

Configuration de RADIUS & TACACS+ pour l'authentification CLI de & GUI sur les WLC 9800

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Restrictions utilisateur en lecture seule](#)

[Configurer l'authentification RADIUS pour le WLC](#)

[Configurer ISE pour RADIUS](#)

[Configuration du WLC TACACS+](#)

[Configuration de TACACS+ ISE](#)

[Dépannage](#)

[Dépannage de l'interface graphique WLC ou de l'accès CLI RADIUS/TACACS+ via l'interface CLI WLC](#)

[Dépannage de l'interface graphique WLC ou de l'accès CLITACACS+ via l'interface ISE](#)

Introduction

Ce document décrit comment configurer un Catalyst 9800 pour l'authentification externe RADIUS ou TACACS+.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modèle de configuration Catalyst Wireless 9800
- Concepts AAA, RADIUS et TACACS+

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- C980-CL v17.9.2

- ISE 3.2.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Lorsqu'un utilisateur tente d'accéder à l'interface de ligne de commande ou à l'interface graphique du WLC, il est invité à entrer un nom d'utilisateur et un mot de passe. Par défaut, ces informations d'identification sont comparées à la base de données locale des utilisateurs, qui est présente sur le périphérique lui-même. Alternativement, le WLC peut être instruit afin de comparer les informations d'identification d'entrée avec un serveur AAA distant : le WLC peut soit parler au serveur avec l'utilisation de RADIUS ou TACACS+.

Configurer

Dans cet exemple, deux types d'utilisateurs sur le serveur AAA (ISE), respectivement le `adminuser`, et le `helpdeskuser` sont configurés. Ces utilisateurs font respectivement partie des `admin-group` et `deshelpdesk-group` groupes. L'utilisateur `adminuser`, qui fait partie de la `admin-group`, doit se voir accorder un accès complet au WLC. D'un autre côté, le `helpdeskuser`, qui fait partie de la `helpdesk-group`, est destiné à n'être accordé que des privilèges de surveillance au WLC. Il n'y a donc pas d'accès à la configuration.

Cet article commence par configurer le WLC et ISE pour l'authentification RADIUS, puis il effectue la même opération pour TACACS+.

Restrictions utilisateur en lecture seule

Lorsque TACACS+ ou RADIUS est utilisé pour l'authentification WebUI 9800, les restrictions suivantes existent :

- Les utilisateurs disposant du niveau de privilège 0 existent mais n'ont pas accès à l'interface utilisateur graphique

-

Les utilisateurs ayant des niveaux de privilège de 1 à 14 peuvent uniquement afficher l'onglet Monitor (équivalent au niveau de privilège d'un utilisateur authentifié localement en lecture seule)

-

Les utilisateurs disposant du niveau de privilège 15 ont un accès complet

-

Les utilisateurs disposant de privilèges de niveau 15 et d'un jeu de commandes autorisant uniquement des commandes spécifiques ne sont pas pris en charge. L'utilisateur peut toujours exécuter des modifications de configuration via l'interface utilisateur Web

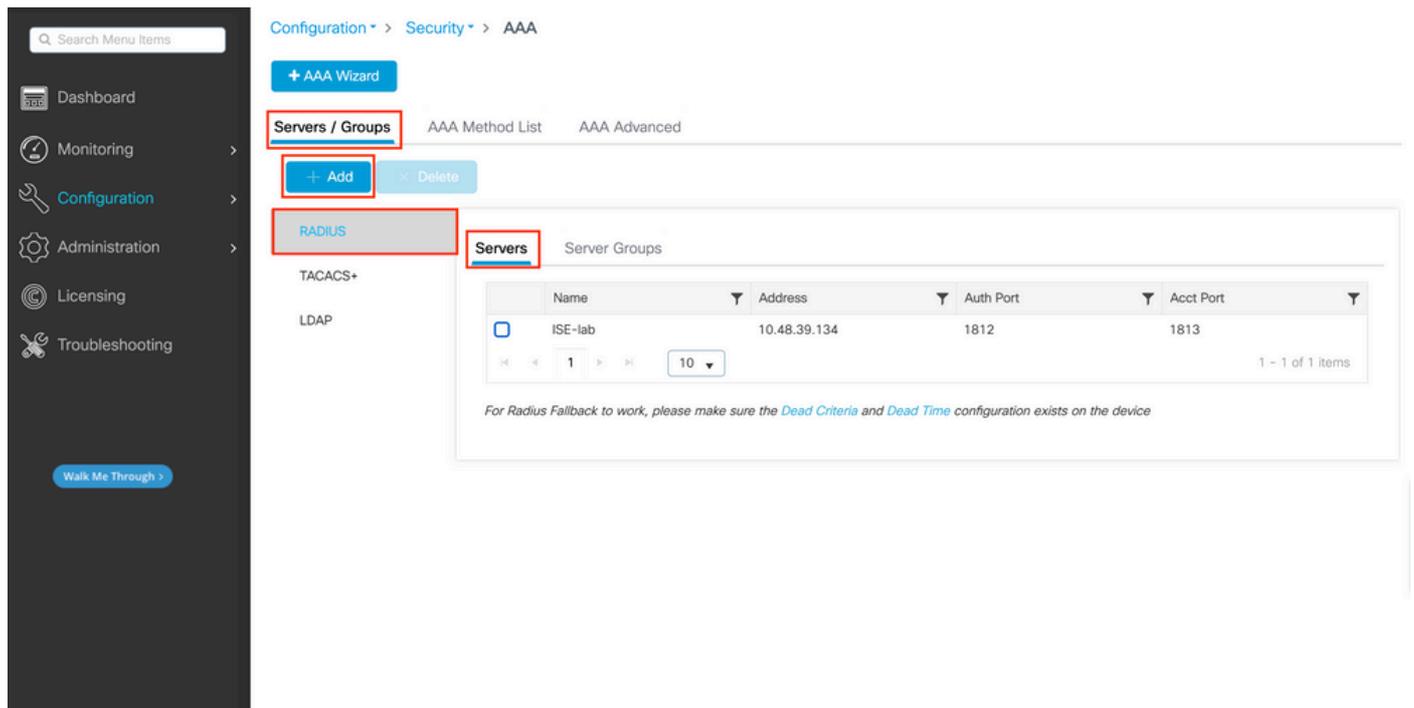
Ces considérations ne peuvent pas être modifiées.

Configurer l'authentification RADIUS pour le WLC

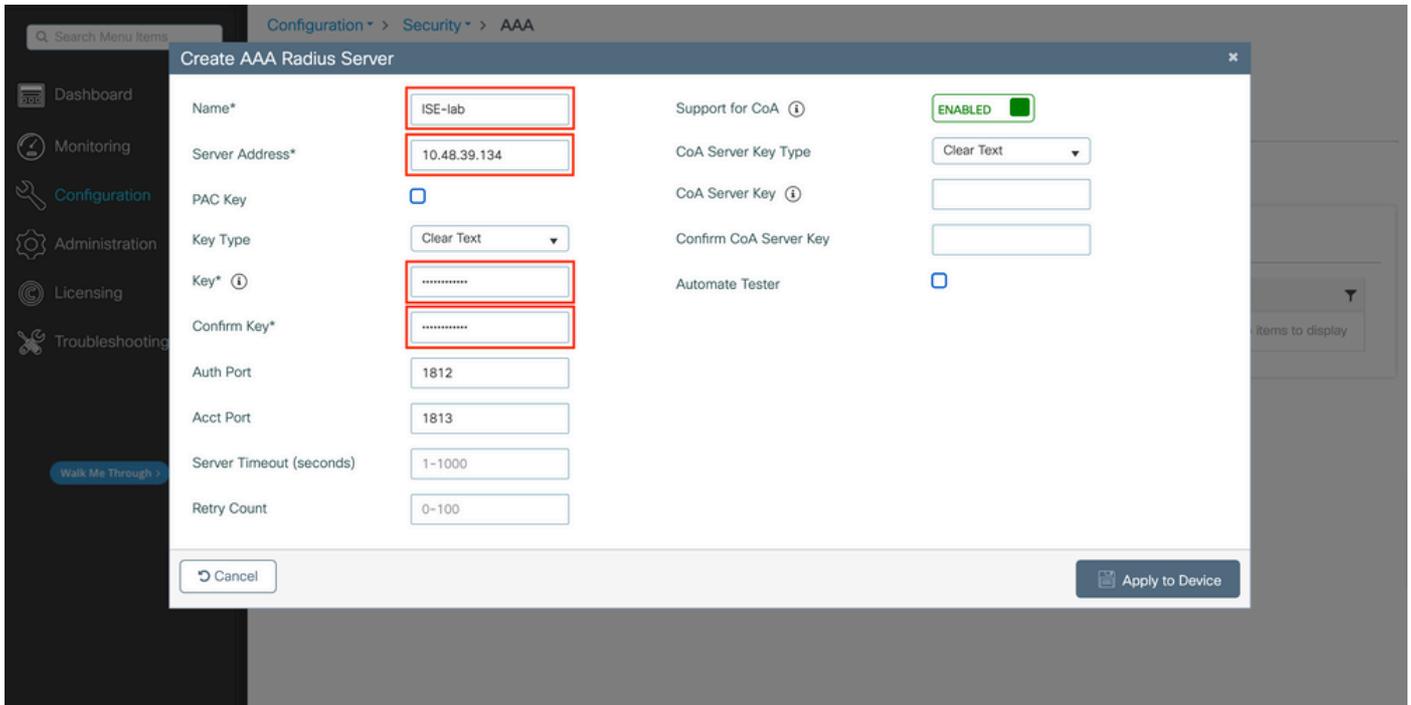
Étape 1. Déclarez le serveur RADIUS.

À partir de la GUI :

Tout d'abord, créez le serveur RADIUS ISE sur le WLC. Cela peut être fait à partir de l'onglet Servers/Groups > RADIUS > Servers de la page GUI WLC accessible dans <https://<WLC-IP>/webui/#/aaa>, ou si vous naviguez vers Configuration > Security > AAA , comme le montre cette image.



Pour ajouter un serveur RADIUS sur le WLC, cliquez sur le bouton Ajouter encadré en rouge dans l'image. La fenêtre contextuelle illustrée dans la capture d'écran s'ouvre.



Dans cette fenêtre contextuelle, vous devez fournir :

- Le nom du serveur (notez qu'il ne doit pas nécessairement correspondre au nom du système ISE)
- Adresse IP du serveur
- Le secret partagé entre le WLC et le serveur RADIUS

D'autres paramètres peuvent être configurés, tels que les ports utilisés pour l'authentification et la gestion des comptes, mais ils ne sont pas obligatoires et sont conservés par défaut pour cette documentation.

À partir de CLI :

```
<#root>
```

```
WLC-9800(config)#radius server
```

```
ISE-lab
```

```
WLC-9800(config-radius-server)#address ipv4
```

```
10.48.39.134
```

```
auth-port 1812 acct-port 1813
```

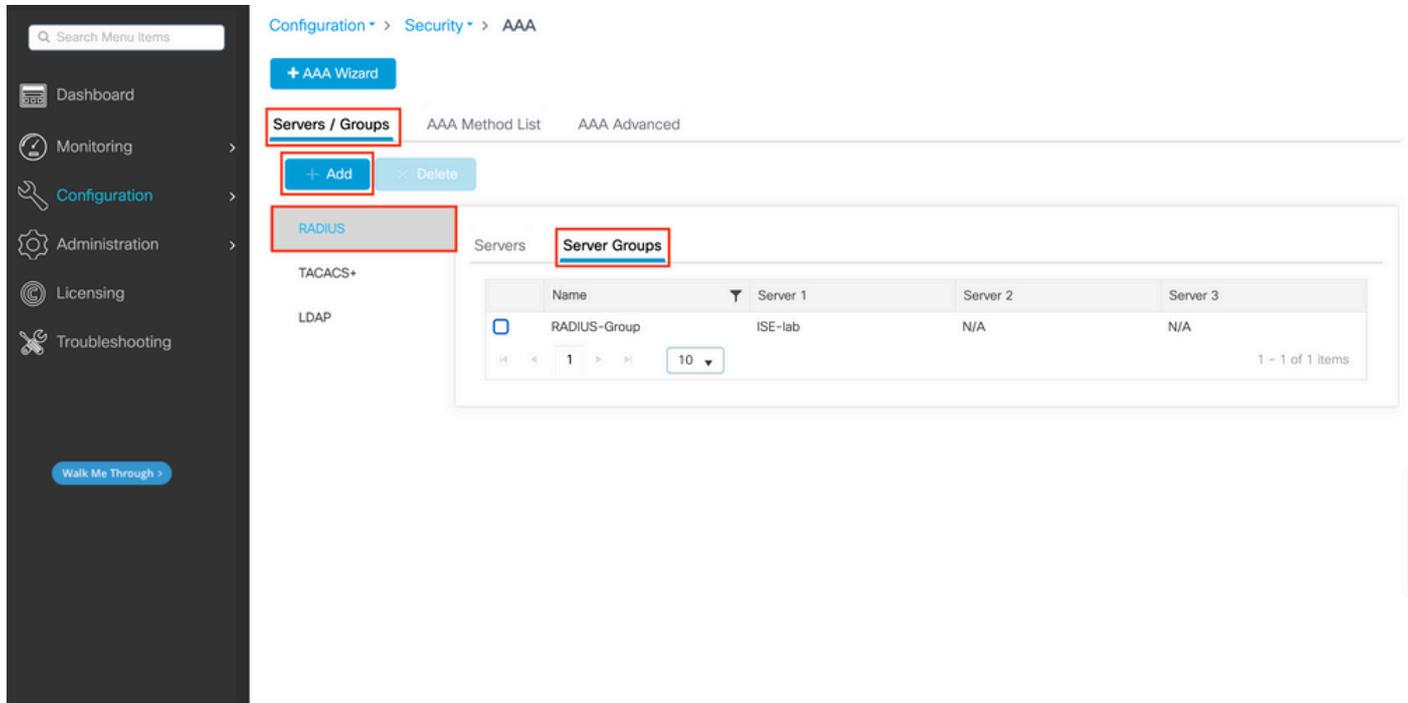
```
WLC-9800(config-radius-server)#key
```

```
Cisco123
```

