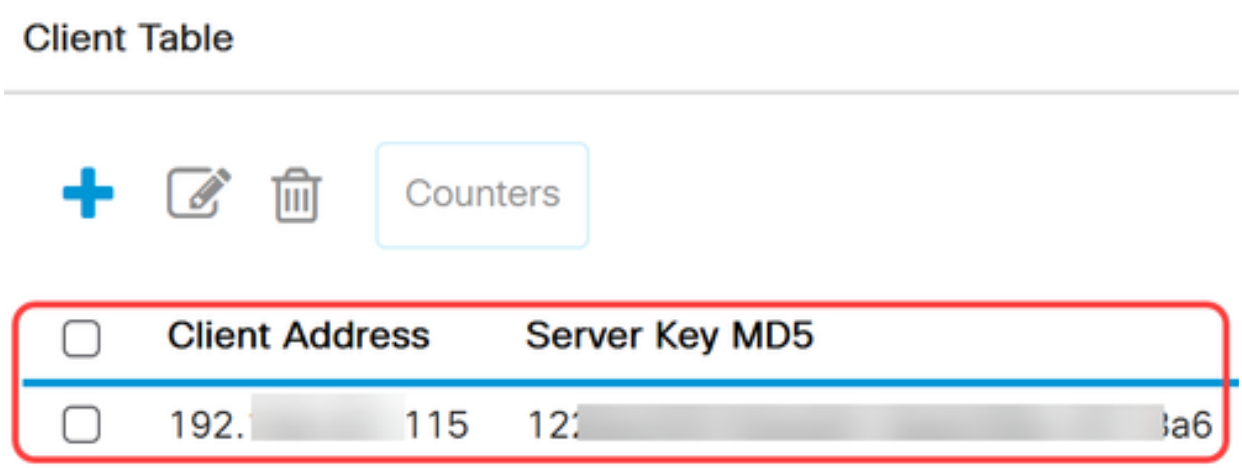


Étape 15

Laissez le port UDP à la valeur par défaut de 1700.

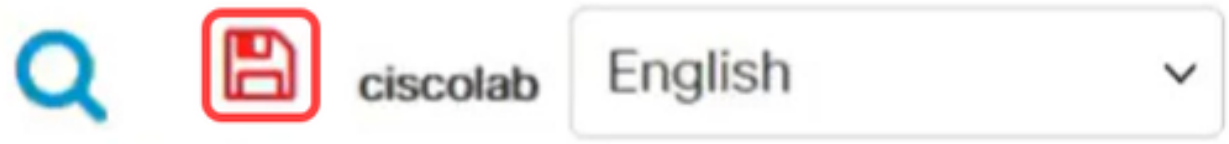
Étape 16

Sous Client Table, assurez-vous que le serveur ISE est ajouté avec la clé de serveur correcte. Cliquez sur Apply.



