

# Configureer een WLC en een ACS om beheergebruikers te verifiëren

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[WLC-configuratie](#)

[Configureer de WLC om beheer te accepteren via Cisco Secure ACS Server](#)

[Cisco Secure ACS-configuratie](#)

[Voeg de WLC als AAA-client toe aan de RADIUS-server](#)

[Gebruikers en hun juiste RADIUS IETF-kenmerken configureren](#)

[Een gebruiker met lees-schrijftoegang configureren](#)

[Een gebruiker met alleen-lezen toegang configureren](#)

[De WLC lokaal en via de RADIUS-server beheren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

---

## Inleiding

Dit document beschrijft hoe u een WLC en een Cisco Secure ACS kunt configureren zodat de AAA-server beheergebruikers op de controller kan verifiëren.

## Voorwaarden

### Vereisten

Voordat u deze configuratie uitvoert, moet aan de volgende vereisten worden voldaan:

- Kennis van hoe u fundamentele parameters op WLC's kunt configureren
- Kennis van hoe u een RADIUS-server kunt configureren zoals de Cisco Secure ACS

### Gebruikte componenten

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

- Cisco 4400 draadloze LAN-controller op versie 7.0.216.0
- Een Cisco Secure ACS-software waarmee softwareversie 4.1 wordt uitgevoerd en die in deze configuratie als RADIUS-server wordt gebruikt.

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.

## Conventies

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

## Achtergrondinformatie

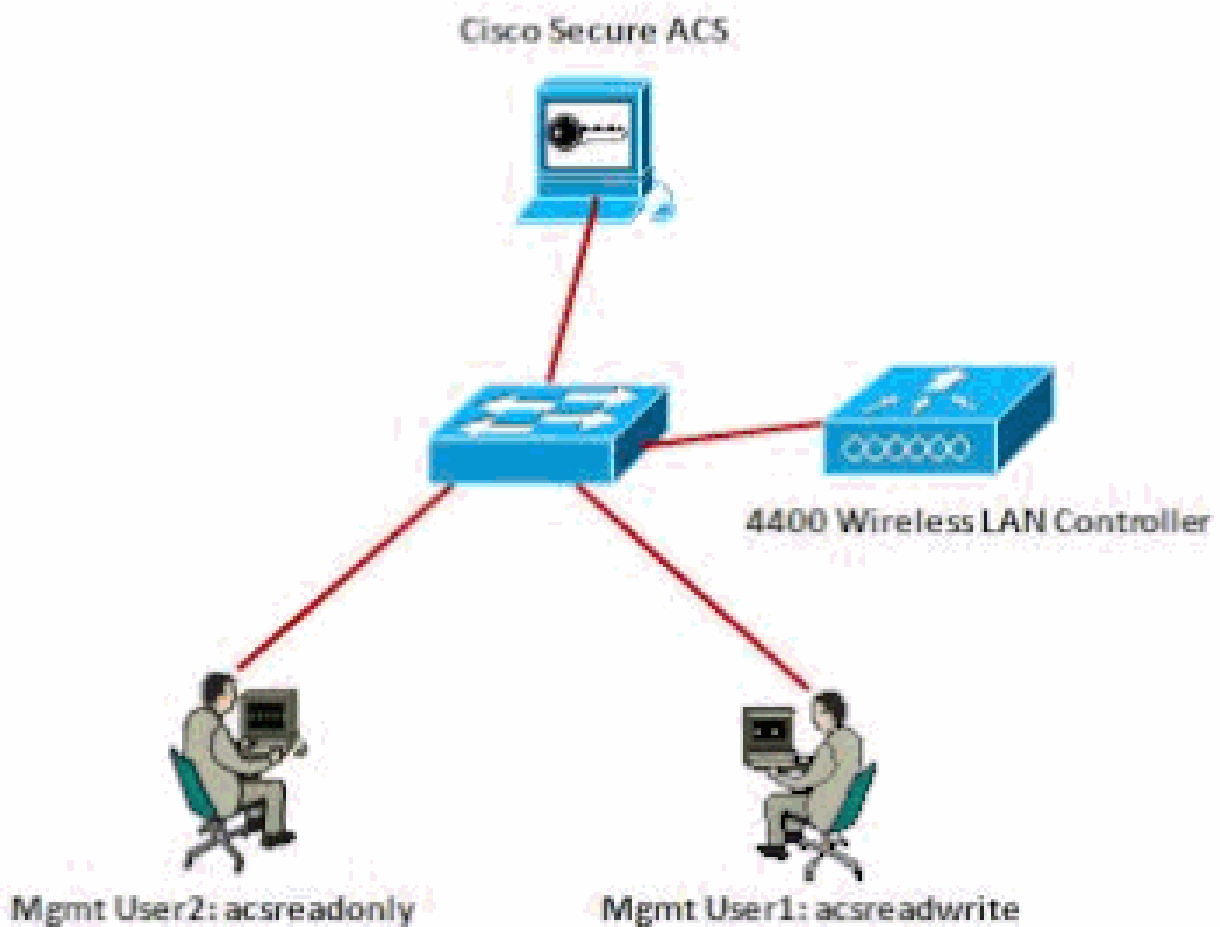
Dit document legt uit hoe u een draadloze LAN-controller (WLC) en een toegangscontroleserver (Cisco Secure ACS) kunt configureren zodat de verificatie-, autorisatie- en accounting (AAA)-server beheergebruikers op de controller kan verifiëren. Het document legt ook uit hoe verschillende beheergebruikers verschillende rechten kunnen ontvangen met leverancierspecifieke kenmerken (VSA's) die zijn geretourneerd van de Cisco Secure ACS RADIUS-server.

## Configureren

In deze sectie, wordt u voorgesteld met de informatie over hoe te om WLC en ACS voor het doel te vormen dat in dit document wordt beschreven.

## Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Netwerkdigram

Dit configuratievoorbeeld gebruikt deze parameters:

- IP-adres van Cisco Secure ACS —172.16.1.1/255.255.0.0
- IP-adres van de beheerinterface van de controller-172.16.1.30/255.255.0.0
- Gedeelde geheime sleutel die wordt gebruikt op het access point (AP) en de RADIUS-server—asdf1234
- Dit zijn de referenties van de twee gebruikers die in dit voorbeeld op ACS worden geconfigureerd:
  - Gebruikersnaam - acsreadwrite  
Wachtwoord - overschrijven
  - Gebruikersnaam - alleen voettekst  
Wachtwoord - alleen voor toegangscontrole

U moet WLC en Cisco Secure Cisco Secure ACS configureren om:

- Elke gebruiker die inlogt in de WLC met de gebruikersnaam en het wachtwoord als acsreadwrite krijgt volledige administratieve toegang tot de WLC.
- Elke gebruiker die inlogt in de WLC met de gebruikersnaam en het wachtwoord als alleen-lezen krijgt alleen-lezen toegang tot de WLC.

