

# Cisco Unified Wireless Network TACACS+ configuratie

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[TACACS+ implementatie in de controller](#)

[Verificatie](#)

[Authorization](#)

[accounting](#)

[TACACS+ configuratie in WLC](#)

[Voeg een TACACS+ verificatieserver toe](#)

[Voeg een TACACS+ licentieserver toe](#)

[Een TACACS+ accounting server toevoegen](#)

[De volgorde van verificatie configureren](#)

[Controleer de configuratie](#)

[Cisco beveiligde ACS-server configureren](#)

[Netwerkconfiguratie](#)

[Interface-configuratie](#)

[Instellen gebruiker/groep](#)

[Boekhoudkundige records in Cisco Secure ACS](#)

[TACACS+ configuratie in WCS](#)

[WCS met virtuele interfaces](#)

[Cisco beveiligde ACS configureren voor gebruik van WCS](#)

[Netwerkconfiguratie](#)

[Interface-configuratie](#)

[Instellen gebruiker/groep](#)

[Debugs](#)

[Debugs van WLC voor role1=ALL](#)

[Debugs van WLC voor meerdere rollen](#)

[Debugs van een WLC voor autorisatiefouten](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Dit document biedt een configuratievoorbeeld van Terminal Access Control System Plus (TACACS+) in een Cisco draadloze LAN-controller (WLC) en een Cisco Wireless Control System

(WCS) voor een Cisco Unified Wireless-netwerk. Dit document bevat ook een aantal eenvoudige tips voor het oplossen van problemen.

TACACS+ is een client/server-protocol dat gecentraliseerde beveiliging biedt voor gebruikers die proberen toegang tot het beheer te krijgen tot een router of netwerktoegangsserver. TACACS+ biedt deze AAA-services:

- Verificatie van gebruikers die proberen in te loggen op de netwerkapparatuur
- Toestemming om te bepalen welk niveau gebruikers van toegang moeten hebben
- Accounting om alle wijzigingen die de gebruiker aanbrengt bij te houden

Raadpleeg [TACACS+](#) voor meer informatie over AAA-services en TACACS+ functionaliteit.

Raadpleeg [TACACS+ en RADIUS-vergelijking](#) voor een vergelijking van TACACS+ en RADIUS.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van het configureren van WLC's en lichtgewicht access points (LAP's) voor gebruik als basiseenheid
- Kennis van Lichtgewicht Access Point Protocol (LWAPP) en draadloze beveiligingsmethoden
- Basiskennis RADIUS en TACACS+
- Basiskennis van de Cisco ACS-configuratie

### Gebruikte componenten

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

- Cisco Secure ACS voor Windows versie 4.0
- Cisco draadloze LAN-controller met versie 4.1.17.0. TACACS+ functionaliteit op WLC's wordt ondersteund op softwareversie 4.1.17.1.0 of hoger.
- Cisco-systeem voor draadloze controle met versie 4.1.8.3.0. De TACACS+-functionaliteit op WCS wordt ondersteund op softwareversie 4.1.8.3.0 of hoger.

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 de potentiële impact van elke opdracht begrijpen.

### Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

## TACACS+ implementatie in de controller

### Verificatie

Verificatie kan worden uitgevoerd met behulp van een lokale database, RADIUS of TACACS+ server die een gebruikersnaam en een wachtwoord gebruikt. De tenuitvoerlegging is niet volledig modulair. Verificatie- en autorisatiediensten zijn met elkaar verbonden. Bijvoorbeeld, als de authenticatie uitgevoerd wordt met RADIUS/lokale database, dan wordt de autorisatie niet uitgevoerd met TACACS+. Het zou de permissies gebruiken die voor de gebruiker in de lokale of RADIUS-database zijn gekoppeld, zoals alleen-lezen of lezen-schrijven, terwijl wanneer de authenticatie met TACACS+ wordt uitgevoerd, de autorisatie aan TACACS+ is gekoppeld.

In gevallen waarin meerdere databases zijn geconfigureerd wordt een CLI geleverd om de volgorde te bepalen waarin de backend-database moet worden doorverwezen.

## Authorization

Goedkeuring is op taken gebaseerd in plaats van op een echte vergunning per opdracht. De taken worden in kaart gebracht aan verschillende tabbladen die overeenkomen met de zeven items van de menubalk die momenteel op de web GUI staan. Dit zijn de items op de menubalk:

- MONITOR
- WLANS
- CONTROLLER
- DRAADLOOS
- SECURITY
- BEHEER
- OPDRACHT

De reden voor deze mapping is gebaseerd op het feit dat de meeste klanten gebruik maken van een webinterface om de controller te configureren in plaats van de CLI-controller.

Er is een extra rol beschikbaar voor lobby-beheer (LOBBY) voor gebruikers die alleen rechten voor lobby's hoeven te hebben.

De taak waarop een gebruiker recht heeft, is ingesteld in de TACACS+ (ACS) server met behulp van de aangepaste eigenschap-waarde (AV) paren. De gebruiker kan zijn geautoriseerd voor een of meer taken. De minimale vergunning is alleen MONITOR en het maximum is ALL (geautoriseerd om alle zeven tabbladen te gebruiken). Als een gebruiker geen recht heeft op een bepaalde taak, heeft de gebruiker nog toegang tot de taak in de alleen-lezen modus. Als verificatie is ingeschakeld en de authenticatieserver onbereikbaar wordt of geen toestemming kan geven, kan de gebruiker niet inloggen bij de controller.

