

& & RADIUS-+ configureren voor GUI-CLI- autorisatie op 9800 WLC's

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Beperkingen van alleen-lezen gebruikers](#)

[RADIUS-verificatie voor de WLC configureren](#)

[Configureer ISE voor RADIUS](#)

[TACACS+ WLC configureren](#)

[Configuratie TACACS+ ISE](#)

[Problemen oplossen](#)

[Probleemoplossing WLC GUI of CLI RADIUS/TACACS+ toegang via WLC CLI](#)

[Probleemoplossing WLC GUI of CLITACACS+ toegang via ISE GUI](#)

Inleiding

Dit document beschrijft hoe u een Catalyst 9800 kunt configureren voor externe verificatie met RADIUS of TACACS+.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Catalyst draadloze 9800 configuratiemodel
- AAA-, RADIUS- en TACACS+-concepten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C980-CL v17.9.2
- ISE 3.2.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Wanneer een gebruiker probeert toegang te krijgen tot de CLI of de GUI van de WLC, wordt hij gevraagd een gebruikersnaam en wachtwoord in te voeren. Standaard worden deze referenties vergeleken met de lokale database van gebruikers, die op het apparaat zelf aanwezig is. De WLC kan ook worden geïnstrueerd om de invoerreferenties te vergelijken met een externe AAA-server: de WLC kan met de server praten met behulp van RADIUS of TACACS+.

Configureren

In dit voorbeeld worden twee typen gebruikers op de AAA-server (ISE), respectievelijk de `adminuser`, en de helpdeskuser, geconfigureerd. Deze gebruikers maken deel uit van respectievelijk de `admin-group` en `dehelpdesk-group` groepen. De gebruiker `adminuser`, een deel van de `admin-group`, zal naar verwachting volledige toegang tot de WLC krijgen. Aan de andere kant is de helpdeskuser, een deel van de `helpdesk-group`, bedoeld om alleen monitorrechten te krijgen aan de WLC. Daarom is er geen configuratietoegang.

Dit artikel configureert eerst WLC en ISE voor RADIUS-verificatie en werkt later ook voor TACACS+.

Beperkingen van alleen-lezen gebruikers

Wanneer TACACS+ of RADIUS wordt gebruikt voor 9800 WebUI-verificatie, bestaan deze beperkingen:

- Gebruikers met rechten op niveau 0 bestaan maar hebben geen toegang tot de GUI

-

Gebruikers met rechten op niveaus 1-14 kunnen alleen het tabblad Monitor bekijken (dit is gelijk aan het rechten van een lokaal geverifieerde gebruiker die alleen kan lezen)

-

Gebruikers met toegangsrechten niveau 15 hebben volledige toegang

-

Gebruikers met rechten op niveau 15 en een opdrachtset die alleen specifieke opdrachten toestaat, worden niet ondersteund. De gebruiker kan nog steeds configuratiewijzigingen uitvoeren via de WebUI

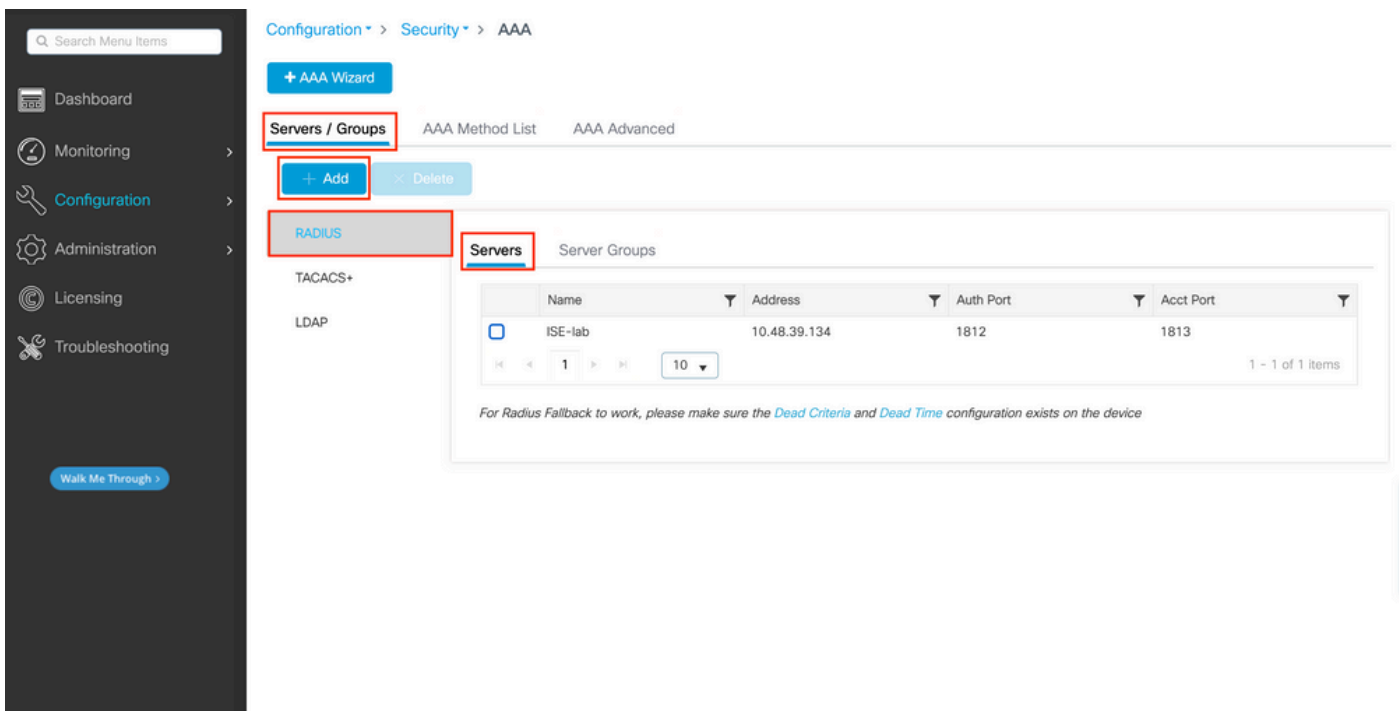
Deze overwegingen kunnen niet worden gewijzigd of aangepast.

RADIUS-verificatie voor de WLC configureren

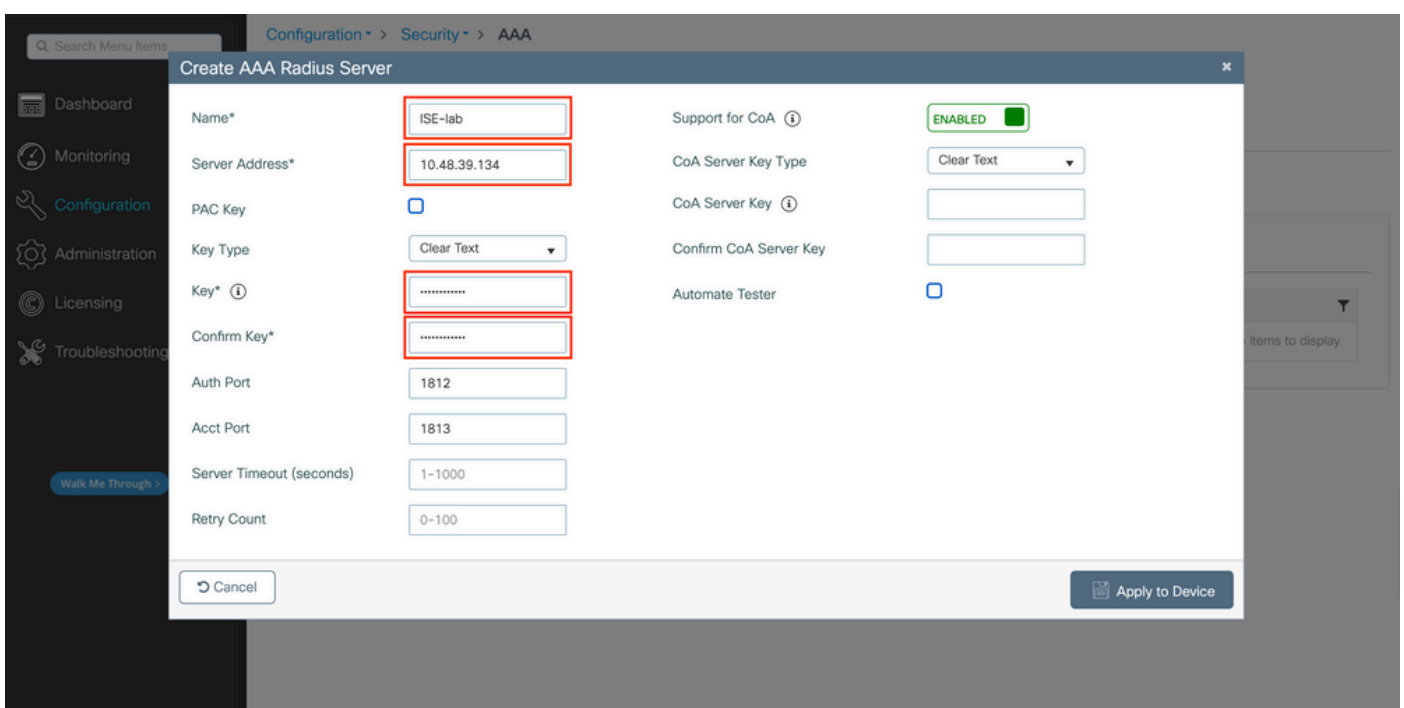
Stap 1. Vermeld de RADIUS-server.

Van GUI:

Ten eerste: maak de ISE RADIUS-server op de WLC. Dit kan worden gedaan via het tabblad Servers/Groups > RADIUS > Servers van de GUI WLC-pagina die toegankelijk is in <https://<WLC-IP>/webui/#/aaa>, of als u navigeert naar Configuration > Security > AAA, zoals in deze afbeelding wordt getoond.



Als u een RADIUS-server aan de WLC wilt toevoegen, klikt u op de knop Toevoegen die in rood is weergegeven in het beeld. Hierdoor wordt het pop-upvenster geopend dat in de screenshot wordt weergegeven.



In dit pop-upvenster moet u het volgende opgeven:

- De servernaam (let op dat deze niet hoeft overeen te komen met de ISE-systeemnaam)
- Het IP-adres van de server
- Het gedeelde geheim tussen WLC en de RADIUS-server

Andere parameters kunnen worden geconfigureerd, zoals de poorten die worden gebruikt voor verificatie en accounting, maar deze zijn niet verplicht en blijven standaard voor deze documentatie.