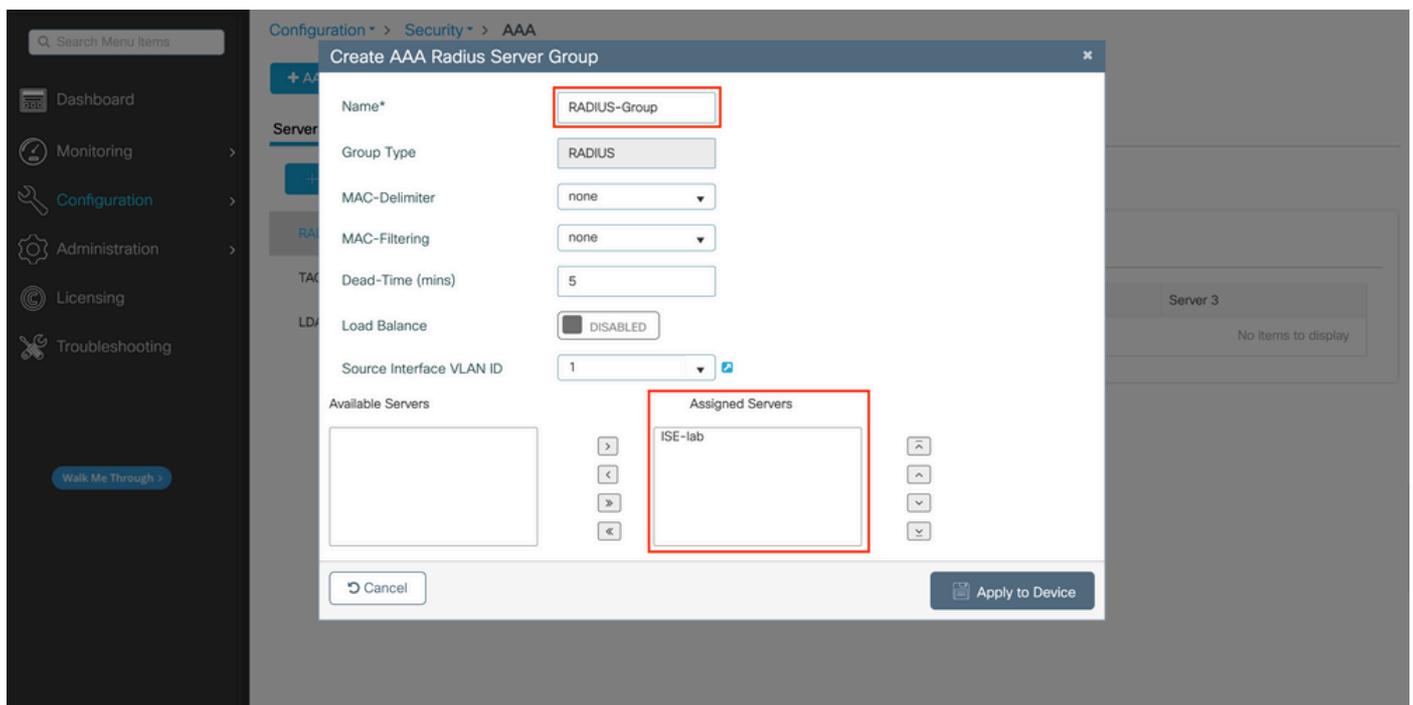
Étape 2. Mappez le serveur RADIUS à un groupe de serveurs.

À partir de la GUI :

Si vous disposez de plusieurs serveurs RADIUS pouvant être utilisés pour l'authentification, il est recommandé de mapper tous ces serveurs au même groupe de serveurs. Le WLC s'occupe de l'équilibrage de charge des différentes authentifications parmi les serveurs dans le groupe de serveurs. Les groupes de serveurs RADIUS sont configurés à partir de l'onglet Servers/Groups > RADIUS > Server Groups de la même page GUI que celle mentionnée à l'étape 1., comme illustré dans l'image.



En ce qui concerne la création du serveur, une fenêtre contextuelle apparaît lorsque vous cliquez sur le bouton Ajouter (encadré dans l'image précédente), qui est représenté ici.



Dans la fenêtre contextuelle, attribuez un nom au groupe et déplacez les serveurs souhaités vers la liste Serveurs affectés.

À partir de CLI :

____<#root>

WLC-9800(config)# aaa group server radius

RADIUS-Group

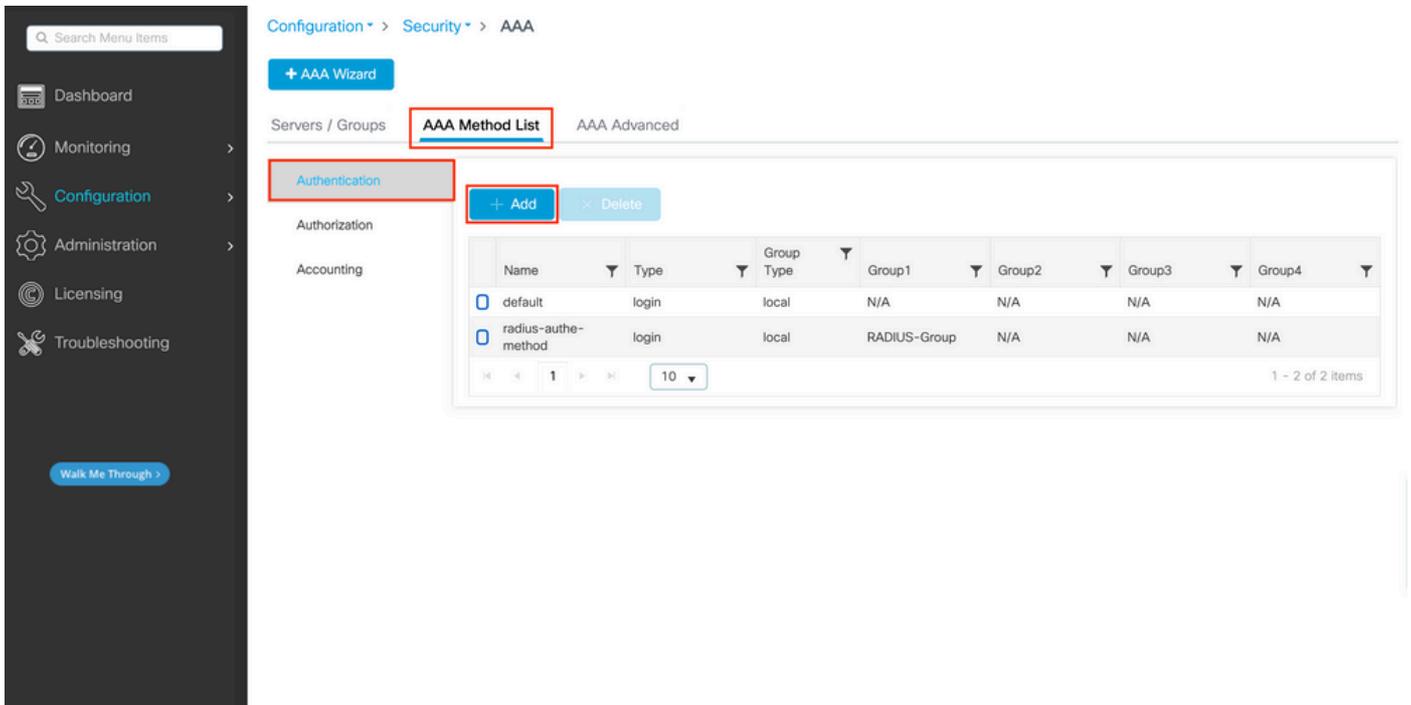
WLC-9800(config-sg-radius)# server name

ISE-lab

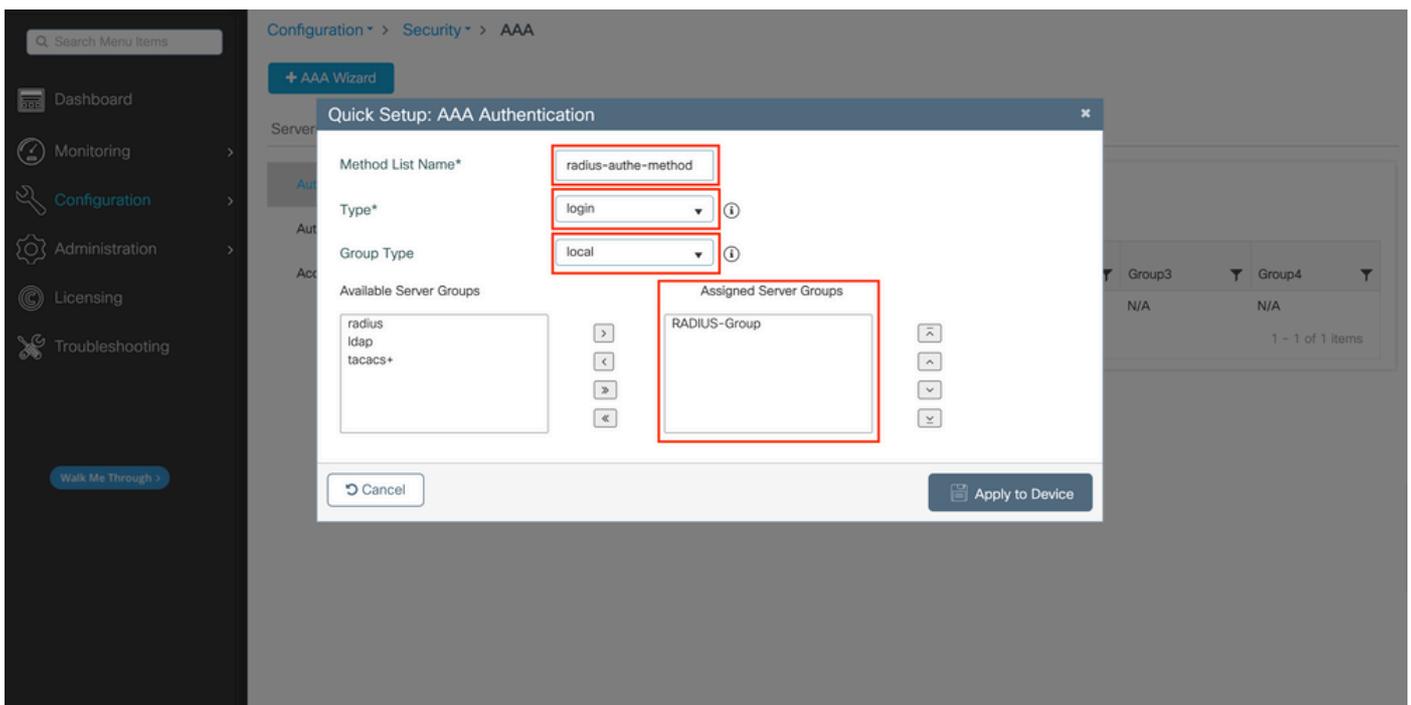
Étape 3. Créez une méthode de connexion d'authentification AAA qui pointe vers le groupe de serveurs RADIUS.

À partir de la GUI :

Toujours à partir de la page GUI <https://<WLC-IP>/webui/#/aaa>, accédez à l'onglet AAA Method List > Authentication et créez une méthode d'authentification comme illustré dans cette image.



Comme d'habitude, lorsque vous utilisez le bouton Ajouter pour créer une méthode d'authentification, une fenêtre contextuelle de configuration s'affiche, semblable à celle illustrée dans cette image.



Dans cette fenêtre contextuelle, attribuez un nom à la méthode. Choisissez Type comme connexion et ajoutez le serveur de groupe créé à l'étape précédente à la Assigned Server Groups liste. En ce qui concerne le champ Type de groupe, plusieurs configurations sont possibles.

- Si vous choisissez Group Type comme local, le WLC vérifie d'abord si les informations d'identification de l'utilisateur existent localement, puis revient au groupe de serveurs.
- Si vous choisissez Group Type comme groupe et ne cochez pas l'option Fall back to local, le WLC vérifie simplement les informations d'identification de l'utilisateur par rapport au groupe de serveurs.

- Si vous choisissez Group Type comme groupe et cochez l'option Fallback to local, le WLC vérifie les informations d'identification de l'utilisateur par rapport au groupe de serveurs et interroge la base de données locale uniquement si le serveur ne répond pas. Si le serveur envoie un refus, l'utilisateur doit être authentifié, même s'il peut exister dans la base de données locale.