**Opmerking:** Om de basisbeheerverificatie via TACACS+ te kunnen slagen, moet u verificatie- en autorisatieservers op de WLC configureren. Boekhoudconfiguratie is optioneel.

## accounting

Accounting vindt plaats wanneer een bepaalde door de gebruiker geïnitieerde actie met succes wordt uitgevoerd. De veranderde eigenschappen worden samen met deze inloggen op de TACACS+ boekhoudserver inlogd:

- Het gebruikersnummer van het individu dat de verandering heeft aangebracht
- De afstandsbediening vanaf waar de gebruiker inlogt
- De datum en het tijdstip waarop de opdracht is uitgevoerd
- Goedkeuringsniveau van de gebruiker

- Een string die informatie geeft over welke actie werd uitgevoerd en de geboden waarden  
Als de accounting server onbereikbaar wordt kan de gebruiker de sessie nog steeds voortzetten.

**Opmerking:** Boekhoudkundige gegevens worden niet gegenereerd door WCS in softwarerelease 4.1 of eerder.

## TACACS+ configuratie in WLC

WLC-softwarerelease 4.1.17.0 introduceert later nieuwe CLI's en web GUI-wijzigingen om de TACACS+-functionaliteit op de WLC in te schakelen. De geïntroduceerde CLI's worden in deze sectie ter referentie vermeld. De corresponderende wijzigingen voor web GUI worden toegevoegd onder het tabblad Beveiliging.

Dit document gaat ervan uit dat de basisconfiguratie van de WLC al is voltooid.

Om TACACS+ in de WLC-controller te configureren moet u de volgende stappen voltooien:

1. [Voeg een TACACS+ verificatieserver toe](#)
2. [Voeg een TACACS+ licentieserver toe](#)
3. [Een TACACS+ accounting server toevoegen](#)
4. [De volgorde van verificatie configureren](#)

### Voeg een TACACS+ verificatieserver toe

Voltooi deze stappen om een TACACS+ verificatieserver toe te voegen:

1. Gebruik de GUI, en ga naar **Security > TACACS+ > Verificatie**.



2. Voeg het IP-adres van de TACACS+ server toe en voer de gedeelde geheime sleutel in. Indien nodig wijzigt u de standaardpoort van TCP/49.

The screenshot shows the Cisco GUI for configuring a new TACACS+ Authentication Server. The left sidebar shows the navigation menu with 'Security' expanded to 'TACACS+ Authentication'. The main area is titled 'TACACS+ Authentication Servers > New'. The configuration fields are as follows:

Server Index (Priority)	1
Server IP Address	10.1.1.12
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Port Number	49
Server Status	Enabled
Retransmit Timeout	2 seconds

3. Klik op **Apply** (Toepassen). U kunt dit vanuit CLI bereiken met behulp van de **configuratie tacs auth add <Server Index> <IP addr> [ascii/hex] <SECURITY>** opdracht:  
(Cisco Controller) >config tacacs auth add 1 10.1.1.12 49 ascii cisco123

## [Voeg een TACACS+ licentieserver toe](#)

Voltooi deze stappen om een TACACS+ licentieserver toe te voegen:

1. Ga vanuit de GUI naar **Security > TACACS+ > autorisatie**.
2. Voeg het IP-adres van de TACACS+ server toe en voer de gedeelde geheime sleutel in. Indien nodig wijzigt u de standaardpoort van TCP/49.

The screenshot shows the Cisco GUI for configuring a new TACACS+ Authorization Server. The left sidebar shows the navigation menu with 'Security' expanded to 'TACACS+ Authorization'. The main area is titled 'TACACS+ Authorization Servers > New'. The configuration fields are as follows:

Server Index (Priority)	1
Server IP Address	10.1.1.12
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Port Number	49
Server Status	Enabled
Retransmit Timeout	2 seconds

3. Klik op **Apply** (Toepassen). U kunt dit vanuit CLI bereiken met behulp van de **configuratie-tacs van de ACS-code van de externe interface <Server Index> <IP-adres> [ascii/hex] <SECURITY>** opdracht:  
(Cisco Controller) >config tacacs athr add 1 10.1.1.12 49 ascii cisco123

## [Een TACACS+ accounting server toevoegen](#)

Voltooi deze stappen om een TACACS+ accounting server toe te voegen:

1. Gebruik de GUI, en ga naar **Security > TACACS+ > accounting**.
2. Voeg het IP adres van de server toe en voer de gedeelde geheime sleutel in. Indien nodig wijzigt u de standaardpoort van TCP/49.

3. Klik op **Apply** (Toepassen). U kunt dit vanuit CLI bereiken met behulp van de **configuratie tacs ACS-code** die **<Server Index> <IP addr> [ascii/hex] <SECURITY>** opdracht toevoegen:  
(Cisco Controller) >config tacacs acct add 1 10.1.1.12 49 ascii cisco123

## [De volgorde van verificatie configureren](#)

Deze stap legt uit hoe de AAA-volgorde van verificatie te configureren wanneer er meerdere databases zijn geconfigureerd. De volgorde van authenticatie kan **lokaal en RADIUS** zijn, of **lokaal en TACACS**. De standaardconfiguratie van de controller voor de volgorde van verificatie is *lokaal en RADIUS*.