## Configuraties

Dit document gebruikt de volgende configuraties:

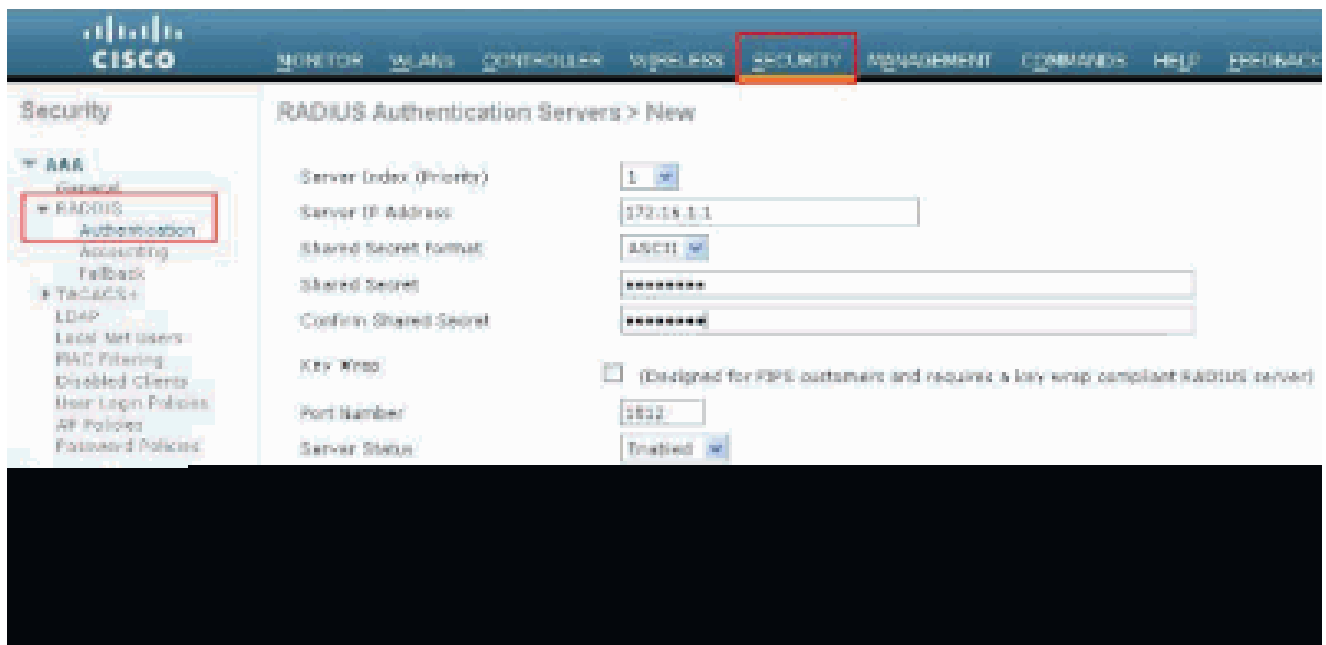
- [WLC-configuratie](#)
- [Cisco Secure ACS-configuratie](#)

## WLC-configuratie

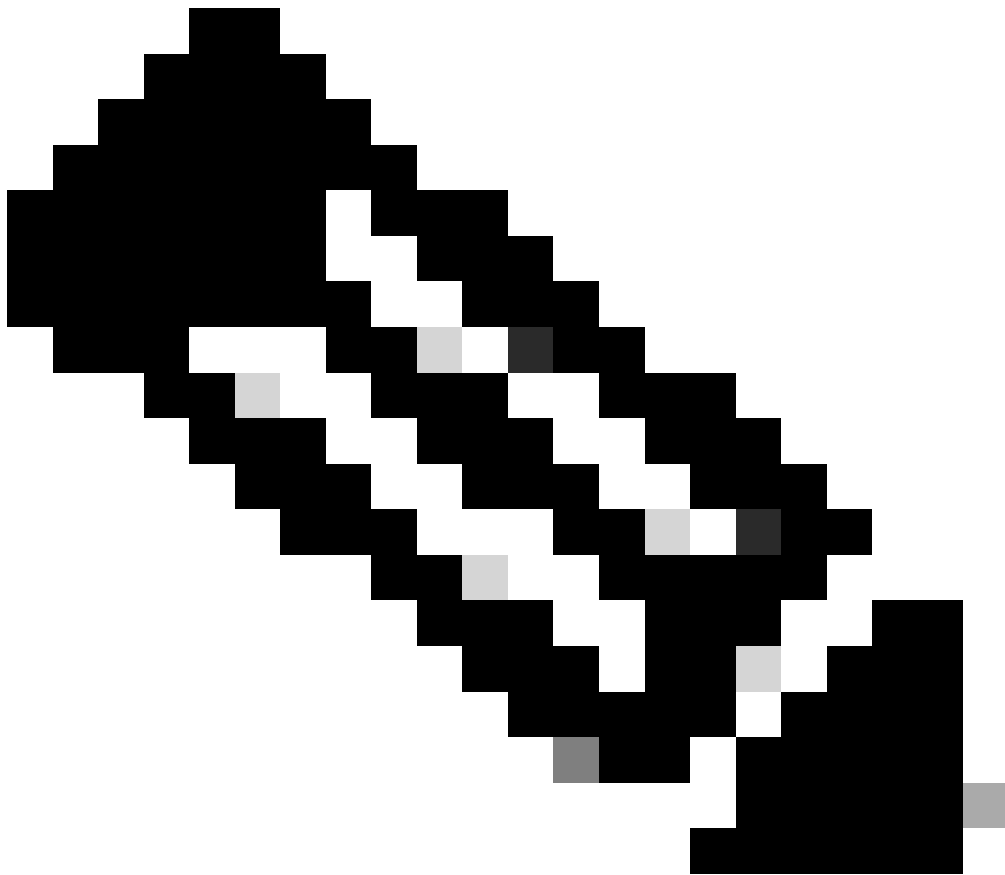
Configureer de WLC om beheer te accepteren via Cisco Secure ACS Server

Voltooi deze stappen om WLC te configureren zodat het communiceert met de RADIUS-server:

1. Klik vanuit de WLC GUI op Security. Klik in het menu links op RADIUS > Verificatie. De pagina RADIUS-verificatieservers wordt weergegeven. Als u een nieuwe RADIUS-server wilt toevoegen, klikt u op Nieuw. Voer op de pagina RADIUS-verificatieservers > Nieuwe pagina de parameters in die specifiek zijn voor de RADIUS-server. Hierna volgt een voorbeeld.

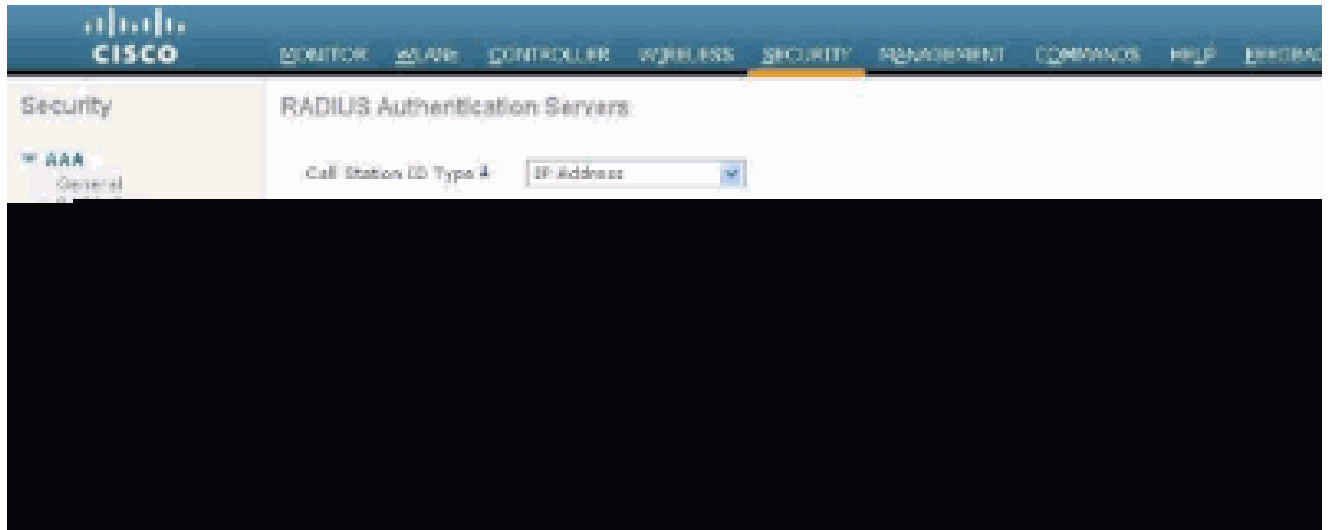


2. Controleer de radioknop Management om de RADIUS-server in staat te stellen gebruikers te verifiëren die inloggen op de WLC.