À partir de CLI :

Si vous souhaitez que les informations d'identification de l'utilisateur soient vérifiées avec un groupe de serveurs uniquement si elles ne sont pas trouvées localement en premier, utilisez :

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

```
radius-auth-method
```

```
local group
```

```
RADIUS-Group
```

Si vous souhaitez que les informations d'identification de l'utilisateur soient vérifiées uniquement avec un groupe de serveurs, utilisez :

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

```
radius-auth-method
```

group

RADIUS-Group

Si vous souhaitez que les informations d'identification de l'utilisateur soient vérifiées avec un groupe de serveurs et si ce dernier ne répond pas par une entrée locale, utilisez :

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

radius-authe-method

group

RADIUS-Group

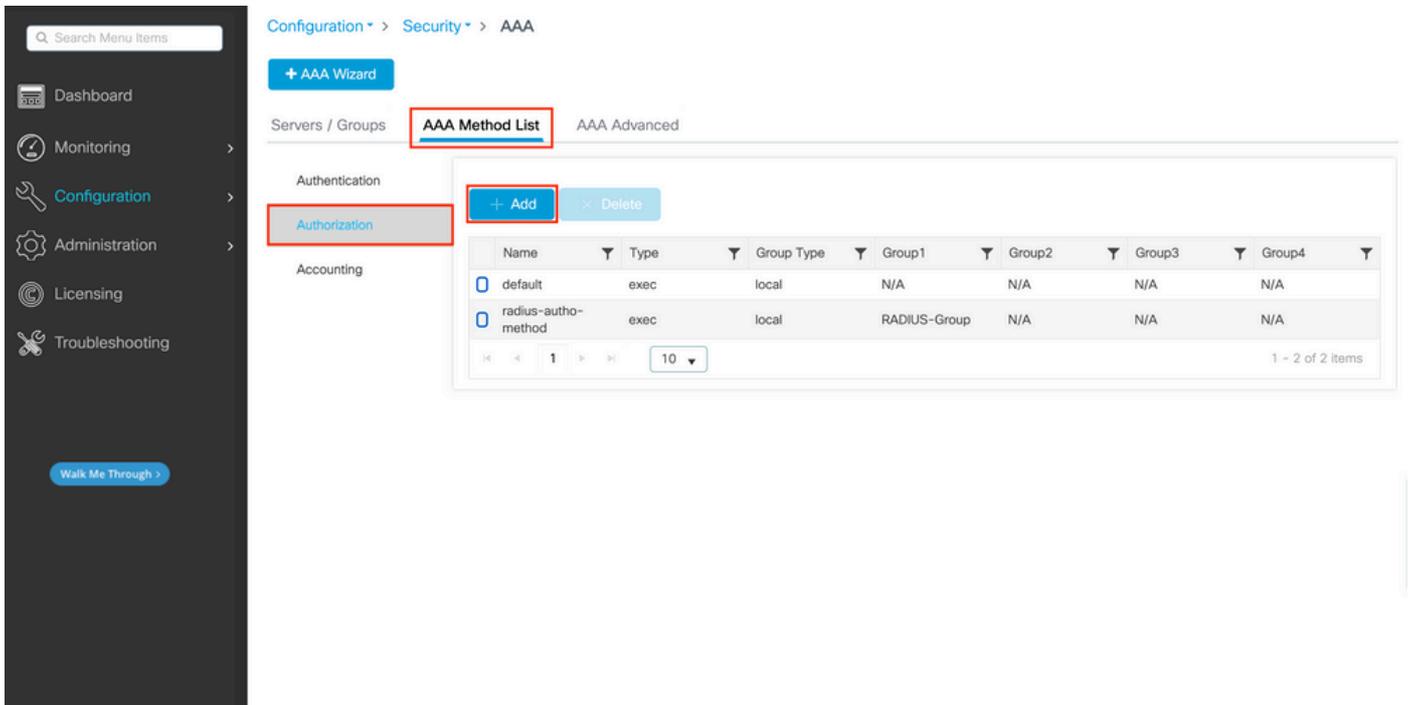
local

Dans cet exemple de configuration, certains utilisateurs sont uniquement créés localement et d'autres uniquement sur le serveur ISE. Par conséquent, utilisez la première option.

Étape 4. Créez une méthode d'exécution d'autorisation AAA qui pointe vers le groupe de serveurs RADIUS.

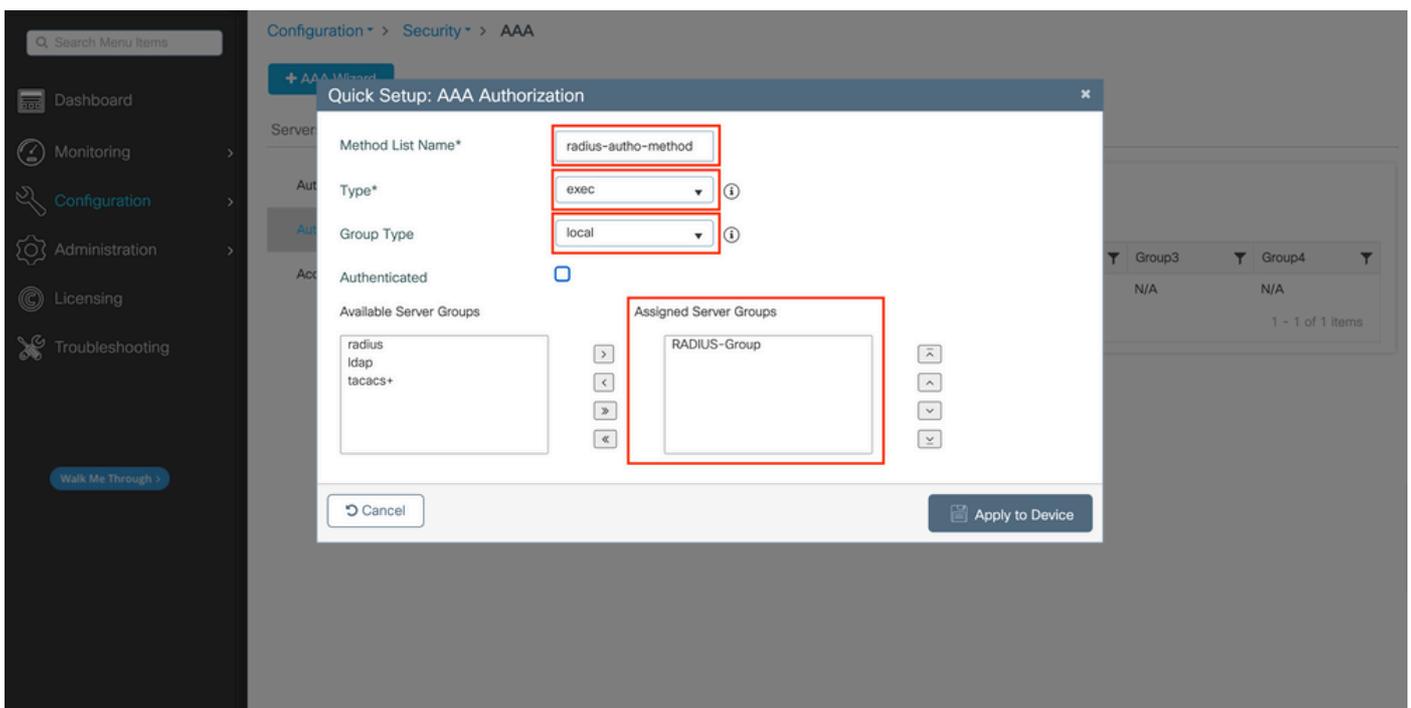
À partir de la GUI :

L'utilisateur doit également être autorisé pour se voir accorder l'accès. Toujours à partir de la GUI Page Configuration > Security > AAA, accédez à l'onglet, AAA Method List > Authorization et créez une méthode d'autorisation comme illustré dans cette image.



Création de méthode d'autorisation

Une fenêtre contextuelle de configuration de méthode d'autorisation similaire à celle illustrée s'affiche lorsque vous en ajoutez une nouvelle à l'aide du bouton Ajouter.



Dans cette fenêtre contextuelle de configuration, attribuez un nom à la méthode d'autorisation, sélectionnez le type exec, puis utilisez le même ordre de type de groupe que celui utilisé pour la méthode d'authentification à l'étape 3.

À partir de CLI :

En ce qui concerne la méthode d'authentification, l'autorisation est d'abord attribuée pour vérifier les utilisateurs par rapport aux entrées locales, puis par rapport aux entrées d'un groupe de serveurs.

WLC-9800(config)#aaa authorization exec

radius-autho-method

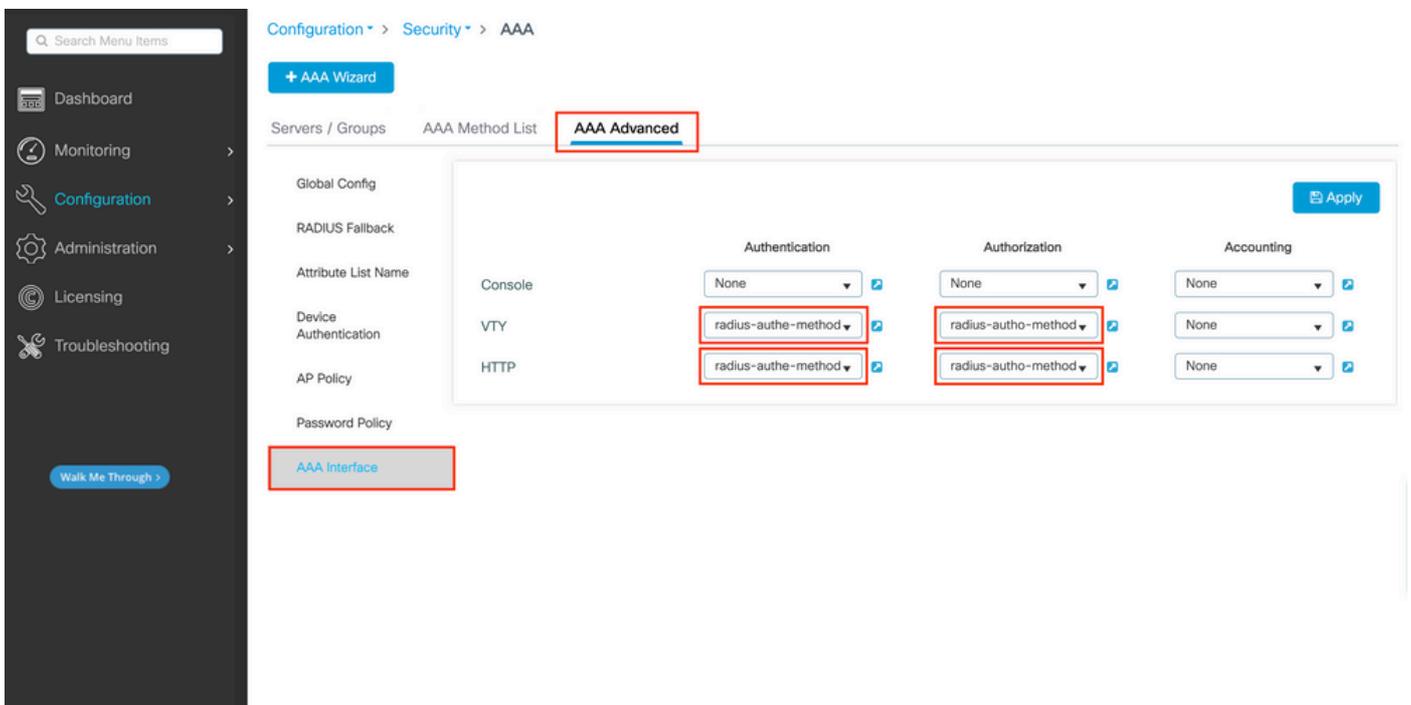
local group

RADIUS-Group

Étape 5. Attribuez les méthodes aux configurations HTTP et aux lignes VTY utilisées pour Telnet/SSH.

À partir de la GUI :

Les méthodes d'authentification et d'autorisation créées peuvent être utilisées pour la connexion utilisateur HTTP et/ou Telnet/SSH, qui est configurable à partir de l'onglet AAA Advanced > AAA Interface, toujours à partir de la page WLC de l'interface utilisateur graphique accessible dans <https://<WLC-IP>/webui/#/aaa>, comme illustré dans cette image :



CLI pour l'authentification GUI :

<#root>

WLC-9800(config)#ip http authentication aaa login-authentication

radius-auth-method

WLC-9800(config)#ip http authentication aaa exec-authorization

radius-auth-method

CLI pour l'authentification Telnet/SSH :

<#root>

WLC-9800(config)#line vty 0 15 WLC-9800(config-line)#login authentication

radius-auth-method

WLC-9800(config-line)#authorization exec

radius-auth-method

Notez que lorsque des modifications sont apportées aux configurations HTTP, il est préférable de redémarrer les services HTTP et HTTPS. Pour ce faire, utilisez les commandes suivantes :

```
WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-server
```

Configurer ISE pour RADIUS

Étape 1. Configurez le WLC comme périphérique réseau pour RADIUS.

À partir de la GUI :

Afin de déclarer le WLC utilisé dans la section précédente comme périphérique réseau pour RADIUS dans ISE, naviguez jusqu'à Administration > Network Ressources > Network Devices et ouvrez l'onglet Périphériques réseau, comme illustré dans l'image suivante.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb path is "Administration > Network Resources > Network Devices". The "Network Devices" tab is selected in the top navigation bar. The left sidebar shows "Network Devices" as the active section. The main content area displays a table with one device: "WLC-9800" with IP/Mask "10.48.39.133/32", Profile Name "Cisco", Location "All Locations", and Type "All Device Types". The "+ Add" button is highlighted in the top toolbar.

Pour ajouter un périphérique réseau, utilisez le bouton Ajouter, qui ouvre le nouvel écran de configuration du périphérique réseau.

Network Devices List > New Network Device

Network Devices

Name **WLC-9800**

Description

IP Address * IP: **10.48.39.133 / 32**

Device Profile **Cisco**

Model Name

Software Version

Network Device Group

Location **All Locations** [Set To Default](#)

IPSEC **Is IPSEC Device** [Set To Default](#)

Device Type **All Device Types** [Set To Default](#)

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret **.....** [Show](#)

Use Second Shared Secret [?](#)

Second Shared Secret [Show](#)

CoA Port **1700** [Set To Default](#)

RADIUS DTLS Settings [?](#)

DTLS Required [?](#)

Shared Secret **radius/dtls** [?](#)

Dans la nouvelle fenêtre, indiquez le nom du périphérique réseau et ajoutez son adresse IP. Choisissez les paramètres d'authentification RADIUS et configurez le même secret partagé RADIUS que celui utilisé sur le WLC.

Étape 2. Créez un résultat d'autorisation pour renvoyer le privilège.

À partir de la GUI :

Pour avoir des droits d'accès d'administrateur, le adminuser doit avoir un niveau de privilège de 15, ce qui permet d'accéder à l'interpréteur de commandes d'invite d'exécution. D'autre part, le helpdeskuser n'a pas besoin d'un accès rapide à l'interpréteur de commandes exec et peut donc être attribué avec un niveau de privilège inférieur à 15. Afin d'attribuer le niveau de privilège approprié aux utilisateurs, des profils d'autorisation peuvent être utilisés. Vous pouvez les configurer à partir de l'ISE GUI Page Policy > Policy Elements > Results, sous l'onglet Authorization > Authorization Profiles présenté dans l'image suivante.

