

Configuratie 9800 LC ambassadeur van de WLC met RADIUS en TACACS+ verificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Verificeren RADIUS](#)

[ISE configureren - RADIUS](#)

[Verifieer TACACS+](#)

[TACACS+ op WLC configureren](#)

[ISE configureren - TACACS+](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Verificeren RADIUS](#)

[Verifieer TACACS+](#)

Inleiding

Dit document beschrijft hoe u Catalyst 9800 draadloze LAN-controllers voor RADIUS en TACACS+ externe verificatie van Lobby Ambassador-gebruikers kunt configureren met behulp van Identity Services Engine (ISE).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Catalyst 9800 configuratiemodel voor draadloos WAN
- AAA, RADIUS en TACACS+ concepten

Gebruikte componenten

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

- Catalyst 9800 draadloze controller Series (Catalyst 9800-CL)
- Cisco IOS®-XE Gibraltar 16.12.1s
- ISE 2.3.0

De informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

De Lobby Ambassador-gebruiker wordt aangemaakt door de beheerder van het netwerk. Een Lobby Ambassador-gebruiker kan de gebruikersnaam, het wachtwoord, de beschrijving en de levensduur van een gastgebruiker maken. Het heeft ook de mogelijkheid om de gastgebruiker te wissen. De gastgebruiker kan worden gemaakt via GUI of CLI.

Configureren

Netwerkdigram



In dit voorbeeld worden de Lobby Ambassadors "lobby" en "lobbyTac" ingesteld. De "lobby" van de Lobby ambassadeur moet geauthentiseerd zijn tegen de RADIUS-server en de "lobbyTac" van de Lobby ambassadeur is geauthentiseerd tegen TACACS+.

De configuratie zal eerst worden uitgevoerd voor de RADIUS-ambassadeur en ten slotte voor de TACACS+ lobby-ambassadeur. De RADIUS en de TACACS+ ISE-configuratie worden ook gedeeld.

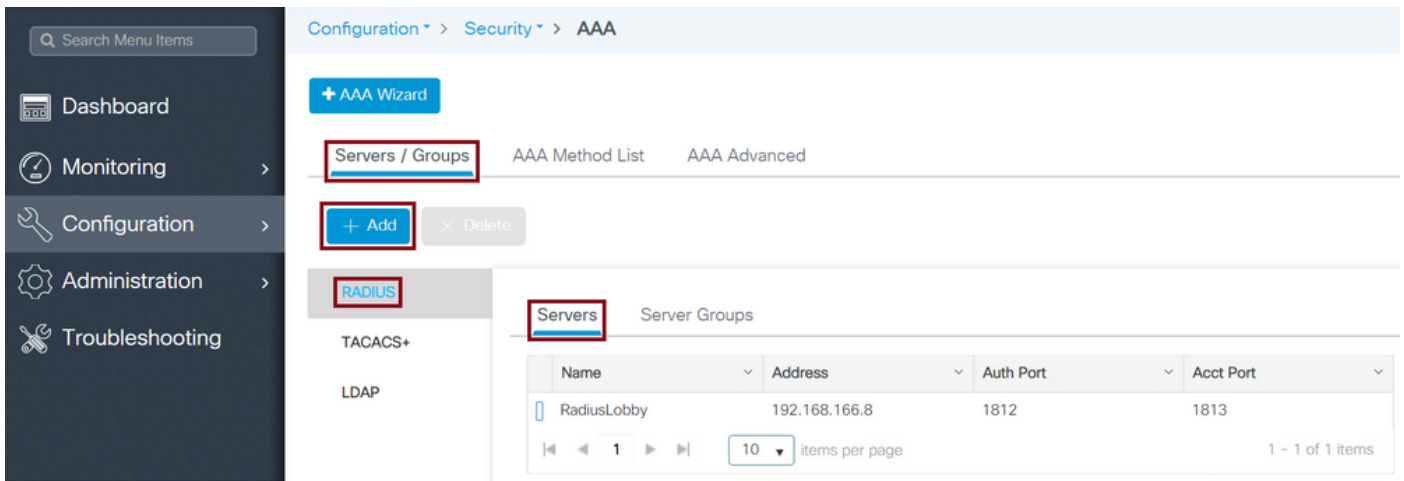
Verificeren RADIUS

Configuratie van RADIUS op draadloze LAN-controller (WLC).

Stap 1. Leg de RADIUS-server vast. Maak de ISE RADIUS-server op het WLC.

GUI:

Navigeer naar **Configuratie > Beveiliging > AAA > servers/groepen > RADIUS > servers > + Add** zoals in de afbeelding.



Wanneer het configuratievenster wordt geopend, zijn de verplichte configuratieparameters de RADIUS-servernaam (deze hoeft niet overeen te komen met de ISE/AAA-systeemnaam), het IP-ADRES van de RADIUS-server en het gedeelde geheim. Elke andere parameter kan standaard blijven of op de gewenste manier worden ingesteld.

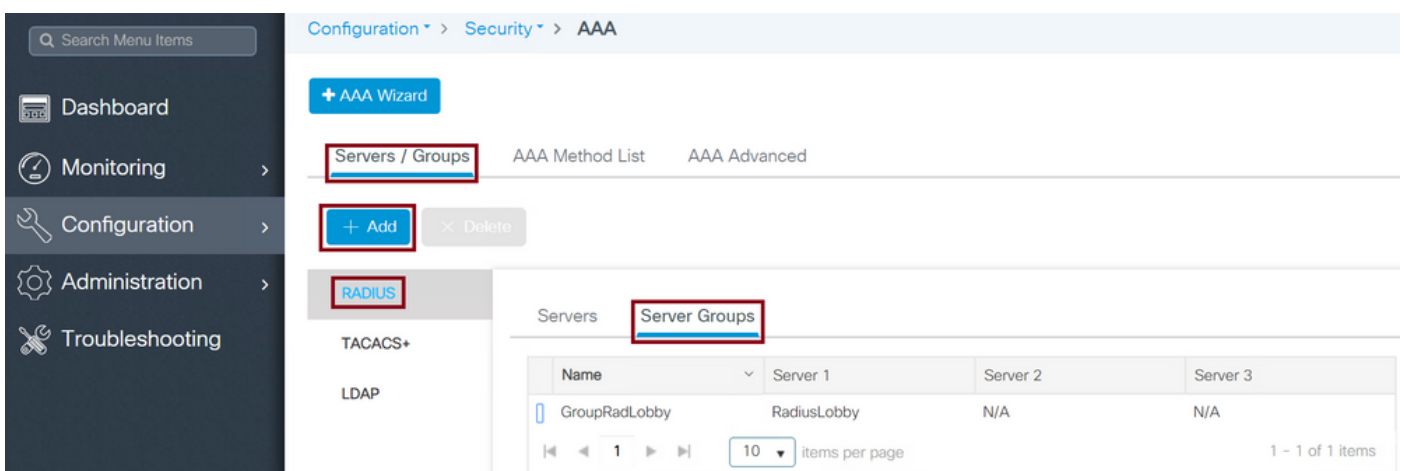
CLI:

```
Tim-eWLC1(config)#radius server RadiusLobby
Tim-eWLC1(config-radius-server)#address ipv4 192.168.166.8 auth-port 1812 acct-port 1813
Tim-eWLC1(config-radius-server)#key 0 Cisco1234
Tim-eWLC1(config)#end
```