Van CLI:

```
<#root>
```

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

```
ISE-1ab
```

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

```
10.48.39.134
```

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

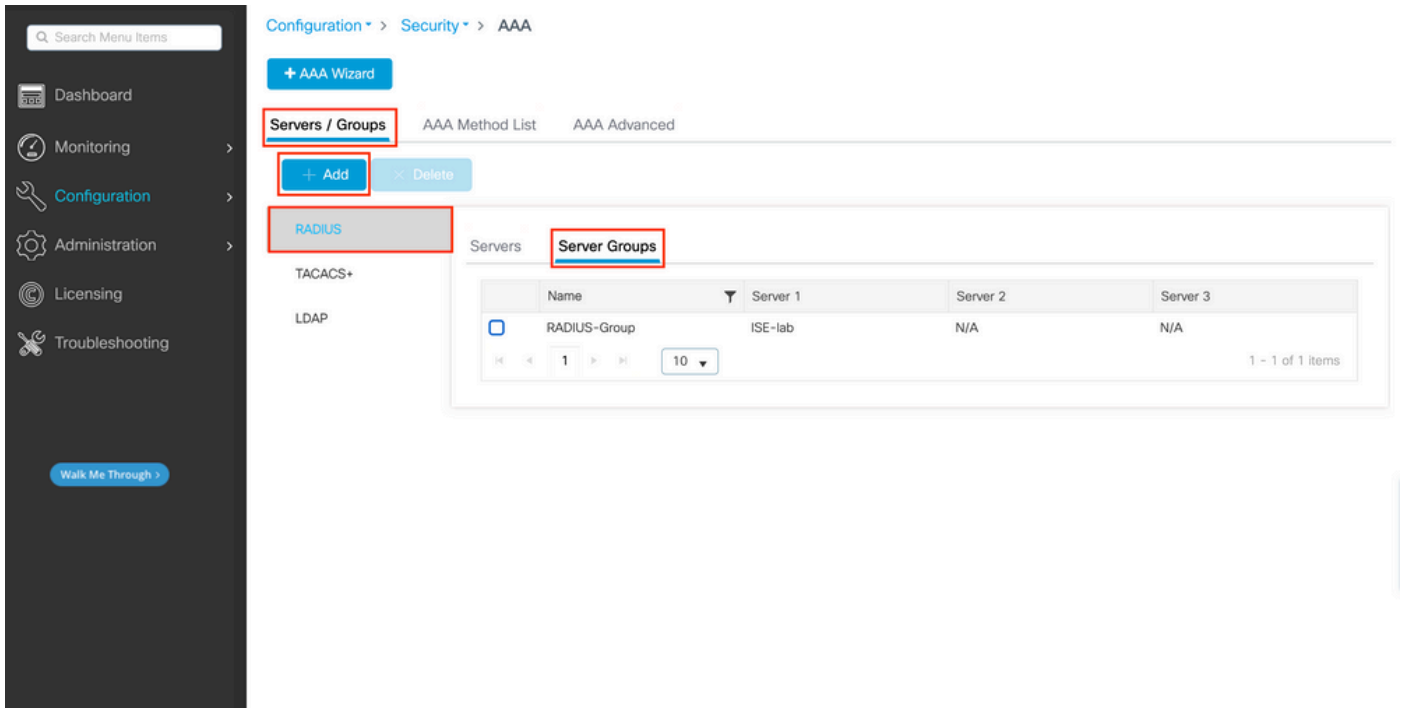
```
WLC-9800(config-radius-server)#key
```

```
Cisco123
```

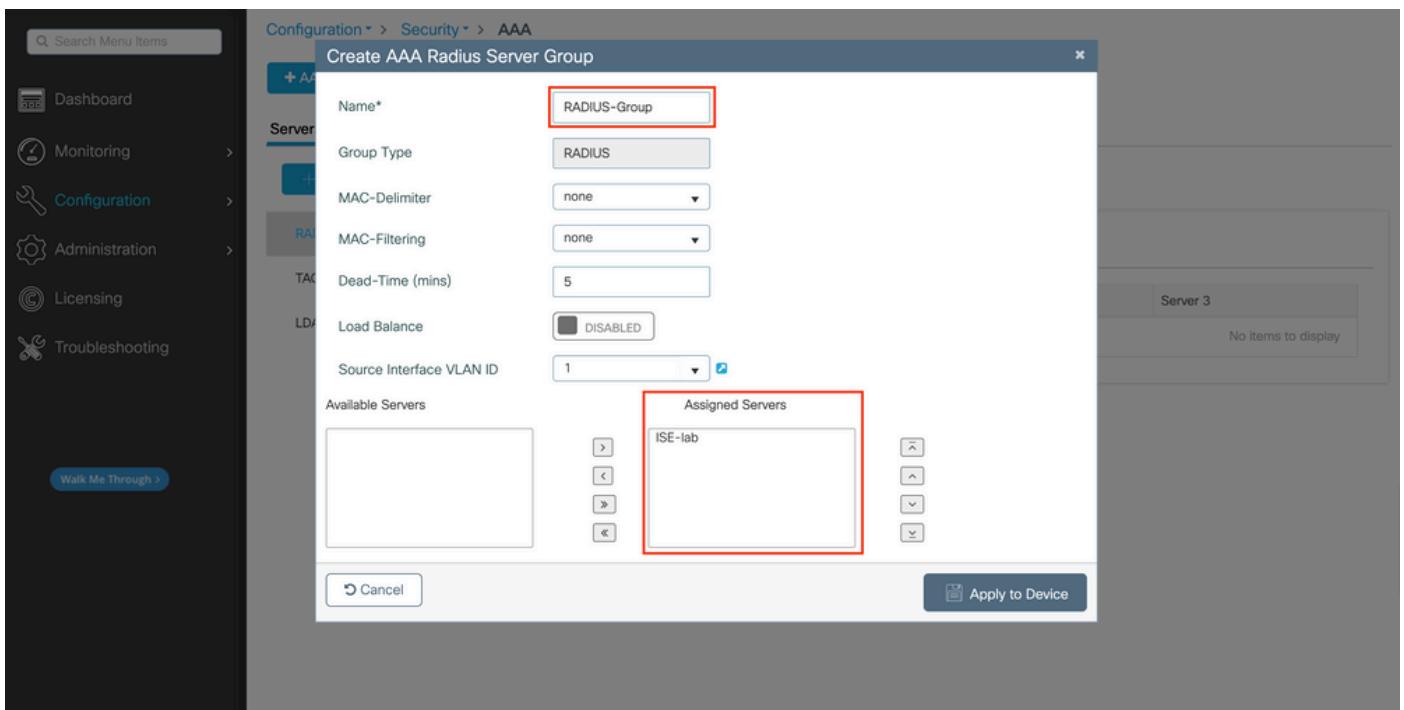
Stap 2. Breng de RADIUS-server aan een servergroep in kaart.

Van GUI:

Als u meerdere RADIUS-servers hebt die kunnen worden gebruikt voor verificatie, wordt aangeraden om al deze servers aan dezelfde servergroep toe te wijzen. De WLC zorgt voor taakverdeling tussen verschillende verificaties van de servers in de servergroep. RADIUS-servergroepen worden geconfigureerd vanuit het Servers/Groups > RADIUS > Server Groups tabblad vanuit dezelfde GUI-pagina als de pagina die in Stap 1 wordt genoemd, zoals in de afbeelding.



Wat de serverconversie betreft, wordt er een pop-upvenster weergegeven wanneer u op de knop Toevoegen (in de vorige afbeelding) klikt. Dit wordt hier weergegeven.



Typ in het pop-upvenster een naam voor de groep en verplaats de gewenste servers naar de lijst Toegewezen servers.

Van CLI:

<#root>

WLC-9800(config)# aaa group server radius

RADIUS-Group

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

ISE-lab

Stap 3. Maak een inlogmethode voor AAA-verificatie die verwijst naar de RADIUS-servergroep.

Van GUI:

Navigeer nog steeds vanaf de GUI-pagina <https://<WLC-IP>/webui/#/aaa> naar het AAA Method List > Authentication tabblad en maak een verificatiemethode zoals in deze afbeelding.

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication **+ Add** Delete

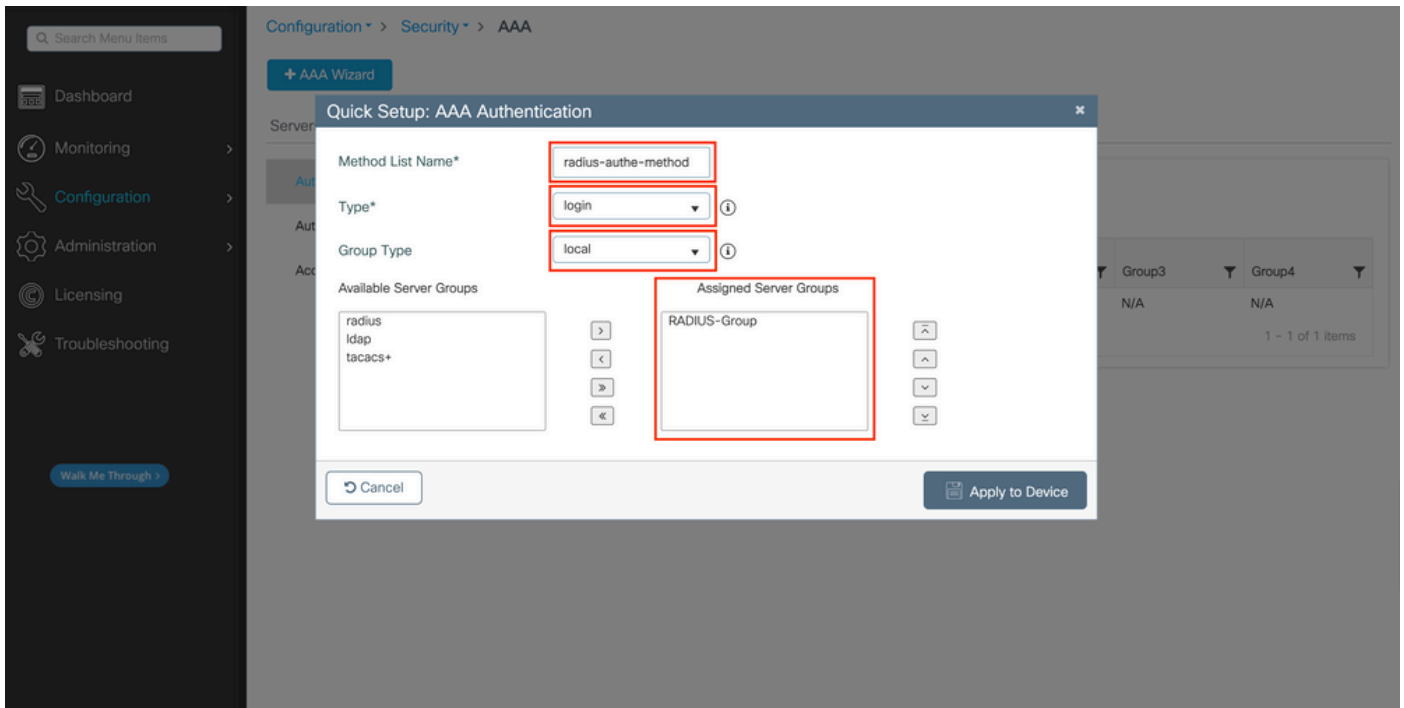
Authorization

Accounting

Name	Type	Group Type	Group1	Group2	Group3	Group4
<input type="checkbox"/> default	login	local	N/A	N/A	N/A	N/A
<input type="checkbox"/> radius-auth-method	login	local	RADIUS-Group	N/A	N/A	N/A

1 - 2 of 2 items

Zoals gebruikelijk, wanneer u de knop Add gebruikt om een verificatiemethode te maken, wordt er een pop-upvenster voor configuratie weergegeven, dat lijkt op het venster dat in deze afbeelding wordt weergegeven.