- Authentication >
- Authorization >
- Authorization Profiles**
- Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >

Standard Authorization Profiles

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Selected 0 Total 11

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

All

<input type="checkbox"/>	Name	Profile	Description
<input type="checkbox"/>	9800-admin-priv	Cisco	
<input type="checkbox"/>	9800-helpdesk-priv	Cisco	
<input type="checkbox"/>	Block_Wireless_Access	Cisco	Default profile used to block wireless devices. Ensure th
<input type="checkbox"/>	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
<input type="checkbox"/>	Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal
<input type="checkbox"/>	NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
<input type="checkbox"/>	Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/>	UDN	Cisco	Default profile used for UDN.
<input type="checkbox"/>	DenyAccess	Cisco	Default Profile with access type as Access-Reject

Pour configurer un nouveau profil d'autorisation, utilisez le bouton Ajouter, qui ouvre le formulaire de configuration du nouveau profil d'autorisation. Ce formulaire doit notamment ressembler à ceci pour configurer le profil qui est attribué à l'adminuser.

Dictionarys Conditions **Results**

Authentication > Authorization Profiles > New Authorization Profile

Authorization Profile

* Name 9800-admin-priv

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

> Common Tasks

Advanced Attributes Settings

Cisco:cisco-av-pair = shell:priv-lvl=15

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = shell:priv-lvl=15

Submit Cancel

La configuration affichée accorde le niveau de privilège 15 à tout utilisateur auquel elle est associée. Comme indiqué précédemment, il s'agit du comportement attendu pour le adminuser qui est créé lors de l'étape suivante. Cependant, le helpdeskuser doit avoir un niveau de privilège inférieur, et par conséquent un deuxième élément de politique doit être créé.

L'élément de stratégie pour le helpdeskuser est similaire à celui créé ci-dessus, à ceci près que la chaîne shell:priv-lvl=15 doit être remplacée par shell:priv-lvl=X, et remplacer X par le niveau de privilège souhaité. Dans cet exemple, l'adresse 1 est utilisée.

Étape 3. Créez des groupes d'utilisateurs sur ISE.

À partir de la GUI :

Les groupes d'utilisateurs ISE sont créés à partir de l'onglet User Identity Groups du Administration > Identity Management > Groups GUI Page, qui est affiché dans la capture d'écran.

The screenshot shows the Cisco ISE Administration interface for Identity Management. The breadcrumb path is Administration > Identity Management. The 'Groups' tab is selected. In the left sidebar, 'User Identity Groups' is highlighted. The main area displays a table of existing groups with the '+ Add' button highlighted in red.

Name	Description
helpdesk-group	This is the group containing all users with read-only privileges.
admin-group	This is the group containing all users with administrator privileges.
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group
GuestType_Weekly (default)	Identity group mirroring the guest type
GuestType_SocialLogin (default)	Identity group mirroring the guest type
GuestType_Daily (default)	Identity group mirroring the guest type
GuestType_Contractor (default)	Identity group mirroring the guest type
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
Employee	Default Employee User Group
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group

Pour créer un nouvel utilisateur, utilisez le bouton Ajouter, qui ouvre le formulaire de configuration du nouveau groupe d'identités d'utilisateur comme illustré.

The screenshot shows the 'New User Identity Group' configuration form. The breadcrumb path is Administration > Identity Management > User Identity Groups > New User Identity Group. The 'Name' field is highlighted in red and contains the value 'admin-group'. The 'Description' field contains the text 'This is the group containing all users with administrator privileges.' There are 'Submit' and 'Cancel' buttons at the bottom.

Fournissez le nom du groupe qui est créé. Créez les deux groupes d'utilisateurs décrits ci-dessus, à savoir le admin-group et le helpdesk-group.

Étape 4. Créez des utilisateurs sur ISE.

À partir de la GUI :

Les utilisateurs ISE sont créés à partir de l'onglet Utilisateurs du Administration > Identity Management > Identities GUI Page, qui est affiché dans la capture d'écran.

Users

Latest Manual Network Scan Res...

Network Access Users

Selected 0 Total 2

Edit **+ Add** Change Status Import Export Delete Duplicate

All

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	Enabled	adminuser				admin-group	
<input type="checkbox"/>	Enabled	helpdeskus...				helpdesk-group	

Pour créer un nouvel utilisateur, utilisez le bouton Ajouter pour ouvrir le formulaire de configuration du nouvel utilisateur d'accès au réseau, comme illustré.

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username **adminuser**

Status Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration
Password will expire in 60 days

Never Expires

Password Re-Enter Password

* Login Password Generate Password

Enable Password Generate Password

> User Information

> Account Options

> Account Disable Policy

User Groups

admin-group

Fournissez les identifiants aux utilisateurs, à savoir son nom d'utilisateur et son mot de passe, qui sont ceux qui sont utilisés pour s'authentifier sur le WLC. Vérifiez également que l'état de l'utilisateur est Enabled. Enfin, ajoutez l'utilisateur à son groupe associé, créé à l'étape 4., avec le menu déroulant Groupes d'utilisateurs à la fin du formulaire.

Créez les deux utilisateurs mentionnés ci-dessus, à savoir le adminuser et le helpdeskuser.

Étape 5. Authentifiez les utilisateurs.

À partir de la GUI :

Dans ce scénario, la stratégie d'authentification des ensembles de stratégies par défaut d'ISE, qui est déjà préconfigurée, autorise l'accès réseau par défaut. Cet ensemble de stratégies est visible à partir Policy > Policy Sets de la page de l'interface utilisateur graphique ISE, comme illustré dans cette image. Il n'est donc pas nécessaire de la modifier.

Policy Sets → Default

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	0

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	0	⚙️
✓	Default		All_User_ID_Stores > Options	0	⚙️

Étape 6. Autorisez les utilisateurs.

À partir de la GUI :

Une fois que la tentative de connexion a réussi la stratégie d'authentification, elle doit être autorisée et ISE doit renvoyer le profil d'autorisation créé précédemment (permit accept, ainsi que le niveau de privilège).

Dans cet exemple, les tentatives de connexion sont filtrées en fonction de l'adresse IP du périphérique (qui est l'adresse IP du WLC) et distinguent le niveau de privilège à accorder en fonction du groupe auquel un utilisateur appartient. Une autre approche valide consiste à filtrer les utilisateurs en fonction de leurs noms d'utilisateur, car chaque groupe ne contient qu'un seul utilisateur dans cet exemple.

Policy Sets → Default

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	152

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

▼ Authorization Policy - Global Exceptions (2)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
✓	9800 Helpdesk Users	AND Network Access-Device IP Address EQUALS 10.48.39.133 InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group	9800-helpdesk-priv	Select from list	1	⚙️
✓	9800 Admin Users	AND Network Access-Device IP Address EQUALS 10.48.39.133 InternalUser-IdentityGroup EQUALS User Identity Groups:admin-group	9800-admin-priv	Select from list	2	⚙️

> Authorization Policy (12)

Reset Save

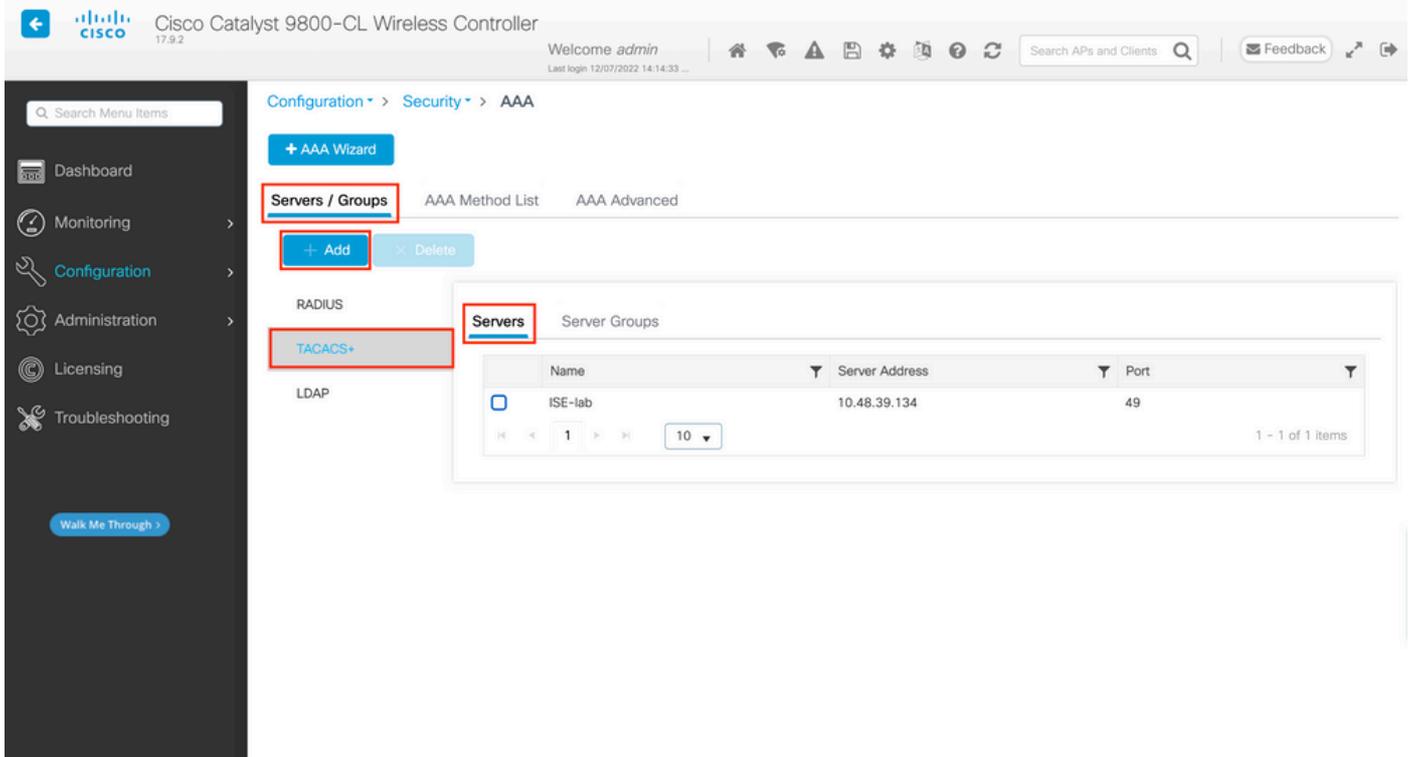
Une fois cette étape terminée, les informations d'identification configurées pour adminuser et helpdesk l'utilisateur peuvent être utilisées pour s'authentifier dans le WLC via l'interface graphique utilisateur ou via Telnet/SSH.

Configuration du WLC TACACS+

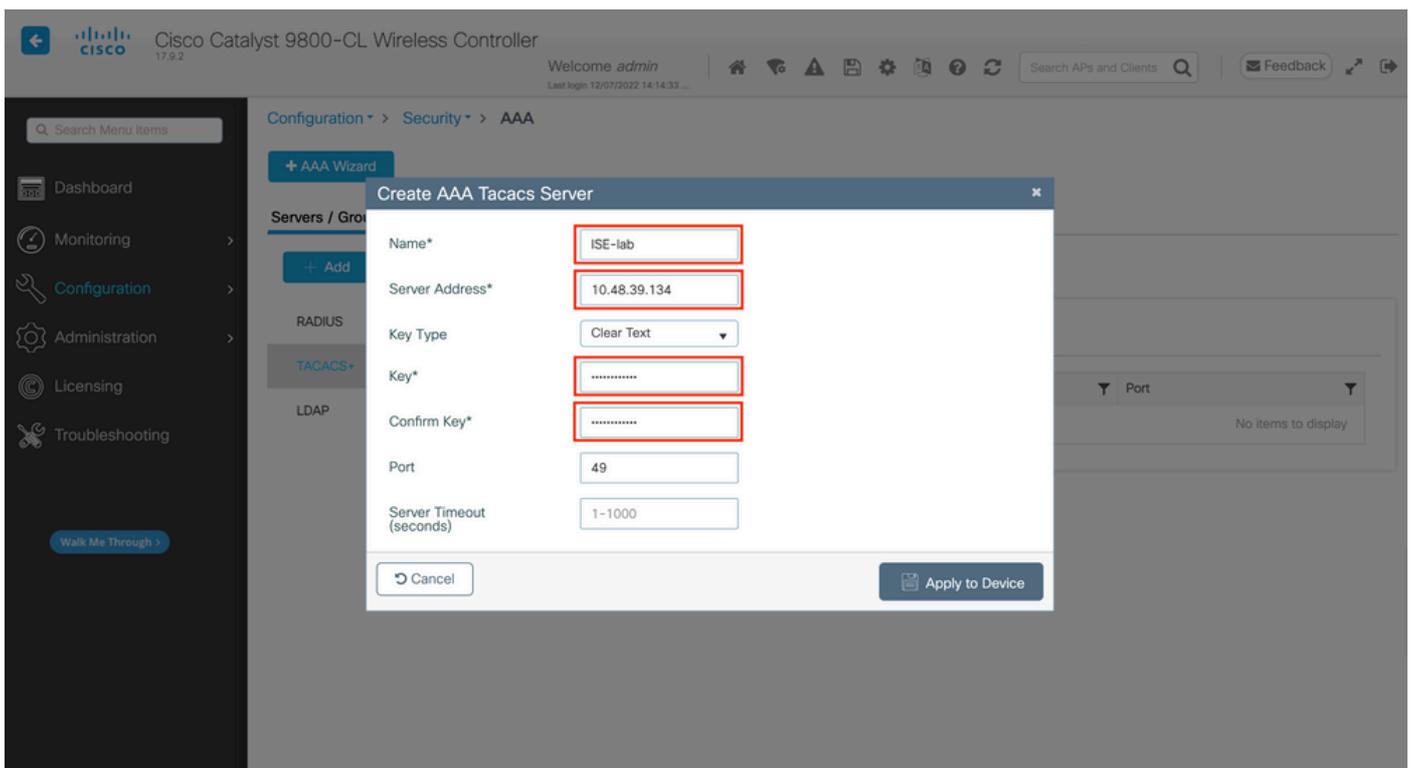
Étape 1. Déclarez le serveur TACACS+.