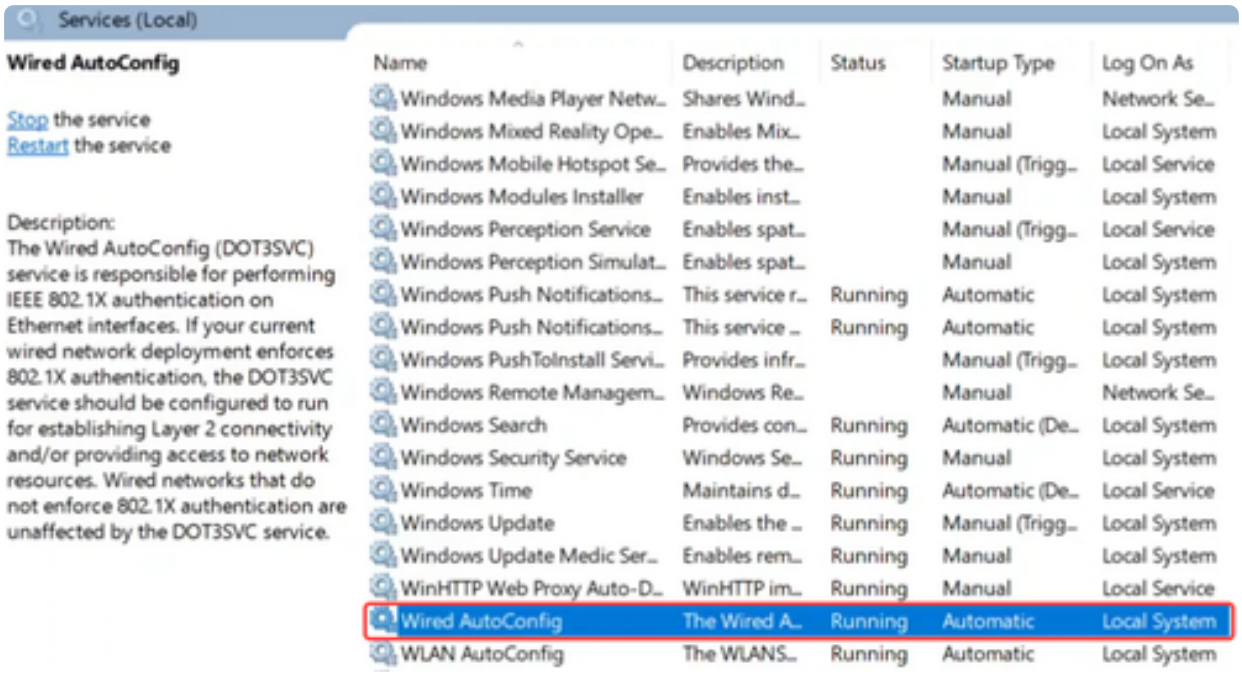
Étape 17

Cliquez sur l'icône rouge clignotante Enregistrer pour enregistrer les configurations.



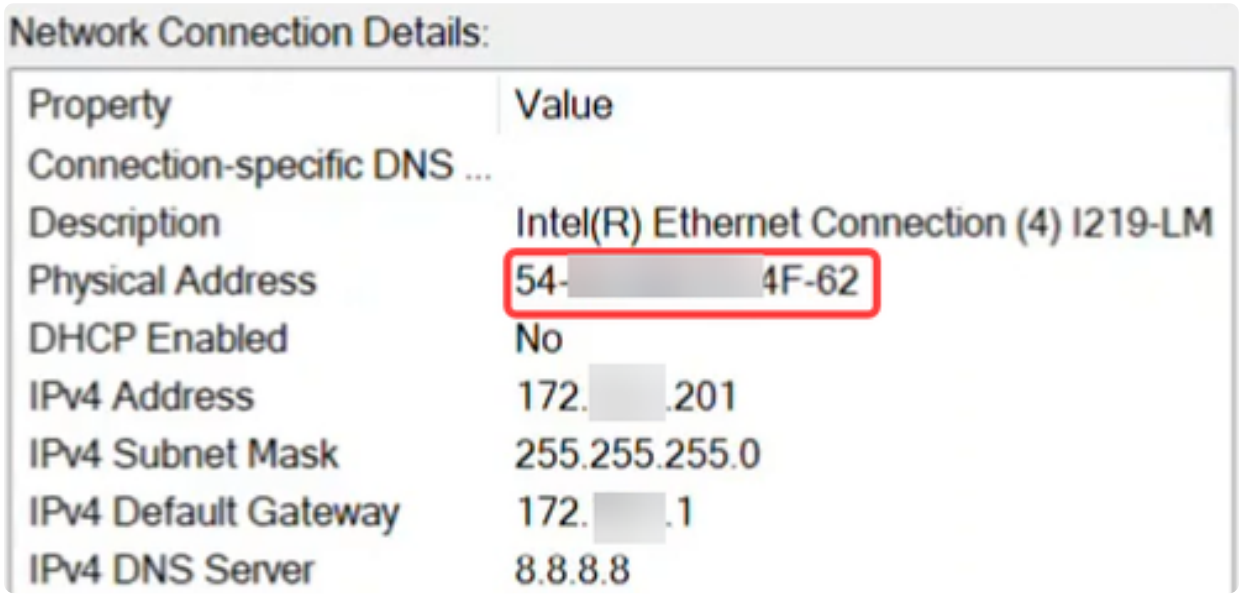
Étape 18

Sur l'ordinateur portable client connecté au port 9, vérifiez que le service Wired AutoConfig est activé pour l'authentification 802.1 X.