Typ in dit venster een naam voor de methode. Kies Type als aanmelding en voeg de groepserver die in de vorige stap is gemaakt, toe aan de lijst Assigned Server Groups. Met betrekking tot het veld Groepstype zijn verschillende configuraties mogelijk.

- Als u Group Type als lokaal kiest, controleert de WLC eerst of de gebruikersreferenties lokaal bestaan, en valt dan terug naar de servergroep.
- Als u kiest voor Groepstype als groep en niet de optie Terugvallen op lokale optie controleert, controleert de WLC alleen de gebruikersreferenties op de servergroep.
- Als u Groepstype als groep kiest en de optie Terugzetten naar lokale optie controleert, controleert WLC de gebruikersreferenties tegen de servergroep en vraagt de lokale database alleen als de server niet reageert. Als de server een weigering verstuurt, moet de gebruiker worden geverifieerd, ook al kan deze in de lokale database voorkomen.

Van CLI:

Als u wilt dat de gebruikersreferenties alleen met een servergroep worden gecontroleerd als ze eerst niet lokaal worden gevonden, gebruikt u:

```
<#root>
```

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

```
radius-auth-method
```

local group

RADIUS-Group

Als u wilt dat de gebruikersreferenties alleen met een servergroep worden gecontroleerd, gebruikt u:

<#root>

WLC-9800(config)#aaa authentication login

radius-auth-method

group

RADIUS-Group

Als u wilt dat de gebruikersreferenties worden gecontroleerd met een servergroep en als deze laatste niet reageert met de lokale vermelding, gebruikt u:

<#root>

WLC-9800(config)#aaa authentication login

radius-auth-method

group

RADIUS-Group

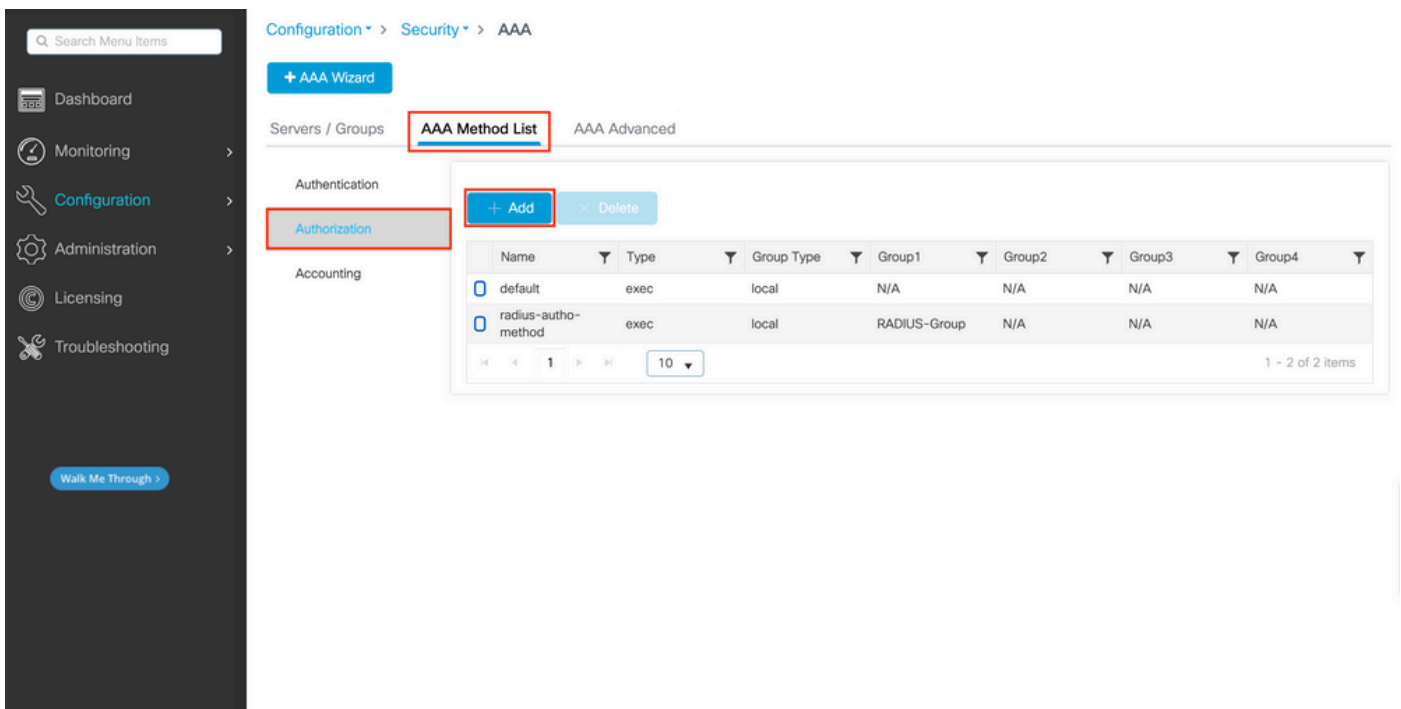
local

In deze voorbeeldinstelling zijn er enkele gebruikers die alleen lokaal worden gemaakt, en sommige gebruikers alleen op de ISE-server, dus gebruik maken van de eerste optie.

Stap 4. Maak een AAA-authorizationmethode die verwijst naar de RADIUS-servergroep.

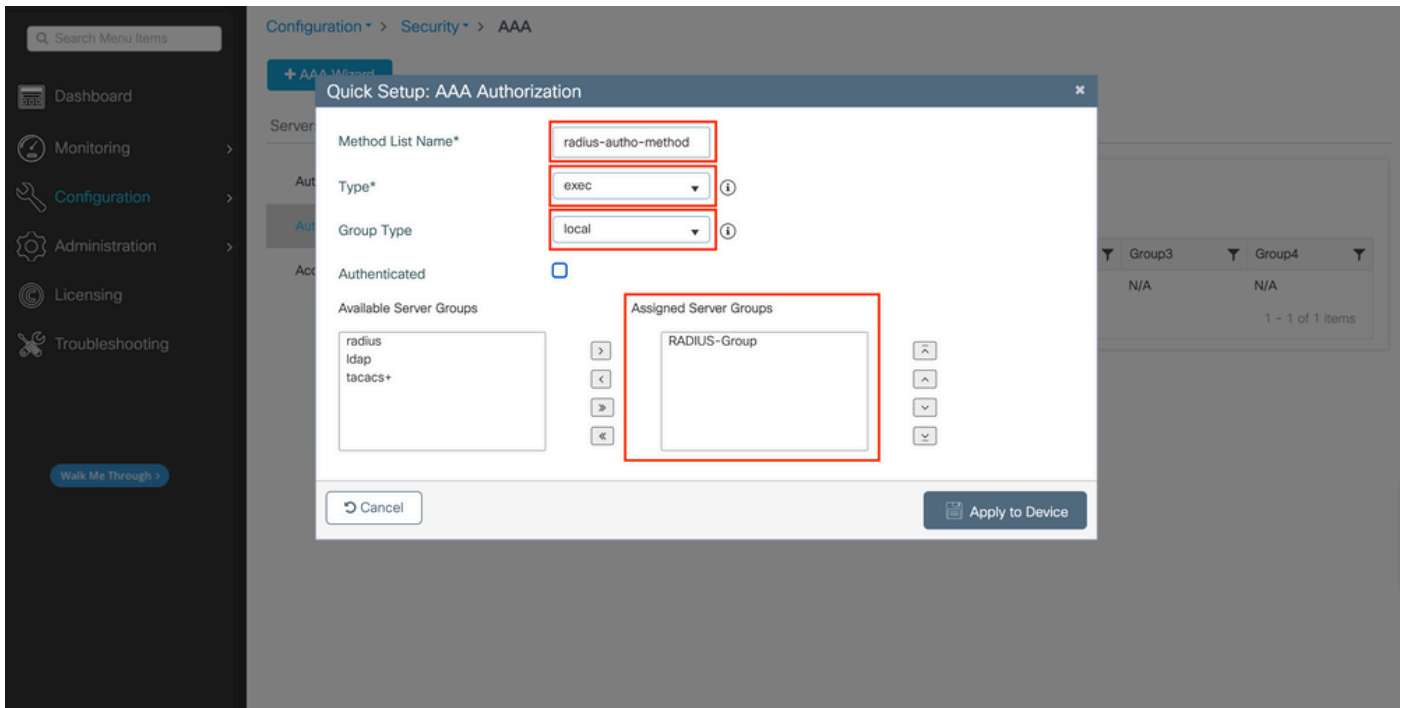
Van GUI:

De gebruiker moet ook gemachtigd zijn om toegang te krijgen. Navigeer vanaf het GUI Page Configuration > Security > AAA tabblad naar het AAA Method List > Authorization tabblad en maak een autorisatiemethode zoals in deze afbeelding.



Creatie van autorisatiemethode

Er verschijnt een pop-up van de configuratie van de autorisatiemethode die vergelijkbaar is met de afbeelding, als u een nieuwe methode toevoegt met de knop Toevoegen.