Opmerking: Zorg ervoor dat het gedeelde geheim dat op deze pagina is geconfigureerd overeenkomt met het gedeelde geheim dat op de RADIUS-server is geconfigureerd. Alleen dan kan de WLC communiceren met de RADIUS-server.

- 
3. Controleer of de WLC is geconfigureerd om te worden beheerd door Cisco Secure ACS. Klik om dit te doen op Security vanuit de WLC GUI. Het resulterende GUI-venster lijkt op dit voorbeeld.



U kunt zien dat het aanvinkvakje Management is ingeschakeld voor RADIUS-server 172.16.1.1. Dit illustreert dat ACS wordt toegestaan om de beheergebruikers op de WLC te authenticeren.

## Cisco Secure ACS-configuratie

Voltooi de stappen in deze secties om ACS te vormen:

1. [Voeg de WLC als AAA-client toe aan de RADIUS-server.](#)
2. [Gebruikers en hun juiste RADIUS IETF-kenmerken configureren.](#)
3. [Configureer een gebruiker met toegang voor lezen en schrijven.](#)
4. [Configureer een gebruiker met alleen-lezen toegang.](#)

Voeg de WLC als AAA-client toe aan de RADIUS-server

Voltooi deze stappen om WLC als AAA-client toe te voegen aan Cisco Secure ACS:

1. Klik in de ACS GUI op Netwerkconfiguratie.
2. Klik onder AAA-clients op Add Entry.
3. Voer in het venster Add AAA Client de WLC-hostnaam, het IP-adres van de WLC en een gedeelde geheime sleutel in.

In dit voorbeeld zijn dit de instellingen:

- AAA-clienthostnaam is WLC-4400
- 172.16.1.30/16 is het IP-adres van de AAA-client, in dit geval de WLC.
- De gedeelde geheime sleutel is "asdf1234".

**Network Configuration**

### Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Shared Secret:

---

**RADIUS Key Wrap**

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format:  ASCII  Hexadecimal

---

Authenticate Using:

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

Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

AAA-clientvenster toevoegen

Deze gedeelte geheime sleutel moet hetzelfde zijn als de gedeelte geheime sleutel die u op de WLC vormt.

4. Kies in het vervolgkeuzemenu Verifiëren met gebruik van RADIUS (Cisco Aironet).
5. Klik op Indienen + opnieuw starten om de configuratie op te slaan.

#### Gebruikers en hun juiste RADIUS IETF-kenmerken configureren

Om een gebruiker via een RADIUS-server te verifiëren, moet u voor de aanmelding en het beheer van de controller de gebruiker aan de RADIUS-database toevoegen met het IETF RADIUS-kenmerk Service-Typeset aan de juiste waarde op basis van de gebruikersrechten.

- Om lees-schrijfrechten voor de gebruiker in te stellen, stelt u het Service-TypeAttribute in op Administrative.
- Om alleen-lezen rechten voor de gebruiker in te stellen, stelt u de Service-TypeAttribute in op NAS-Prompt.

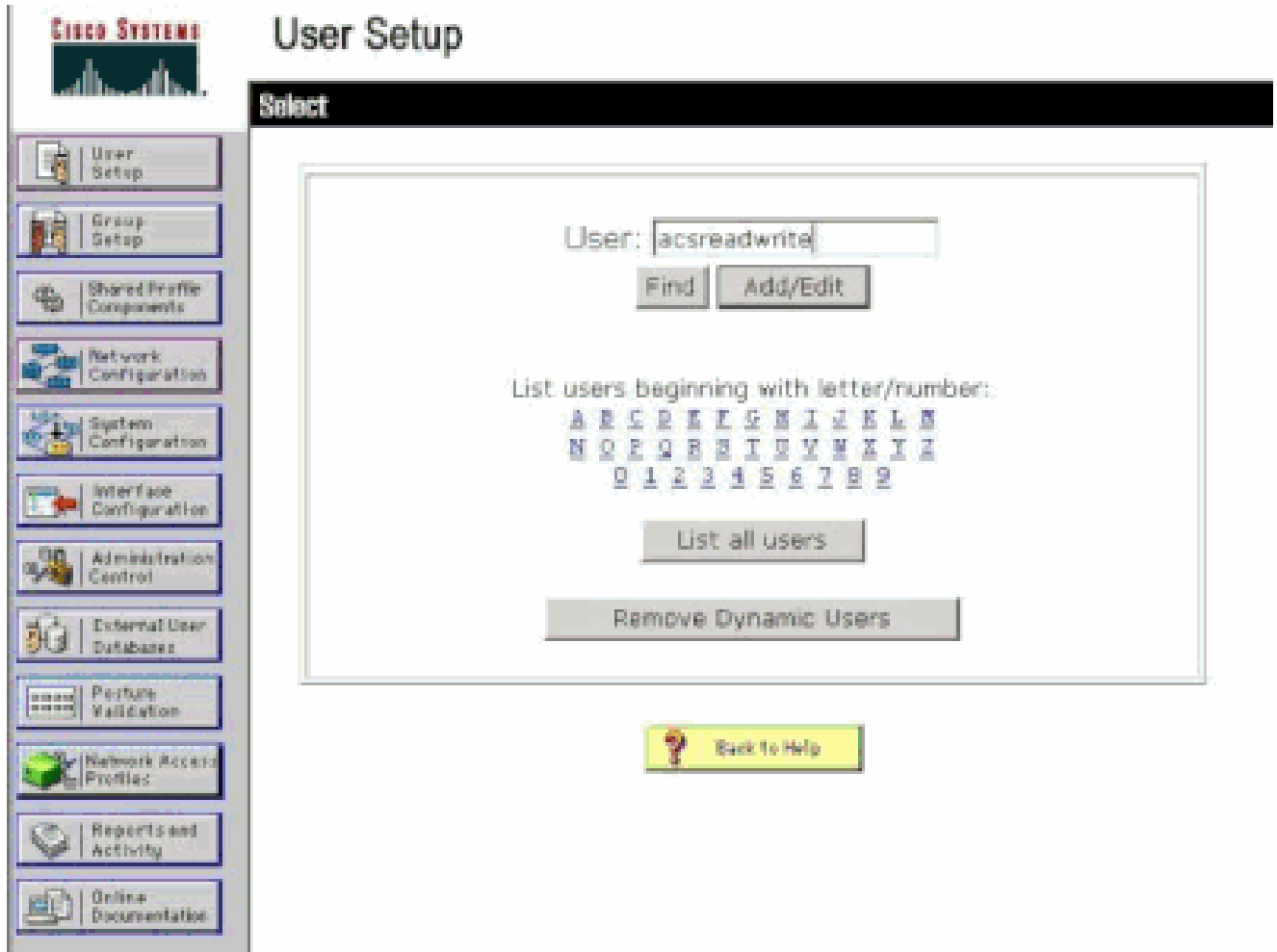
#### Een gebruiker met lees-schrijftoegang configureren

Het eerste voorbeeld toont de configuratie van een gebruiker met volledige toegang tot de WLC. Wanneer deze gebruiker probeert in te loggen op de controller, wordt de RADIUS-server geverifieerd en biedt deze gebruiker volledige administratieve toegang.

