Management Access for Aire OS WLC via Microsoft NPS

Inhoud

Inleiding

Dit document beschrijft hoe u beheerstoegang voor AireOS WLC GUI en CLI kunt configureren via de Microsoft Network Policy Server (NPS).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van draadloze beveiligingsoplossingen
- AAA en RADIUS-concepten
- Basiskennis van Microsoft Server 2012
- Installatie van Microsoft NPS en Active Directory (AD)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardwareonderdelen.

- AireOS-controller (5520) op 8.8.120.0
- Microsoft Server 2012

> Opmerking: Dit document is bedoeld om de lezers een voorbeeld te geven van de configuratie die op een Microsoft-server vereist is voor toegang tot het WLC-beheer. De Microsoft Windows serverconfiguratie die in dit document wordt gepresenteerd, is getest in het laboratorium en bleek te werken zoals verwacht. Als u problemen hebt met de configuratie, neemt u contact op met Microsoft voor ondersteuning. Het Cisco Technical Assistance Center (TAC) ondersteunt de Microsoft Windows-serverconfiguratie niet. U vindt

de installatie- en configuratiehandleidingen van Microsoft Windows 2012 in Microsoft Tech Net.

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.

Achtergrondinformatie

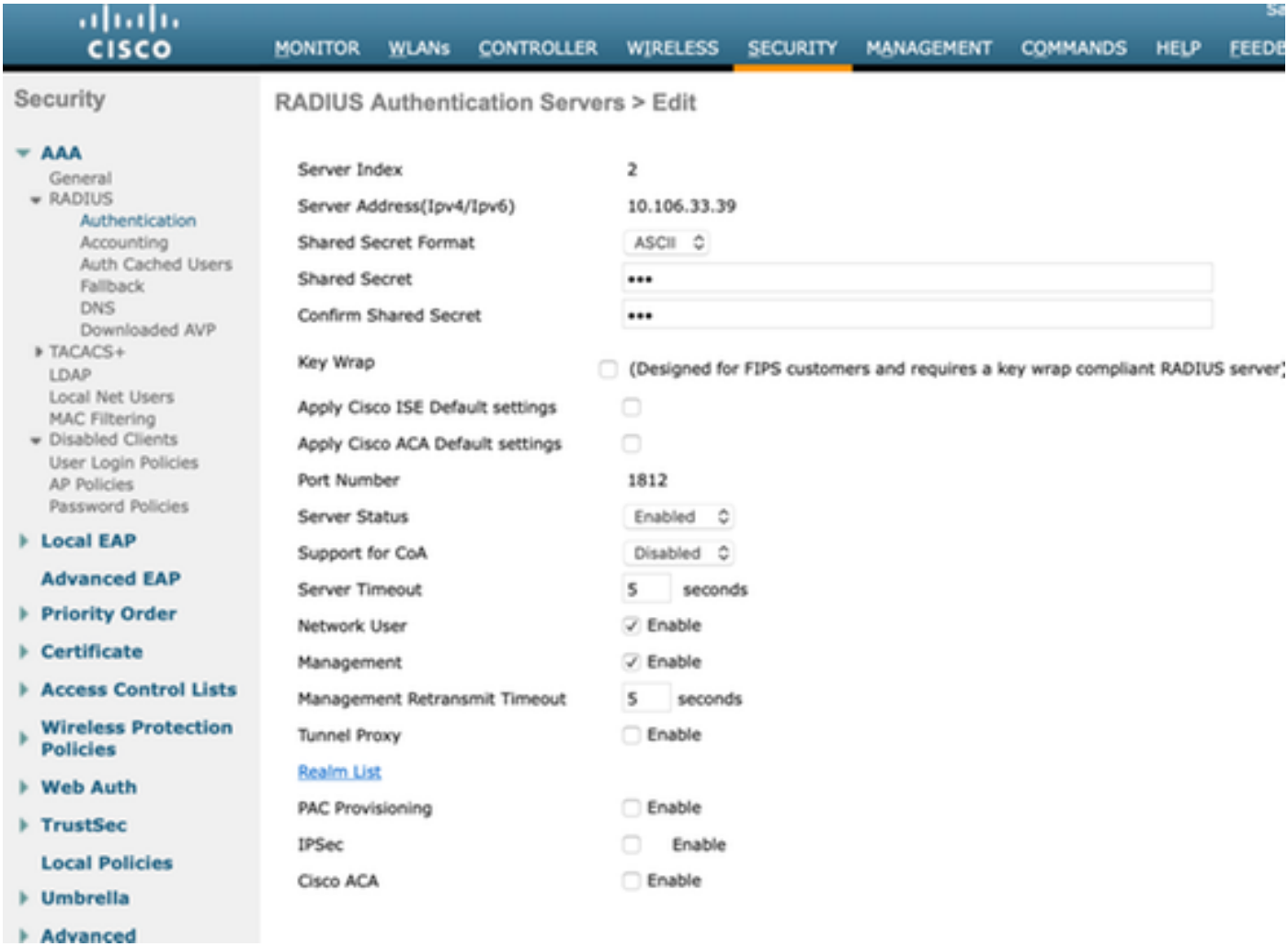
Wanneer de WLC CLI/GUI wordt benaderd, wordt de gebruiker gevraagd om de inloggegevens in te voeren. De geloofsbrieven kunnen tegen of een lokale gegevensbestand of een externe AAA server worden geverifieerd. In dit document wordt Microsoft NPS gebruikt als externe verificatieserver.