In deze configuratie pop-up, geef een naam voor de autorisatiemethode, kies het Type als exec, en gebruik dezelfde volgorde van Groepstype als die gebruikt voor de verificatiemethode in Stap 3.

Van CLI:

Wat de verificatiemethode betreft, wordt de autorisatie eerst toegewezen om gebruikers te controleren op lokale vermeldingen en vervolgens op vermeldingen in een servergroep.

<#root>

WLC-9800(config)#aaa authorization exec

radius-autho-method

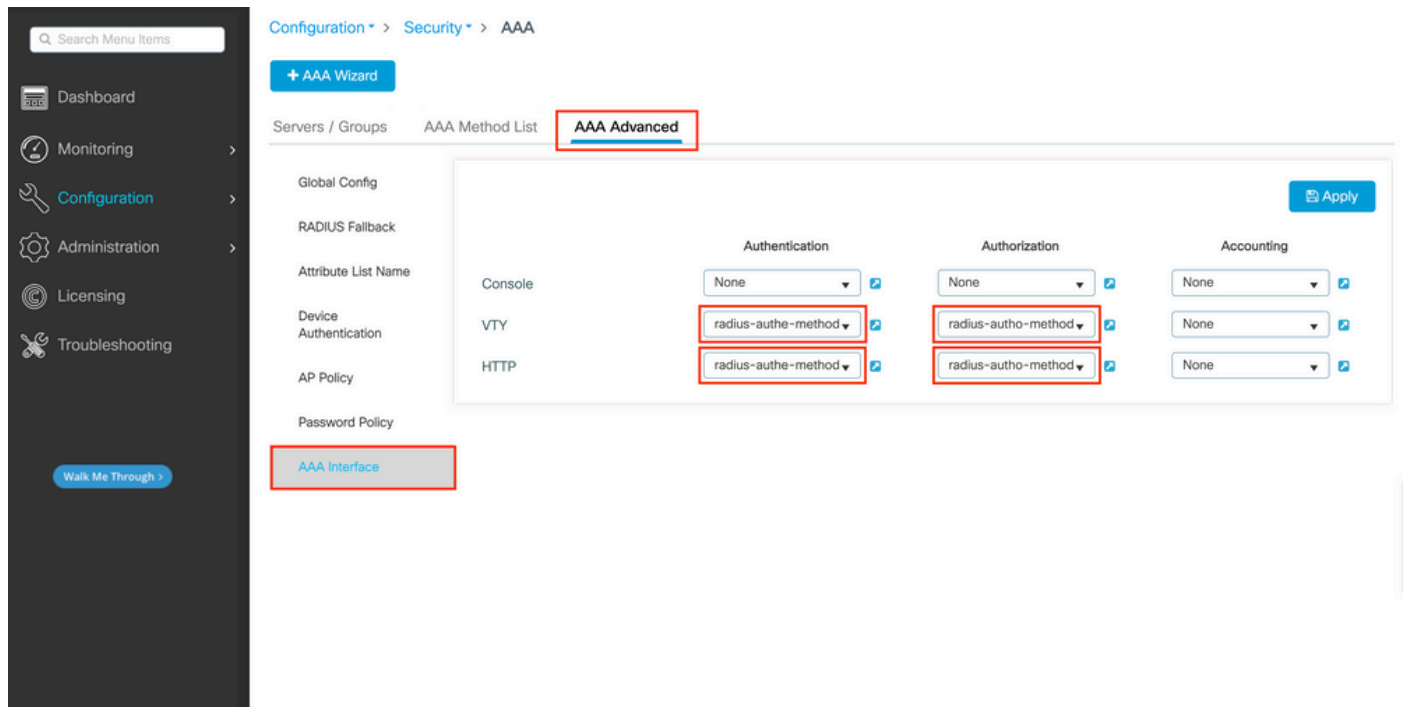
local group

RADIUS-Group

Stap 5. Wijs de methoden toe aan de HTTP-configuraties en aan de VTY-lijnen die worden gebruikt voor Telnet/SSH.

Van GUI:

De gemaakte verificatie- en autorisatiemethoden kunnen worden gebruikt voor HTTP- en/of Telnet/SSH-gebruikersverbinding, die nog kan worden geconfigureerd AAA Advanced > AAA Interface vanaf de GUI WLC-pagina die toegankelijk is in <https://<WLC-IP>/webui/#/aaa>, zoals in dit beeld wordt getoond:



CLI voor GUI-verificatie:

<#root>

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

radius-auth-method

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

radius-autho-method

CLI voor Telnet/SSH-verificatie:

```
<#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
```

Merk op dat wanneer de veranderingen in de configuraties van HTTP worden uitgevoerd, het best is om de diensten HTTP en HTTPS opnieuw te beginnen. Dit kan met deze opdrachten worden bereikt:

```
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
```

Configureer ISE voor RADIUS

Stap 1. Configureer de WLC als netwerkapparaat voor RADIUS.

Van GUI:

Als u de WLC in de vorige sectie wilt declareren als netwerkapparaat voor RADIUS in ISE, navigeert u naar Administration > Network Resources > Network Devices het tabblad Netwerkapparaten en opent u dit tabblad, zoals in de volgende afbeelding.

Network Devices

- Network Device Groups
- Network Device Profiles
- External RADIUS Servers
- RADIUS Server Sequences
- More

Network Devices

- Default Device
- Device Security Settings

Network Devices

Selected 0 Total 1

- Edit
- + Add**
- Duplicate
- Import
- Export
- Generate PAC
- Delete

All

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	WLC-9800	10.48.39.133/32	Cisco	All Locations	All Device Types	

Als u een netwerkkapparaat wilt toevoegen, gebruikt u de knop Toevoegen, waarmee het nieuwe configuratieformulier voor netwerkkapparaten wordt geopend.

Network Devices

Default Device

Device Security Settings

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

Typ in het nieuwe venster een naam voor het netwerkapparaat en voeg het IP-adres toe. Kies de RADIUS-verificatie-instellingen en configureer hetzelfde RADIUS gedeelde geheim als de RADIUS-verificatie die op de WLC wordt gebruikt.

Stap 2. Maak een autorisatieresultaat om het recht terug te geven.

Van GUI:

Om beheerderstoegangsrechten te hebben, moet het adminuser een voorrangsniveau van 15 hebben, wat het mogelijk maakt om toegang te krijgen tot de snelle shell. Aan de andere kant heeft de helpdeskuser geen directe shell toegang nodig en kan daarom worden toegewezen met een voorrangsniveau lager dan 15. Om het juiste voorrangsniveau aan gebruikers toe te wijzen, kunnen autorisatieprofielen worden gebruikt. Deze kunnen vanuit de ISE GUI Page Policy > Policy Elements > Results worden geconfigureerd, onder het tabblad Authorization > Authorization Profiles dat in het volgende beeld wordt weergegeven.

- Dictionarys
- Conditions
- Results**
- 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 [Filter](#)

<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 ti
<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

Als u een nieuw autorisatieprofiel wilt configureren, gebruikt u de knop Toevoegen om het nieuwe configuratieformulier voor het autorisatieprofiel te openen. Dit formulier moet er met name zo uitzien om het profiel te configureren dat aan het adminuser is toegewezen.

Dictionary 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

De configuratie toonde subsidies voorrecht niveau 15 aan om het even welke gebruiker aan wie het wordt geassocieerd. Zoals eerder vermeld, is dit het verwachte gedrag voor het adminuser dat tijdens de volgende stap wordt gecreëerd. Het helpdeskuser moet echter een lager niveau van voorrechten hebben en daarom moet er een tweede beleidselement worden gecreëerd.

Het beleidselement voor het helpdeskuser is gelijk aan het element dat net boven is gemaakt, behalve dat de string shell:priv-lvl=15 moet worden veranderd in shell:priv-lvl=X, en X moet vervangen met het gewenste prioriteitsniveau. In dit voorbeeld wordt 1 gebruikt.

Stap 3. Creer gebruikersgroepen op ISE.

Via de GUI:

ISE-gebruikersgroepen worden gemaakt op het tabblad Gebruikersidentiteitsgroepen van het Administration > Identity Management > Groups GUI Page programma, dat in de schermopname wordt weergegeven.

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

Als u een nieuwe gebruiker wilt maken, gebruikt u de knop Toevoegen, waarmee het configuratieformulier voor de nieuwe gebruikersidentiteitsgroep wordt geopend, zoals aangegeven op de afbeelding.

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 filled with 'admin-group' and is highlighted in red. 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.

Geef de naam op van de groep die wordt gemaakt. Maak de twee hierboven besproken gebruikersgroepen aan, namelijk de admin-group en helpdesk-group.

Stap 4. Gebruikers maken op ISE.

Via de GUI:

ISE-gebruikers worden gemaakt van het tabblad Gebruikers van het Administration > Identity Management > Identities GUI Page, dat in de schermopname wordt weergegeven.

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	

Om een nieuwe gebruiker te maken, gebruikt u de knop Add om het nieuwe gebruikersconfiguratieformulier voor netwerktoegang te openen zoals aangegeven op de afbeelding.

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

Verstrek de referenties aan de gebruikers, namelijk zijn/haar gebruikersnaam en wachtwoord, die worden gebruikt om te authenticeren op de WLC. Controleer ook of de status van de gebruiker is Enabled. Voeg de gebruiker tot slot toe aan de verwante groep die is gemaakt in Stap 4., met het vervolgkeuzemenu Gebruikersgroepen aan het einde van het formulier.

Creëer de twee gebruikers die hierboven besproken zijn, namelijk de adminuser en helpdeskuser.

Stap 5. Verifieer de gebruikers.

Van GUI:

In dit scenario biedt het verificatiebeleid van de standaard-beleidssets van ISE, dat al vooraf is geconfigureerd, standaard netwerktoegang. Deze beleidsset kan worden bekeken vanuit het Policy > Policy Sets scherm van de ISE GUI-pagina, zoals in deze afbeelding wordt getoond. Daarom hoeft dit niet te worden gewijzigd.

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	⚙️

Stap 6. Machtigen van de gebruikers.

Van GUI:

Nadat de inlogpoging het verificatiebeleid doorgeeft, moet het worden geautoriseerd en moet ISE het eerder gemaakte autorisatieprofiel retourneren (autorisatieacceptatie, samen met het voorrangsniveau).

In dit voorbeeld worden de inlogpogingen gefilterd op basis van het IP-adres van het apparaat (het WLC IP-adres) en onderscheiden ze het te verlenen voorrecht op basis van de groep waartoe een gebruiker behoort. Een andere geldige benadering is om gebruikers te filteren op basis van hun gebruikersnamen, aangezien elke groep maar één gebruiker in dit voorbeeld bevat.