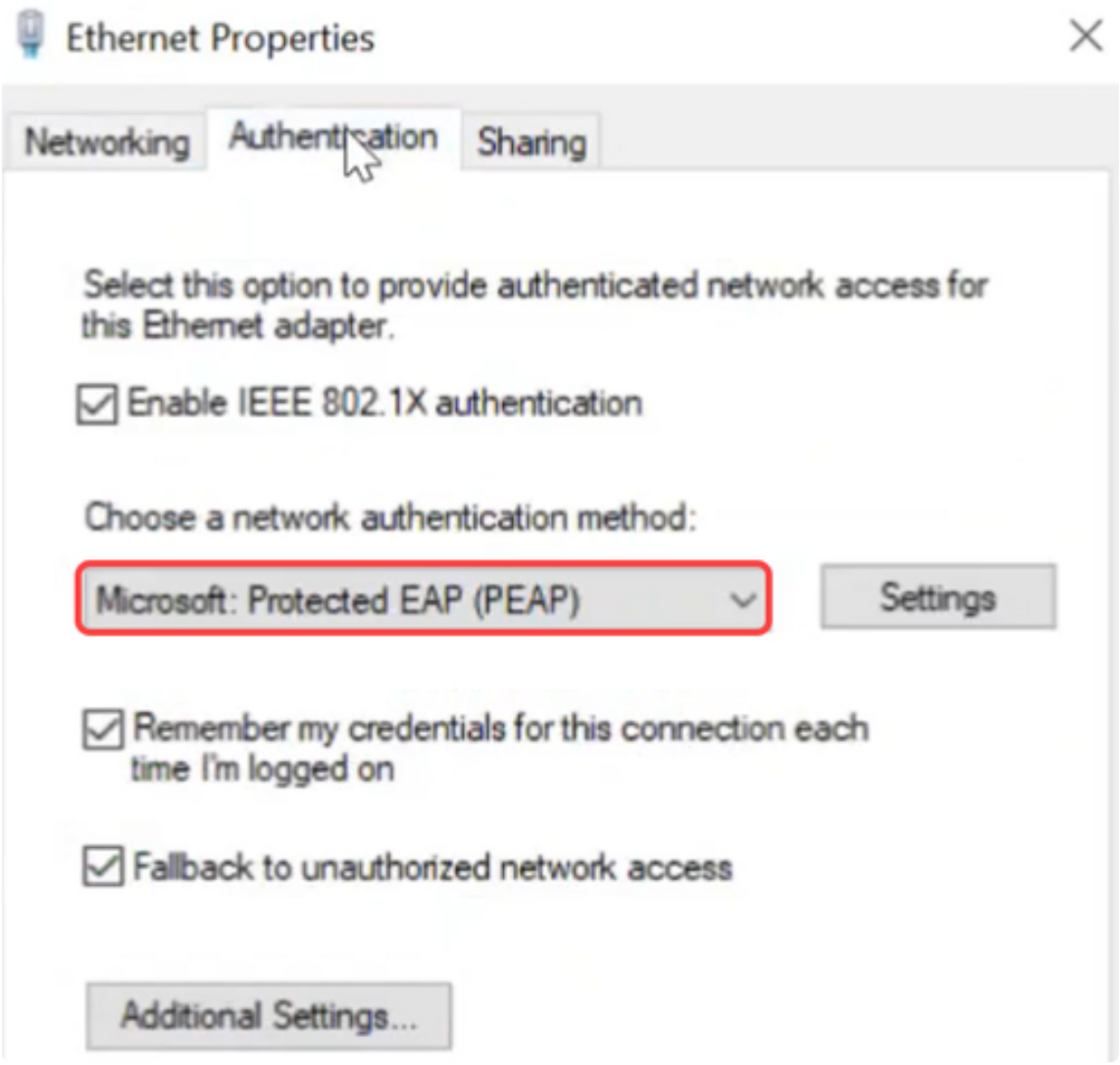
Étape 19

Dans les paramètres de la carte Ethernet, vérifiez que l'adresse MAC correspond.



Étape 20

Cliquez sur le bouton Properties sous Ethernet settings et sous l'onglet Authentication, vérifiez que les cases à cocher sont activées. Assurez-vous également que la méthode d'authentification est PEAP (Protected EAP).