Configuraties

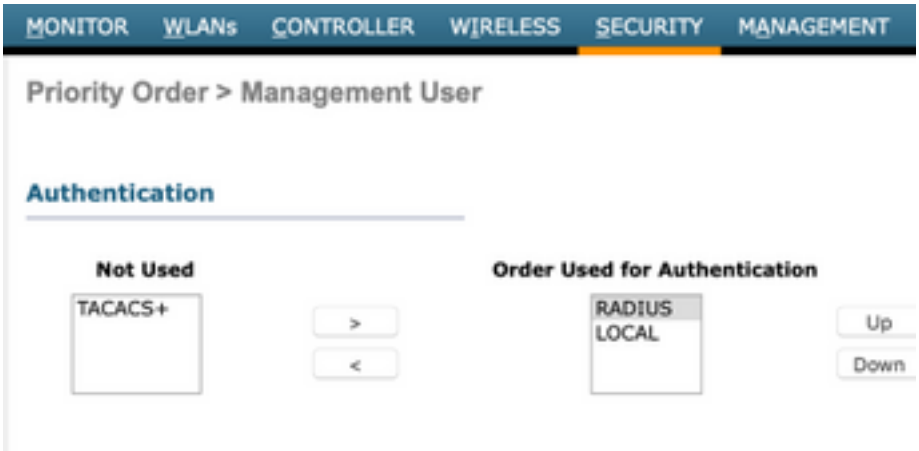
In dit voorbeeld worden twee gebruikers ingesteld op AAA (NPS), d.w.z. **loginuser** en **adminuser**. **loginuser** heeft alleen de read-only toegang terwijl **adminuser** volledige toegang krijgt.

WLC-configuratie

Stap 1. Voeg de RADIUS-server toe aan de controller. Navigeer naar **Security > RADIUS > Verificatie**. Klik op **New** om de server toe te voegen. Zorg ervoor dat de beheeroptie is ingeschakeld zodat deze server kan worden gebruikt voor beheertoegang, zoals in deze afbeelding wordt weergegeven.



Stap 2. Navigeer naar **security > prioriteitsopdracht > beheergebruiker**. Zorg ervoor dat de RADIUS is geselecteerd als een van de authenticatietypen.