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

Nadat deze stap is voltooid, kunnen de referenties die zijn geconfigureerd voor adminuser enhelpdesk gebruiker worden gebruikt om te authenticeren in de WLC via de GUI of via Telnet/SSH.

TACACS+ WLC configureren

Step 1. Vermeld de TACACS+ server.

Van GUI:

Maak eerst de Tacacs+ server ISE op de WLC. Dit kan worden gedaan via het tabblad Servers/Groups > TACACS+ > Servers van de GUI WLC-pagina die toegankelijk is in het https://<WLC-IP>/webui/#/aaa of als u navigeert naar Configuration > Security > AAA, zoals in deze afbeelding wordt getoond.

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add - Delete

RADIUS

TACACS+

LDAP

Servers Server Groups

Name	Server Address	Port
ISE-lab	10.48.39.134	49

1 - 1 of 1 items

Als u een TACACS-server aan de WLC wilt toevoegen, klikt u op de knop Toevoegen die in rood is weergegeven in de afbeelding hierboven. Hierdoor wordt het weergegeven venster geopend.

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

+ Add

RADIUS

TACACS+

LDAP

Create AAA Tacacs Server

Name* ISE-lab

Server Address* 10.48.39.134

Key Type Clear Text

Key*

Confirm Key*

Port 49

Server Timeout (seconds) 1-1000

Cancel Apply to Device

Wanneer het pop-upvenster wordt geopend, typt u de servernaam (de naam van het ISE-systeem hoeft niet overeen te komen), het IP-adres, de gedeelde sleutel, de gebruikte poort en de tijdelijke versie.

In dit pop-upvenster moet u het volgende opgeven:

- De servernaam (let op dat deze niet hoeft overeen te komen met de ISE-systeemnaam)

- Het IP-adres van de server
- Het gedeelde geheim tussen WLC en de TACACS+ server

Andere parameters kunnen worden geconfigureerd, zoals de poorten die worden gebruikt voor verificatie en accounting, maar deze zijn niet verplicht en blijven standaard voor deze documentatie.

Van CLI:

```
<#root>
```

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

```
ISE-lab
```

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

```
10.48.39.134
```

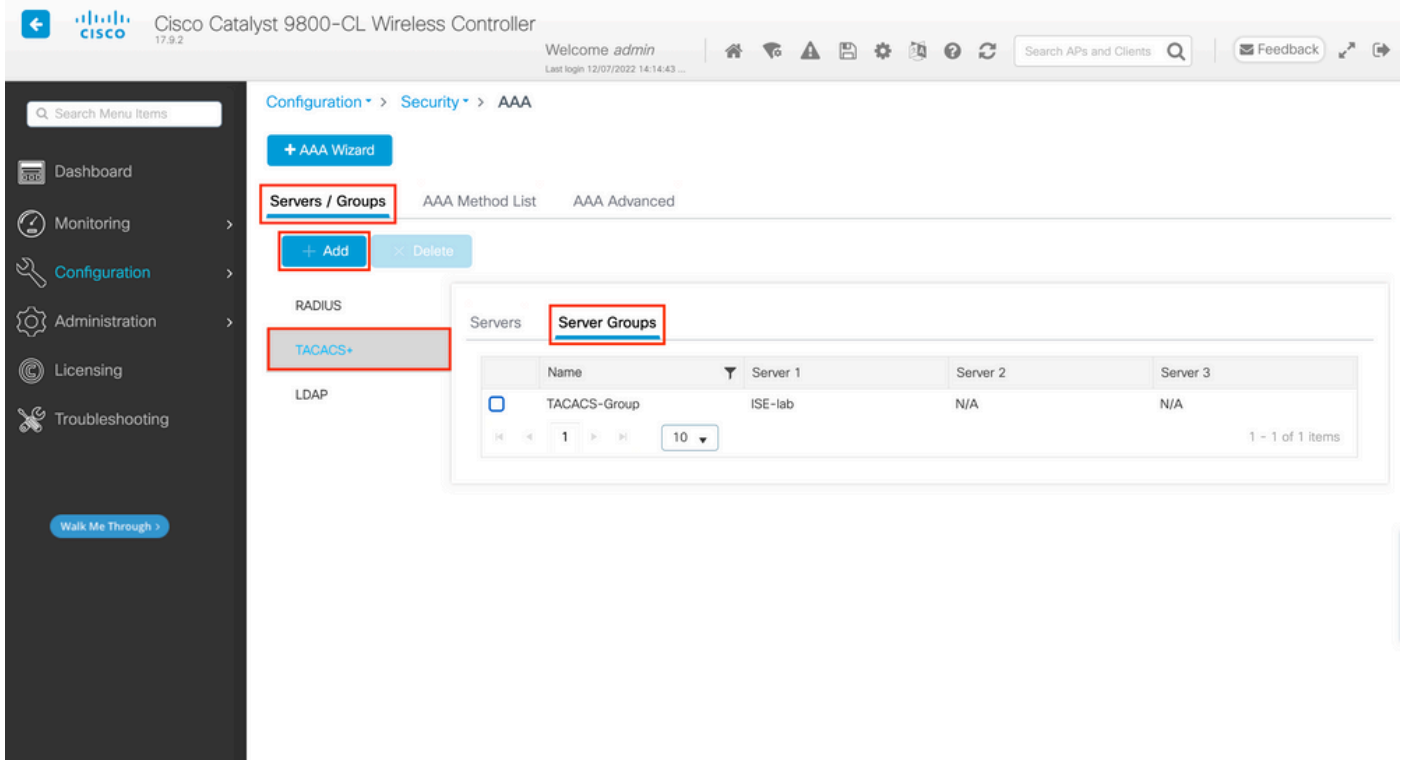
```
WLC-9800(config-server-tacacs)#key
```

```
Cisco123
```

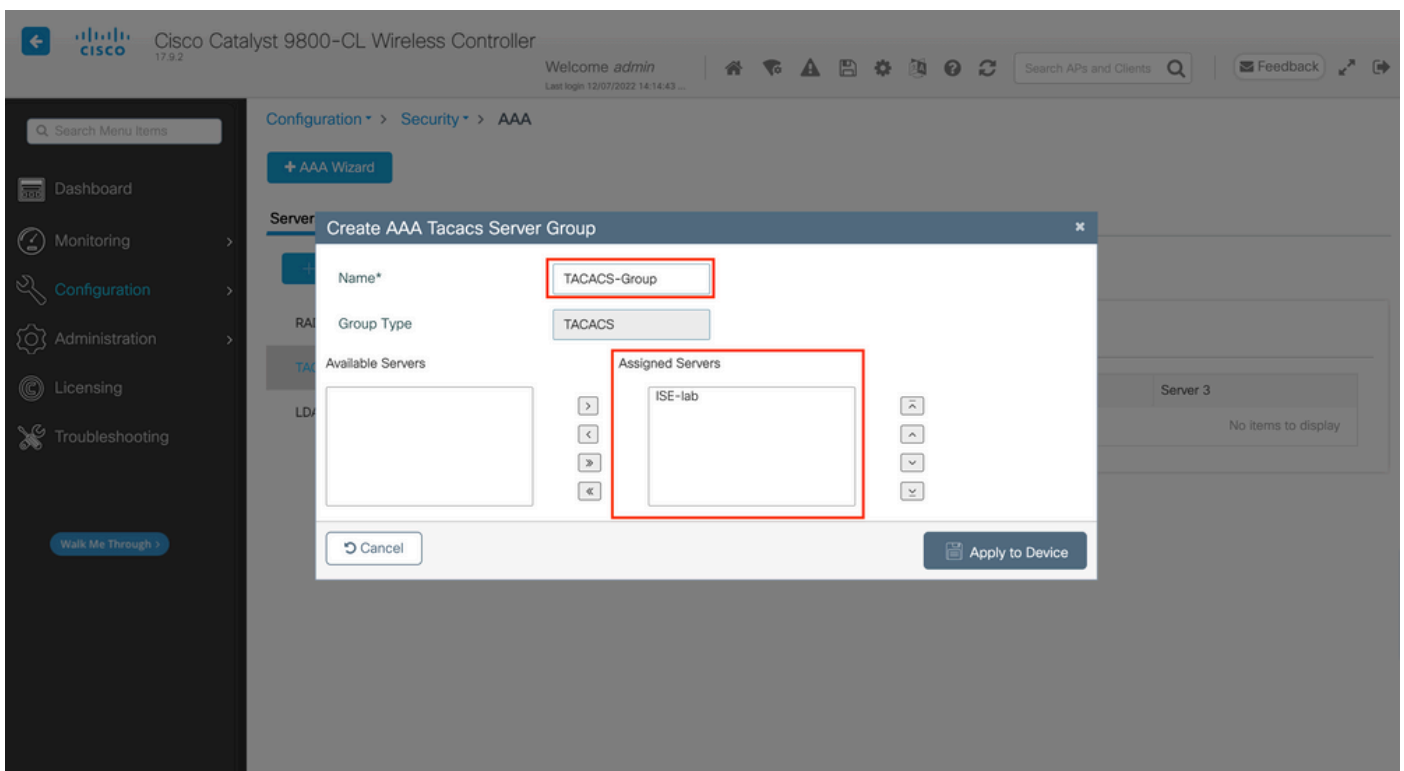
Stap 2. Breng de TACACS+ server aan een servergroep in kaart.

Van GUI:

Als u meerdere TACACS+ servers hebt die kunnen worden gebruikt voor verificatie, is het raadzaam om al deze servers toe te wijzen aan dezelfde servergroep. De WLC zorgt dan voor taakverdeling tussen de verschillende verificaties in de servergroep. De groepen TACACS+ servers zijn ingesteld vanuit het Servers/Groups > TACACS > Server Groups tabblad van dezelfde GUI-pagina als de pagina die in Stap 1 wordt genoemd, die in de afbeelding wordt weergegeven.



Wat de serverbewerking betreft, wordt er een pop-upvenster weergegeven wanneer u op de knop Toevoegen klikt die in de eerdere afbeelding is ingesloten en die in de afbeelding wordt weergegeven.



Geef in het pop-upvenster een naam aan de groep en verplaats de gewenste servers naar de lijst Toegewezen servers.

Van CLI:

<#root>

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

TACACS-Group

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

ISE-lab

Stap 3. Maak een loginmethode voor AAA-verificatie die verwijst naar de TACACS+-servergroep.