In dit voorbeeld, zijn de gebruikersnaam en het wachtwoord acsreadwrite.

Voltooi deze stappen op Cisco Secure ACS.

1. Klik vanuit de ACS GUI op Gebruikersinstelling.
2. Typ de gebruikersnaam die moet worden toegevoegd aan de ACS zoals dit voorbeeldvenster toont.



Venster Instellen gebruiker

3. Klik op Toevoegen/Bewerken om naar de pagina Bewerken door gebruiker te gaan.
4. Geef op de pagina Gebruikersbewerking de gegevens Real Name, Description and Password van deze gebruiker op.
5. Blader naar beneden naar de instelling IETF RADIUS-kenmerken en controleer servicetype-kenmerken.
6. Aangezien in dit voorbeeld, gebruiker acsreadwrite volledige toegang moet worden gegeven, kies Administratief voor het Service-Type pull-down menu en klik op Indienen.

Dit zorgt ervoor dat deze bepaalde gebruiker lees-schrijftoegang tot WLC heeft.



The screenshot shows the Cisco ACS GUI. On the left is a navigation menu with options like 'User Setup', 'Group Setup', 'Shared Profile Components', 'Network Configuration', 'System Configuration', 'Interface Configuration', 'Administration Control', 'External User Databases', 'Feature Validation', 'Network Access Profiles', 'Reports and Activity', and 'Online Documentation'. The main area is divided into two windows. The top window, titled 'Account Disable', has a 'Never' radio button selected. The bottom window, titled 'IETF RADIUS Attributes', has a checked checkbox for '[006] Service-Type'. A dropdown menu is open for this attribute, showing options: Administrative, Authenticate only, NAS Prompt, Outbound, Callback NAS Prompt, Administrative (highlighted), Callback Administrative, Callback login, Framed, Login, Call Check, and Callback framed. A 'Back to Help' button is also visible in the bottom window.

Instellingen ETF RADIUS-kenmerken

Soms is dit kenmerk Service-Type niet zichtbaar onder de gebruikersinstellingen. Voltooi in dat geval de stappen om deze zichtbaar te maken.

1. Kies in de ACS GUI de optie Interface Configuration > RADIUS (IETF) om IETF-kenmerken in het venster Gebruikersconfiguratie in te schakelen.

U gaat nu naar de pagina RADIUS (IETF)-instellingen.

2. Op de pagina RADIUS-instellingen (IETF) kunt u het IETF-kenmerk inschakelen dat zichtbaar moet zijn onder de instellingen van de gebruiker of groep. Voor deze configuratie, controleer Service-Type voor de kolom van de Gebruiker en klik op Indienen. Dit venster toont een voorbeeld.



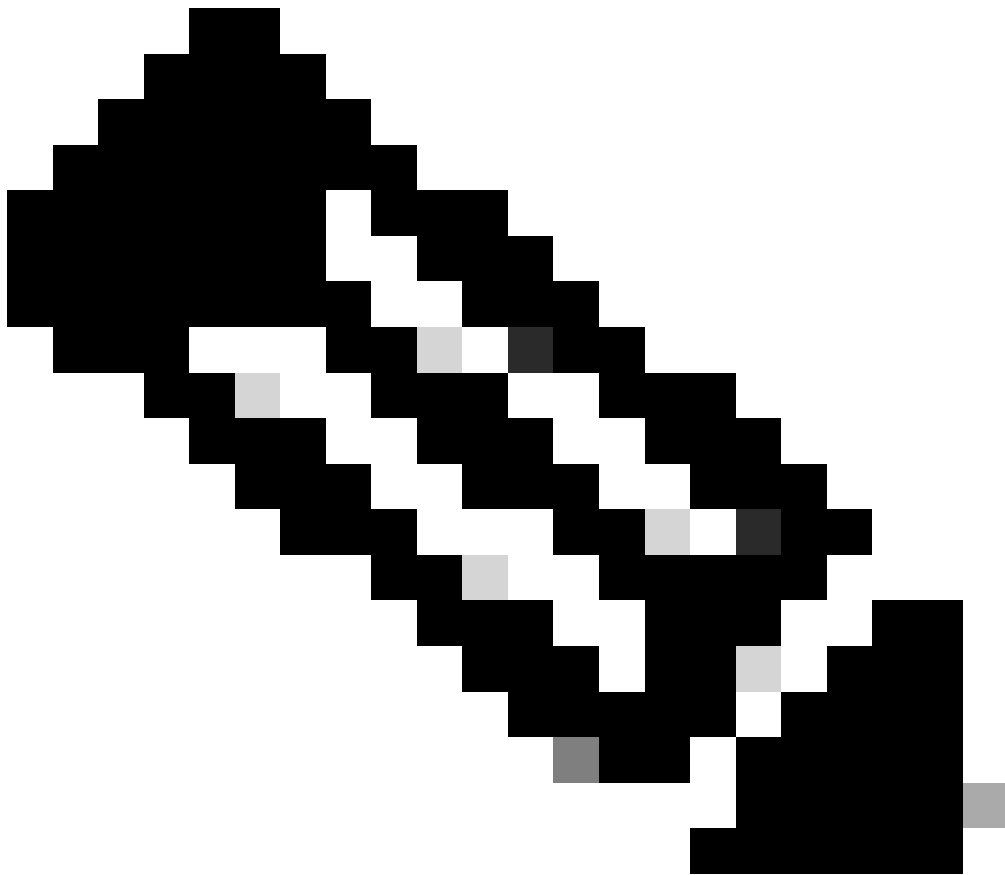
## Interface Configuration

### RADIUS (IETF)

- 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

User	Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> [006] Service-Type
<input type="checkbox"/>	<input checked="" type="checkbox"/> [007] Framed-Protocol
<input type="checkbox"/>	<input checked="" type="checkbox"/> [009] Framed-IP-Netmask
<input type="checkbox"/>	<input checked="" type="checkbox"/> [010] Framed-Routing
<input type="checkbox"/>	<input checked="" type="checkbox"/> [011] Filter-Id
<input type="checkbox"/>	<input checked="" type="checkbox"/> [012] Framed-MTU
<input type="checkbox"/>	<input checked="" type="checkbox"/> [013] Framed-Compression
<input type="checkbox"/>	<input checked="" type="checkbox"/> [014] Login-IP-Host
<input type="checkbox"/>	<input checked="" type="checkbox"/> [015] Login-Service
<input type="checkbox"/>	<input checked="" type="checkbox"/> [016] Login-TCP-Port
<input type="checkbox"/>	<input checked="" type="checkbox"/> [018] Reply-Message
<input type="checkbox"/>	<input checked="" type="checkbox"/> [020] Callback-Id
<input type="checkbox"/>	<input checked="" type="checkbox"/> [022] Framed-Route
<input type="checkbox"/>	<input checked="" type="checkbox"/> [023] Framed-IPX-Network
<input type="checkbox"/>	<input checked="" type="checkbox"/> [024] State
<input type="checkbox"/>	<input checked="" type="checkbox"/> [025] Class
<input type="checkbox"/>	<input checked="" type="checkbox"/> [027] Session-Timeout
<input type="checkbox"/>	<input checked="" type="checkbox"/> [028] Idle-Timeout