Voltooi deze stappen om de volgorde van de authenticatie te configureren:

1. Ga vanuit de GUI naar **Security > Priority order > Management gebruiker**.
2. Selecteer de verificatieprioriteit. In dit voorbeeld is TACACS+ geselecteerd.
3. Klik op **Toepassen** om de selectie uit te voeren.

U kunt dit vanuit CLI bereiken met behulp van de **configuratie configuratie van een auth gmt**

<server1> <server2> opdracht:

(Cisco Controller) >config aaa auth mgmt tacacs local

## Controleer de configuratie

In dit gedeelte worden de opdrachten beschreven die worden gebruikt om de configuratie van TACACS+ op de WLC te controleren. Dit zijn een paar nuttige **tonen** opdrachten die helpen om te bepalen of de configuratie juist is:

- **tonen a auth**—geeft informatie over de volgorde van de authenticatie.

(Cisco Controller) >**show aaa auth**

Management authentication server order:

```
1..... local
2..... Tacacs
```

- **Laat de tacs samenvatting**-Toont een samenvatting van de TACACS+ services en statistieken zien.

(Cisco Controller) >**show tacacs summary**

Authentication Servers

Idx	Server Address	Port	State	Tout
1	10.1.1.12	49	Enabled	2

Authorization Servers

Idx	Server Address	Port	State	Tout
1	10.1.1.12	49	Enabled	2

Accounting Servers

Idx	Server Address	Port	State	Tout
1	10.1.1.12	49	Enabled	2

- **Tacacs auth stats**-displays TACACS+ verificatieserver statistieken

(Cisco Controller) >**show tacacs auth statistics**

Authentication Servers:

```
Server Index..... 1
Server Address..... 10.1.1.12
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 7
Retry Requests..... 3
Accept Responses..... 3
Reject Responses..... 0
Error Responses..... 0
Restart Responses..... 0
Follow Responses..... 0
GetData Responses..... 0
Encrypt no secret Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Timeout Requests..... 12
Unknowntype Msgs..... 0
Other Drops..... 0
```

- **Tacacs tonen de statistieken van de TACACS+ autorisatieserver van de statistieken van de status**-Toont.

(Cisco Controller) >**show tacacs athr statistics**

Authorization Servers:

```
Server Index..... 1
Server Address..... 10.1.1.12
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 3
Retry Requests..... 3
Received Responses..... 3
Authorization Success..... 3
Authorization Failure..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

- **Tacacs-accs-status**-displays TACACS+ boekhoudserverstatistieken tonen

(Cisco Controller) >**show tacacs acct statistics**

Accounting Servers:

```
Server Index..... 1
Server Address..... 10.1.1.12
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 133
Retry Requests..... 0
Accounting Response..... 0
Accounting Request Success..... 0
Accounting Request Failure..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Timeout Requests..... 399
Unknowntype Msgs..... 0
Other Drops..... 0
```

## [Cisco beveiligde ACS-server configureren](#)

Deze sectie verschaft de stappen die betrokken zijn bij de TACACS+ server om services en aangepaste eigenschappen te maken en de rollen toe te wijzen aan de gebruikers of groepen.

De creatie van gebruikers en groepen wordt in deze paragraaf niet toegelicht. Er wordt aangenomen dat de gebruikers en groepen naar behoefte worden gevormd. Raadpleeg de [gebruikersgids voor Cisco Secure ACS voor Windows Server 4.0](#) voor informatie over het maken van gebruikers en gebruikersgroepen.

## [Netwerkconfiguratie](#)

Voltooi deze stap:

Voeg het IP-adres van het controllerbeheer toe als AAA-client met verificatiemechanisme als TACACS+ (Cisco IOS).



## Interface-configuratie

Voer de volgende stappen uit:

1. Selecteer in het menu Interface Configuration de TACACS+ (Cisco IOS)-link.
2. Schakel de **nieuwe services** in.
3. Controleer zowel de vinkjes **Gebruiker** als **Groep**.
4. Voer **ciscowlc** in voor de service en voor het protocol **gemeenschappelijk**.
5. Schakel de **geavanceerde TACACS+ functies** in.

Address <http://127.0.0.1:1767/> Go Links

**CISCO SYSTEMS**

## Interface Configuration

**TACACS+ Services**

User	Group	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	PPP IP
<input type="checkbox"/>	<input type="checkbox"/>	PPP IPX
<input type="checkbox"/>	<input type="checkbox"/>	PPP Multilink
<input type="checkbox"/>	<input type="checkbox"/>	PPP Apple Talk
<input type="checkbox"/>	<input type="checkbox"/>	PPP VPDN
<input type="checkbox"/>	<input type="checkbox"/>	PPP LCP
<input type="checkbox"/>	<input type="checkbox"/>	ARAP
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Shell (exec)
<input type="checkbox"/>	<input type="checkbox"/>	PIX Shell (pixshell)
<input type="checkbox"/>	<input type="checkbox"/>	SLIP

---

**New Services**

		Service	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="ciscowlc"/>	<input type="text" value="common"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

---

**Advanced Configuration Options**

Advanced TACACS+ Features

Display a Time-of-Day access grid for every TACACS+ service where you can

Submit Cancel

6. Klik op **Inzenden** om de wijzigingen toe te passen.

### [Instellen gebruiker/groep](#)

Voer de volgende stappen uit:

1. Selecteer een eerder gemaakte gebruiker/groep.
2. Ga naar **TACACS+ instellingen**.
3. Controleer het aankruisvakje dat overeenkomt met de *ciscowlc*-service die is gecreëerd in het gedeelte Interface Configuration.
4. Controleer het aanvinkvakje **Aangepaste eigenschappen**.



## Group Setup

Jump To Access Restrictions

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

### Shell Command Authorization Set

- None
  - Assign a Shell Command Authorization Set for any network device
  - Per Group Command Authorization
- Unmatched Cisco IOS commands
- Permit
  - Deny

Command:

Arguments:

Unlisted arguments

- Permit
- Deny

**ciscowlc common**

Custom attributes

**Wireless-WCS HTTP**

Custom attributes

### IETF RADIUS Attributes

[006] Service-Type

Callback NAS Prompt

Submit

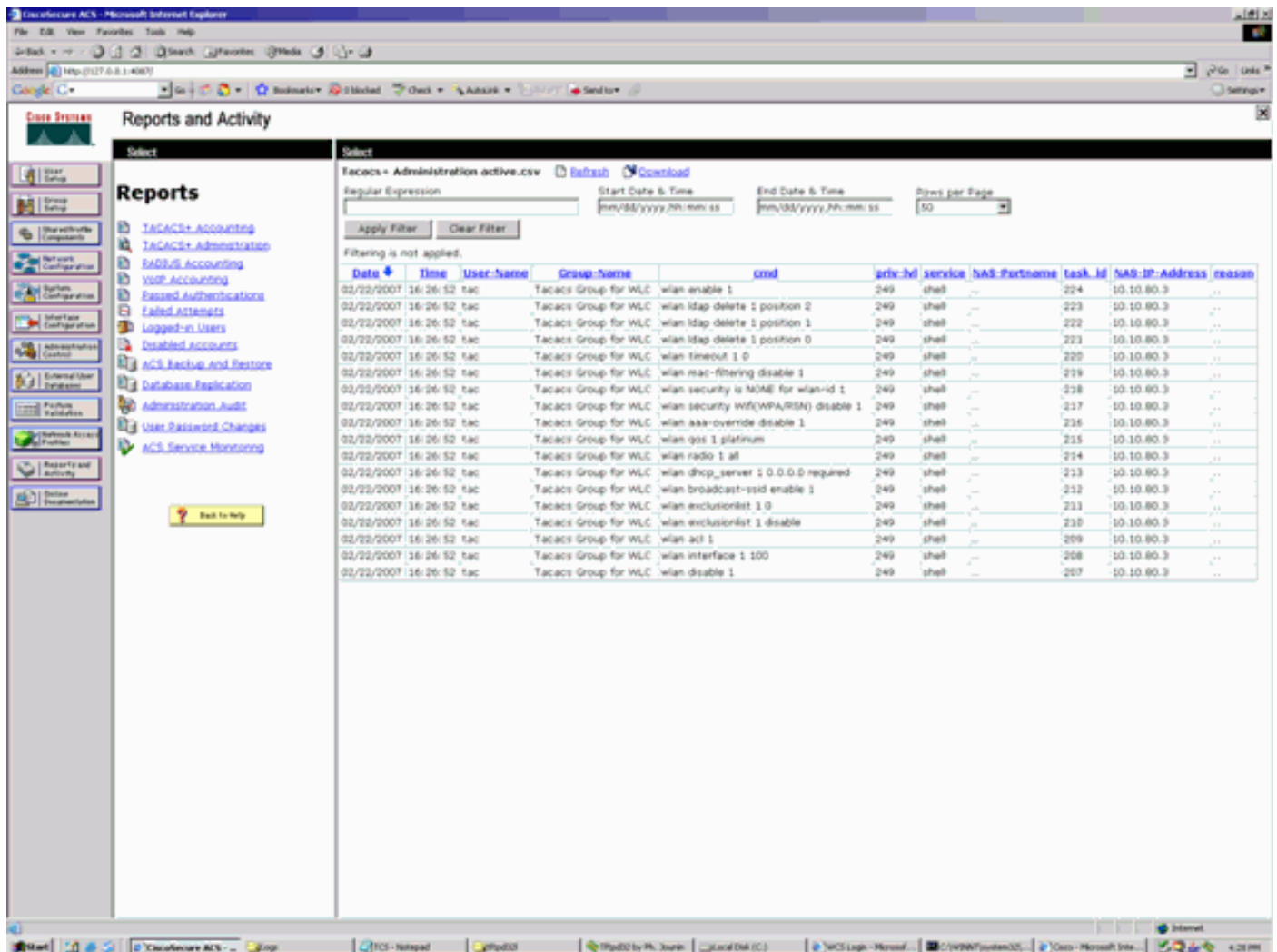
Submit + Restart

Cancel