Étape 21

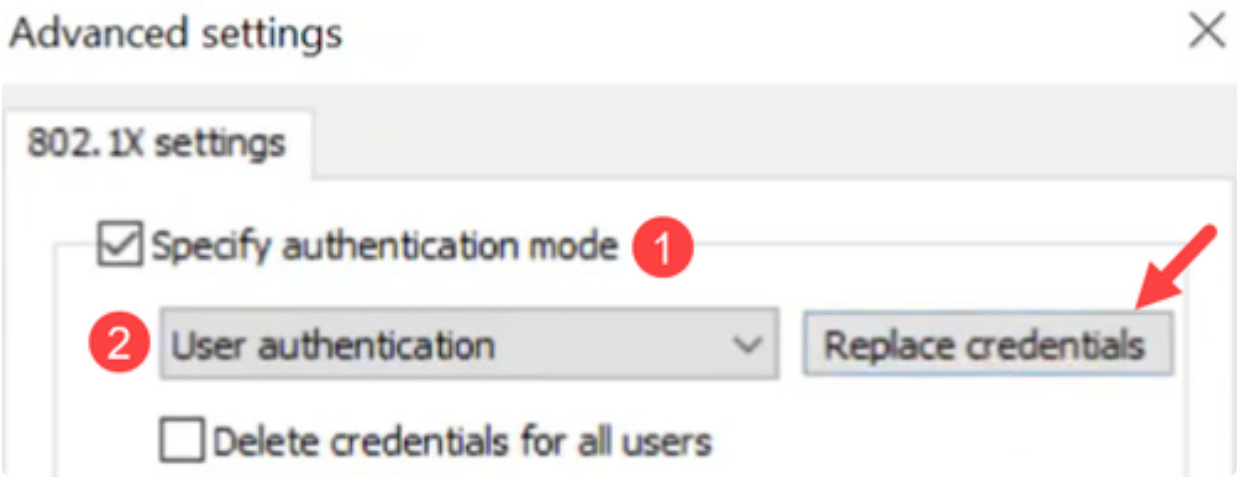
Cliquez sur le bouton Settings pour vous assurer que la case à cocher en regard de Verify the server’s identity by validating the certificate est décochée.

Étape 22

La case Enable Fast Reconnect doit être cochée.

Étape 23

Sous Additional settings, assurez-vous que Specify authentication mode est activé et que User authentication est sélectionné dans le menu déroulant. Vous pouvez enregistrer les informations d'identification créées sur ISE ou les remplacer à l'aide du bouton Remplacer les informations d'identification.



coopération administrative

Avant de lancer une opération CoA, activez la capture de paquets sur le commutateur.

Étape 1

Sur PuTTY, connectez-vous à votre commutateur Catalyst et spécifiez la taille de tampon et le mode de capture à l'aide de la commande monitor capture cap1 buffer size 20 circulaire.

Étape 2

Spécifiez le plan de contrôle comme étant les deux à l'aide de la commande monitor capture cap1 control-plane both.

Étape 3

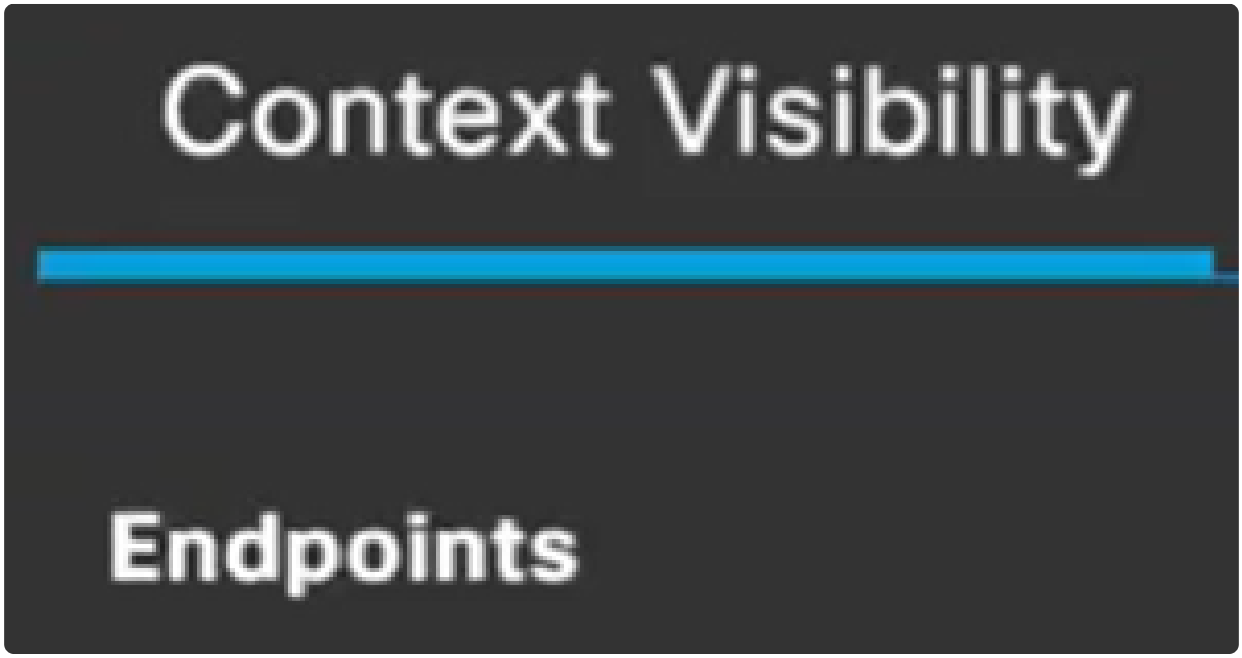
Saisissez le critère de correspondance comme suit : La commande pour cela sera monitor capture cap1 match any.