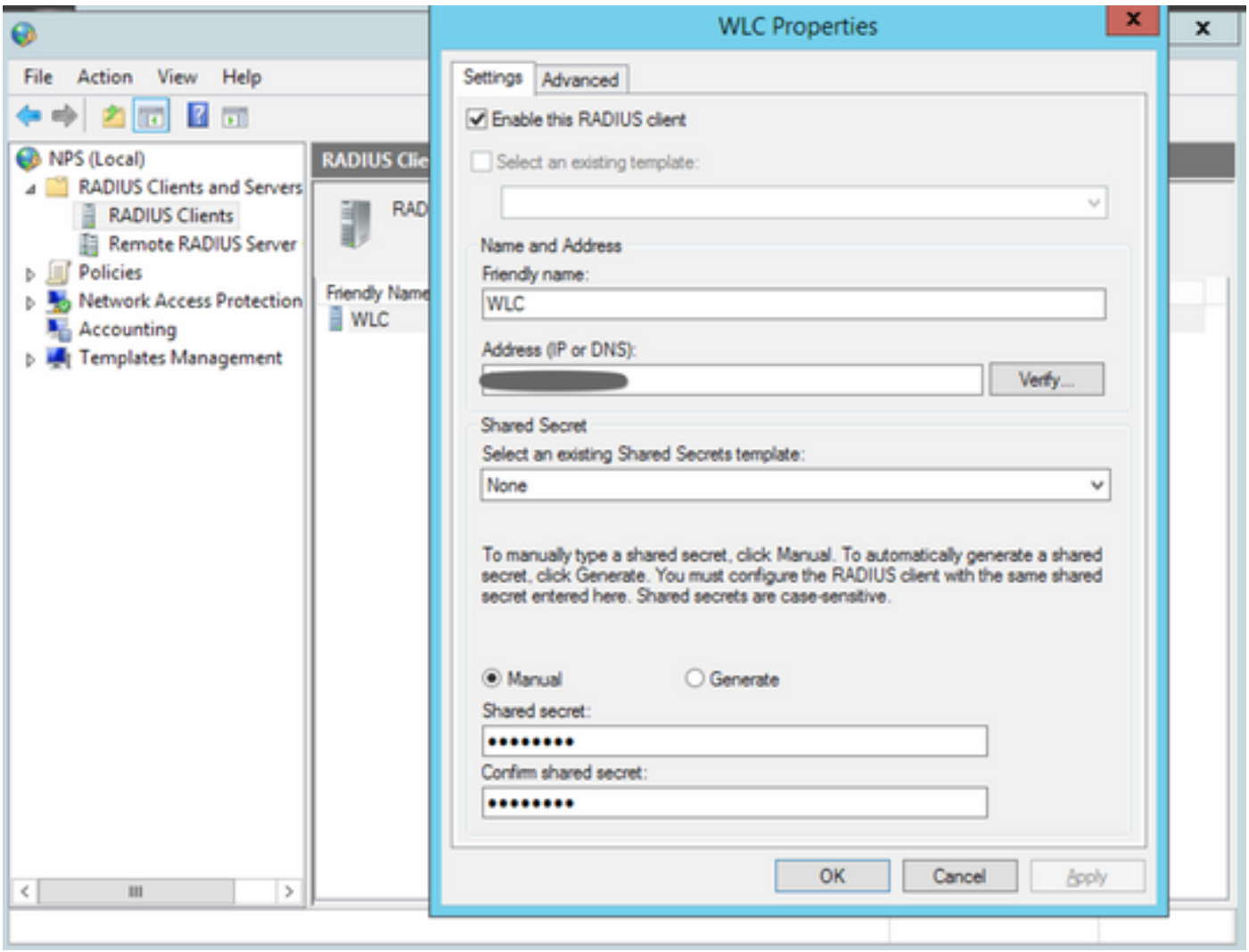
> Opmerking: Als RADIUS is geselecteerd als eerste prioriteit in de authenticatievolgorde, worden lokale geloofsbrieven alleen gebruikt voor authenticatie als de RADIUS-server onbereikbaar is. Als RADIUS als tweede prioriteit wordt geselecteerd, worden de RADIUS-referenties eerst geverifieerd via de lokale database en vervolgens gecontroleerd via de geconfigureerde RADIUS-servers.