Instellingen RADIUS (IETF) op pagina



Opmerking: dit voorbeeld specificeert verificatie per gebruiker. U kunt ook verificatie uitvoeren op basis van de groep waartoe een bepaalde gebruiker behoort. Schakel in dat geval het selectievakje Groep in zodat dit kenmerk zichtbaar is onder Groepsinstellingen. Ook, als de authenticatie op groepsbasis is, moet u gebruikers toewijzen aan een bepaalde groep en de groepsinstellingseigenschappen IETF configureren om toegangsrechten te verlenen aan gebruikers van die groep. Raadpleeg Groepsbeheer voor gedetailleerde informatie over het configureren en beheren van groepen.

---

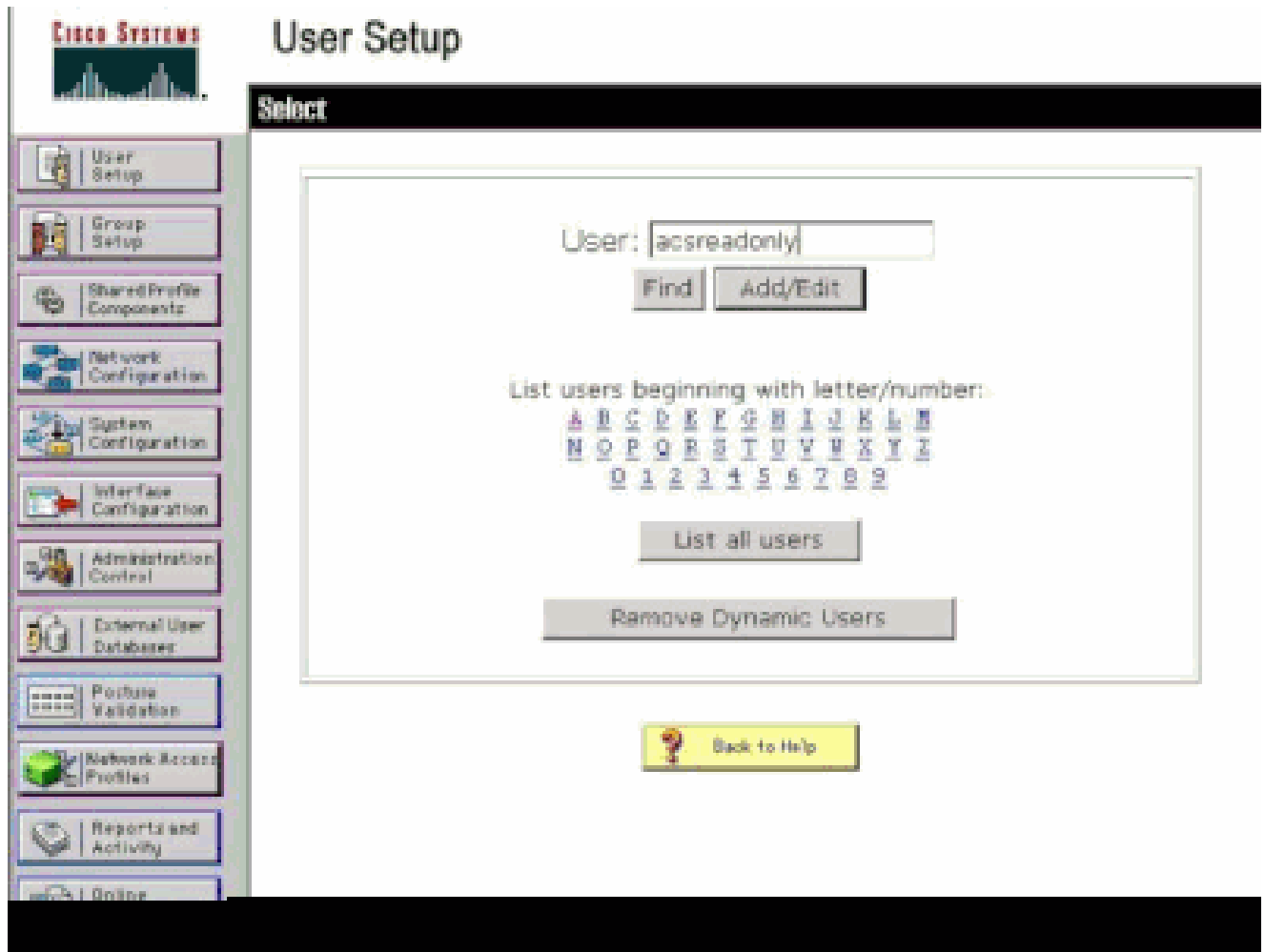
### Een gebruiker met alleen-lezen toegang configureren

Dit voorbeeld toont de configuratie van een gebruiker met alleen-lezen toegang tot de WLC. Wanneer deze gebruiker probeert in te loggen op de controller, wordt de RADIUS-server geverifieerd en biedt deze gebruiker alleen-lezen toegang.

In dit voorbeeld zijn de gebruikersnaam en het wachtwoord alleen toegankelijk.


Voltooi deze stappen op Cisco Secure ACS:

1. Klik vanuit de ACS GUI op Gebruikersinstelling.
2. Typ de gebruikersnaam die u aan de ACS wilt toevoegen en klik op Toevoegen/Bewerken om naar de pagina Bewerken door gebruiker te gaan.



Gebruikersnaam toevoegen

3. Vermeld de Real Name, Description en Password van deze gebruiker. Dit venster toont een voorbeeld.



# User Setup

**Edit**

## User: acsreadonly (New User)

Account Disabled

### Supplementary User Info

Real Name:

Description:

---

### User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password:

Confirm Password:

Separate (CHAP/MS-CHAP/ARAP)

Password:

Confirm Password:

When a token server is used for authentication, supplying a

Geef de echte naam, beschrijving en wachtwoord van de toegevoegde gebruiker

- Blader naar beneden naar de instelling IETF RADIUS-kenmerken en controleer servicetype-kenmerken.
- Aangezien in dit voorbeeld alleen gebruikers toegang nodig hebben tot alleen-lezen, kiest u NAS-prompt uit het vervolkeuzemenu Service-Type en klikt u op Indienen.

Dit zorgt ervoor dat deze bepaalde gebruiker alleen-lezen toegang tot de WLC heeft.

Servicetype-kenmerk controleren

## De WLC lokaal en via de RADIUS-server beheren

U kunt de beheergebruikers ook lokaal configureren op de WLC. Dit kan worden gedaan via de controller GUI, onder Management > Local Management Gebruikers.