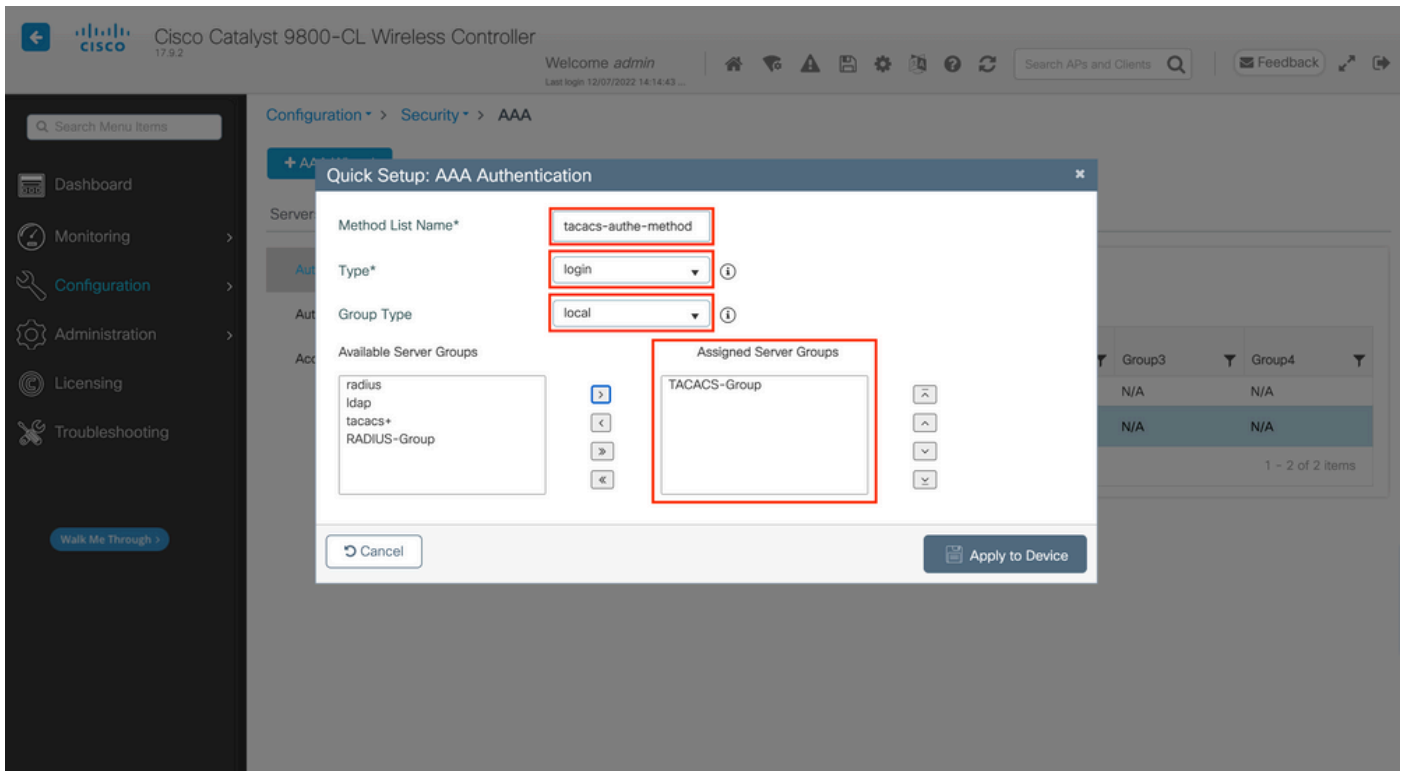
Van GUI:

Navigeer nog steeds vanaf de GUI-pagina <https://<WLC-IP>/webui/#/aaa> naar het AAA Method List > Authentication tabblad en maak een verificatiemethode zoals in de afbeelding.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is Configuration > Security > AAA. The 'AAA Method List' tab is active, and the 'Authentication' sub-tab is selected. A table displays the current AAA methods:

Name	Type	Group Type	Group1	Group2	Group3	Group4
default	login	local	N/A	N/A	N/A	N/A
radius-auth-method	login	local	RADIUS-Group	N/A	N/A	N/A
tacacs-auth-method	login	local	TACACS-Group	N/A	N/A	N/A

Zoals gebruikelijk, wanneer u de knop Add gebruikt om een verificatiemethode te maken, wordt er een pop-upvenster voor configuratie weergegeven, dat lijkt op het venster dat in deze afbeelding wordt weergegeven.



Typ in dit pop-upvenster een naam voor de methode, kies Type als login en voeg de groepserver die in de vorige stap is gemaakt, toe aan de lijst Toegewezen servergroepen. Met betrekking tot het veld Groepstype zijn verschillende configuraties mogelijk.

- Als u Group Type als lokaal kiest, controleert de WLC eerst of de gebruikersreferenties lokaal bestaan, en valt dan terug naar de servergroep.
- Als u kiest voor Groepstype als groep en niet de optie Terugvallen op lokale optie controleert, controleert de WLC alleen de gebruikersreferenties op de servergroep.
- Als u Groepstype als groep kiest en de optie Terugzetten naar lokale optie controleert, controleert WLC de gebruikersreferenties tegen de servergroep en vraagt de lokale database alleen als de server niet reageert. Als de server een weigering verstuurt, moet de gebruiker worden geverifieerd, ook al kan deze in de lokale database voorkomen.

Van CLI:

Als u wilt dat de gebruikersreferenties alleen met een servergroep worden gecontroleerd als ze eerst niet lokaal worden gevonden, gebruikt u:

```
<#root>
```

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

```
tacacs-auth-method
```

local group

TACACS-Group

Als u wilt dat de gebruikersreferenties alleen met een servergroep worden gecontroleerd, gebruikt u:

```
<#root>
```

WLC-9800(config)#aaa authentication login

tacacs-auth-method

group

TACACS-Group

Als u wilt dat de gebruikersreferenties worden gecontroleerd met een servergroep en als deze laatste niet reageert met een lokale ingang, gebruik dan:

```
<#root>
```

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

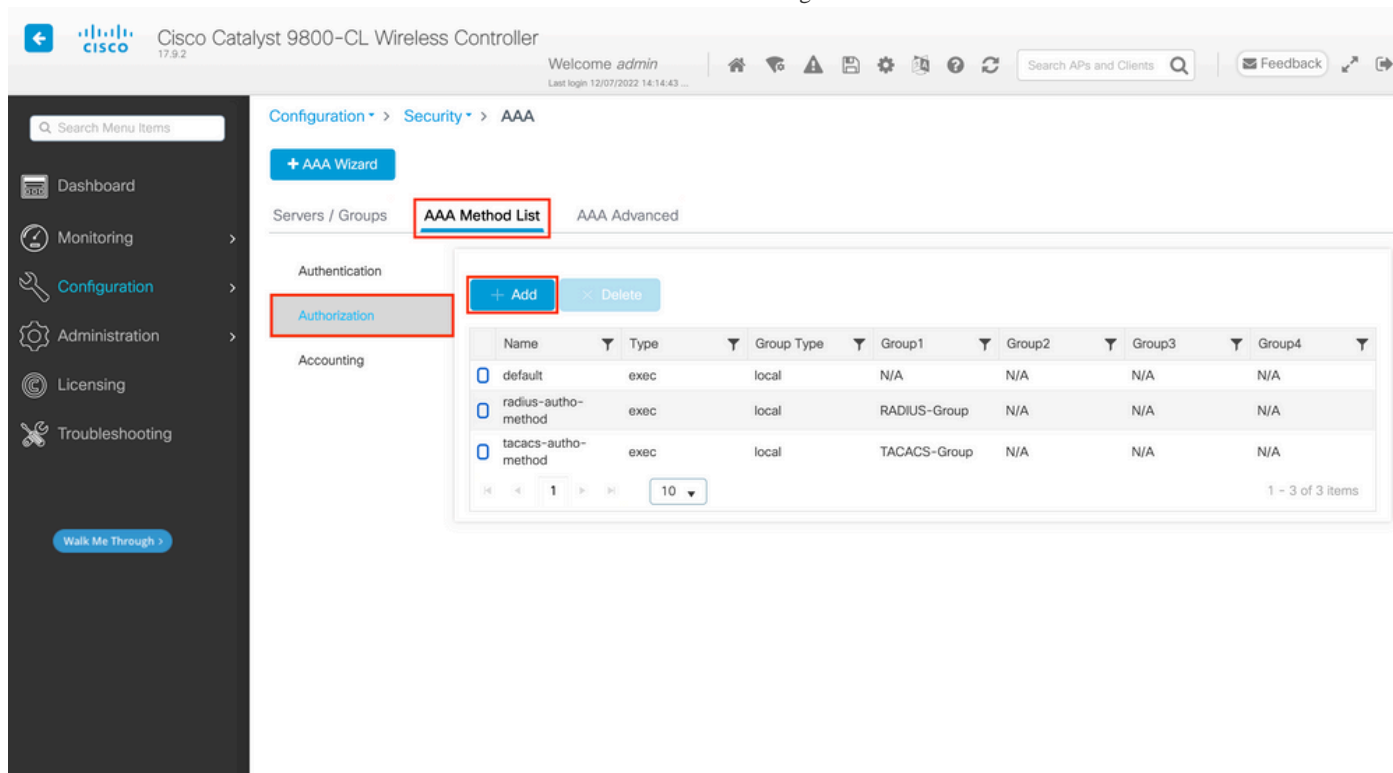
local

In deze voorbeeldinstelling zijn er enkele gebruikers die alleen lokaal worden gemaakt, en sommige gebruikers alleen op de ISE-server, dus gebruik maken van de eerste optie.