Microsoft NPS-configuratie

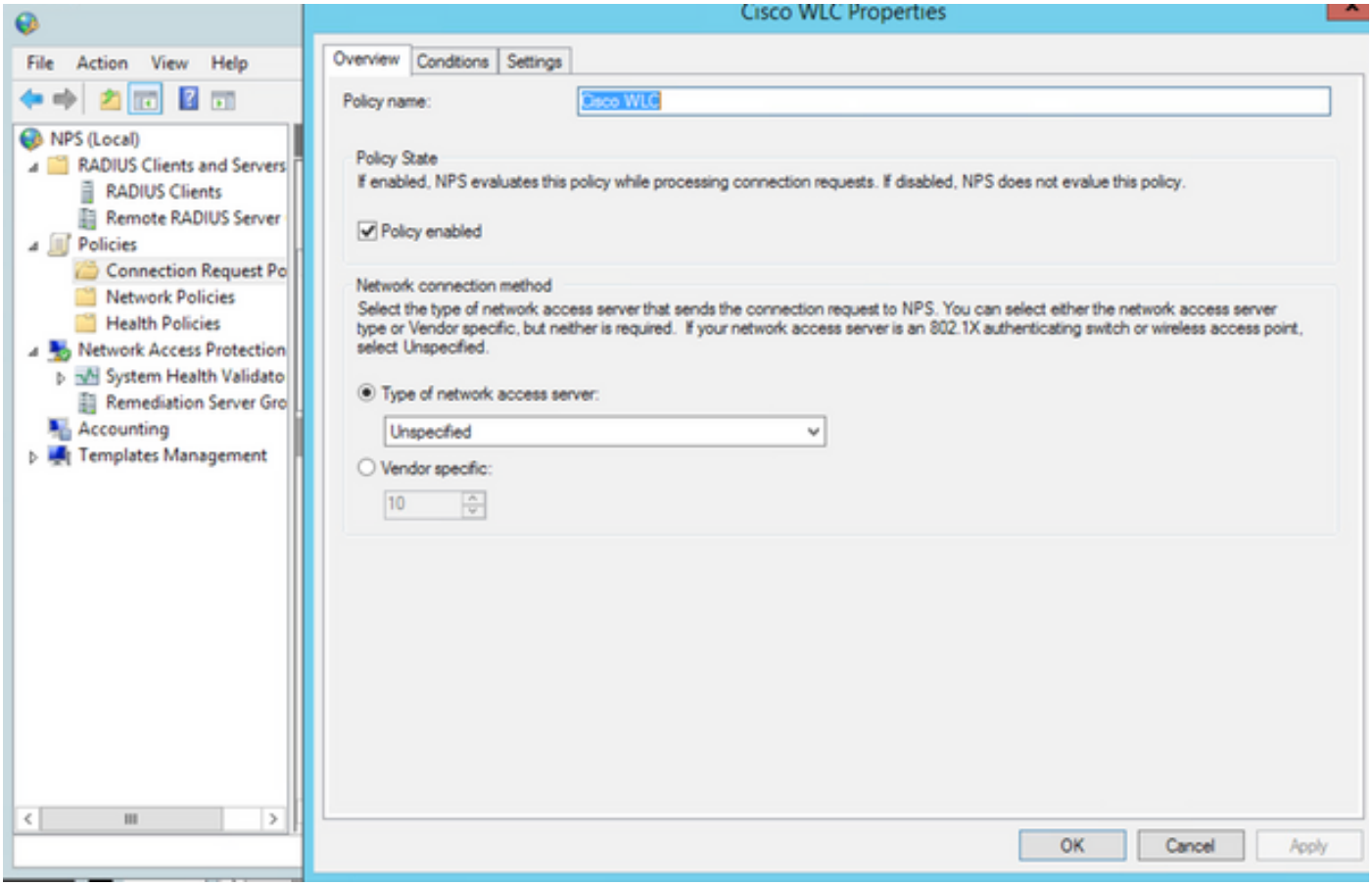
Stap 1. Open de Microsoft NPS-server. Klik met de rechtermuisknop op **RADIUS-clients**. Klik op

New om de WLC als de RADIUS-client toe te voegen.