5. Typ in het tekstvak hieronder Aangepaste eigenschappen deze tekst als de door de gebruiker gemaakte software alleen toegang nodig heeft tot WLAN, SECURITY en CONTROLLER: **role1=WLAN role2=SECURITY rol3=CONTROLLER**. Als de gebruiker alleen toegang tot het tabblad BEVEILIGING nodig heeft, voert u deze tekst in: **Ro1=BEVEILIGING**. De rol komt overeen met de zeven menubalken in de controller web GUI. De menubalkitems zijn MONITOR, WLAN, CONTROLLER, DRAADLOOS, SECURITY, MANAGEMENT en OPDRACHT.
6. Geef de rol op die een gebruiker nodig heeft voor rol1, rol2 enzovoort. Als een gebruiker alle rollen nodig heeft, dan zou het sleutelwoord **ALL** moeten worden gebruikt. Voor de lobby admin rol, moet het sleutelwoord **LOBBY** worden gebruikt.

# Boekhoudkundige records in Cisco Secure ACS

De TACACS+-boekhouding van de WLC is beschikbaar in Cisco Secure ACS in het TACACS+-beheer van rapporten en activiteit:



## TACACS+ configuratie in WCS

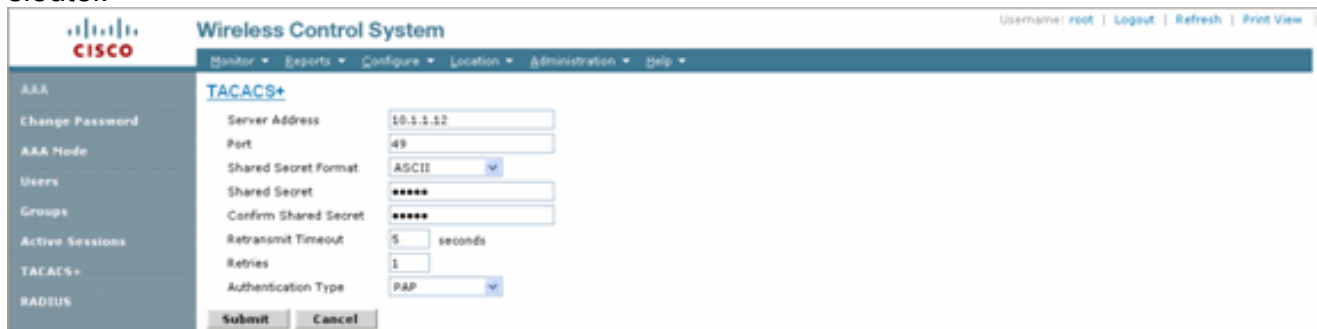
Voer de volgende stappen uit:

1. vanuit de GUI, log in naar de WCS met de basisaccount.
2. Voeg de TACACS+ server toe. Ga naar **Beheer > AAA > TACACS+ > Add TACACS+ Server**.



3. Voeg de TACACS+ serverdetails toe, zoals IP adres, poortnummer (49 is standaard) en gedeelde geheime

sleutel.



4. Schakel TACACS+ verificatie in voor toediening in de WCS. Ga naar **Beheer > AAA > AAA-modus > Selecteer TACACS+**.



## WCS met virtuele interfaces

Virtueel domein is een nieuwe functie die met WCS versie 5.1 wordt geïntroduceerd. Een virtueel WCS-domein bestaat uit een reeks apparaten en kaarten en beperkt de visie van een gebruiker tot informatie die relevant is voor deze apparaten en kaarten. Via een virtueel domein kan een beheerder ervoor zorgen dat de gebruikers alleen de apparaten en kaarten kunnen bekijken waarvoor ze verantwoordelijk zijn. Bovendien kunnen gebruikers, door de filters van het virtuele domein, alarmen configureren en rapporten genereren voor alleen hun toegewezen deel van het netwerk. De beheerder specificeert een reeks toegestane virtuele domeinen voor elke gebruiker. Bij inloggen kan slechts één van deze functies voor die gebruiker actief zijn. De gebruiker kan het huidige virtuele domein wijzigen door een ander toegestaan virtueel domein te selecteren in het vervolgkeuzemenu Virtual Domain boven in het scherm. Alle rapporten, alarmen en andere functionaliteit worden nu gefilterd door dat virtuele domein.

Als er slechts één virtueel domein is gedefinieerd (wortel) in het systeem en de gebruiker geen virtuele domeinen heeft in de velden met aangepaste eigenschappen op de TACACS+/RADIUS-server, krijgt de gebruiker standaard het virtuele domein van de wortel toegewezen.

Als er meer dan één virtueel domein is en de gebruiker geen specifieke eigenschappen heeft, dan is de gebruiker geblokkeerd bij het loggen. Om de gebruiker toe te staan om in te loggen, moeten de virtuele eigenschappen van het Domein naar de server Radius/TACACS+ worden geëxporteerd.

Met het venster Virtual Domain Custom Attributes kunt u de juiste protocol-specifieke gegevens voor elk virtueel domein aangeven. De knop Exporteren op de virtuele Hierarchy-knoppenbalk van het domein stelt de RADIUS- en TACACS+-kenmerken van het virtuele domein voor. U kunt deze eigenschappen kopiëren en plakken in de ACS-server. Hierdoor kunt u alleen de toepasbare virtuele domeinen naar het ACS-serverscherm kopiëren en zorgt u ervoor dat de gebruikers alleen toegang hebben tot deze virtuele domeinen.

Om de vooraf geformatteerde RADIUS- en TACACS+-kenmerken op de ACS-server toe te passen, dient u de stappen te voltooien die zijn uitgelegd in de sectie [Virtuele Domain RADIUS en TACACS+ Attributen](#).

## [Cisco beveiligde ACS configureren voor gebruik van WCS](#)

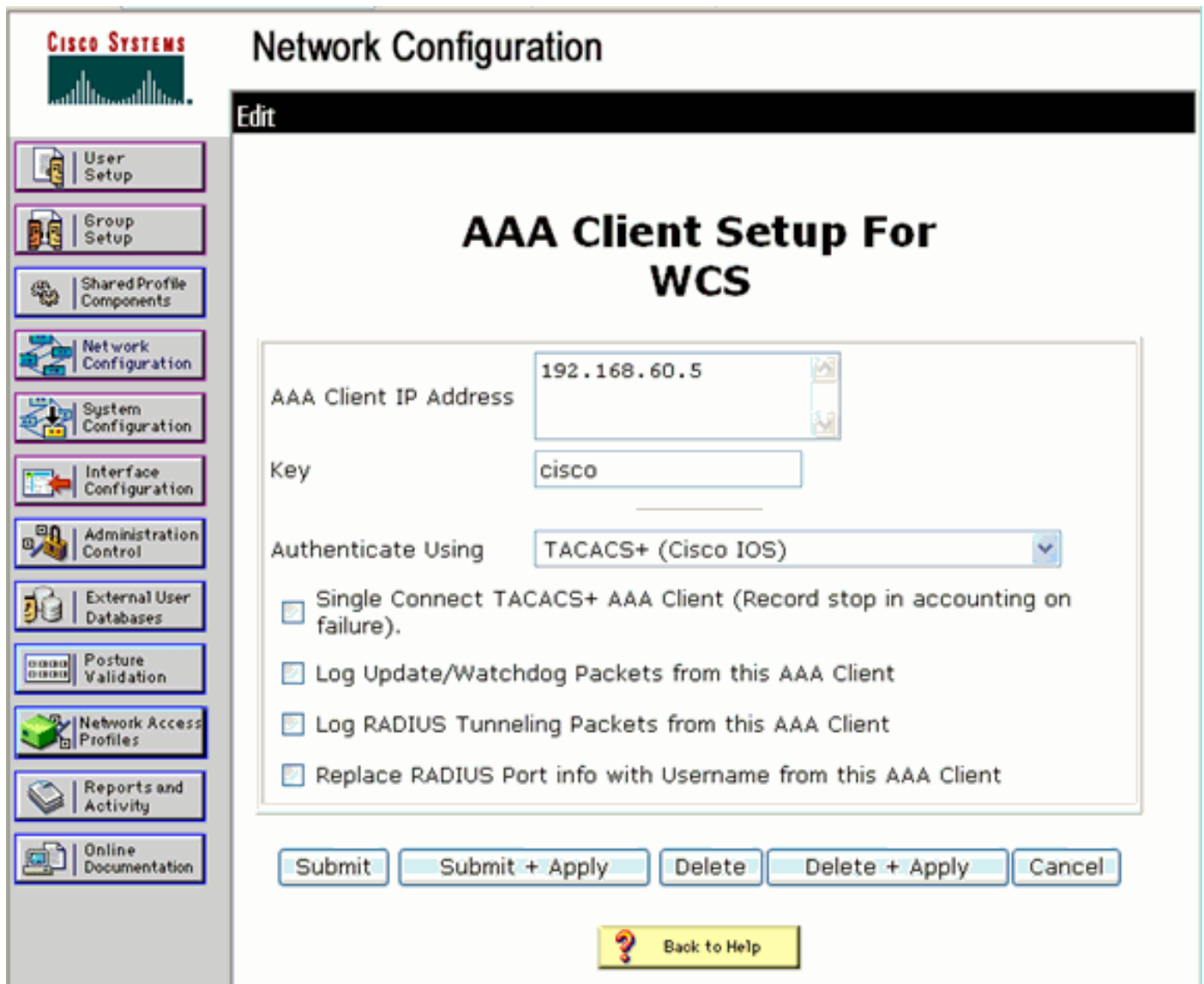