Stap 2. Voeg de RADIUS-server toe aan een servergroep. Definieer een servergroep en voeg de geconfigureerde RADIUS-server toe. Dit is de RADIUS-server die wordt gebruikt voor de verificatie van de Lobby Ambassador-gebruiker. Als er meerdere RADIUS-servers zijn geconfigureerd in de WLC die kunnen worden gebruikt voor verificatie, wordt aanbevolen alle RADIUS-servers aan dezelfde servergroep toe te voegen. Als u dit wel doet, laat u de WLC-lading de authenticaties tussen de RADIUS-servers in de servergroep in balans brengen.

GUI:

Navigeer naar **Configuratie > Beveiliging > AAA > servers / Groepen > RADIUS > servergroepen > + Add** zoals in de afbeelding.



Wanneer het configuratievenster wordt geopend om een naam aan de groep te geven, verplaatst de geconfigureerde RADIUS-servers van de lijst Beschikbare servers naar de lijst Aangepaste servers.

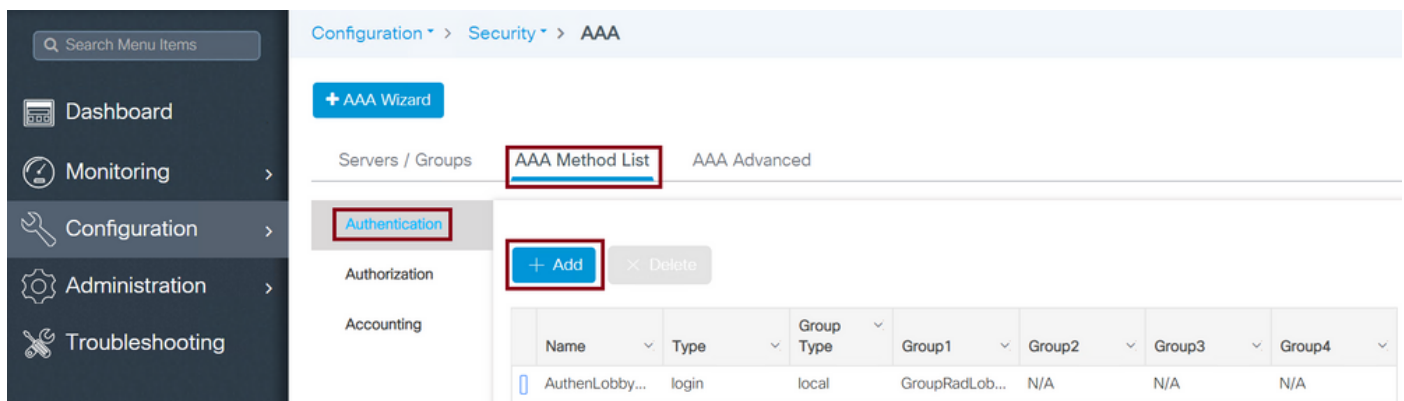
CLI:

```
Tim-eWLC1(config)#aaa group server radius GroupRadLobby  
Tim-eWLC1(config-sg-radius)#server name RadiusLobby  
Tim-eWLC1(config-sg-radius)#end
```

Stap 3. Maak een verificatiemethodelijst. De lijst Verificatiemethode definieert het type verificatie dat u zoekt en hecht ook hetzelfde type aan de servergroep die u definieert. U weet of de verificatie lokaal op de WLC of extern aan een RADIUS-server zal worden uitgevoerd.

GUI:

Navigeer naar **Configuration > Security > AAA > AAA-methodelijst > Verificatie > + Add** zoals in de afbeelding.



Wanneer het configuratievenster wordt geopend, typt u een naam, selecteert u de optie **Aanmelden** en wijst u de eerder gemaakte servergroep toe.

groepstype als lokaal.

GUI:

Als u het groepstype als 'lokaal' selecteert, controleert de WLC eerst of de gebruiker in de lokale database bestaat en slaat hij dan alleen terug naar de servergroep als de Lobby Ambassador-gebruiker niet in de lokale database aanwezig is.

CLI:

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod local group GroupRadLobby  
Tim-eWLC1(config)#end
```

Opmerking: Let op fouten van [CSCvs87163](#) als u eerst lokale gebruikers gebruikt. Dit is vastgelegd in 17.3.

groepstype als groep.

GUI:

Als u het groepstype als 'groep' selecteert en de lokale optie niet wordt gewijzigd, wordt de WLC alleen de gebruiker gecontroleerd tegen de servergroep. De WLC zal de lokale database niet

controleren.

CLI:

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod group GroupRadLobby  
Tim-eWLC1(config)#end
```

Het groepstype als een groep en de back-up naar de lokale optie worden ingeschakeld.

GUI:

Als u het groepstype als 'groep' selecteert en de back-up van de lokale optie wordt ingeschakeld, controleert de WLC de gebruiker tegen de servergroep en stelt hij de lokale database alleen vragen als de RADIUS-servertijden in de respons worden weergegeven. Als de server reageert, zal de WLC geen lokale authenticatie starten.

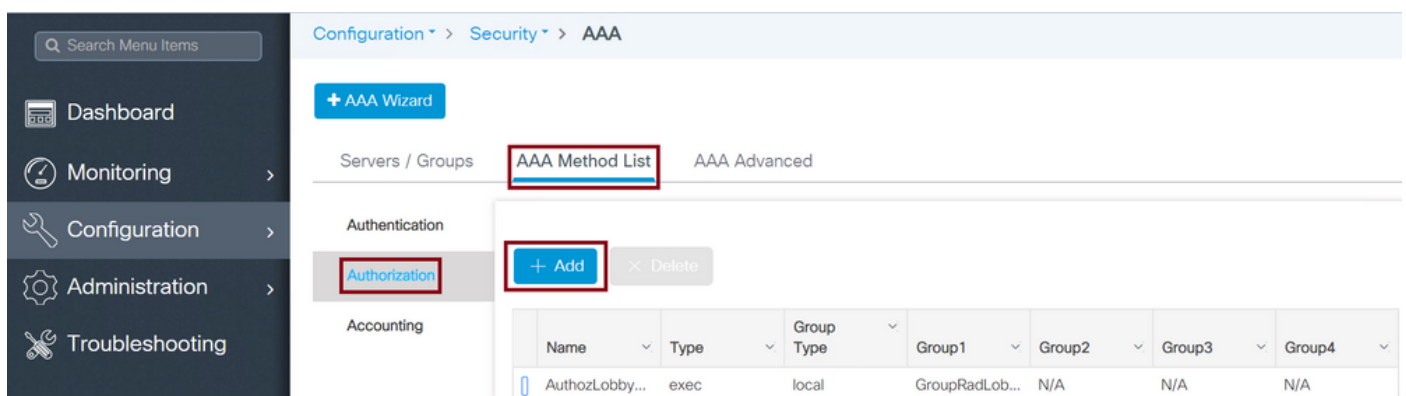
CLI:

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod group GroupRadLobby local  
Tim-eWLC1(config)#end
```

Stap 4. Maak een lijst met autorisatiemethoden. De lijst van vergunningverlenende methoden definieert het type vergunning dat u nodig hebt voor de ambassadeur van Lobby, die in dit geval "exec" zal zijn. Het wordt ook toegevoegd aan dezelfde servergroep die is gedefinieerd. Tevens kan worden geselecteerd of de verificatie lokaal op de WLC of extern aan een RADIUS-server zal worden uitgevoerd.

GUI:

Blader naar **Configuratie > Beveiliging > AAA > Methode Lijst van AAA > Vergunning > + Add** zoals in de afbeelding.



The screenshot shows the Cisco WLC GUI configuration page for AAA Method List. The breadcrumb navigation is Configuration > Security > AAA. The 'AAA Method List' tab is selected. Under the 'Authorization' section, the 'Add' button is highlighted. Below, a table shows the configuration for 'AuthozLobby...':

Name	Type	Group Type	Group1	Group2	Group3	Group4
AuthozLobby...	exec	local	GroupRadLob...	N/A	N/A	N/A

Wanneer het configuratievenster wordt geopend om een naam te geven, selecteert u de optie Type als 'EXec' en wijst u de servergroep toe die eerder is gemaakt.

Houd er rekening mee dat het groepstype op dezelfde manier wordt toegepast als in het gedeelte Lijst met verificatiemethoden is beschreven.

CLI:

groepstype als lokaal.

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod local group GroupRadLobby
Tim-eWLC1(config)#end
```

groepstype als groep.

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby
Tim-eWLC1(config)#end
```

Het type groep als groep en de back-up naar de lokale optie worden ingeschakeld.

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby local
Tim-eWLC1(config)#end
```

Stap 5. Pas de methoden aan. Zodra de methoden zijn geconfigureerd moeten ze aan de opties worden toegewezen om in te loggen op de WLC om de gastgebruiker te maken, zoals line VTY (SSH/telnet) of HTTP (GUI).

Deze stappen kunnen niet vanuit GUI worden ondernomen, dus moeten ze vanuit CLI worden gezet.

HTTP/GUI-verificatie:

```
Tim-eWLC1(config)#ip http authentication aaa login-authentication AuthenLobbyMethod
Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozLobbyMethod
Tim-eWLC1(config)#end
```

Wanneer u wijzigingen in de HTTP-configuraties uitvoert, is het beter om de HTTP- en HTTPS-services opnieuw te starten:

```
Tim-eWLC1(config)#no ip http server
Tim-eWLC1(config)#no ip http secure-server
Tim-eWLC1(config)#ip http server
Tim-eWLC1(config)#ip http secure-server
Tim-eWLC1(config)#end
```

Lijn VTY.

```
Tim-eWLC1(config)#line vty 0 15
Tim-eWLC1(config-line)#login authentication AuthenLobbyMethod
Tim-eWLC1(config-line)#authorization exec AuthozLobbyMethod
Tim-eWLC1(config-line)#end
```

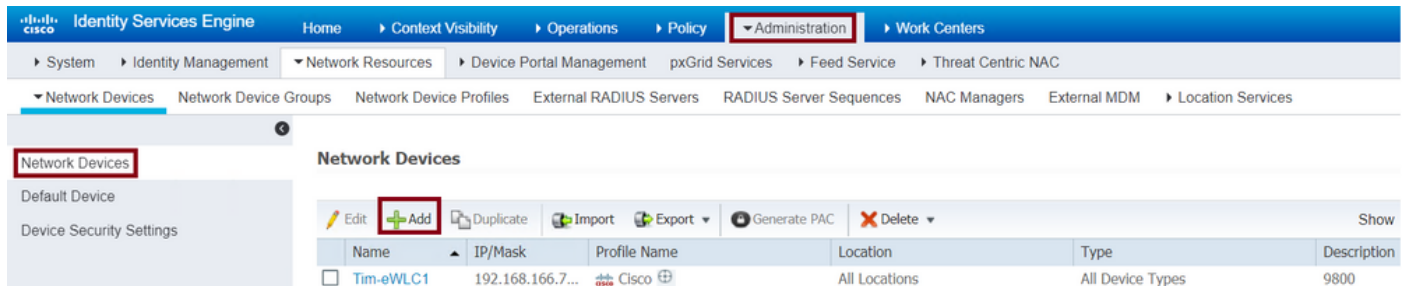
Stap 6. Deze stap is alleen vereist in softwareversies vóór 17.5.1 of 17.3.3 en is niet vereist na die releases waar [CSCvu29748](#) is uitgevoerd. Definieert de externe gebruiker. De gebruikersnaam die op ISE is gemaakt voor de lobbyambassadeur moet worden gedefinieerd als een externe gebruikersnaam voor de WLC. Als de naam van de gebruiker op afstand niet in de WLC is gedefinieerd, zal de authenticatie correct verlopen, maar de gebruiker krijgt volledige toegang tot de WLC in plaats van alleen toegang tot de voorrechten van de ambassadeur van Lobby. Deze configuratie kan alleen via CLI worden uitgevoerd.

CLI:

```
Tim-eWLC1(config)#aaa remote username lobby
```

ISE configureren - RADIUS

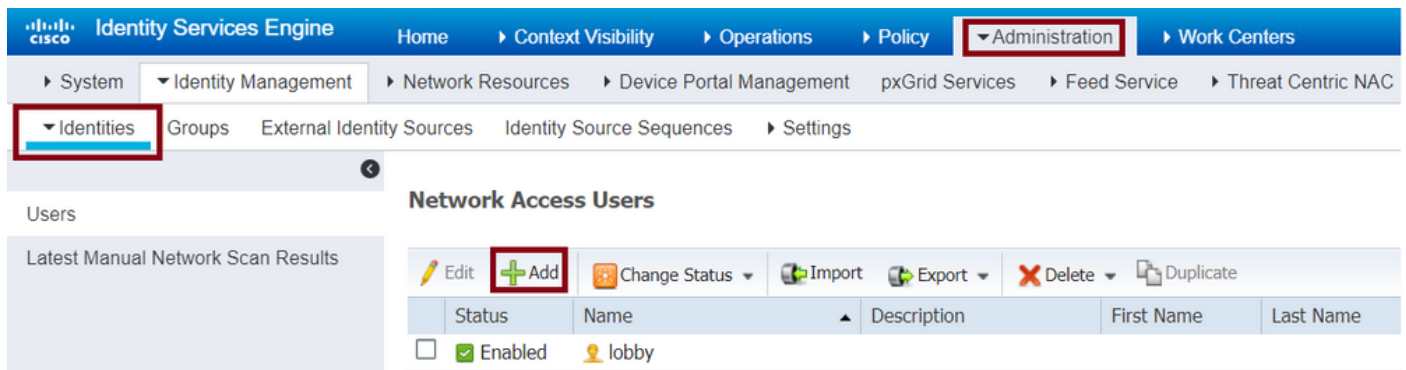
Stap 1. Voeg de WLC toe aan ISE. Navigeer in op **Beheer > Netwerkbronnen > Netwerkapparaten > Toevoegen**. De WLC moet aan ISE worden toegevoegd. Wanneer u de WLC aan ISE toevoegt, schakelt u RADIUS-verificatie-instellingen in en configureren u de gewenste parameters zoals in de afbeelding.