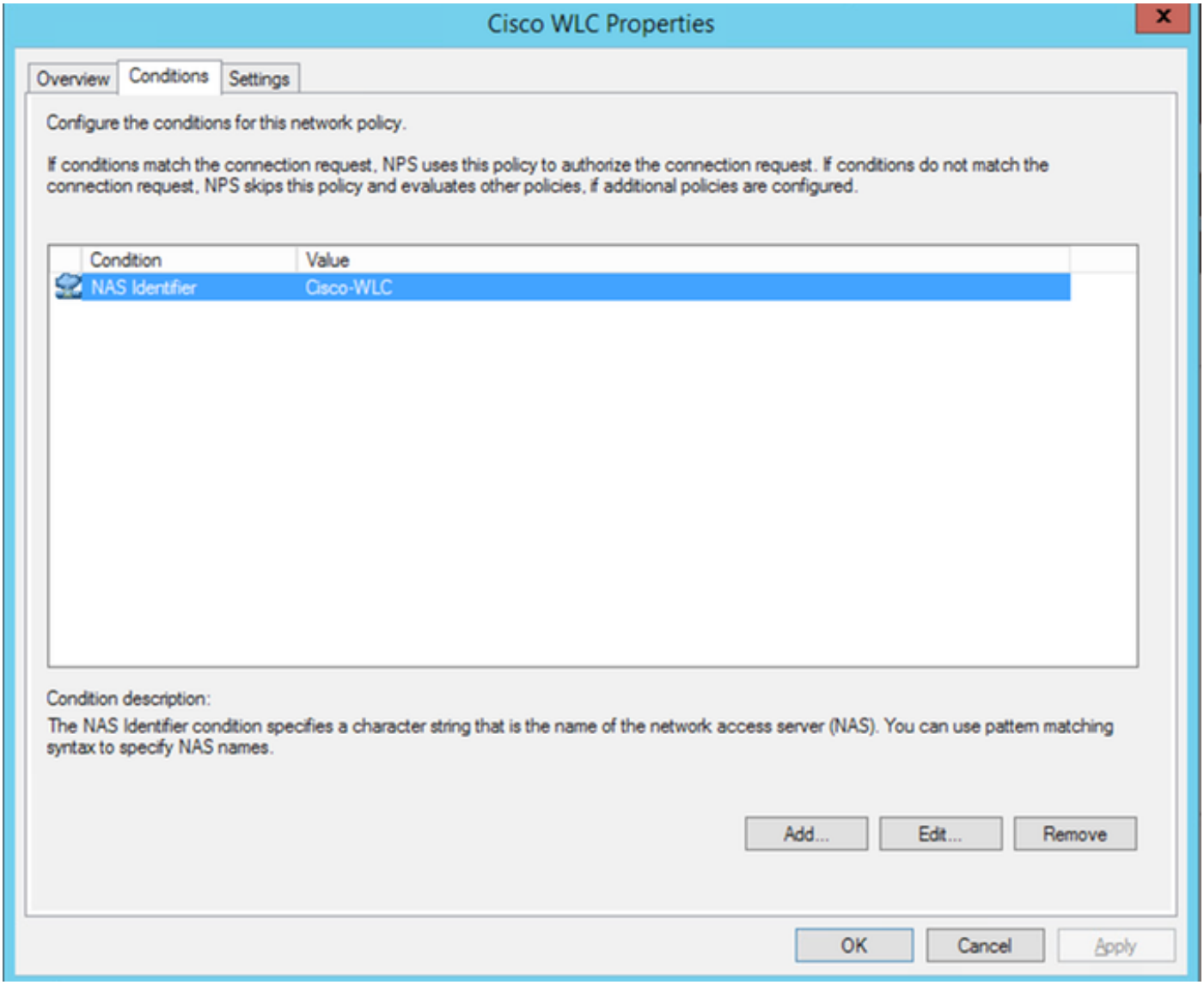
Voer de gewenste gegevens in. Zorg ervoor dat het gedeelde geheim hetzelfde is als dat welke is ingesteld op de controller terwijl de RADIUS-server wordt toegevoegd.