Étape 4

Démarrez la capture de paquets.

Étape 5

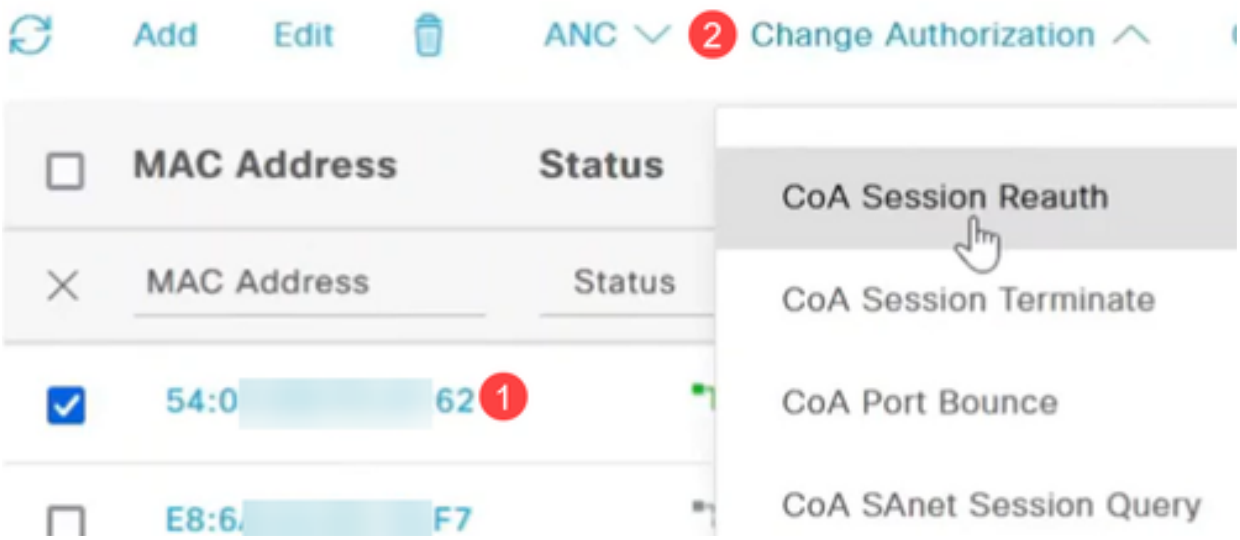
Sur l'interface ISE, accédez à l'option Endpoints sous Context Visibility.



Étape 6

Choisissez l'adresse MAC et sélectionnez l'opération CoA dans le menu déroulant Change of Authorization. Dans cet exemple, CoA Session Reauth est sélectionné.

Cela force la réauthentification sur le port en envoyant un paquet CoA avec une commande de réauthentification.



Étape 7

Revenez au terminal PuTTY pour vérifier si l'opération CoA a réussi.

```
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"
```

Étape 8

Si vous sélectionnez CoA Session Terminate, il enverra une demande de déconnexion avec une commande de fin basée sur une demande administrative.

```
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
```

Étape 9

L'option CoA Port Bounce envoie un paquet de requête CoA avec une commande bounce host port, désactivant et réactivant le port sur le commutateur. La carte réseau se déconnecte pendant 10 secondes et devient non autorisée. Il sera le retour en ligne,

devient autorisé et peut transférer des paquets.

```
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
```

Étape 10

La fin de la session CoA avec le renvoi du port met fin à la session existante, renvoie le port pendant 10 secondes et devient non autorisée. Il se reconnecte, devient autorisé et peut transférer des paquets.

```
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
```

Étape 11

La fin de la session CoA avec arrêt du port met fin à la session et arrête administrativement le port.