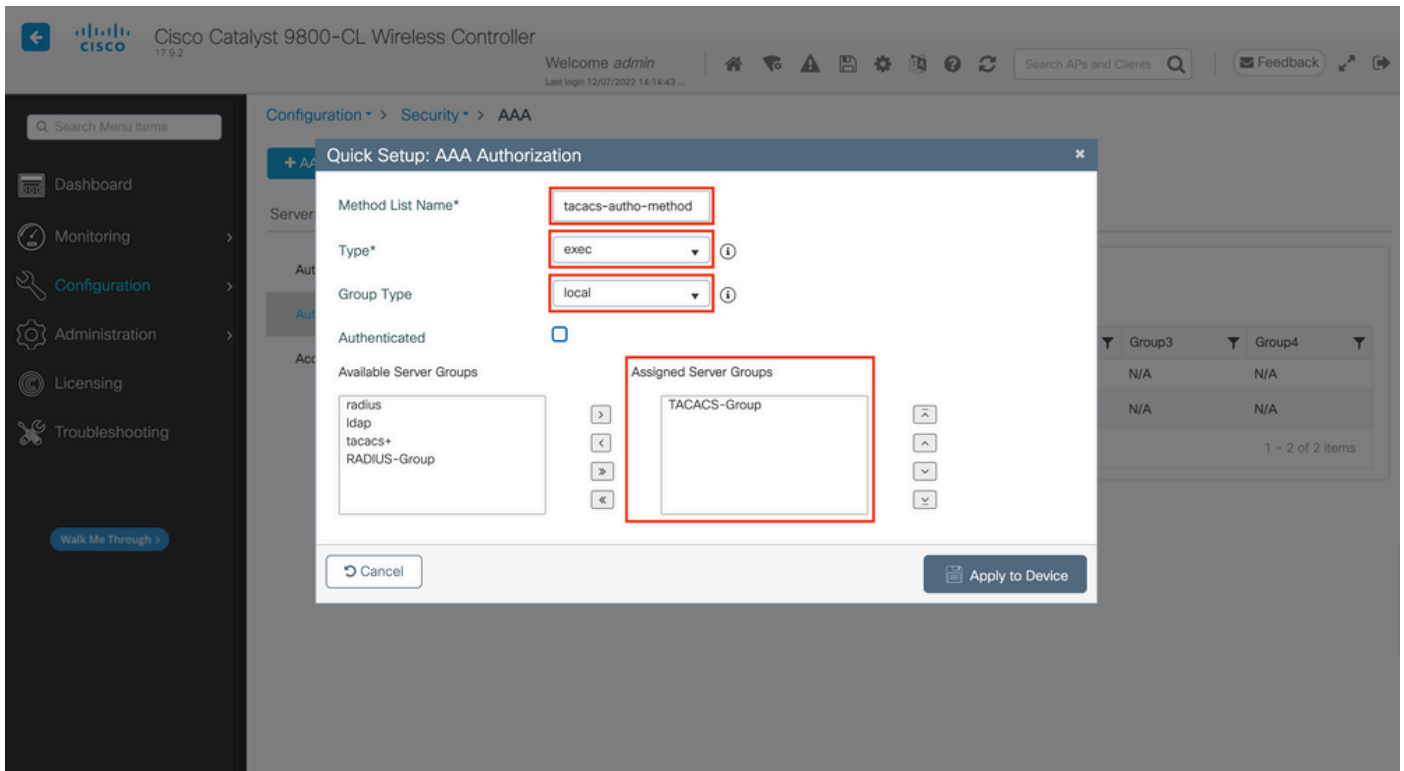
Step 4. Maak een AAA-autorisatiemethode die verwijst naar de TACACS+ servergroep.

Van GUI:

De gebruiker moet ook gemachtigd zijn om toegang te krijgen. Ga Configuration > Security > AAA vanaf de GUI-pagina naar het AAA Method List > Authorization tabblad en maak een autorisatiemethode zoals in de afbeelding.



Er verschijnt een pop-up van de configuratie van de autorisatiemethode die vergelijkbaar is met de afbeelding, als u een nieuwe methode toevoegt met de knop Toevoegen.



In deze configuratie pop-up, geef een naam voor de autorisatiemethode, kies Type als exec en gebruik dezelfde volgorde van Groepstype als die gebruikt voor de verificatiemethode in de vorige stap.

Van CLI:

```
<#root>
```

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

```
tacacs-autho-method
```

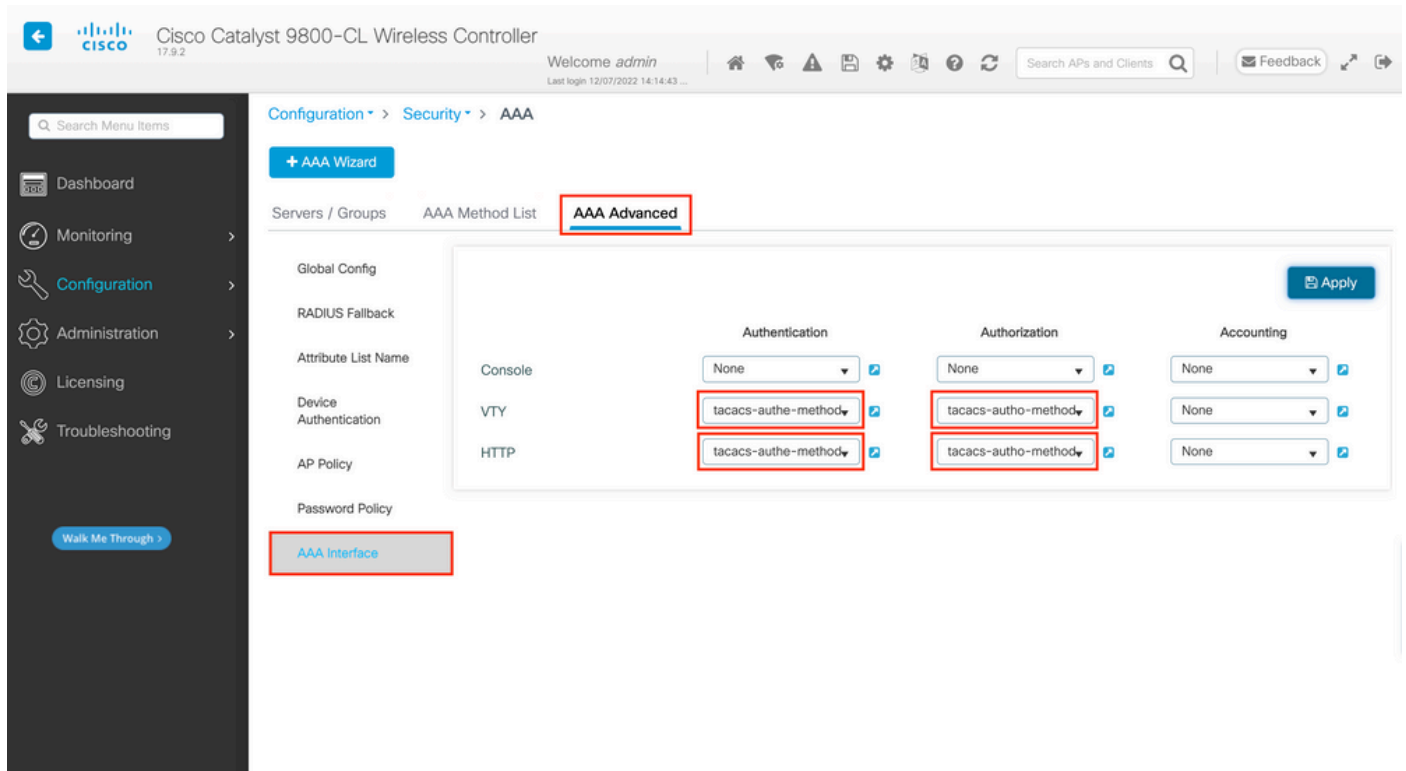
```
local group
```

```
TACACS-Group
```

Stap 5. Wijs de methoden toe aan de HTTP-configuraties en aan de VTY-lijnen die worden gebruikt voor Telnet/SSH.

Van GUI:

De gecreëerde verificatie- en autorisatiemethoden kunnen worden gebruikt voor HTTP- en/of Telnet/SSH-gebruikersverbinding, die kan worden geconfigureerd vanuit het AAA Advanced > AAA Interface tabblad nog vanuit de GUI WLC-pagina die toegankelijk is in <https://<WLC-IP>/webui/#/aaa>, zoals in het beeld wordt getoond.



Van CLI:

Voor de GUI-verificatie:

```
<#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
```

Voor Telnet/SSH-verificatie:

```
<#root>
```

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

```
tacacs-authe-method
```

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

```
tacacs-autho-method
```

Merk op dat wanneer de veranderingen in de configuraties van HTTP worden uitgevoerd, het best is om de diensten HTTP en HTTPS opnieuw te beginnen. Dit kan met deze opdrachten worden bereikt.

```
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
```

Configuratie TACACS+ ISE

Stap 1. Configureer de WLC als netwerkapparaat voor TACACS+.

Van GUI:

Als u de WLC in de vorige sectie wilt declareren als netwerkapparaat voor RADIUS in ISE, navigeert u naar Administration > Network Resources > Network Devices het tabblad Netwerkapparaten en opent u dit tabblad, zoals in deze afbeelding.

Administration · Network Resources

Network Devices

Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences More

Network Devices

Default Device
Device Security Settings

Network Devices

Selected 1 Total 1

Edit + Add Duplicate Import Export Generate PAC Delete

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input checked="" type="checkbox"/>	WLC-9800	10.48.39....	Cisco	All Locations	All Device Types	

In dit voorbeeld is de WLC al toegevoegd voor RADIUS-verificatie (zie Stap 1. van de sectie [RADIUS ISE configureren](#)). Daarom moet de configuratie eenvoudig worden aangepast om TACACS-verificatie te configureren, wat kan worden gedaan wanneer u de WLC kiest in de lijst van netwerkapparaten en op de knop Bewerken klikt. Hiermee opent u het configuratieformulier voor het netwerkapparaat zoals in deze afbeelding wordt weergegeven.