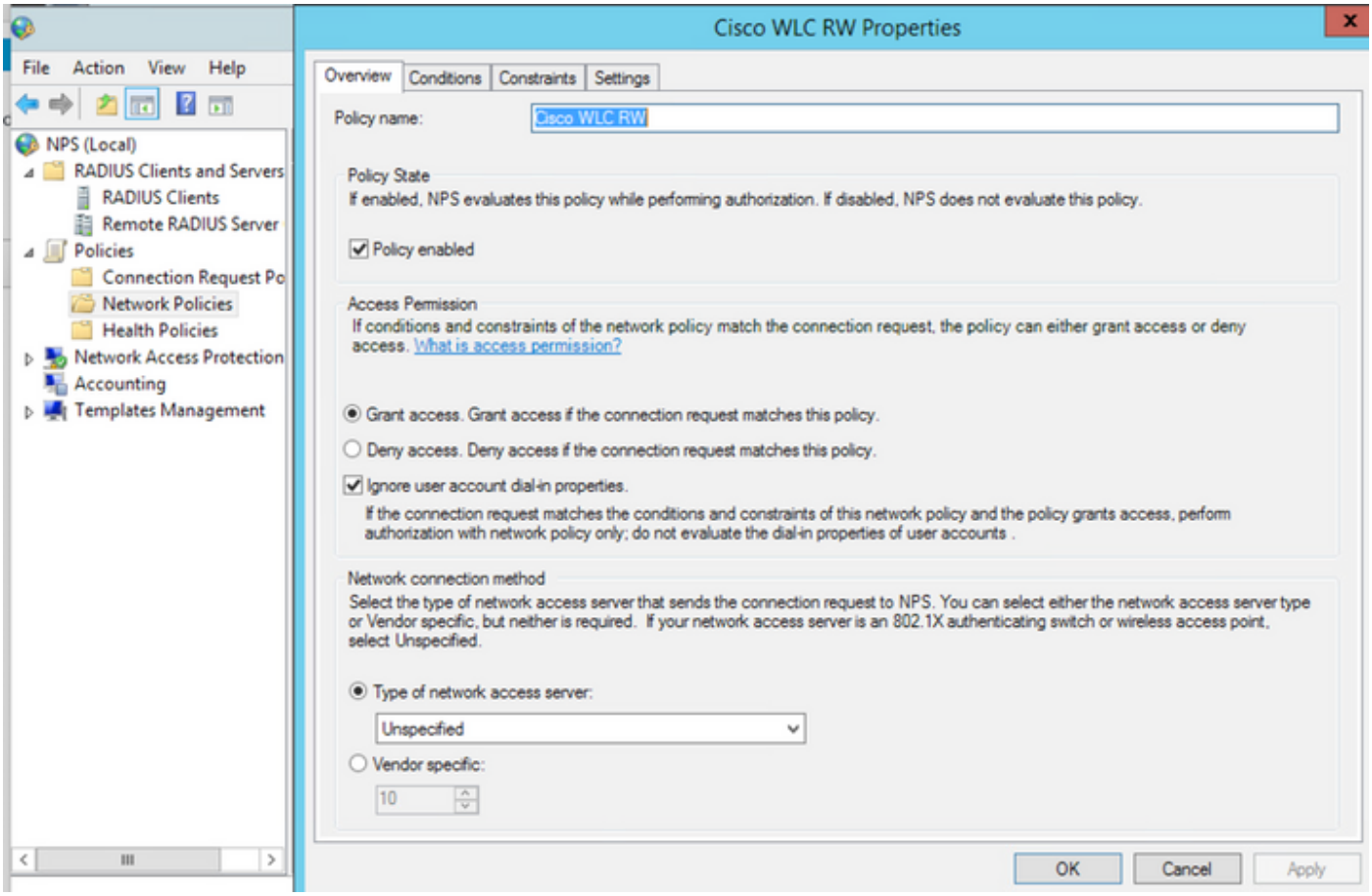
Stap 2. Navigeer naar **beleid > Aanvraagbeleid**. Klik met de rechtermuisknop om een nieuw beleid toe te voegen, zoals in de afbeelding.