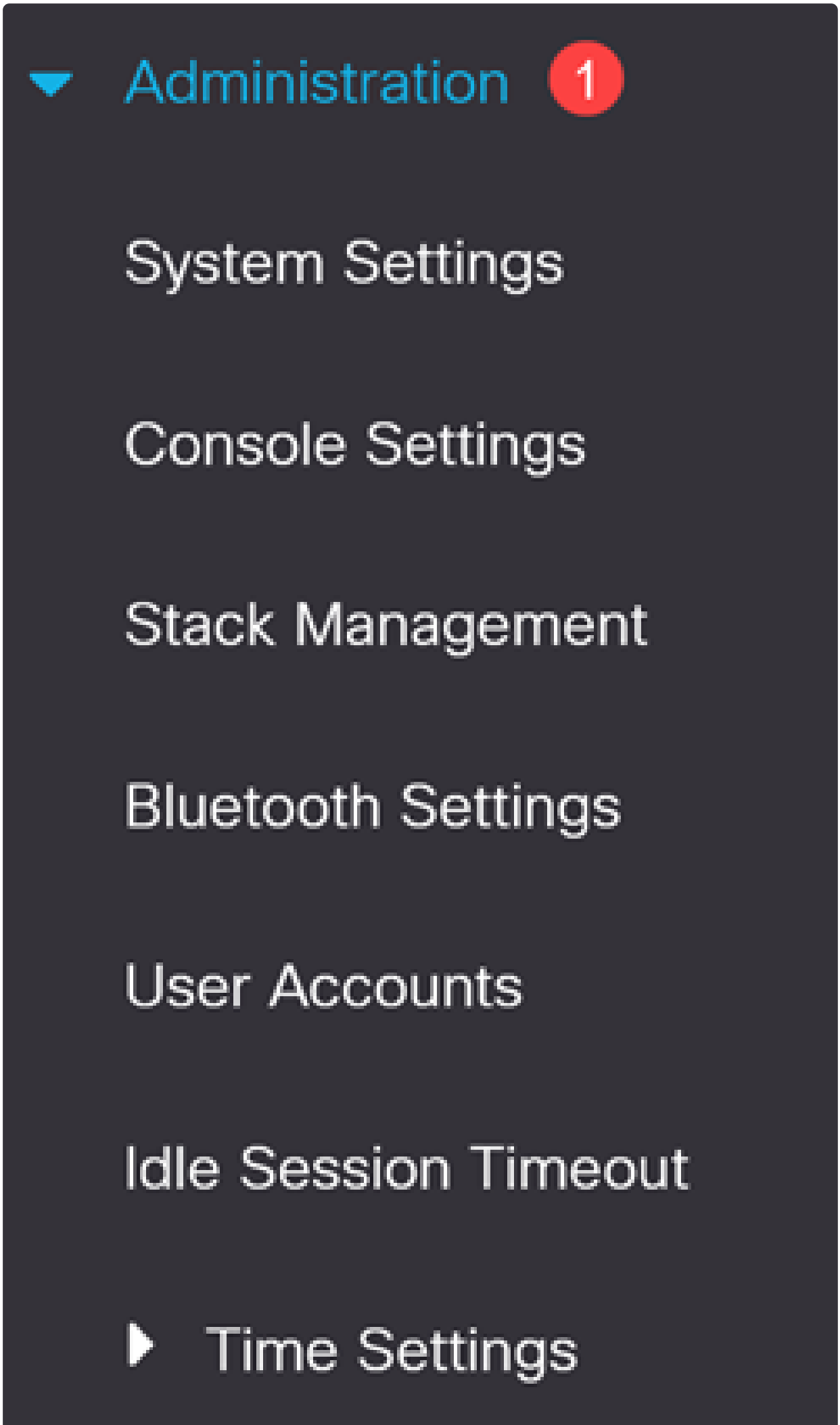
```
Cat1300-1#04-Jul-2024 20:51:47 %SEC-W-COADISPORT: Interface gi1/0/9 suspended by CoA Request "disab
le host port" for host 54:          :62
04-Jul-2024 20:51:47 %LINK-W-Down:  gi1/0/9
```

Étape 12

Pour arrêter la capture de paquets, utilisez la commande monitor capture cap1 stop.