De sectie verschaft de stappen die betrokken zijn bij de TACACS+ server om services en aangepaste eigenschappen te maken en de rollen toe te wijzen aan de gebruikers of groepen.

De creatie van gebruikers en groepen wordt in deze paragraaf niet toegelicht. Er wordt aangenomen dat de gebruikers en groepen naar behoefte worden gevormd.

### [Netwerkconfiguratie](#)

Voltooi deze stap:

Voeg het WCS IP-adres toe als AAA-client met verificatiemechanisme als TACACS+ (Cisco IOS).



The screenshot shows the Cisco Network Configuration interface. The main heading is "Network Configuration" with a sub-heading "Edit". The page title is "AAA Client Setup For WCS". The configuration fields are as follows:

- AAA Client IP Address: 192.168.60.5
- Key: cisco
- Authenticate Using: TACACS+ (Cisco IOS)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure):
- Log Update/Watchdog Packets from this AAA Client:
- Log RADIUS Tunneling Packets from this AAA Client:
- Replace RADIUS Port info with Username from this AAA Client:

At the bottom, there are buttons for "Submit", "Submit + Apply", "Delete", "Delete + Apply", and "Cancel". A "Back to Help" button is also present.

### [Interface-configuratie](#)

Voer de volgende stappen uit:

1. Selecteer in het menu Interface Configuration de **TACACS+** (Cisco IOS)-link.
2. Schakel de **nieuwe services in**.
3. Controleer zowel de vinkjes **Gebruiker** als **Groep**.
4. Voer **Wireless-WCS** in voor service en **HTTP** voor protocol. **Opmerking:** HTTP moet in CAPS zijn.
5. Schakel de **geavanceerde TACACS+ functies** in.

**CISCO SYSTEMS**

## Interface Configuration

<input type="checkbox"/>	<input checked="" type="checkbox"/>	PPP IP
<input type="checkbox"/>	<input type="checkbox"/>	PPP IPX
<input type="checkbox"/>	<input type="checkbox"/>	PPP Multilink
<input type="checkbox"/>	<input type="checkbox"/>	PPP Apple Talk
<input type="checkbox"/>	<input type="checkbox"/>	PPP VPDN
<input type="checkbox"/>	<input type="checkbox"/>	PPP LCP
<input type="checkbox"/>	<input type="checkbox"/>	ARAP
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Shell (exec)
<input type="checkbox"/>	<input type="checkbox"/>	PIX Shell (pixshell)
<input type="checkbox"/>	<input type="checkbox"/>	SLIP

### New Services

		Service	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscowlc	common
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Wireless-WCS	HTTP
<input type="checkbox"/>	<input type="checkbox"/>		

### Advanced Configuration Options

Advanced TACACS+ Features

6. Klik op **Inzenden** om de wijzigingen toe te passen.

## [Instellen gebruiker/groep](#)

Voer de volgende stappen uit:

1. In de WCS GUI, navigeer naar **Administratie > AAA > Groepen** om een van de vooraf ingestelde gebruikersgroepen te selecteren, zoals SuperGebruikers in het WCS.

Group Name	Members	Audit Trail	Export
Admin	...		<a href="#">Task List</a>
ConfMnstrs	...		<a href="#">Task List</a>
System Monitors	...		<a href="#">Task List</a>
Users Assistant	...		<a href="#">Task List</a>
LibbyAmbassador	libby		<a href="#">Task List</a>
Monitor Libs	...		<a href="#">Task List</a>
North Bound API	...		<a href="#">Task List</a>
Subscribers	...		<a href="#">Task List</a>
Root	root		<a href="#">Task List</a>
User Defined 1	...		<a href="#">Task List</a>
User Defined 2	...		<a href="#">Task List</a>
User Defined 3	...		<a href="#">Task List</a>
User Defined 4	...		<a href="#">Task List</a>

2. Selecteer de taaklijst voor de vooraf ingestelde gebruikersgroepen en kopieer het plakje naar de ACS.

Please cut and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

**TACACS+ Custom Attributes**