The screenshot shows the Cisco WLC Management interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The left sidebar shows 'Management' with sub-items: 'Summary', 'SNMP', 'HTTP-HTTPS', 'Telnet-SSH', 'Serial Port', 'Local Management Users' (highlighted), and 'User Sessions'. The main content area is titled 'Local Management Users > New' and contains the following fields:

User Name	<input type="text" value="User1"/>
Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>
User Access Mode	<input type="text" value="ReadOnly"/>

The 'User Access Mode' dropdown menu is open, showing the following options: 'ReadOnly', 'ReadWrite', and 'LobbyAdmin'.

De beheergebruikers lokaal configureren op de WLC

Stel dat de WLC is geconfigureerd met beheergebruikers zowel lokaal als in de RADIUS-server met de optie Beheer ingeschakeld. In zo een scenario, standaard, wanneer een gebruiker probeert in te loggen op de WLC, gedraagt de WLC zich op deze manier:

1. De WLC kijkt eerst naar de lokale beheergebruikers die zijn gedefinieerd om de gebruiker te valideren. Als de gebruiker in zijn lokale lijst bestaat, dan staat het authenticatie voor deze gebruiker toe. Als deze gebruiker niet lokaal verschijnt, dan kijkt hij naar de RADIUS-server.
2. Als dezelfde gebruiker zowel lokaal als in de RADIUS-server bestaat, maar met verschillende toegangsrechten, dan verifieert de WLC de gebruiker met de lokaal gespecificeerde rechten. Met andere woorden, de lokale configuratie op de WLC heeft altijd voorrang in vergelijking met de RADIUS-server.

De volgorde van verificatie voor beheergebruikers kan op de WLC worden gewijzigd. Om dit te doen, klikt u vanaf de Security-pagina op de WLC op Priority Order > Management User. Op deze pagina kunt u de volgorde van de verificatie instellen. Hierna volgt een voorbeeld.

CISCO

MONITOR WLAN CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Security: Priority Order > Management User

AAA

- General
- RADIUS
  - Authentication
  - Accounting
  - Fallback
- TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
  - Disabled Clients
  - User Logs Policies
  - AP Policies
  - Password Policies
- Local ERP
- Priority Order
  - Management User
- Certificate
- Access Control Lists

**Authentication:**

Not Used: TACACS+ [Right Arrow] [Left Arrow]

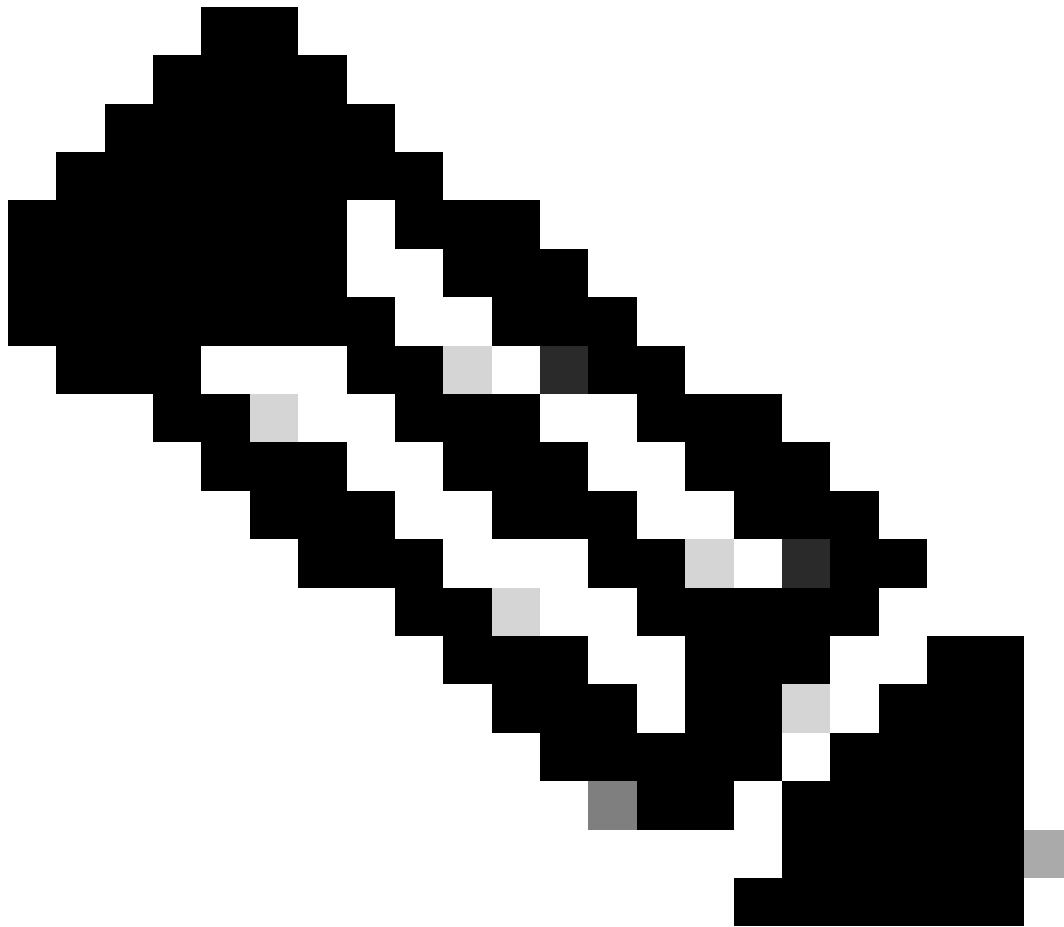
Order Used for Authentication: LOCAL RADIUS [Up] [Down]

*If LOCAL is selected as second priority, then user will be authenticated against LOCAL only if first priority is unreachable.*

## Gebruikersselectie beheren" />

Prioriteitsvolgorde > Gebruikersselectie beheren





Opmerking: als LOCAL is geselecteerd als tweede prioriteit, wordt de gebruiker met deze methode alleen geverifieerd als de methode die is gedefinieerd als de eerste prioriteit (RADIUS/TACACS) onbereikbaar is.

---

## Verifiëren

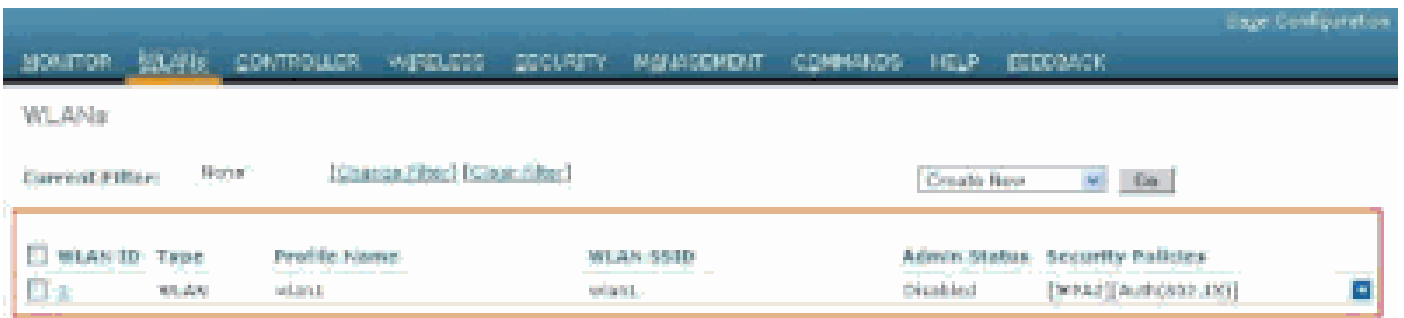
Om te verifiëren of uw configuratie correct werkt, hebt u toegang tot de WLC via de CLI- of GUI-modus (HTTP/HTTPS). Wanneer de inlogprompt verschijnt, typt u de gebruikersnaam en het wachtwoord zoals deze zijn ingesteld op de Cisco Secure ACS.