À partir de la GUI :

Tout d'abord, créez le serveur ISE Tacacs+ sur le WLC. Cela peut être fait à partir de l'onglet Servers/Groups > TACACS+ > Servers de la page GUI WLC accessible dans le <https://<WLC-IP>/webui/#/aaa>, ou si vous naviguez vers Configuration > Security > AAA, comme le montre cette image.



Pour ajouter un serveur TACACS sur le WLC, cliquez sur le bouton Add encadré en rouge dans l'image ci-dessus. La fenêtre contextuelle illustrée s'ouvre.



Lorsque la fenêtre contextuelle s'ouvre, indiquez le nom du serveur (il ne doit pas nécessairement correspondre au nom du système ISE), son adresse IP, la clé partagée, le port utilisé et le délai d'attente.

Dans cette fenêtre contextuelle, vous devez fournir :

- Le nom du serveur (notez qu'il ne doit pas nécessairement correspondre au nom du système ISE)

- Adresse IP du serveur
- Le secret partagé entre le WLC et le serveur TACACS+

D'autres paramètres peuvent être configurés, tels que les ports utilisés pour l'authentification et la comptabilité, mais ils ne sont pas obligatoires et restent par défaut pour cette documentation.

À partir de CLI :

```
<#root>
```

```
WLC-9800(config)#tacacs server
```

```
ISE-lab
```

```
WLC-9800(config-server-tacacs)#address ipv4
```

```
10.48.39.134
```

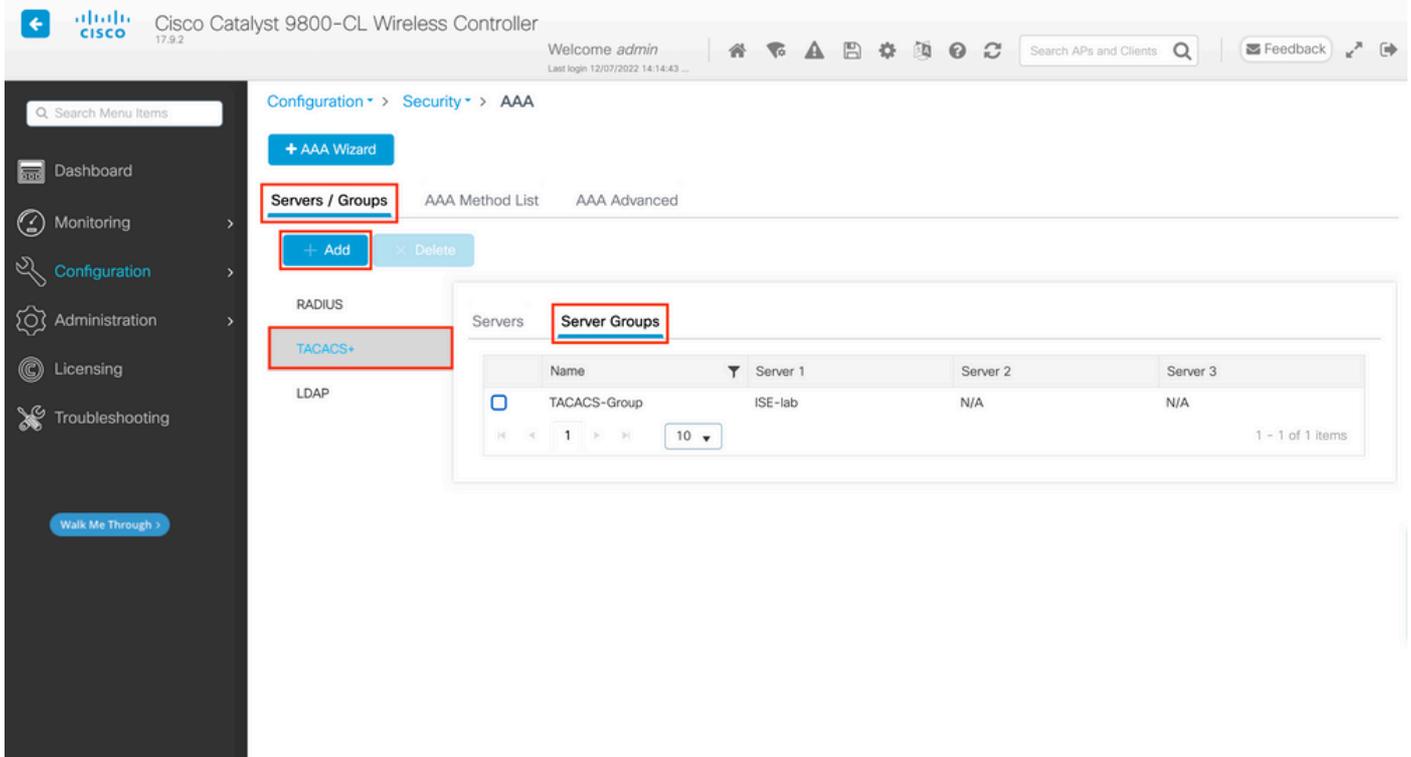
```
WLC-9800(config-server-tacacs)#key
```

```
Cisco123
```

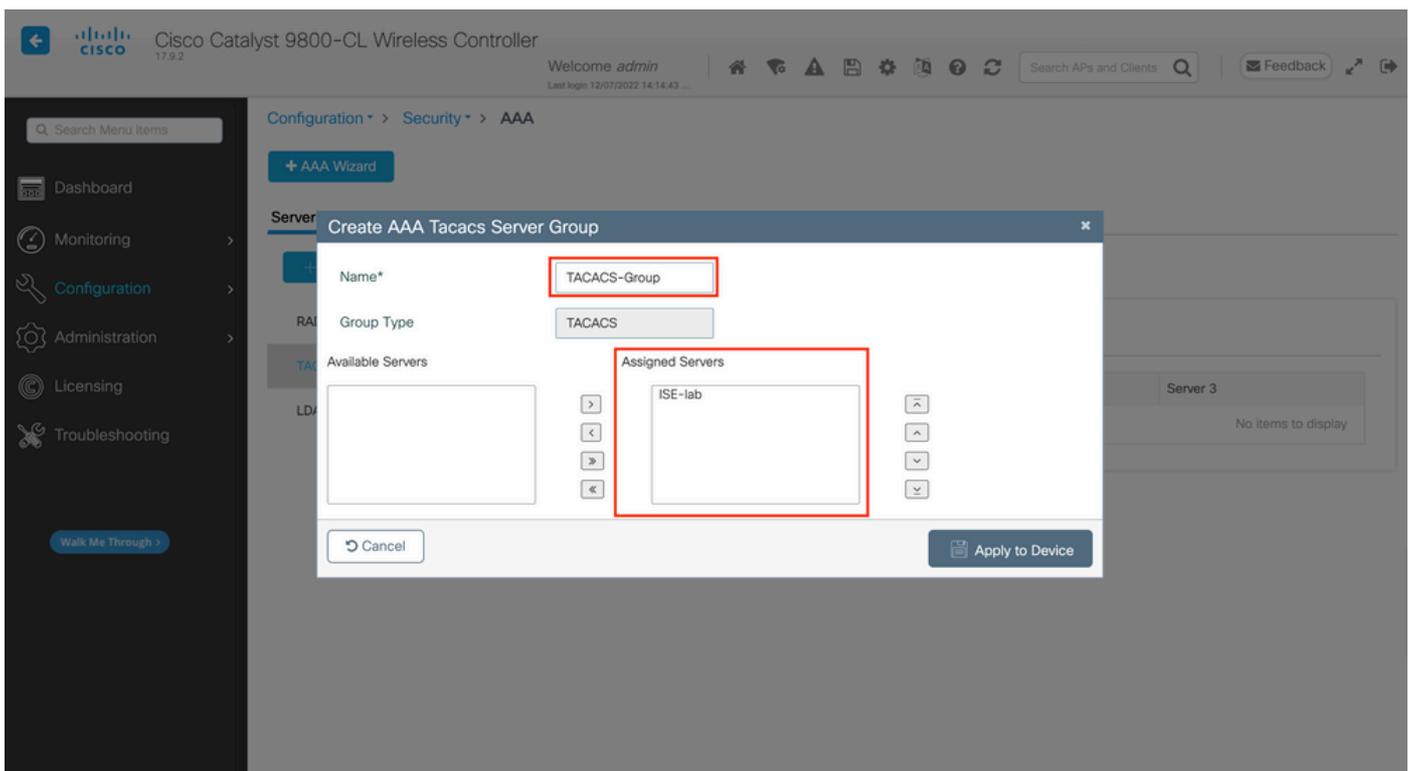
Étape 2. Mappez le serveur TACACS+ à un groupe de serveurs.

À partir de la GUI :

Si vous disposez de plusieurs serveurs TACACS+ pouvant être utilisés pour l'authentification, il est recommandé de mapper tous ces serveurs au même groupe de serveurs. Le WLC s'occupe ensuite de l'équilibrage de charge des différentes authentifications parmi les serveurs dans le groupe de serveurs. Les groupes de serveurs TACACS+ sont configurés à partir de l'onglet Servers/Groups > TACACS > Server Groups de la même page GUI que celle mentionnée à l'étape 1, qui est illustrée dans l'image.



En ce qui concerne la création du serveur, une fenêtre contextuelle apparaît lorsque vous cliquez sur le bouton Ajouter encadré dans l'image précédente, qui est représentée dans l'image.



Dans la fenêtre contextuelle, attribuez un nom au groupe et déplacez les serveurs souhaités vers la liste Serveurs affectés.

À partir de CLI :