Wanneer het configuratievenster wordt geopend, typt u een naam, IP ADD, zet u RADIUS-verificatie-instellingen in en voert u onder Protocol Radius het gewenste gedeelte geheim in.

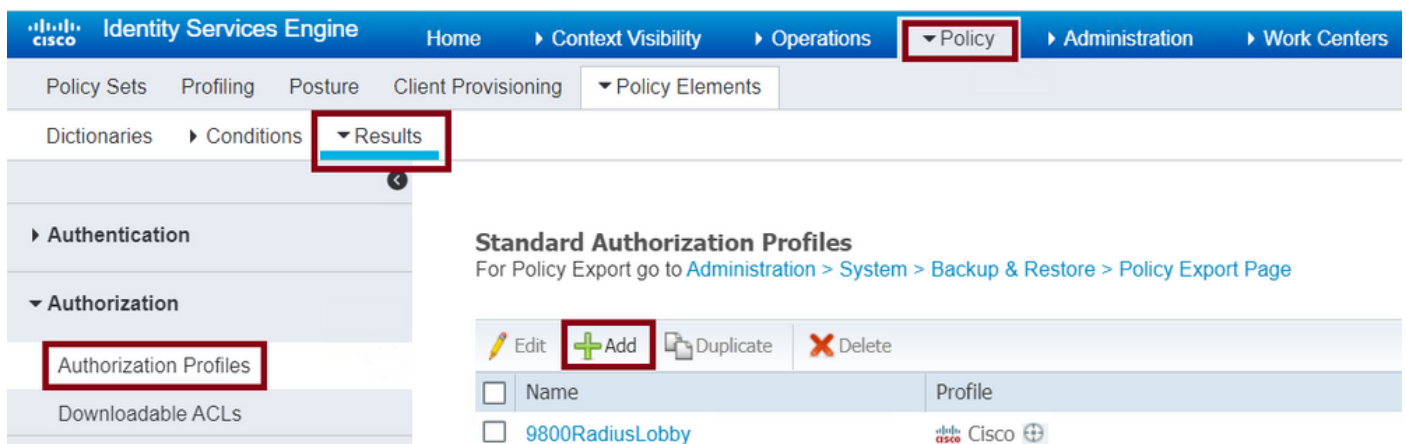
Stap 2. Maak de Lobby Ambassador-gebruiker op ISE. Navigeer in op **Administratie > identiteitsbeheer > Identiteiten > Gebruikers > Toevoegen**.

Voeg aan ISE de gebruikersnaam en het wachtwoord toe die aan de Lobby Ambassador zijn toegewezen die de gastgebruikers maakt. Dit is de gebruikersnaam die de beheerder aan de Lobby Ambassador zal toewijzen.



Wanneer het configuratievenster wordt geopend, typt u de naam en het wachtwoord voor de Lobby Ambassador-gebruiker. Zorg er ook voor dat de status is ingeschakeld.

Stap 3. Maak een profiel voor een vergunning van resultaten. Navigeren in op **beleid > Beleidselementen > Resultaten > autorisatie > autorisatieprofielen > Toevoegen**. Maak een vergunningprofiel voor het resultaat om naar de WLC terug te keren en aanvaard de gewenste eigenschappen zoals in de afbeelding.



Zorg ervoor dat het profiel is geconfigureerd om een access-Accept te verzenden zoals in de afbeelding.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. The left sidebar shows 'Policy Sets', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. Under 'Policy Elements', 'Results' is selected. The main content area displays 'Authorization Profiles > 9800RadiusLobby' and 'Authorization Profile'. The configuration fields are: '* Name' (9800RadiusLobby), 'Description' (empty), and '* Access Type' (ACCESS_ACCEPT). The '* Access Type' field is highlighted with a red box.

U moet de eigenschappen handmatig toevoegen onder Geavanceerde Attributen Instellingen. De eigenschappen zijn nodig om de gebruiker te definiëren als Lobby Ambassador en het voorrecht te verlenen zodat de Lobby Ambassador de nodige wijzigingen kan aanbrengen.

Advanced Attributes Settings

The screenshot shows the 'Advanced Attributes Settings' section. Two attribute entries are visible, both highlighted with red boxes:

- Cisco:cisco-av-pair = user-type=lobby-admin
- Cisco:cisco-av-pair = shell:priv-lvl=15

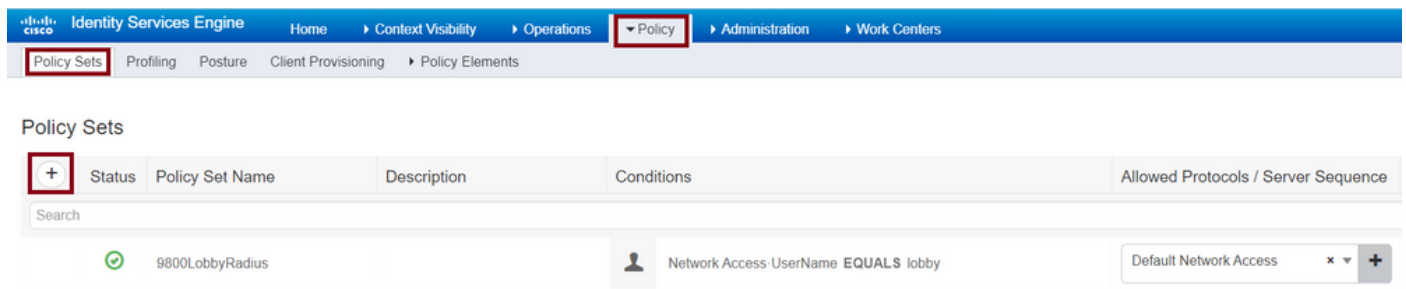
Attributes Details

```
Access Type = ACCESS_ACCEPT  
cisco-av-pair = user-type=lobby-admin  
cisco-av-pair = shell:priv-lvl=15
```