Als u de juiste configuraties hebt, wordt u met succes geauthentiseerd in WLC.

U kunt er ook voor zorgen dat de geverifieerde gebruiker wordt voorzien van toegangsbeperkingen zoals gespecificeerd door de ACS. Toegang tot de WLC GUI via HTTP/HTTPS (zorg ervoor dat WLC is geconfigureerd om HTTP/HTTPS toe te staan).

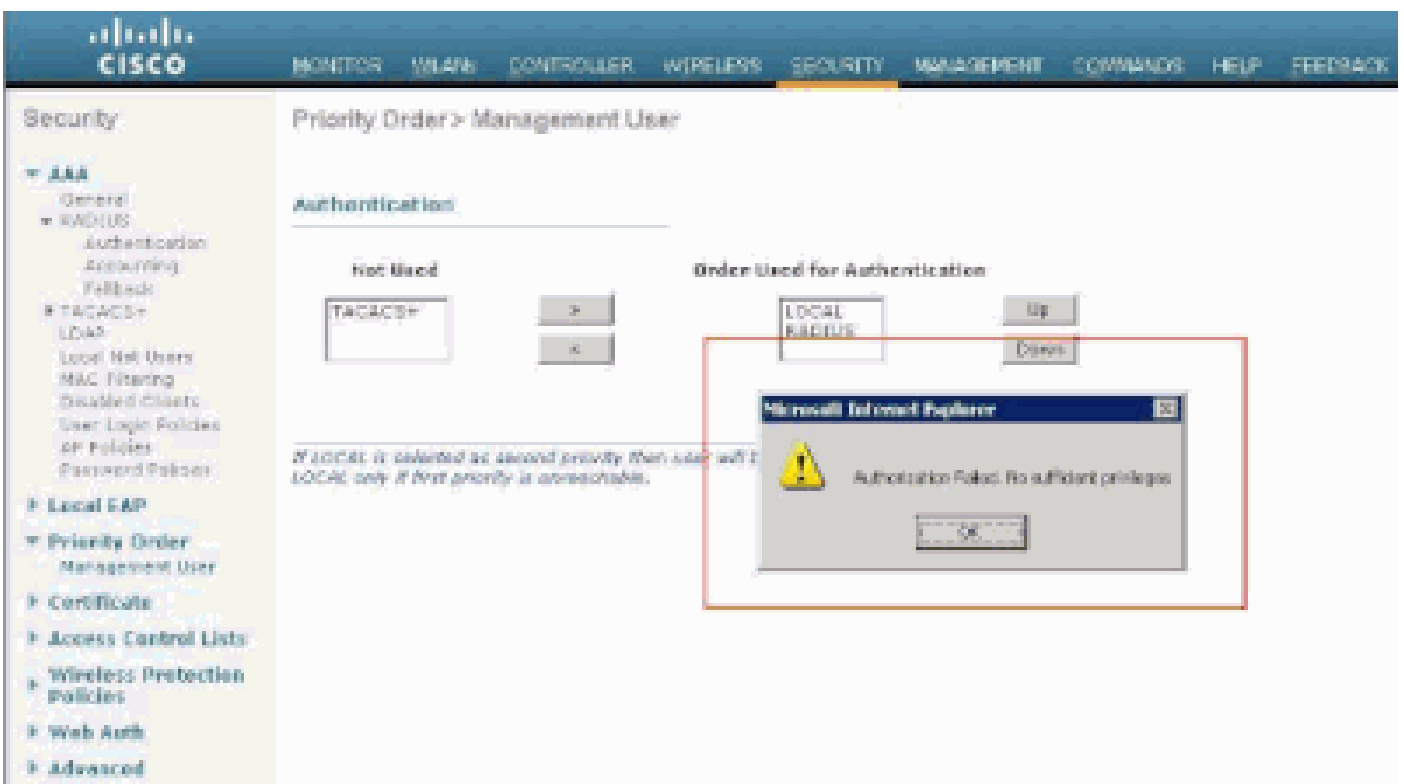
Een gebruiker met lees-schrijftoegang die in ACS wordt geplaatst heeft verscheidene

configureerbare voorrechten in WLC. Een lees-schrijfgebruiker heeft bijvoorbeeld het recht om een nieuw WLAN te maken onder de WLAN-pagina van de WLC. Dit venster toont een voorbeeld.



Configureerbare rechten in de WLC

Wanneer een gebruiker met alleen-lezen bevoegdheden de configuratie op de controller probeert te wijzigen, ziet de gebruiker dit bericht.



Kan controller niet wijzigen met alleen-lezen toegang

Deze toegangsbeperkingen kunnen ook worden geverifieerd via de CLI van de WLC. Deze output toont een voorbeeld.

```
<#root>
```

```
(Cisco Controller) >
```

```
?
```

```
debug          Manages system debug options.
help           Help
linktest       Perform a link test to a specified MAC address.
logout        Exit this session. Any unsaved changes are lost.
```

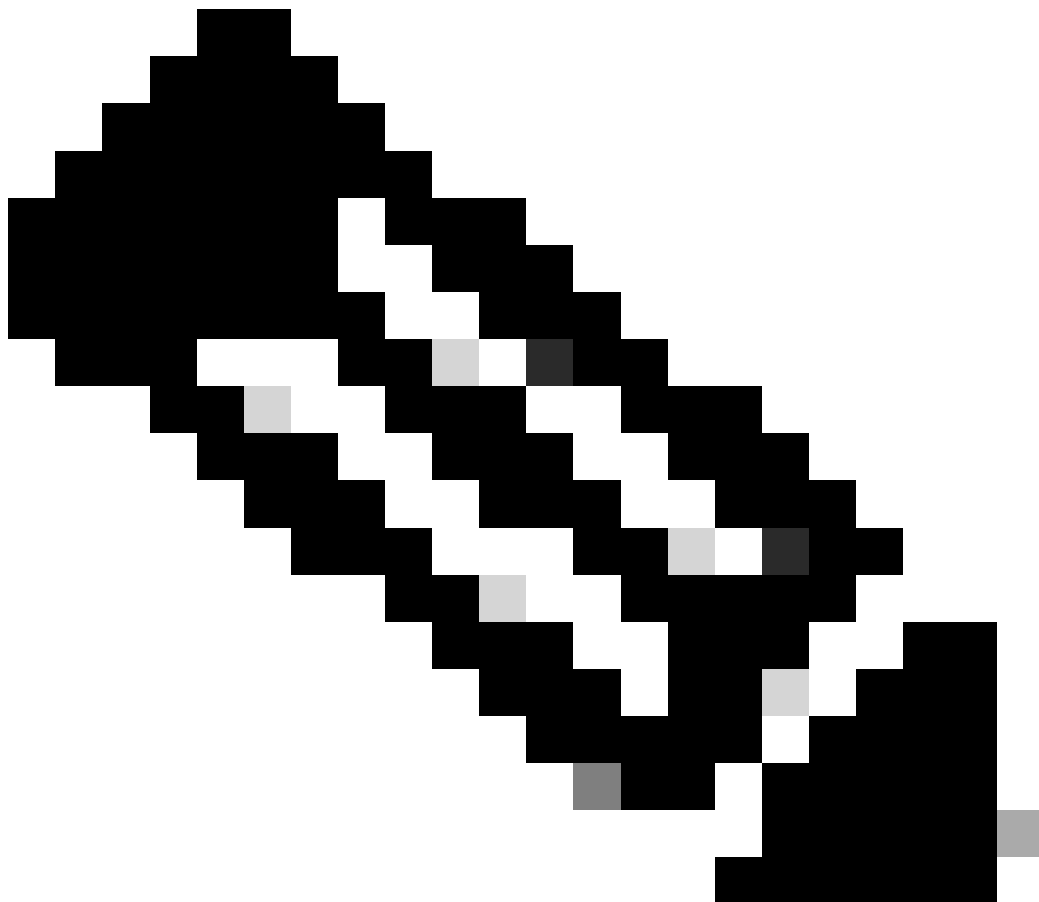
show            Display switch options and settings.