<#root>

WLC-9800(config)#aaa group server tacacs+

TACACS-Group

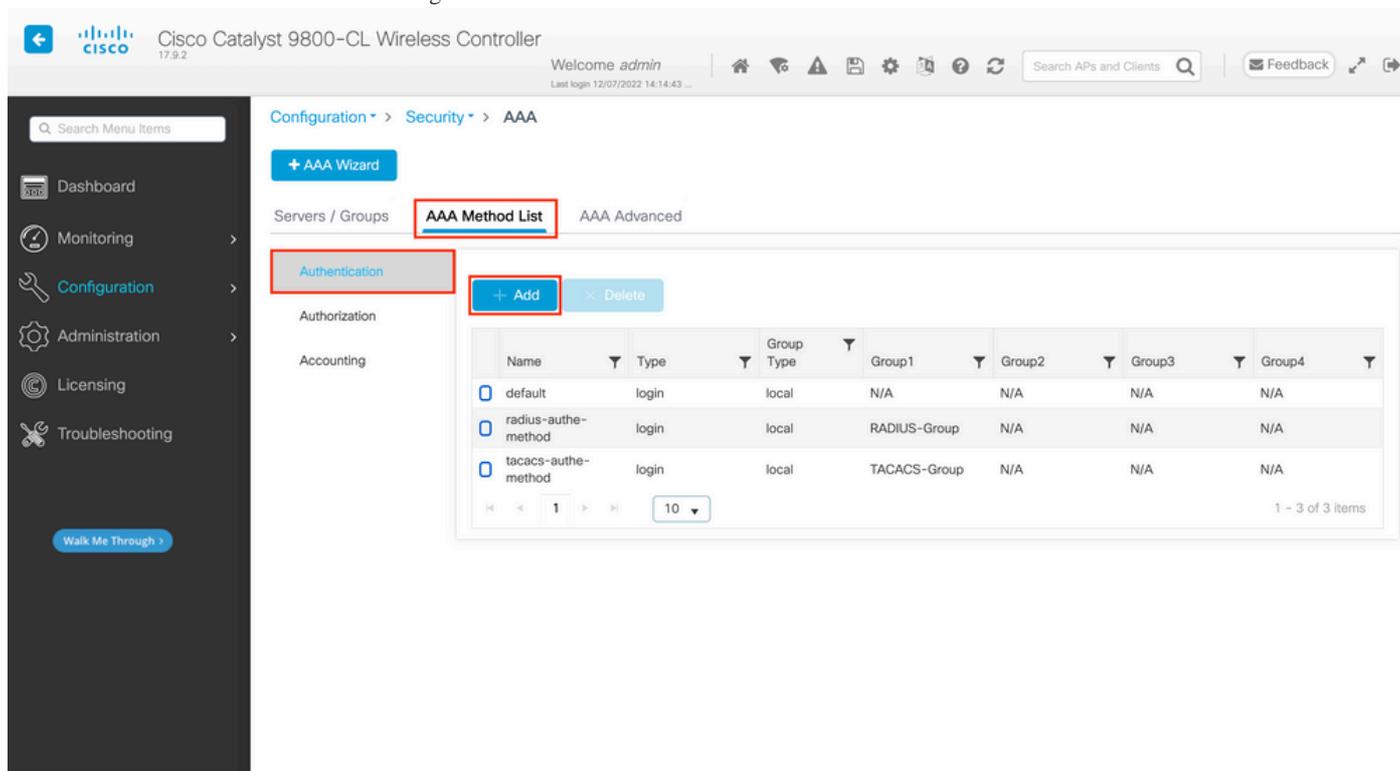
WLC-9800(config-sg-tacacs+)#server name

ISE-lab

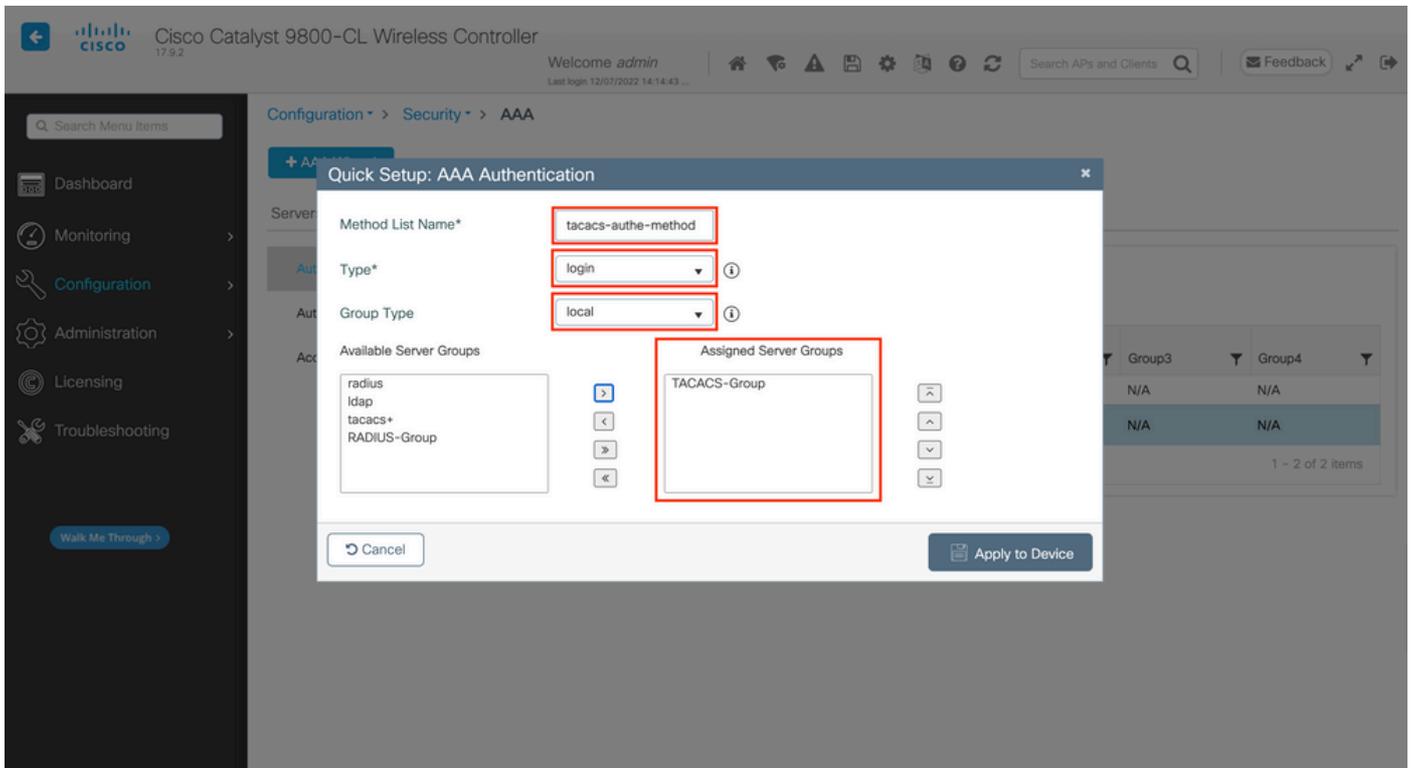
Étape 3. Créez une méthode de connexion d'authentification AAA qui pointe vers le groupe de serveurs TACACS+.

À partir de la GUI :

Toujours à partir de la page GUI <https://<WLC-IP>/webui/#/aaa>, accédez à l'AAA Method List > Authentication onglet et créez une méthode d'authentification comme illustré dans l'image.



Comme d'habitude, lorsque vous utilisez le bouton Ajouter pour créer une méthode d'authentification, une fenêtre contextuelle de configuration s'affiche, semblable à celle illustrée dans cette image.



Dans cette fenêtre contextuelle, attribuez un nom à la méthode, choisissez Type comme login, puis ajoutez le serveur de groupe créé à l'étape précédente à la liste Groupes de serveurs affectés. En ce qui concerne le champ Type de groupe, plusieurs configurations sont possibles.

- Si vous choisissez Group Type comme local, le WLC vérifie d'abord si les informations d'identification de l'utilisateur existent localement, puis revient au groupe de serveurs.
- Si vous choisissez Group Type comme groupe et ne cochez pas l'option Fall back to local, le WLC vérifie simplement les informations d'identification de l'utilisateur par rapport au groupe de serveurs.
- Si vous choisissez Group Type comme groupe et cochez l'option Fallback to local, le WLC vérifie les informations d'identification de l'utilisateur par rapport au groupe de serveurs et interroge la base de données locale uniquement si le serveur ne répond pas. Si le serveur envoie un refus, l'utilisateur doit être authentifié, même s'il peut exister dans la base de données locale.

À partir de CLI :

Si vous souhaitez que les informations d'identification de l'utilisateur soient vérifiées avec un groupe de serveurs uniquement si elles ne sont pas trouvées localement en premier, utilisez :

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

tacacs-auth-method

local group

TACACS-Group

Si vous souhaitez que les informations d'identification de l'utilisateur soient vérifiées uniquement avec un groupe de serveurs, utilisez :

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

group

TACACS-Group

Si vous souhaitez que les informations d'identification de l'utilisateur soient vérifiées avec un groupe de serveurs et si ce dernier ne répond pas avec une entrée locale, utilisez :

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

group

TACACS-Group

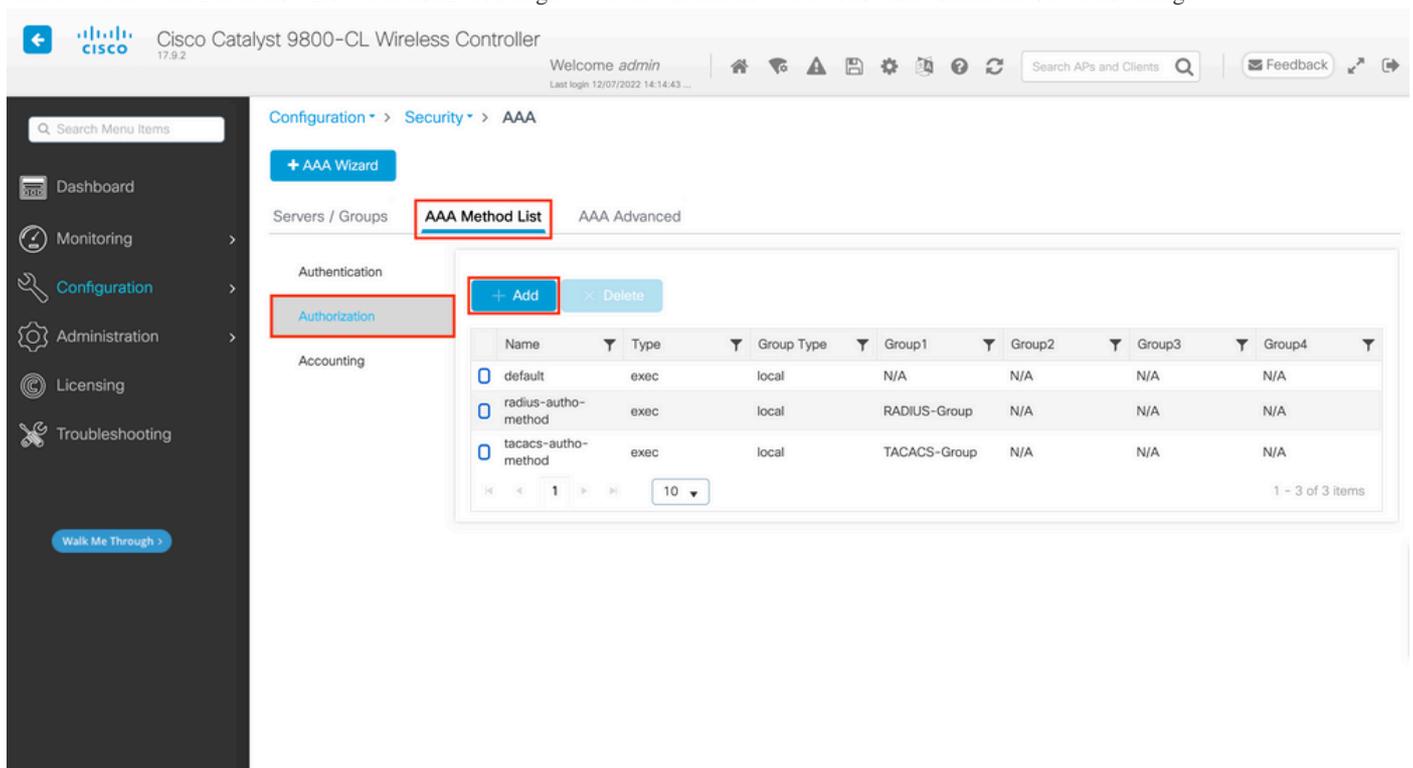
local

Dans cet exemple de configuration, certains utilisateurs sont uniquement créés localement, et d'autres uniquement sur le serveur ISE. Par conséquent, utilisez la première option.

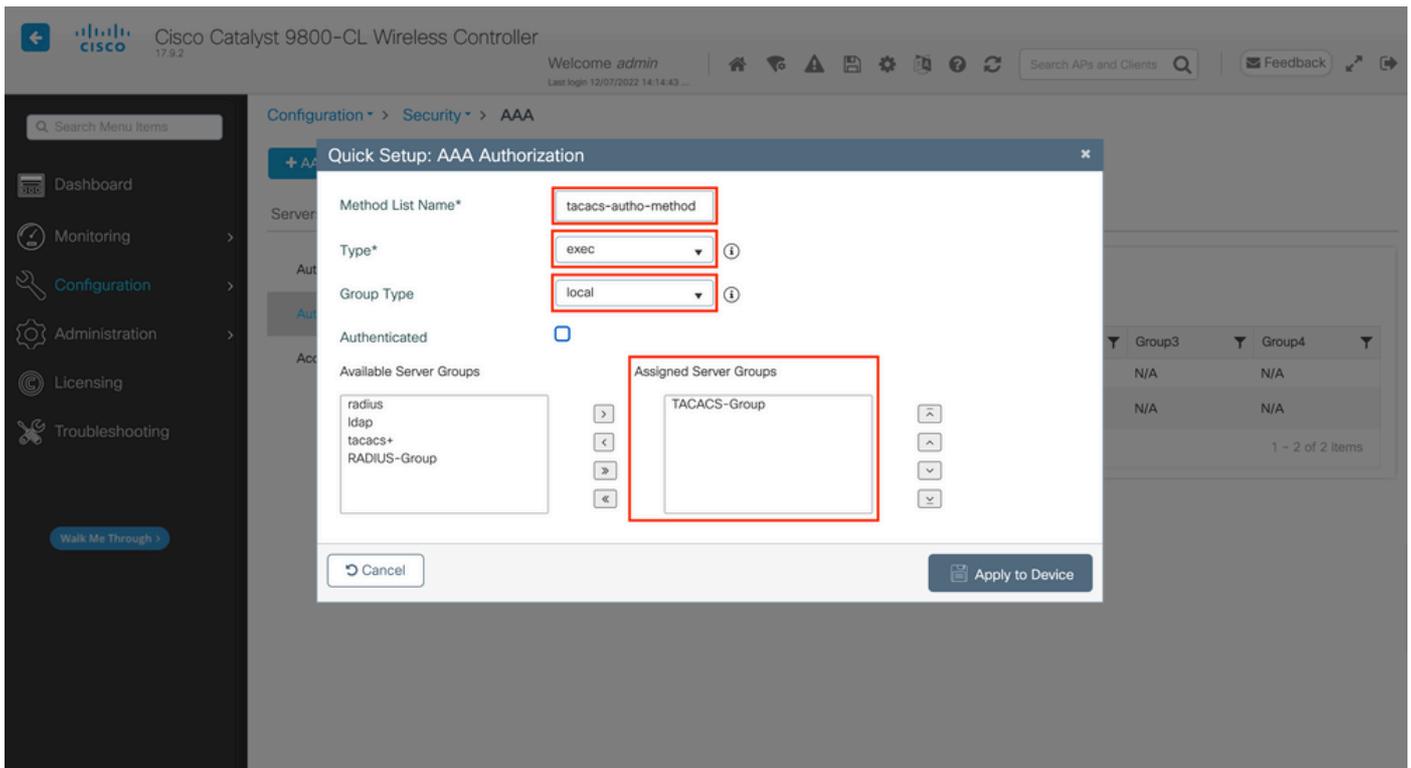
Étape 4. Créez une méthode d'exécution d'autorisation AAA qui pointe vers le groupe de serveurs TACACS+.

À partir de la GUI :

L'utilisateur doit également être autorisé pour se voir accorder l'accès. Toujours à partir de la page GUI, Configuration > Security > AAA accédez à l'AAA Method List > Authorization onglet et créez une méthode d'autorisation comme illustré dans l'image.



Une fenêtre contextuelle de configuration de méthode d'autorisation similaire à celle illustrée s'affiche lorsque vous en ajoutez une nouvelle à l'aide du bouton Ajouter.



Dans cette fenêtre contextuelle de configuration, attribuez un nom à la méthode d'autorisation, choisissez Type as exec et utilisez le même ordre de type de groupe que celui utilisé pour la méthode d'authentification à l'étape précédente.