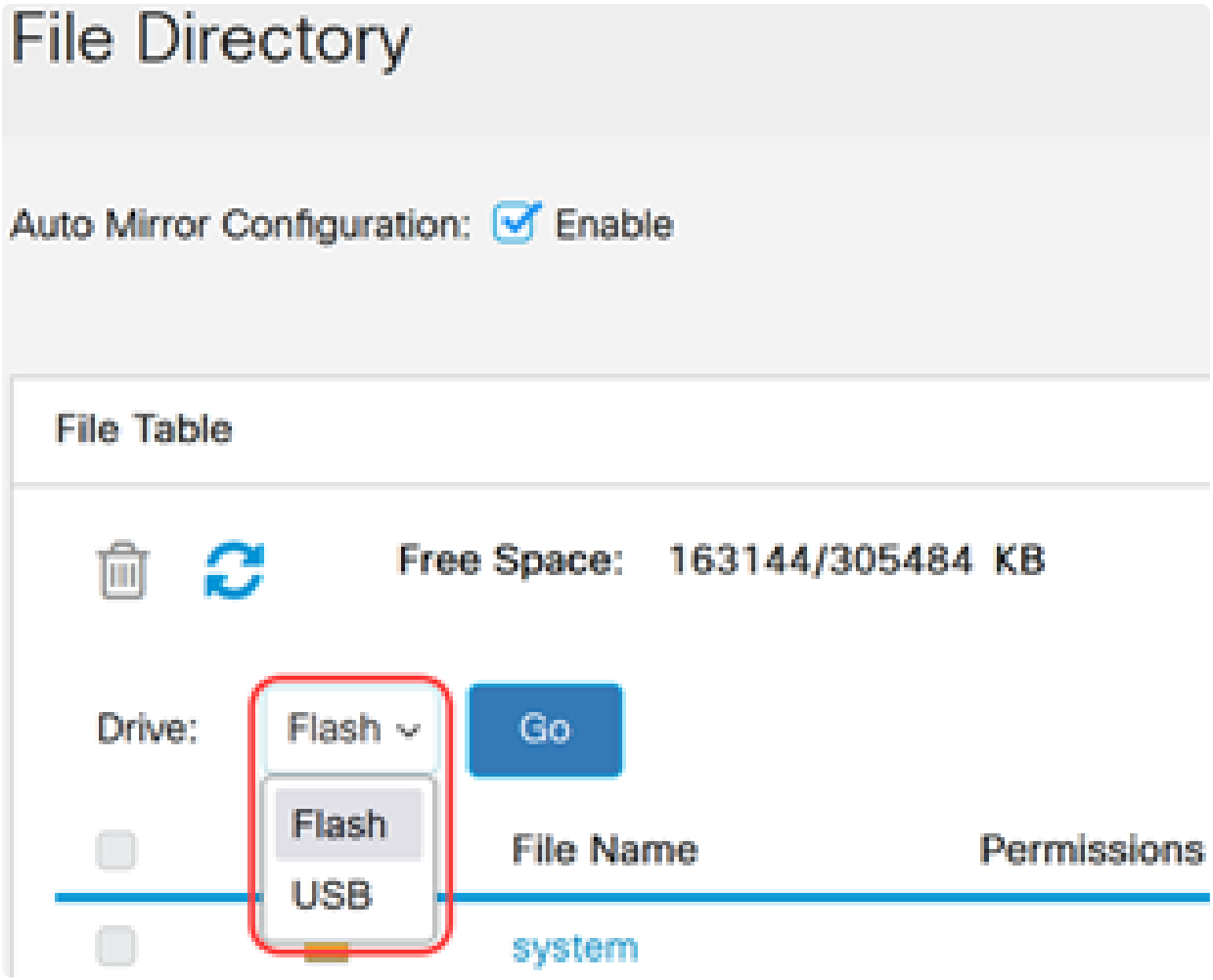
Étape 13

Pour copier les fichiers, accédez à Administration > File Management > File Directory.


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

Étape 14

La mémoire Flash par défaut est disponible. Vous pouvez également sélectionner USB dans le menu déroulant Drive (Lecteur).



Conclusion

Vous savez maintenant tout sur ISE et comment configurer CoA dans les commutateurs Catalyst 1300.

Pour plus d'informations, regardez la vidéo ci-dessous.

Visionner une vidéo connexe à cet article...

Cliquez ici pour consulter les autres discussions techniques (Tech Talks) de Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.