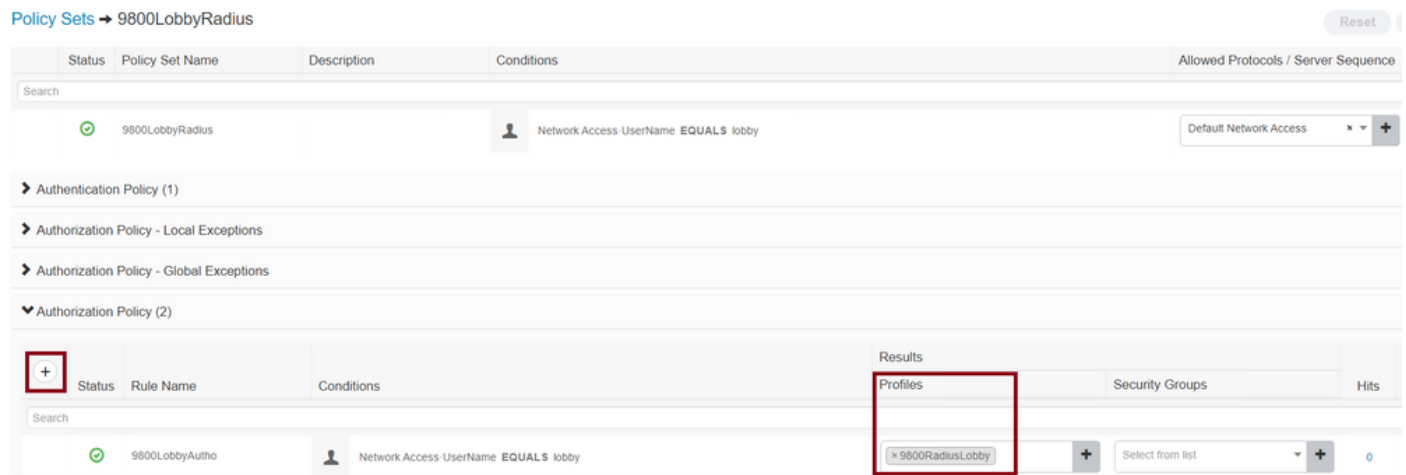
Stap 4. Maak een beleid om de authenticatie te verwerken. Navigeren in op **beleid > beleidssets > Toevoegen**. De voorwaarden om het beleid te configureren dienen afhankelijk te zijn van de beheerder. Hieronder wordt de voorwaarde voor toegang tot een netwerk en het standaard protocol voor netwerktoegang gebruikt.

Het is verplicht ervoor te zorgen dat in het kader van het machtigingsbeleid het profiel dat bij de Resultaten-autorisatie is ingesteld, wordt geselecteerd, zodat u de benodigde eigenschappen aan

de WLC kunt teruggeven zoals in de afbeelding wordt getoond.



Wanneer het venster voor de configuratie wordt geopend, specificeert u het autorisatiebeleid. Het verificatiebeleid kan standaard worden ingesteld.



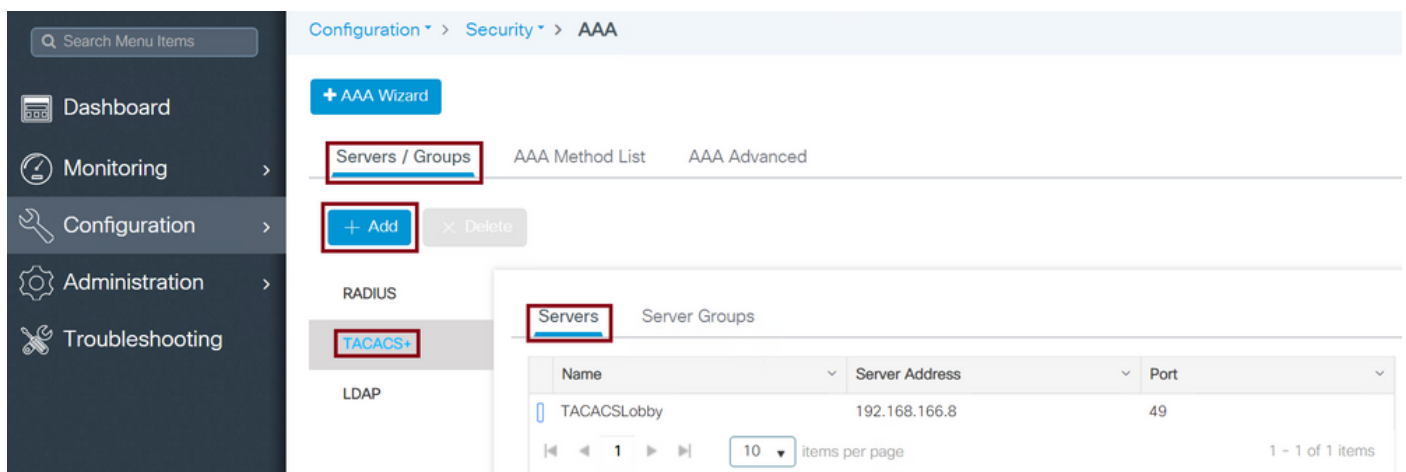
Verifieer TACACS+

TACACS+ op WLC configureren

Stap 1. verklaar de TACACS+ server. Maak de ISE TACACS-server in de WLC.

GUI:

Navigeer naar **Configuratie > Beveiliging > AAA > servers/groepen > TACACS+ > servers > + Add** zoals in de afbeelding.



Wanneer het configuratievenster wordt geopend, zijn de verplichte configuratieparameters de naam van de TACACS+ server (het hoeft niet overeen te komen met de systeemnaam ISE/AAA),

het IP-ADRES van de TACACS-server en het gedeelde geheim. Elke andere parameter kan standaard blijven of indien nodig worden geconfigureerd.