À partir de CLI :

```
<#root>
```

```
WLC-9800(config)#aaa authorization exec
```

```
tacacs-autho-method
```

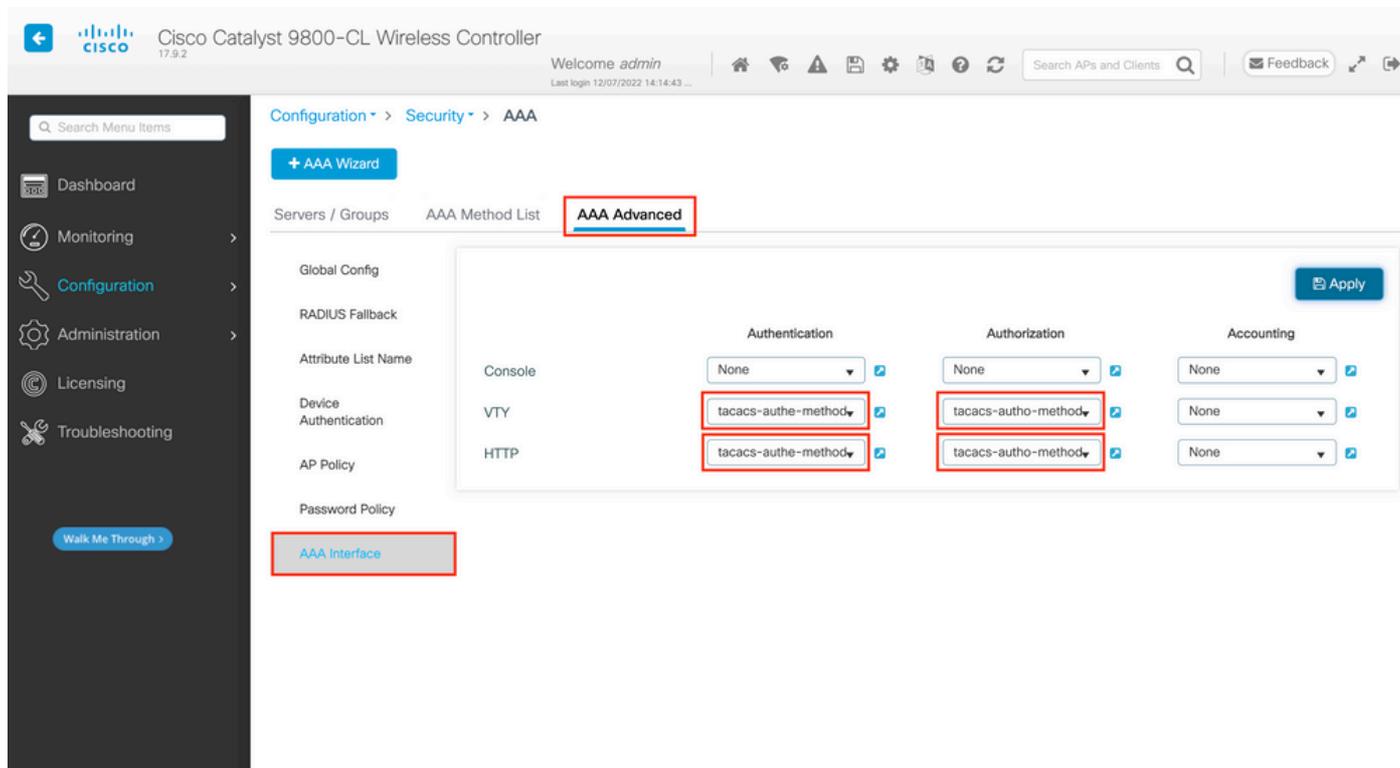
```
local group
```

```
TACACS-Group
```

Étape 5. Attribuez les méthodes aux configurations HTTP et aux lignes VTY utilisées pour Telnet/SSH.

À partir de la GUI :

Les méthodes d'authentification et d'autorisation créées peuvent être utilisées pour la connexion utilisateur HTTP et/ou Telnet/SSH, qui est configurable à partir de l'onglet AAA Advanced > AAA Interface, toujours à partir de la page GUI WLC accessible dans <https://<WLC-IP>/webui/#/aaa>, comme illustré dans l'image.



À partir de CLI :

Pour l'authentification GUI :

```
<#root>
```

```
WLC-9800(config)#ip http authentication aaa login-authentication
```

```
tacacs-auth-method
```

```
WLC-9800(config)#ip http authentication aaa exec-authorization
```

```
tacacs-auth-method
```

Pour l'authentification Telnet/SSH :

```
<#root>
```

```
WLC-9800(config)#line vty 0 15  
WLC-9800(config-line)#login authentication
```

```
tacacs-auth-method
```

```
WLC-9800(config-line)#authorization exec
```

```
tacacs-auth-method
```

Notez que lorsque des modifications sont apportées aux configurations HTTP, il est préférable de redémarrer les services HTTP et HTTPS. Ces commandes permettent d'y parvenir.

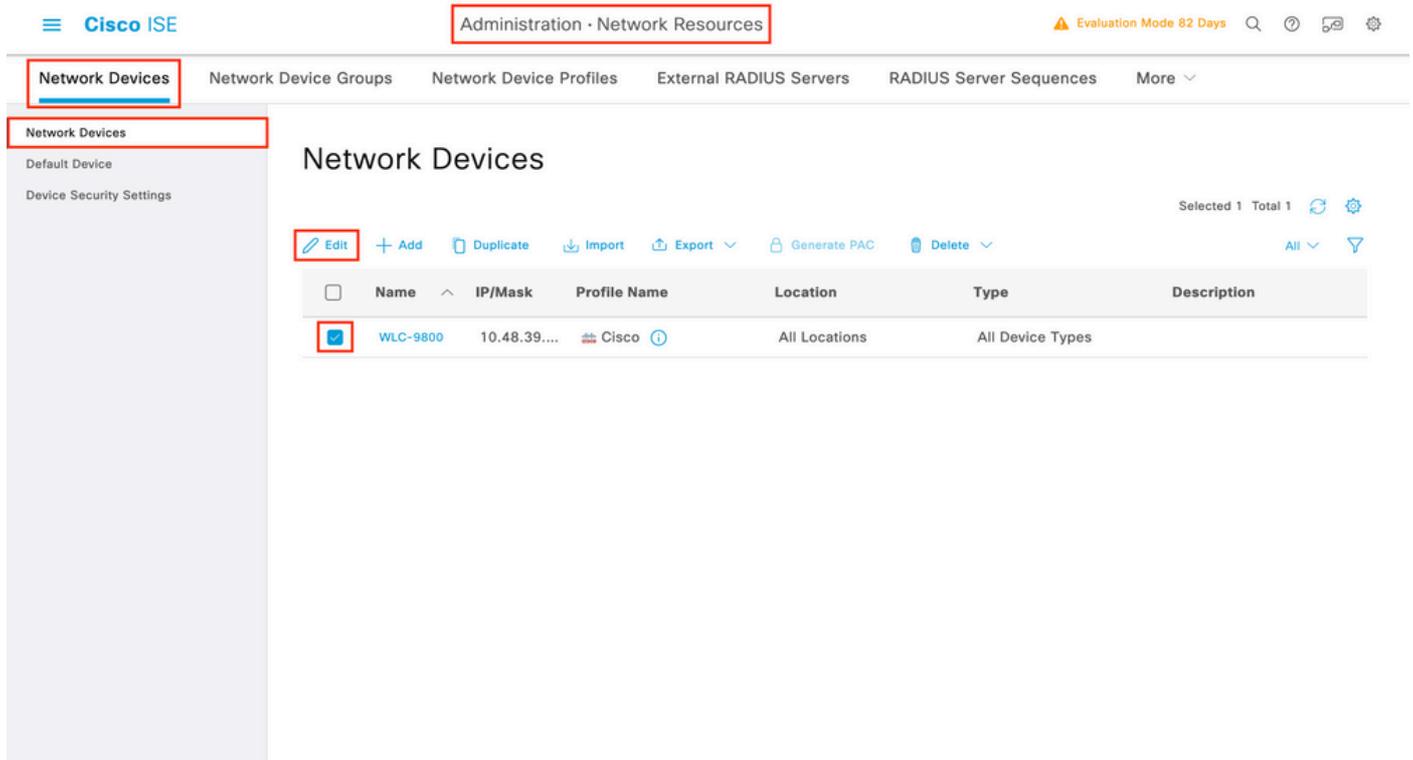
```
WLC-9800(config)#no ip http server  
WLC-9800(config)#no ip http secure-server  
WLC-9800(config)#ip http server  
WLC-9800(config)#ip http secure-server
```

Configuration de TACACS+ ISE

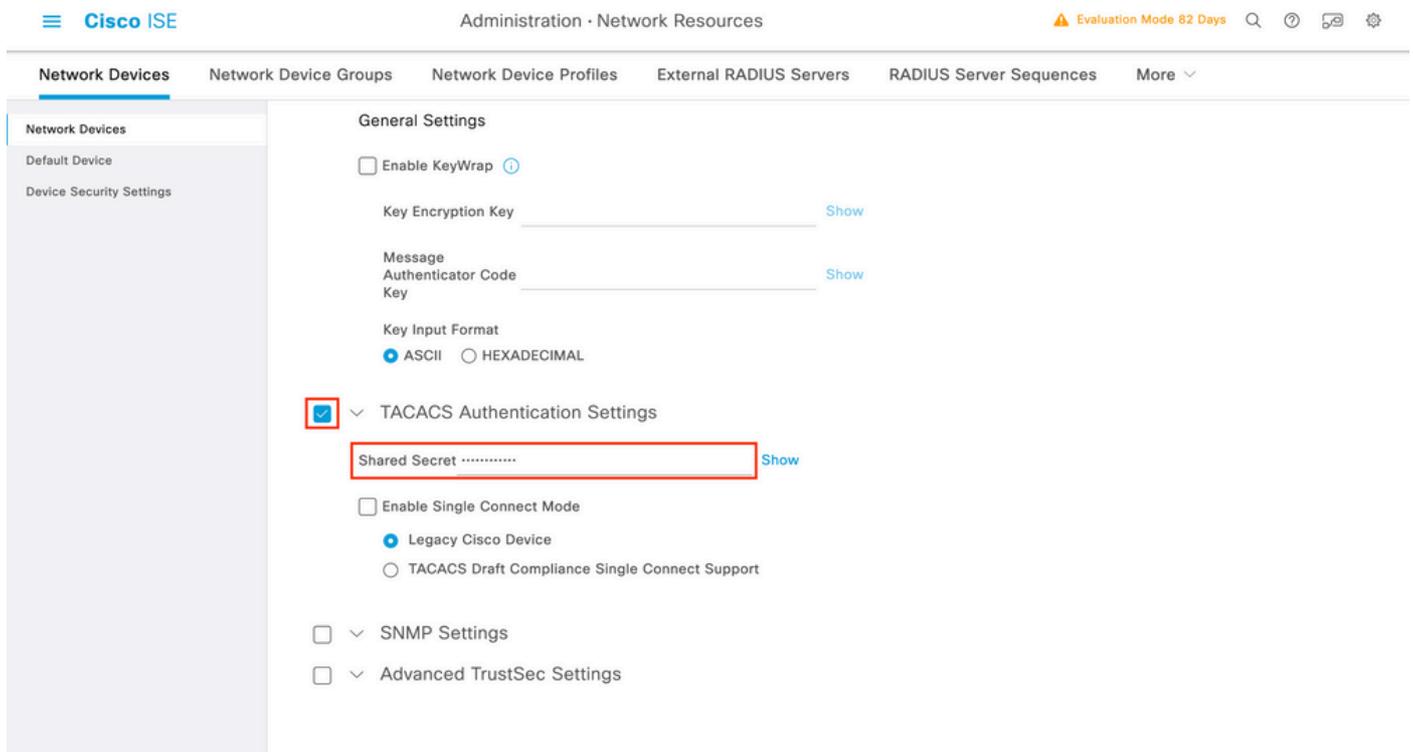
Étape 1. Configurez le WLC en tant que périphérique réseau pour TACACS+.

À partir de la GUI :

Afin de déclarer le WLC utilisé dans la section précédente comme périphérique réseau pour RADIUS dans ISE, naviguez jusqu'à Administration > Network Resources > Network Devices et ouvrez l'onglet Périphériques réseau, comme illustré dans cette image.

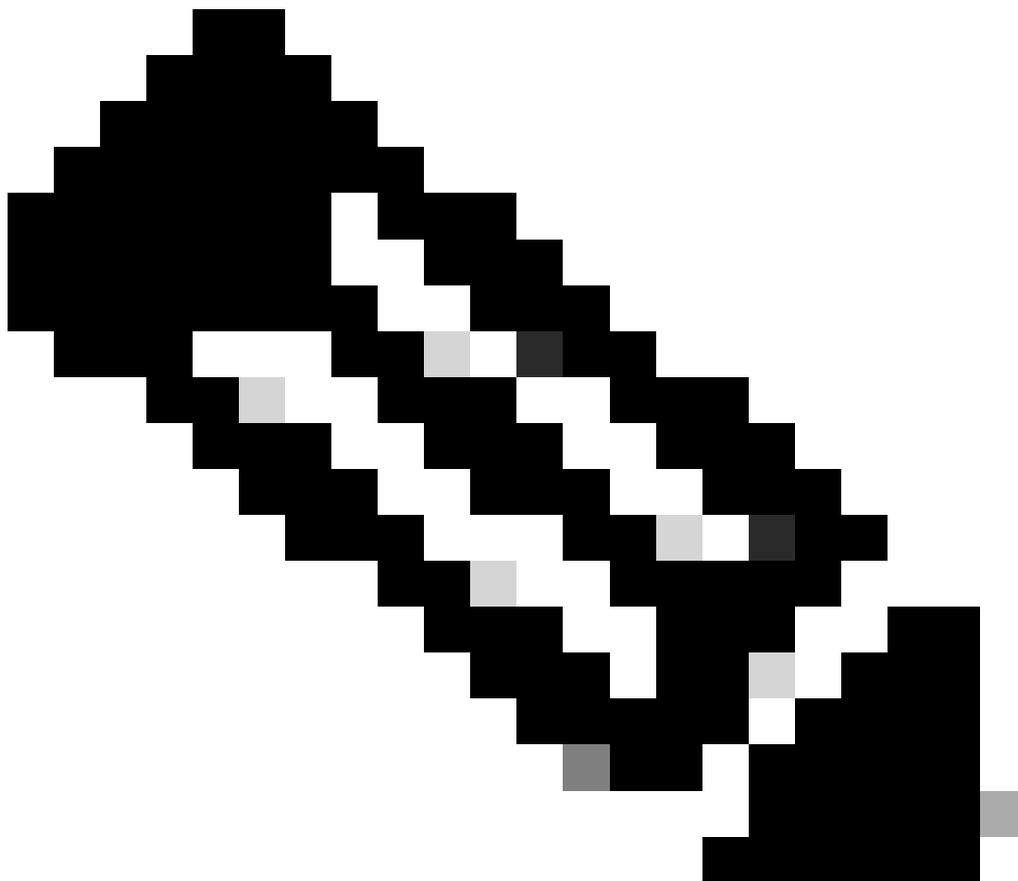


Dans cet exemple, le WLC a déjà été ajouté pour l'authentification RADIUS (référez-vous à l'étape 1. de la section [Configurer RADIUS ISE](#)). Par conséquent, sa configuration doit simplement être modifiée pour configurer l'authentification TACACS, ce qui peut être fait lorsque vous choisissez le WLC dans la liste des périphériques réseau et cliquez sur le bouton Edit. L'écran de configuration du périphérique réseau s'ouvre, comme illustré dans cette image.