```

role=root
task0=Users and Groups
task1=Audit Trails
task2=TACACS+ Servers
task3=RADIUS Servers
task4=Logging
task5=Logging
task6=Schedule Tasks and Data Collection
task7=User Preferences
task8=System Settings
task9=Diagnostic Information
task10=View Alerts and Events
task11=View Alerts and Events
task12=Email Notification
task13>Delete and Clear Alerts
task14=Push and Unpush Alerts
task15=Severity Configuration
task16=Configure Controllers
task17=Configure Templates
task18=Configure Config Groups
task19=Configure Access Points
task20=Configure Access Point Templates
task21=Configure Choke Points
task22=Monitor Controllers
task23=Monitor Controllers
task24=Monitor Access Points
task25=Monitor Access Points
task26=Monitor Clients
task27=Monitor Clients
task28=Monitor Tags

```

**RADIUS Custom Attributes**

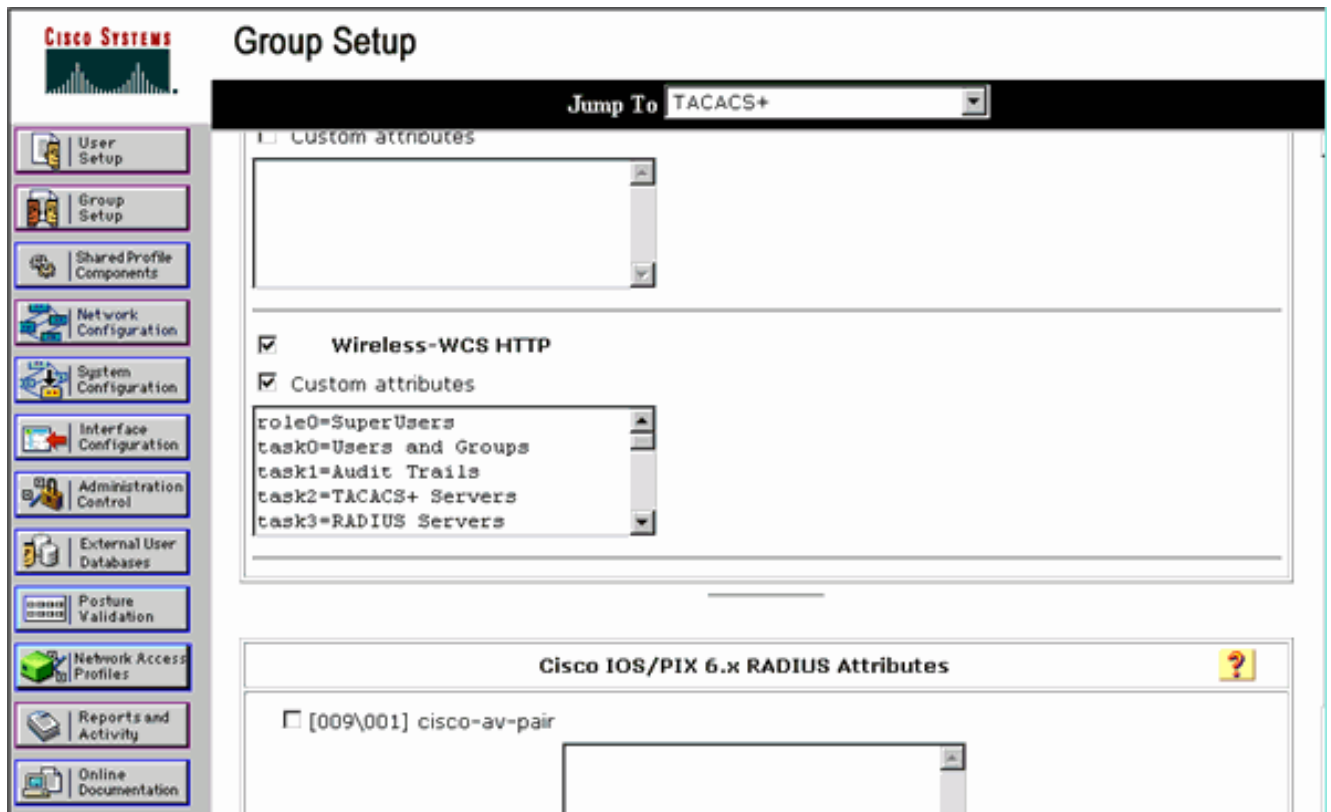
```