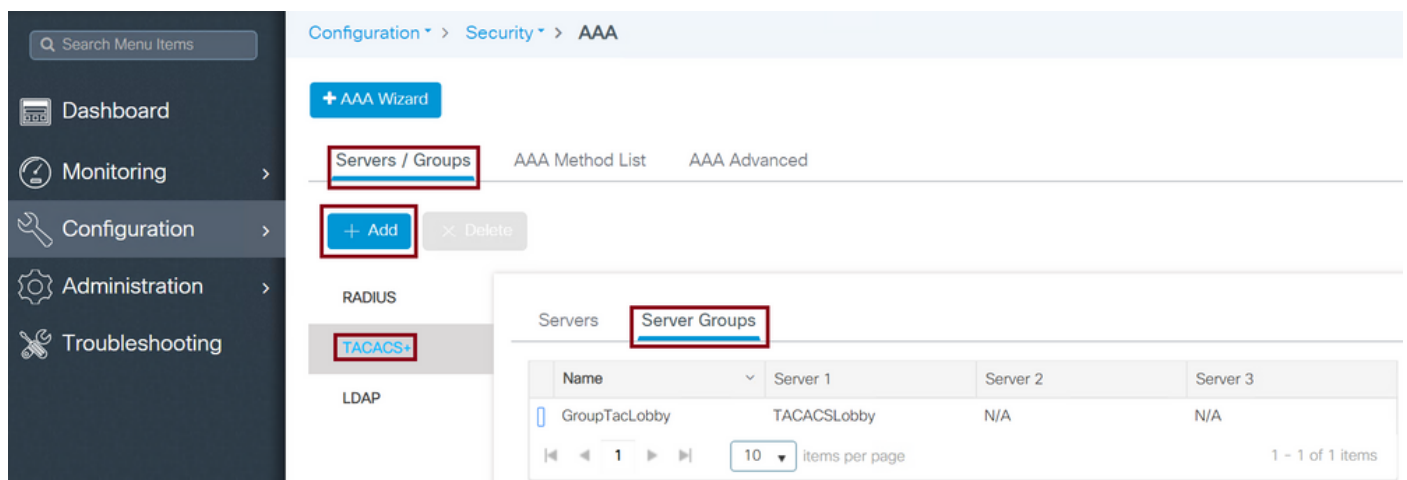
CLI:

```
Tim-eWLC1(config)#tacacs server TACACSLobby
Tim-eWLC1(config-server-tacacs)#address ipv4 192.168.166.8
Tim-eWLC1(config-server-tacacs)#key 0 Cisco123
Tim-eWLC1(config-server-tacacs)#end
```

Stap 2. Voeg de TACACS+ server toe aan een servergroep. Definieert een servergroep en voegt de gewenste geconfigureerde TACACS+ server toe. Dit zijn de TACACS+ servers die gebruikt worden voor verificatie.

GUI:

Navigeer naar **Configuratie > Beveiliging > AAA > servers / Groepen > TACACS > servergroepen > + Add** zoals in de afbeelding.



Wanneer het configuratievenster wordt geopend, geef dan een naam aan de groep en verplaats de gewenste TACACS+ servers van de lijst Beschikbare servers naar de lijst Aangepaste servers.

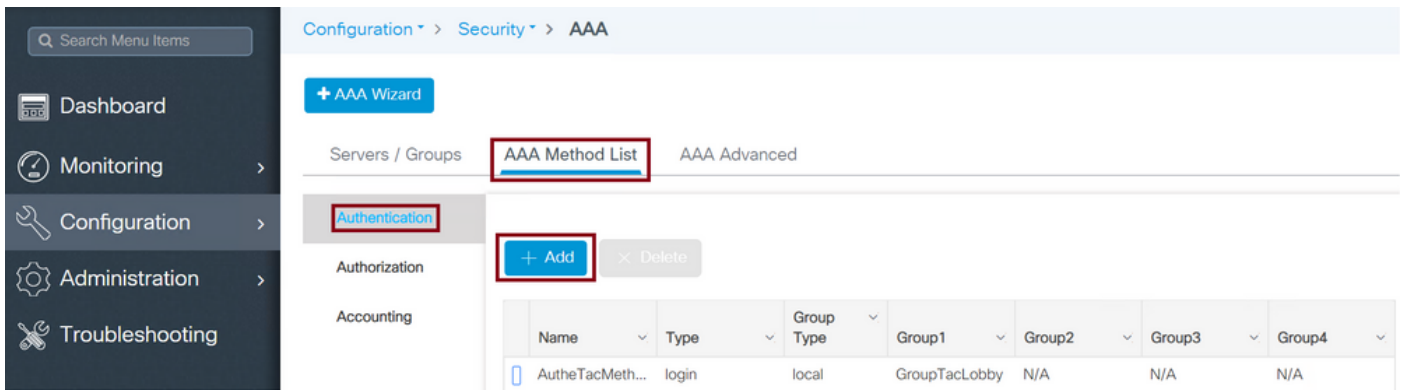
CLI:

```
Tim-eWLC1(config)#aaa group server tacacs+ GroupTacLobby
Tim-eWLC1(config-sg-tacacs+)#server name TACACSLobby
Tim-eWLC1(config-sg-tacacs+)#end
```

Stap 3. Maak een verificatiemodellijst. De lijst Verificatiemethode definieert het type verificatie dat nodig is en hecht bovendien hetzelfde type aan de geconfigureerde servergroep. Het staat ook toe om te selecteren of de authenticatie lokaal op de WLC of extern aan een TACACS+ server kan worden gedaan.

GUI:

Navigeer naar **Configuration > Security > AAA > AAA-methodelijst > Verificatie > + Add** zoals in de afbeelding.



Wanneer het configuratievenster wordt geopend, typt u een naam, selecteert u de optie **Aanmelden** en wijst u de eerder gemaakte servergroep toe.

groepstype als lokaal.

GUI:

Als u het groepstype als 'lokaal' selecteert, controleert de WLC eerst of de gebruiker in de lokale database bestaat en slaat hij dan alleen terug naar de servergroep als de gebruiker van Lobby Ambassador in de lokale database niet gevonden is.

Opmerking: Let op dit bug [CSCvs87163](#) dat is vastgesteld in 17.3.

CLI:

```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod local group GroupTacLobby
Tim-eWLC1(config)#end
```

groepstype als groep.

GUI:

Als u het groepstype als groep selecteert en de lokale optie niet wordt tegengewerkt, wordt de WLC-toets gewoon door de gebruiker gecontroleerd tegen de servergroep. De WLC-toets wordt dan niet ingeschakeld in de lokale database.

CLI:

```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby
Tim-eWLC1(config)#end
```

Het type groep als groep en de back-up naar de lokale optie worden ingeschakeld.

GUI:

Als u het groepstype als 'groep' selecteert en de back-up naar de lokale optie wordt ingeschakeld, controleert de WLC de gebruiker tegen de servergroep en stelt hij de lokale database alleen vragen als de tijden voor de TACACS-server in de respons worden weergegeven. Als de server een fout verstuurt, wordt de gebruiker niet geauthentiseerd, zelfs als het op de lokale databank bestaat.