Administration · Network Resources

Network Devices

Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences More

Network Devices

Default Device
Device Security Settings

General Settings

Enable KeyWrap

Key Encryption Key Show

Message Authenticator Code Show

Key Input Format

ASCII HEXADECIMAL

TACACS Authentication Settings

Shared Secret Show

Enable Single Connect Mode

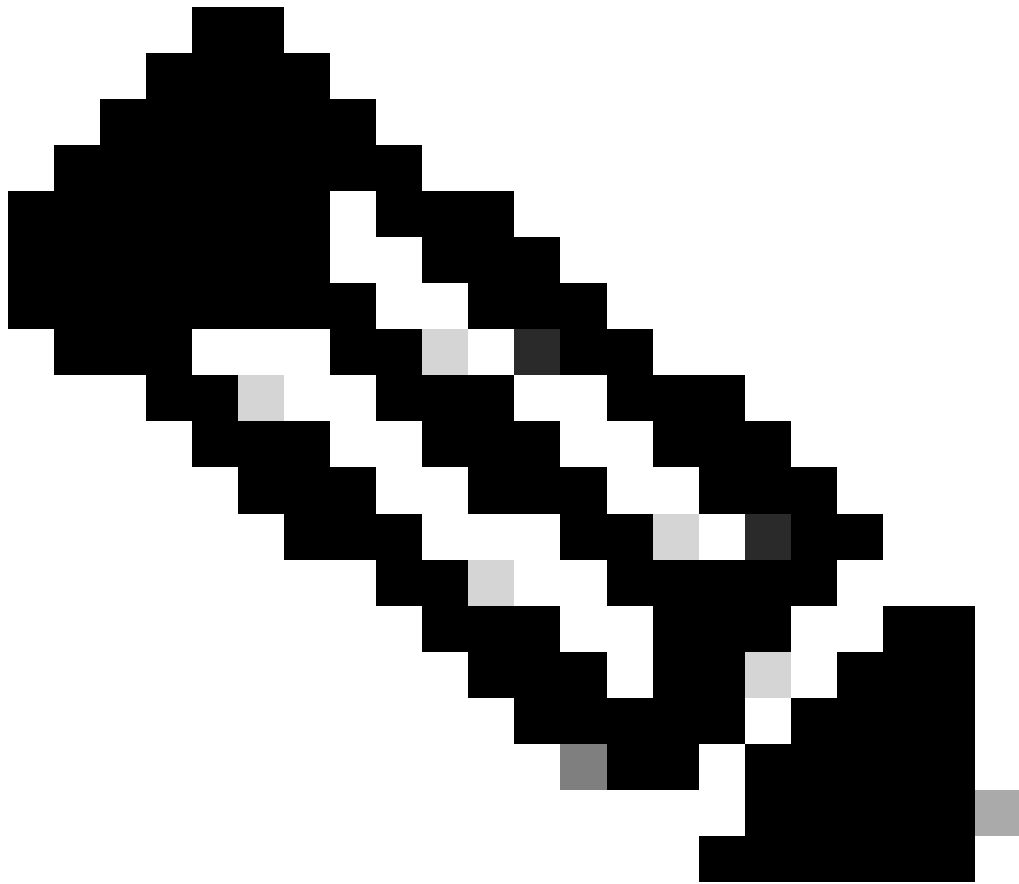
Legacy Cisco Device
 TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

Nadat het nieuwe venster is geopend, scrolt u omlaag naar de sectie TACACS-verificatie-instellingen, schakelt u deze instellingen in en voegt u het gedeelde geheim toe dat u hebt ingevoerd tijdens Stap 1. van de sectie [TACACS+ WLC configureren](#).

Stap 2. Schakel de functie Apparaatbeheer in voor de knooppunt.



Opmerking: als u ISE als de TACACS+ server wilt gebruiken, moet u beschikken over een apparaatbeheerlicentiepakket en een Base- of een Mobility-licentie.

Van GUI:

Nadat de Apparaatbeheerlicenties zijn geïnstalleerd, moet u de functie Apparaatbeheer voor de knooppunt inschakelen om ISE als de TACACS+-server te kunnen gebruiken. Om dit te doen, moet u de configuratie van het gebruikte ISE-implementatieknooppunt bewerken, dat u kunt vinden onder Administrator > Deployment, en klikt u op de naam of doet u dit met behulp van de knopEdit.

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"/>

Nadat het venster voor de configuratie van de knooppunt is geopend, controleert u de optie Apparaatbeheer inschakelen onder de sectie Beleidsservice, zoals in deze afbeelding wordt getoond.

Deployment

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](#)

Stap 3. Maak TACACS-profielen, om de privilege terug te geven.

Van GUI:

Om beheerderstoegangsrechten te hebben, moet hetadminuser een voorrangsniveau van 15 hebben, wat het mogelijk maakt om toegang te krijgen tot de snelle shell. Aan de andere kant heeft dehelpdeskuser geen directe shell toegang nodig en kan daarom worden toegewezen met een voorrangsniveau lager dan 15. Om het juiste voorrangsniveau aan gebruikers toe te wijzen, kunnen autorisatieprofielen worden gebruikt. Deze kunnen worden geconfigureerd vanaf de ISE GUI-pagina Work Centers > Device Administration > Policy Elements, onder het tabblad Results > TACACS Profiles zoals in het volgende beeld.

- 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](#)

<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

Als u een nieuw TACACS-profiel wilt configureren, gebruikt u de knop Toevoegen. Hierdoor wordt het nieuwe profielconfiguratieformulier geopend, dat lijkt op het formulier dat in het beeld wordt weergegeven. Dit formulier moet er vooral zo uitzien om het profiel te configureren dat is toegewezen aan het adminuser (namelijk met shell-voorrechten op niveau 15).

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

<input checked="" type="checkbox"/> Default Privilege	15	(Select 0 to 15)
<input checked="" type="checkbox"/> Maximum Privilege	15	(Select 0 to 15)
<input type="checkbox"/> Access Control List		
<input type="checkbox"/> Auto Command		
<input type="checkbox"/> No Escape		(Select true or false)
<input type="checkbox"/> Timeout		Minutes (0-9999)
<input type="checkbox"/> Idle Time		Minutes (0-9999)

Custom Attributes

Add Trash Edit

Type	Name	Value
No data found.		

Cancel Save

Herhaal de bewerking voor het helpdesk profiel. Voor deze laatste zijn de Default Privilege en de Maximum Privilege beide ingesteld op 1.

Stap 4. Creer gebruikersgroepen op ISE.

Dit is hetzelfde als in Stap 3. van het gedeelte [RADIUS ISE](#)-instellingen van dit document.

Stap 5. Creer de gebruikers op ISE.

Dit is hetzelfde als in Stap 4. van het gedeelte [RADIUS ISE](#)-instellingen van dit document.


Stap 6. Maak een beleidsset voor apparaatbeheer.

Van GUI:

Wat de RADIUS-toegang betreft, moeten, zodra gebruikers zijn gecreëerd, hun authenticatie- en autorisatiebeleid nog worden vastgesteld op ISE om hen de juiste toegangsrechten te verlenen. Voor de TACACS-verificatie wordt gebruikgemaakt van Apparaatbeheer Policy Sets voor dat doel, die kunnen worden geconfigureerd vanuit de Work Centers > Device Administration > Device Admin Policy Sets GUI Page zoals aangegeven op de afbeelding.

Policy Sets

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

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
							
	Search						
	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](#)

Als u een beleidsset voor apparaatbeheer wilt maken, gebruikt u de knop Toevoegen in rood in de vorige afbeelding, waarmee u een item toevoegt aan de lijst met beleidssets. Geef een naam op voor de nieuwe set, een voorwaarde waaronder deze moet worden toegepast en de toegestane protocollen/serverreeks (hier volstaat het Default Device Admin). Gebruik de knop om de toevoeging van de beleidsset af te ronden en gebruik de pijlpunt rechts ervan om toegang te krijgen tot de configuratiepagina, zoals deze op de afgebeelde pagina ziet.

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

De specifieke Policy Set 'WLC TACACS-verificatie' in dit voorbeeld filtert aanvragen met het IP-adres gelijk aan het voorbeeld C9800 WLC IP-adres.

Als authenticatiebeleid is de standaardregel achtergelaten omdat deze voldoet aan de behoefte van de gebruiker. Er zijn twee machtigingsregels opgesteld:

- De eerste wordt geactiveerd wanneer de gebruiker tot de gedefinieerde groep behoort admin-group. Het staat alle opdrachten toe (via de standaardPermit_all regel) en kent privilege 15 toe (via het gedefinieerde IOS_Admin TACACS-profiel).
- De tweede wordt geactiveerd wanneer de gebruiker tot de gedefinieerde groep behoort helpdesk-group. Het staat alle opdrachten toe (via de standaard Permit_all regel) en kent privilege 1 toe (via het gedefinieerde IOS_Helpdesk TACACS-profiel).

Nadat deze stap is voltooid, kunnen de referenties die zijn geconfigureerd voor adminuser enhelpdesk gebruikers worden gebruikt om te

authenticeren in de WLC via de GUI of met Telnet/SSH.

Problemen oplossen

Als uw RADIUS-server verwacht dat het service-type RADIUS-kenmerk wordt verzonden, kunt u op de WLC toevoegen:

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

Probleemoplossing voor WLC GUI of CLI RADIUS/TACACS+ toegang via WLC CLI

debug tacacs Om de TACACS+ toegang tot de WLC GUI of CLI probleemoplossing te bieden, geeft u de opdracht, samen met de terminalmonitor, uit en ziet u de live-uitvoer wanneer een inlogpoging wordt gedaan.

adminuser Bijvoorbeeld, een succesvolle login gevolgd door een logout van de gebruiker genereert deze output.

```
<#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
```

Uit deze logbestanden kan worden opgemaakt dat de TACACS+ server het juiste voorrecht (dat AV priv-lvl=15 is) teruggeeft.

Wanneer u RADIUS-verificatie uitvoert, wordt een soortgelijke debug-uitvoer weergegeven die betrekking heeft op het RADIUS-verkeer.

De opdrachten debug aaa authentication en debug aaa authorization in plaats daarvan tonen welke methodelijst wordt gekozen door de WLC

wanneer de gebruiker probeert in te loggen.

Probleemoplossing voor WLC GUI of CLI TACACS+ toegang via ISE GUI

Vanaf pagina Operations > TACACS > Live Logs, kan elke gebruikersverificatie gemaakt met de TACACS+ tot de laatste 24 uur worden bekeken. Om de details van een TACACS+-autorisatie of verificatie uit te breiden, gebruikt u de knop Details met betrekking tot deze gebeurtenis.

The screenshot displays the Cisco ISE interface for TACACS operations. The breadcrumb path is Operations > TACACS > Live Logs. The page includes a navigation menu with 'Live Logs' selected, a status indicator for 'Evaluation Mode 82 Days', and a search bar. The main content area features a table of log entries with the following columns: Logged Time, Status, Details, Identity, Type, Authentication Policy, Authorization Policy, and Ise Node. The table contains six rows of data, with the first row highlighted by a red box around the 'Details' column, which contains a lock icon. The table also includes a 'Refresh' button set to 'Never', a 'Show' dropdown set to 'Latest 20 records', and a 'Within' dropdown set to 'Last 3 hours'. The table footer indicates '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		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

Als deze optie wordt uitgebreid, ziet een succesvolle verificatiepoging voorhelpdeskuser de computer er als volgt uit:

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

```

Hieruit kunt u opmaken dat de gebruiker helpdeskuser met succes is geverifieerd op het netwerkapparaat WLC-9800 met behulp van het verificatiebeleid WLC TACACS Authentication > Default. Bovendien is het autorisatieprofiel IOS Helpdesk aan deze gebruiker toegewezen en krijgt deze het voorrangsniveau 1.

Over deze vertaling

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