Une fois la nouvelle fenêtre ouverte, faites défiler jusqu'à la section TACACS Authentication Settings, activez ces paramètres et ajoutez le secret partagé entré au cours de l'étape 1. de la section [Configure TACACS+ WLC](#).

Étape 2. Activez la fonctionnalité Device Admin pour le noeud.



Remarque : pour utiliser ISE comme serveur TACACS+, vous devez disposer d'un package de licence Device Administration et d'une licence Base ou Mobility.

À partir de la GUI :

Une fois les licences Device Administration installées, vous devez activer la fonctionnalité Device Admin pour le noeud afin de pouvoir utiliser ISE comme serveur TACACS+. Pour ce faire, modifiez la configuration du noeud de déploiement ISE utilisé, qui se trouve sous Administrator > Deployment, et cliquez sur son nom ou effectuez-le à l'aide du Edit bouton.

Deployment

- Deployment
- PAN Failover

Deployment Nodes

Selected 0 Total 1

Edit Register Syncup Deregister

<input type="checkbox"/>	Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/>	ise	Administration, Monitoring, Policy Service	STANDALO...	SESSION,PROFILER	<input checked="" type="checkbox"/>

Une fois la fenêtre de configuration du noeud ouverte, vérifiez l'option Enable Device Admin Service sous la section Policy Service, comme illustré dans cette image.

Deployment Nodes List > ise

Edit Node

General Settings Profiling Configuration

Hostname **ise**

FQDN **ise.cisco.com**

IP Address **10.48.39.134**

Node Type **Identity Services Engine (ISE)**

Role **STANDALONE** [Make Primary](#)

Administration

Monitoring

Role **PRIMARY**

Other Monitoring Node _____

Dedicated MnT ⓘ

Policy Service

Enable Session Services ⓘ

Include Node in Node Group **None**

Enable Profiling Service ⓘ

Enable Threat Centric NAC Service ⓘ

Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

pxGrid ⓘ

[Reset](#) [Save](#)

Étape 3. Créez des profils TACACS pour renvoyer le privilège.

À partir de la GUI :

Pour avoir des droits d'accès d'administrateur, le adminuser doit avoir un niveau de privilège de 15, ce qui permet d'accéder à l'interpréteur de commandes d'invite d'exécution. D'autre part, le helpdeskuser n'a pas besoin d'un accès rapide à l'interpréteur de commandes exec et peut donc être attribué avec un niveau de privilège inférieur à 15. Afin d'attribuer le niveau de privilège approprié aux utilisateurs, des profils d'autorisation peuvent être utilisés. Vous pouvez les configurer à partir de la page de l'interface utilisateur graphique ISEWork Centers > Device Administration > Policy Elements, sous l'onglet Results > TACACS Profiles, comme illustré dans l'image suivante.

- Conditions
 - Library Conditions
 - Smart Conditions
- Network Conditions
- Results
 - Allowed Protocols
 - TACACS Command Sets
 - TACACS Profiles**

TACACS Profiles

Rows/Page 6 << 1 >> Go 6 Total Rows

[Add](#) [Duplicate](#) [Trash](#) [Edit](#) [Filter](#)

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	IOS Admin	Shell	Assigned to each user in the group admin-group
<input type="checkbox"/>	IOS Helpdesk	Shell	Assigned to each user in the group helpdesk-group
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR

Afin de configurer un nouveau profil TACACS, utilisez le bouton Ajouter, qui ouvre le nouveau formulaire de configuration de profil similaire à celui illustré dans l'image. Ce formulaire doit notamment ressembler à ceci pour configurer le profil qui est assigné à la adminuser (c'est-à-dire, avec des privilèges d'interpréteur de commandes de niveau 15).

Cisco ISE Work Centers - Device Administration Evaluation Mode 82 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets More

TACACS Profiles > IOS Admin
TACACS Profile

Name: **IOS Admin**

Description: Assigned to each user in the group admin-group

Task Attribute View Raw View

Common Tasks

Common Task Type: **Shell**

Default Privilege 15 (Select 0 to 15)

Maximum Privilege 15 (Select 0 to 15)

Access Control List

Auto Command

No Escape (Select true or false)

Timeout Minutes (0-9999)

Idle Time Minutes (0-9999)

Custom Attributes

Add Trash Edit

Type	Name	Value
No data found.		

Cancel Save

Répétez l'opération pour le profilhelpdesk. Pour ce dernier, le privilège par défaut, ainsi que le privilège maximal, sont tous deux définis sur 1.

Étape 4. Créez des groupes d'utilisateurs sur ISE.

Il s'agit du même que celui présenté à l'étape 3. de la section [Configurer RADIUS ISE](#) de ce document.

Étape 5. Créez les utilisateurs sur ISE.

Il s'agit du même que celui présenté à l'étape 4. de la section [Configurer RADIUS ISE](#) de ce document.

Étape 6. Créez un ensemble de stratégies d'administration de périphériques.

À partir de la GUI :

En ce qui concerne l'accès RADIUS, une fois les utilisateurs créés, leurs stratégies d'authentification et d'autorisation doivent encore être définies sur ISE afin de leur accorder les droits d'accès appropriés. L'authentification TACACS utilise des ensembles de stratégies d'administration de périphériques à cette fin, qui peuvent être configurés à partir de la Work Centers > Device Administration > Device Admin Policy Sets GUI Page comme illustré.

Policy Sets

Reset [Reset Policyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	WLC TACACS Authentication		Network Access-Device IP Address EQUALS 10.48.39.133	Default Device Admin	0		
✓	Default	Tacacs Default policy set		Default Device Admin	0		

Reset [Save](#)

Pour créer un ensemble de stratégies d'administration de périphériques, utilisez le bouton Ajouter encadré en rouge dans l'image précédente, afin d'ajouter un élément à la liste des ensembles de stratégies. Donnez un nom au jeu nouvellement créé, une condition dans laquelle il doit être appliqué et les protocoles autorisés/la séquence de serveur (ici, les Default Device Admin suffisent). Save Utilisez le bouton pour finaliser l'ajout de l'ensemble de stratégies et utilisez la flèche située sur son droit pour accéder à sa page de configuration, telle qu'elle apparaît sur la page représentée.

Policy Sets → **WLC TACACS Authentication**

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	WLC TACACS Authentication		Network Access-Device IP Address EQUALS 10.48.39.133	Default Device Admin	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		All_User_ID_Stores > Options	0	

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
✓	Helpdesk users authorization	InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group	AllowAllCommands	IOS Helpdesk	0		
✓	Admin users authorization	InternalUser-IdentityGroup EQUALS User Identity Groups:admin-group	AllowAllCommands	IOS Admin	0		
✓	Default		DenyAllCommands	Deny All Shell Profile	0		

Reset Save

L'ensemble de stratégies spécifique 'Authentification TACACS WLC' dans cet exemple filtre les requêtes avec l'adresse IP égale à l'exemple d'adresse IP WLC C9800.

En tant que stratégie d'authentification, la règle par défaut a été conservée car elle répond au besoin de la casse d'utilisation. Deux règles d'autorisation ont été définies :

- La première est déclenchée lorsque l'utilisateur appartient au groupe défini admin-group. Elle autorise toutes les commandes (via la règle par défaut Permit_all) et attribue le privilège 15 (via le profil TACACS défini IOS_Admin).
- Le second est déclenché lorsque l'utilisateur appartient au groupe défini helpdesk-group. Elle autorise toutes les commandes (via la Permit_all règle par défaut) et attribue le privilège 1 (via le profil TACACS défini IOS_Helpdesk).

Une fois cette étape terminée, les informations d'identification configurées pour administrer et les helpdesk utilisateurs peuvent être utilisées pour

s'authentifier dans le WLC via l'interface graphique utilisateur ou avec Telnet/SSH.

Dépannage

Si votre serveur RADIUS attend l'envoi de l'attribut RADIUS de type de service, vous pouvez ajouter sur le WLC :

```
radius-server attribute 6 on-for-login-auth
```

Dépannage de l'interface graphique WLC ou de l'accès CLI RADIUS/TACACS+ via l'interface CLI WLC

Afin de déboguer l'accès TACACS+ à l'interface graphique WLC ou CLI, émettez la commande, debug tacacs avec terminal monitor on et voyez le résultat en direct quand une tentative de connexion est faite.

Par exemple, une connexion réussie suivie d'une déconnexion de l'adminuser utilisateur génère cette sortie.

```
<#root>
```

```
WLC-9800#
```

```
terminal monitor
```

```
WLC-9800#
```

```
debug tacacs
```

```
TACACS access control debugging is on
```

```
WLC-9800#
```

```
Dec 8 11:38:34.684: TPLUS: Queuing AAA Authentication request 15465 for processing
```

```
Dec 8 11:38:34.684: TPLUS(00003C69) login timer started 1020 sec timeout Dec 8 11:38:34.684: TPLUS: pro
```

Ces journaux indiquent que le serveur TACACS+ renvoie le privilège correct (qui est AV priv-lvl=15).

Lorsque vous effectuez l'authentification RADIUS, une sortie de débogage similaire s'affiche, qui concerne le trafic RADIUS.

Les commandes debug aaa authentication et debug aaa authorization, à la place, montrent quelle liste de méthodes est choisie par le WLC quand

l'utilisateur essaie de se connecter.

Dépannage de l'interface graphique WLC ou de l'accès CLI TACACS+ via l'interface graphique ISE

Depuis cette page Operations > TACACS > Live Logs, chaque authentification utilisateur effectuée avec TACACS+ jusqu'aux dernières 24 heures peut être visualisée. Pour développer les détails d'une autorisation ou d'une authentification TACACS+, utilisez le bouton Détails associé à cet événement.

The screenshot shows the Cisco ISE interface for 'Operations · TACACS'. The 'Live Logs' tab is selected. The interface includes a navigation bar with 'Cisco ISE', 'Operations · TACACS', and 'Evaluation Mode 82 Days'. Below the navigation bar, there are controls for 'Refresh' (Never), 'Show' (Latest 20 records), and 'Within' (Last 3 hours). A table of logs is displayed with columns: Logged Time, Status, Details, Identity, Type, Authentication Policy, Authorization Policy, Ise Node, and N. The first row shows a successful authorization for 'helpdeskuser' at 'Dec 08, 2022 06:51:46.1...'. The second row shows a successful authentication for 'helpdeskuser' at 'Dec 08, 2022 06:51:46.0...'. The third row shows a successful authorization for 'adminuser' at 'Dec 08, 2022 06:38:38.2...'. The fourth row shows a successful authentication for 'adminuser' at 'Dec 08, 2022 06:38:38.1...'. The fifth row shows a successful authorization for 'adminuser' at 'Dec 08, 2022 06:34:54.0...'. The sixth row shows a successful authentication for 'adminuser' at 'Dec 08, 2022 06:34:53.9...'. The 'Type' column for the first and fifth rows is highlighted with a red box. The 'Details' column for the first row also has a red box around the details icon. At the bottom, it says 'Last Updated: Thu Dec 08 2022 12:57:09 GMT+0100 (Central European Standard Time)' and 'Records Shown: 6'.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	N
Dec 08, 2022 06:51:46.1...	✓		helpdeskuser	Authorization	Authentication Policy	WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:51:46.0...	✓		helpdeskuser	Authentication	WLC TACACS Authentication >...		ise	W
Dec 08, 2022 06:38:38.2...	✓		adminuser	Authorization		WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:38:38.1...	✓		adminuser	Authentication	WLC TACACS Authentication >...		ise	W
Dec 08, 2022 06:34:54.0...	✓		adminuser	Authorization		WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:34:53.9...	✓		adminuser	Authentication	WLC TACACS Authentication >...		ise	W

Last Updated: Thu Dec 08 2022 12:57:09 GMT+0100 (Central European Standard Time) Records Shown: 6

Une fois développée, une tentative d'authentification réussie pour le helpdeskuser ressemble à ceci :

Overview

Request Type	Authentication
Status	Pass
Session Key	ise/459637517/243
Message Text	Passed-Authentication: Authentication succeeded
Username	helpdeskuser
Authentication Policy	WLC TACACS Authentication >> Default
Selected Authorization Profile	IOS Helpdesk

Authentication Details

Generated Time	2022-12-08 06:51:46.077000 -05:00
Logged Time	2022-12-08 06:51:46.077
Epoch Time (sec)	1670500306
ISE Node	ise
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	helpdeskuser
Network Device Name	WLC-9800
Network Device IP	10.48.39.133
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	tty5
Remote Address	10.61.80.151

Steps

```

13013 Received TACACS+ Authentication START Request
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - Network Access.Device IP Address
15041 Evaluating Identity Policy
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
13045 TACACS+ will use the password prompt from global
TACACS+ configuration
13015 Returned TACACS+ Authentication Reply
13014 Received TACACS+ Authentication CONTINUE Request (
🚧 Step latency=3149ms)
15041 Evaluating Identity Policy
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
22037 Authentication Passed
15036 Evaluating Authorization Policy
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - InternalUser.IdentityGroup
13015 Returned TACACS+ Authentication Reply

```

De là, vous pouvez voir que l'utilisateur helpdeskuser a été authentifié avec succès sur le périphérique réseau WLC-9800 à l'aide de la stratégie d'authentification WLC TACACS Authentication > Default. En outre, le profil d'autorisation IOS Helpdesk a été attribué à cet utilisateur et a obtenu le niveau de privilège 1.

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.