CLI:

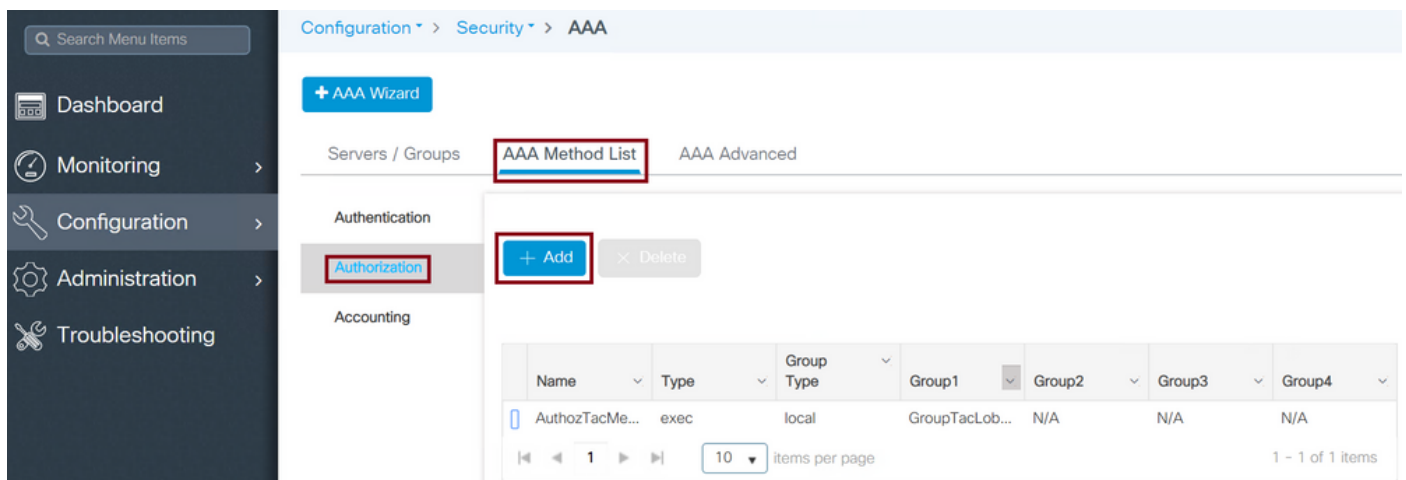
```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

Stap 4. Maak een lijst met autorisatiemethoden.

In de lijst van vergunningverleningsmethoden wordt het type vergunning omschreven dat nodig is voor de ambassadeur van Lobby, die in dit geval vrij zal zijn. Het wordt ook toegevoegd aan dezelfde servergroep die is geconfigureerd. Ook mag worden geselecteerd of de verificatie lokaal op de WLC of extern aan een TACACS+ server wordt uitgevoerd.

GUI:

Blader naar **Configuratie > Beveiliging > AAA > Methode Lijst van AAA > Vergunning > + Add** zoals in de afbeelding.



Wanneer het configuratievenster wordt geopend, typt u een naam, selecteert u de gewenste optie en wijst u de eerder gemaakte servergroep toe.

Houd er rekening mee dat het groepstype op dezelfde manier wordt uitgelegd in het gedeelte Lijst met verificatiemethoden.

CLI:

groepstype als lokaal.

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod local group GroupTacLobby
Tim-eWLC1(config)#end
```

groepstype als groep.

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby
Tim-eWLC1(config)#end
```

Het groepstype als groep en de back-up naar lokale optie worden ingeschakeld.

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

Stap 5. Pas de methoden aan. Zodra de methoden zijn geconfigureerd moeten ze aan de opties

worden toegewezen om in te loggen op de WLC om de gastgebruiker te maken, zoals line VTY of HTTP (GUI). Deze stappen kunnen niet vanuit GUI worden ondernomen, dus moeten ze vanuit CLI worden gezet.

HTTP/GUI-verificatie:

```
Tim-eWLC1(config)#ip http authentication aaa login-authentication AutheTacMethod
Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozTacMethod
Tim-eWLC1(config)#end
```

Wanneer u wijzigingen aanbrengt in de HTTP-configuraties, is het beter om de HTTP- en HTTPS-services opnieuw te starten:

```
Tim-eWLC1(config)#no ip http server
Tim-eWLC1(config)#no ip http secure-server
Tim-eWLC1(config)#ip http server
Tim-eWLC1(config)#ip http secure-server
Tim-eWLC1(config)#end
```

LijnVTY:

```
Tim-eWLC1(config)#line vty 0 15
Tim-eWLC1(config-line)#login authentication AutheTacMethod
Tim-eWLC1(config-line)#authorization exec AuthozTacMethod
Tim-eWLC1(config-line)#end
```

Stap 6. Bepaal de externe gebruiker. De gebruikersnaam die op ISE is gemaakt voor de lobbyambassadeur moet worden gedefinieerd als een externe gebruikersnaam voor de WLC. Als de naam van de gebruiker op afstand niet in de WLC is gedefinieerd, zal de authenticatie correct verlopen, maar de gebruiker krijgt volledige toegang tot de WLC in plaats van alleen toegang tot de voorrechten van de ambassadeur van Lobby. Deze configuratie kan alleen via CLI worden uitgevoerd.

CLI:

```
Tim-eWLC1(config)#aaa remote username lobbyTac
```

ISE configureren - TACACS+

Stap 1. Schakel apparaatbeheer in. Navigeer naar **Administratie > Systeem > Plaatsing**. Voordat u verder gaat, selecteert u de optie **Apparaatbeheer inschakelen** en zorgt u ervoor dat ISE is ingeschakeld zoals in de afbeelding.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration (highlighted), and Work Centers. Under Administration, the Deployment menu is highlighted. The main content area shows the 'Deployment Nodes List' for 'timise23' with an 'Edit Node' button. The configuration is divided into 'General Settings' and 'Profiling Configuration'. Under General Settings, the Role is 'STANDALONE' with a 'Make Primary' button. Under Profiling Configuration, several services are checked: Administration, Monitoring (with Role set to PRIMARY), Policy Service (with 'Enable Device Admin Service' highlighted), and 'Enable Session Services' (with 'Include Node in Node Group' set to None). Other services like 'Enable Profiling Service', 'Enable Threat Centric NAC Service', and 'Enable SXP Service' are unchecked.

Stap 2. Voeg de WLC toe aan ISE. Navigeer in op **Beheer > Netwerkbronnen > Netwerkkapparaten > Toevoegen**. De WLC moet aan ISE worden toegevoegd. Wanneer u WLC aan ISE toevoegt, schakelt u TACACS+ verificatie-instellingen in en configureren u de gewenste parameters zoals in de afbeelding.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration (highlighted), and Work Centers. Under Administration, the Network Resources menu is highlighted, and the 'Network Devices' sub-menu is selected. The main content area shows the 'Network Devices' configuration page. The 'Add' button is highlighted. Below the table, there is a table with the following data:

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> Tim-eWLC1	192.168.166.7...	Cisco	All Locations	All Device Types	9800

Wanneer het configuratievenster wordt geopend om een naam, IP ADD te verstrekken, schakelt u TACACS+ Verificatieinstellingen in en voert u het gewenste Gedeeld Geheime Gezicht in.

Stap 3. Maak de Lobby Ambassador-gebruiker op ISE. Navigeer in op **Administratie > identiteitsbeheer > Identiteiten > Gebruikers > Toevoegen**. Voeg toe aan ISE, de gebruikersnaam en het wachtwoord die aan de Lobby Ambassador zijn toegewezen die de gastgebruikers zal maken. Dit is de gebruikersnaam die de beheerder aan de Lobby Ambassador heeft toegewezen, zoals in de afbeelding wordt weergegeven.

Identity Services Engine Administration

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Network Access Users

Latest Manual Network Scan Results

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

Status	Name	Description	First Name	Last Name
<input checked="" type="checkbox"/> Enabled	lobbyTac			

Wanneer het configuratievenster wordt geopend, typt u de naam en het wachtwoord voor de Lobby Ambassador-gebruiker. Zorg er ook voor dat de status is ingeschakeld.

Stap 4. Maak een Resultaten van TACACS+ profiel. Navigeer naar **werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS profielen** zoals in de afbeelding getoond. Met dit profiel retourneert u de gewenste eigenschappen naar het WLC om de gebruiker te plaatsen als Lobby ambassadeur.

Identity Services Engine Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

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

Conditions

Network Conditions

Results

- Allowed Protocols
- TACACS Command Sets
- TACACS Profiles**

TACACS Profiles

0 Selected

Refresh **Add** Duplicate Trash Edit

Name	Type	Description
Default Shell Profile	Shell	Default Shell Profile
Deny All Shell Profile	Shell	Deny All Shell Profile
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR

Wanneer het configuratievenster nu wordt geopend, typt u een naam voor het profiel. Specificeer vervolgens een standaardkwaliteit 15 en een aangepaste eigenschap als type verplicht, naam als gebruikerstype en waarde lobby-beheerder. Laat ook het **Common Task Type** worden geselecteerd als Shell zoals in het beeld wordt weergegeven.

Task Attribute View

Raw View

Common Tasks

Common Task Type Shell

<input checked="" type="checkbox"/> Default Privilege	15	(Select 0 to 15)
<input type="checkbox"/> Maximum Privilege		(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

1 Selected

+ Add 🗑️ Trash ✎ Edit

Type	Name	Value
MANDATORY	user-type	lobby-admin

Stap 5. Maak een beleidsset. Navigeer naar **werkcentra > Apparaatbeheer > Beleidsformaten** zoals in de afbeelding. De voorwaarden om het beleid te configureren vertrouwen op de beslissing van de beheerder. Voor dit document worden de voorwaarde voor de toegang tot het netwerk en het protocol voor het standaard apparaatbeheer gebruikt. Het is verplicht er in het kader van het machtigingsbeleid voor te zorgen dat het profiel dat bij de Resultaten-autorisatie is ingesteld, wordt geselecteerd, zodat u de benodigde eigenschappen aan de WLC kunt teruggeven.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

Policy Sets Reset Save

+ Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
OK	9800TacacsLobby		Network Access-UserName EQUALS lobbyTac	Default Device Admin	0		

Wanneer het venster voor de configuratie wordt geopend, moet u het Automation Policy configureren. Het verificatiebeleid kan standaard als in de afbeelding worden weergegeven.

Policy Sets → 9800TacacsLobby Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	9800TacacsLobby		Network.Access.UserName EQUALS lobbyTac	Default Device Admin	0

▶ Authentication Policy (1)
 ▶ Authorization Policy - Local Exceptions
 ▶ Authorization Policy - Global Exceptions
 ▼ Authorization Policy (2)

Status	Rule Name	Conditions	Results	Command Sets	Shell Profiles	Hits	Actions
✔	9800TacacsAuth	Network.Access.UserName EQUALS lobbyTac		Select from list	9800TacacsLobby	0	⚙️

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

```
show run aaa
show run | sec remote
show run | sec http
show aaa method-lists authentication
show aaa method-lists authorization
show aaa servers
show tacacs
```

Zo ziet de Lobby Ambassador GUI er uit na een succesvolle authenticatie.

+ Add
x Delete

User Name	Description	Created By
No items to display		

⏪ 0 ⏩ 10 items per page

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Verificeren RADIUS

Voor RADIUS-verificatie kunnen deze uiteinden worden gebruikt:

```
Tim-eWLC1#debug aaa authentication
Tim-eWLC1#debug aaa authorization
Tim-eWLC1#debug aaa attr
Tim-eWLC1#terminal monitor
```

Zorg ervoor dat de juiste methodelijst is geselecteerd in het debug. De gewenste eigenschappen worden ook teruggegeven door de ISE Server met de juiste gebruikersnaam, type gebruiker en voorrecht.

```
Feb 5 02:35:27.659: AAA/AUTHEN/LOGIN (00000000): Pick method list 'AuthenLobbyMethod'
```

```
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(0):
7FBA5500C870 0 00000081 username(450) 5 lobby
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(1):
7FBA5500C8B0 0 00000001 user-type(1187) 4 lobby-admin
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(2):
7FBA5500C8F0 0 00000001 priv-lvl(335) 4 15(F)
Feb 5 02:35:27.683: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host
192.168.166.104 by user 'lobby' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256'
```

Verifieer TACACS+

Voor TACACS+ verificatie kan dit debug worden gebruikt:

```
Tim-eWLC1#debug tacacs
Tim-eWLC1#terminal monitor
```

Zorg ervoor dat de verificatie wordt verwerkt met de juiste gebruikersnaam en ISE IP ADD. Ook de status "PASS" moet worden gezien. In hetzelfde debug wordt meteen na de legalisatiefase het vergunningsproces gepresenteerd. In deze autorisatie garandeert ase dat de juiste gebruikersnaam samen met de juiste ISE IP ADD wordt gebruikt. Vanaf deze fase zou u de eigenschappen moeten kunnen zien die op ISE zijn ingesteld die de WLC als een Lobby Ambassadeur-gebruiker met het juiste voorrecht aangeven.

Verificatiefase:

```
Feb 5 02:06:48.245: TPLUS: Queuing AAA Authentication request 0 for processing
Feb 5 02:06:48.245: TPLUS: Authentication start packet created for 0(lobbyTac)
Feb 5 02:06:48.245: TPLUS: Using server 192.168.166.8
Feb 5 02:06:48.250: TPLUS: Received authen response status GET_PASSWORD (8)
Feb 5 02:06:48.266: TPLUS(00000000)/0/7FB7819E2100: Processing the reply packet
Feb 5 02:06:48.266: TPLUS: Received authen response status PASS (2)
```

Voorbeeld van de autorisatiefase:

```
Feb 5 02:06:48.267: TPLUS: Queuing AAA Authorization request 0 for processing
Feb 5 02:06:48.267: TPLUS: Authorization request created for 0(lobbyTac)
Feb 5 02:06:48.267: TPLUS: Using server 192.168.166.8
Feb 5 02:06:48.279: TPLUS(00000000)/0/7FB7819E2100: Processing the reply packet
Feb 5 02:06:48.279: TPLUS: Processed AV priv-lvl=15
Feb 5 02:06:48.279: TPLUS: Processed AV user-type=lobby-admin
Feb 5 02:06:48.279: TPLUS: received authorization response for 0: PASS
```

De debug voorbeelden die eerder voor RADIUS en TACACS+ zijn genoemd, hebben de belangrijke stappen voor een succesvolle inlognaam. De debugs zijn breder en de output groter. Om de knoppen uit te schakelen, kan deze opdracht worden gebruikt:

```
Tim-eWLC1#undebug all
```