(Cisco Controller) >config

Incorrect usage. Use the '?' or <TAB> key to list commands.

Zoals deze voorbeelduitvoer laat zien? Bij de controller CLI wordt een lijst met opdrachten weergegeven die beschikbaar zijn voor de huidige gebruiker. Merk ook op dat het **config** commando niet beschikbaar is in deze voorbeelduitvoer. Dit illustreert dat een alleen-lezen gebruiker niet het voorrecht heeft om enige configuraties op de WLC te doen. Een lees-schrijfgebruiker heeft echter wel de rechten om configuraties op de controller uit te voeren (zowel GUI- als CLI-modus).

---



**Opmerking:** zelfs nadat u een WLC-gebruiker door de RADIUS-server hebt geauthenticeerd, terwijl u van pagina naar pagina bladert, wordt de client elke keer nog steeds volledig geverifieerd door de HTTP[S]-server. De enige reden waarom u niet wordt

---

---

gevraagd voor verificatie op elke pagina is dat uw browser caches en replay uw referenties.

---

## Problemen oplossen

Er zijn bepaalde omstandigheden wanneer een controller beheers gebruikers via de ACS authenticceert, de authenticatie eindigt met succes (toegang-accepteren), en u ziet geen autorisatiefout op de controller. *Maar de gebruiker wordt opnieuw gevraagd voor authenticatie.*

In zulke gevallen kunt u niet interpreteren wat er mis is en waarom de gebruiker niet kan inloggen in de WLC met alleen de **debug aaa events enable** opdracht. In plaats daarvan geeft de controller een andere vraag voor verificatie weer.

Een mogelijke reden hiervoor is dat de ACS niet is geconfigureerd om de Service-Type attributen voor die bepaalde gebruiker of groep te verzenden, ook al zijn de gebruikersnaam en het wachtwoord correct ingesteld op de ACS.

De output van de **debug aaa events enable** opdracht geeft niet aan dat een gebruiker niet de vereiste kenmerken heeft (bijvoorbeeld het kenmerk Service-Type), ook al wordt een **toegangsbewijs** teruggestuurd vanaf de AAA-server. Deze voorbeeld **debug aaa events enable** opdrachtoutput toont een voorbeeld.

```
<#root>
```

```
(Cisco Controller) >
```

```
debug aaa events enable
```

```
Mon Aug 13 20:14:33 2011: AuthenticationRequest: 0xa449a8c
```

```
Mon Aug 13 20:14:33 2011: Callback.....0x8250c40
```

```
Mon Aug 13 20:14:33 2011: protocolType.....0x00020001
```

```
Mon Aug 13 20:14:33 2011: proxyState.....1A:00:00:00:00-00:00
```

```
Mon Aug 13 20:14:33 2011: Packet contains 5 AVPs (not shown)
```

```
Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Successful transmission of
```

Authentication Packet (id 8) to 172.16.1.1:1812, proxy state  
1a:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: \*\*\*\*Enter processIncomingMessages: response code=2

Mon Aug 13 20:14:33 2011: \*\*\*\*Enter processRadiusResponse: response code=2

Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Access-Accept  
received from RADIUS server 172.16.1.1 for mobile 1a:00:00:00:00:00 receiveId = 0

Mon Aug 13 20:14:33 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:14:33 2011: structureSize.....28

Mon Aug 13 20:14:33 2011: resultCode.....0

Mon Aug 13 20:14:33 2011: protocolUsed.....0x00000001

Mon Aug 13 20:14:33 2011: proxyState.....1A:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: Packet contains 0 AVPs:

In dit eerste voorbeeld **debug aaa events enable** opdrachtoutput, ziet u dat Access-Accept met succes wordt ontvangen van de RADIUS-server maar dat het Service-Type-kenmerk niet wordt doorgegeven aan de WLC. Dit komt doordat de specifieke gebruiker niet met deze eigenschap op ACS is geconfigureerd.

Cisco Secure ACS moet worden geconfigureerd om het servicetype-kenmerk na gebruikersverificatie te herstellen. De waarde van het kenmerk Service-Type moet worden ingesteld op **Administratief** of **NAS-Prompt** op basis van de gebruikersrechten.

Dit tweede voorbeeld toont opnieuw de **debug aaa events enable**opdrachtoutput. Dit keer is het kenmerk Service-Type ingesteld op **Administratief** op ACS.

<#root>

*(Cisco Controller)>*

**debug aaa events enable**

Mon Aug 13 20:17:02 2011: AuthenticationRequest: 0xa449f1c  
Mon Aug 13 20:17:02 2011: Callback.....0x8250c40  
Mon Aug 13 20:17:02 2011: protocolType.....0x00020001  
Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00-00:00  
Mon Aug 13 20:17:02 2011: Packet contains 5 AVPs (not shown)  
Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Successful transmission of  
Authentication Packet (id 11) to 172.16.1.1:1812, proxy state  
1d:00:00:00:00-00:00  
Mon Aug 13 20:17:02 2011: \*\*\*\*Enter processIncomingMessages: response code=2  
Mon Aug 13 20:17:02 2011: \*\*\*\*Enter processRadiusResponse: response code=2

Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Access-Accept received  
from RADIUS server 172.16.1.1 for mobile 1d:00:00:00:00:00 receiveId = 0

Mon Aug 13 20:17:02 2011: AuthorizationResponse: 0x9802520  
Mon Aug 13 20:17:02 2011: structureSize.....100  
Mon Aug 13 20:17:02 2011: resultCode.....0  
Mon Aug 13 20:17:02 2011: protocolUsed.....0x00000001  
Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00-00:00  
Mon Aug 13 20:17:02 2011: Packet contains 2 AVPs:

Mon Aug 13 20:17:02 2011: AVP[01] Service-Type.....0x00000006 (6) (4 bytes)

Mon Aug 13 20:17:02 2011: AVP[02] Class.....  
CISCOACS:000d1b9f/ac100128/acserver (36 bytes)

U kunt in deze vorige voorbeeldoutput zien dat het Service-Type attribuut op WLC wordt overgegaan.

## Gerelateerde informatie

- [Draadloze LAN-controller configureren - Configuratiehandleiding](#)
- [VLAN's configureren op draadloze LAN-controllers](#)
- [Een RADIUS-server en WLC voor dynamische VLAN-toewijzing configureren](#)
- [Wireless LAN Controller en Lightweight Access Point Basic configureren](#)
- [De AP-groep VLAN's configureren met draadloze LAN-controllers](#)
- [Cisco Technical Support en downloads](#)

## 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.