Wireless-WCS:role=root
Wireless-WCS:task0=Users and Groups
Wireless-WCS:task1=Audit Trails
Wireless-WCS:task2=TACACS+ Servers
Wireless-WCS:task3=RADIUS Servers
Wireless-WCS:task4=Logging
Wireless-WCS:task5=Logging
Wireless-WCS:task6=Schedule Tasks and Data Collection
Wireless-WCS:task7=User Preferences
Wireless-WCS:task8=System Settings
Wireless-WCS:task9=Diagnostic Information
Wireless-WCS:task10=View Alerts and Events
Wireless-WCS:task11=View Alerts and Events
Wireless-WCS:task12=Email Notification
Wireless-WCS:task13>Delete and Clear Alerts
Wireless-WCS:task14=Push and Unpush Alerts
Wireless-WCS:task15=Severity Configuration
Wireless-WCS:task16=Configure Controllers
Wireless-WCS:task17=Configure Templates
Wireless-WCS:task18=Configure Config Groups
Wireless-WCS:task19=Configure Access Points
Wireless-WCS:task20=Configure Access Point Templates
Wireless-WCS:task21=Configure Choke Points
Wireless-WCS:task22=Monitor Controllers
Wireless-WCS:task23=Monitor Controllers
Wireless-WCS:task24=Monitor Access Points
Wireless-WCS:task25=Monitor Access Points
Wireless-WCS:task26=Monitor Clients
Wireless-WCS:task27=Monitor Clients
Wireless-WCS:task28=Monitor Tags

```

3. Selecteer een eerder gemaakte gebruiker/groep en ga naar **TACACS+-instellingen**.
4. In ACS GUI, selecteer het aankruisvakje dat overeenkomt met de Wireless-WCS-service die eerder is gemaakt.
5. In ACS GUI, controleer de optie **Aangepaste eigenschappen**.
6. Typ deze rol en taakinformatie in het tekstvak onder Aangepaste eigenschappen die uit de WCS zijn gekopieerd. Voer bijvoorbeeld de lijst in van taken die door de SuperGebruikers zijn toegestaan.





7. Log dan in bij de WCS met de nieuwe gebruikersnaam/wachtwoord in het ACS.

## Debugs

### Debugs van WLC voor role1=ALL

```
(Cisco Controller) >debug aaa tacacs enable
```

```
(Cisco Controller) >Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=2 session_id=5eaa857e
length=16 encrypted=0
Wed Feb 28 17:36:37 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e
length=6 encrypted=0
Wed Feb 28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0
Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: author response body: status=1 arg_cnt=1 msg_len=0 data_len=0
Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL]
Wed Feb 28 17:36:37 2007: User has the following mgmtRole ffffffff8
```

### Debugs van WLC voor meerdere rollen

```
(Cisco Controller) >debug aaa tacacs enable
```

```
Wed Feb 28 17:59:33 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2
session_id=b561ad88 length=16 encrypted=0
Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:59:34 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:59:34 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=4 session_id=b561ad88
```

```
length=6 encrypted=0
Wed Feb 28 17:59:34 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:59:34 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: author response body: status=1 arg_cnt=4 msg_len=0 data_len=0
Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN]
Wed Feb 28 17:59:34 2007: arg[1] = [16][role2=CONTROLLER]
Wed Feb 28 17:59:34 2007: arg[2] = [14][role3=SECURITY]
Wed Feb 28 17:59:34 2007: arg[3] = [14][role4=COMMANDS]
Wed Feb 28 17:59:34 2007: User has the following mgmtRole 150
```

## [Debugs van een WLC voor autorisatiefouten](#)

```
(Cisco Controller) >debug aaa tacacs enable
```

```
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
length=16 encrypted=0
Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:53:04 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:53:04 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=4 session_id=89c553a1
length=6 encrypted=0
Wed Feb 28 17:53:04 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: author response body: status=16 arg_cnt=0 msg_len=0 data_len=0
Wed Feb 28 17:53:04 2007: User has the following mgmtRole 0
Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

## [Gerelateerde informatie](#)

- [Cisco draadloze LAN-controller \(WLC\) en Cisco ACS 5.x \(TACACS+\) configuratievoorbeeld voor webverificatie](#)
- [TACACS+ configureren](#)
- [Het configureren van TACACS-verificatie en -autorisatie voor Admin en niet-Admin gebruikers in ACS 5.1](#)
- [Vergelijking van TACACS+ en RADIUS](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)