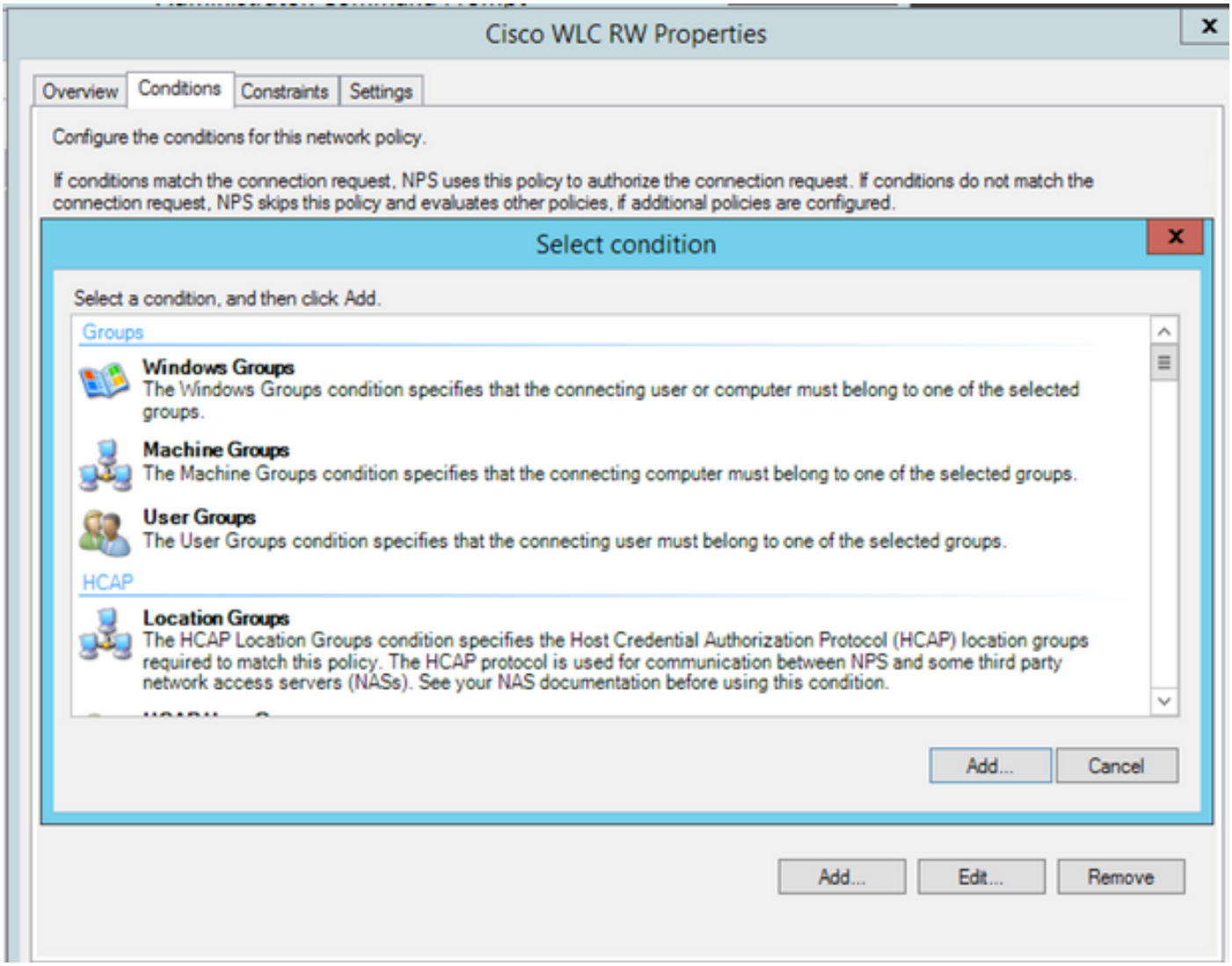
Stap 3. Onder het tabblad **Voorwaarden** selecteert u **NAS-identificator** als de nieuwe voorwaarde. Voer desgevraagd de hostnaam van de controller in als de waarde, zoals in de afbeelding.



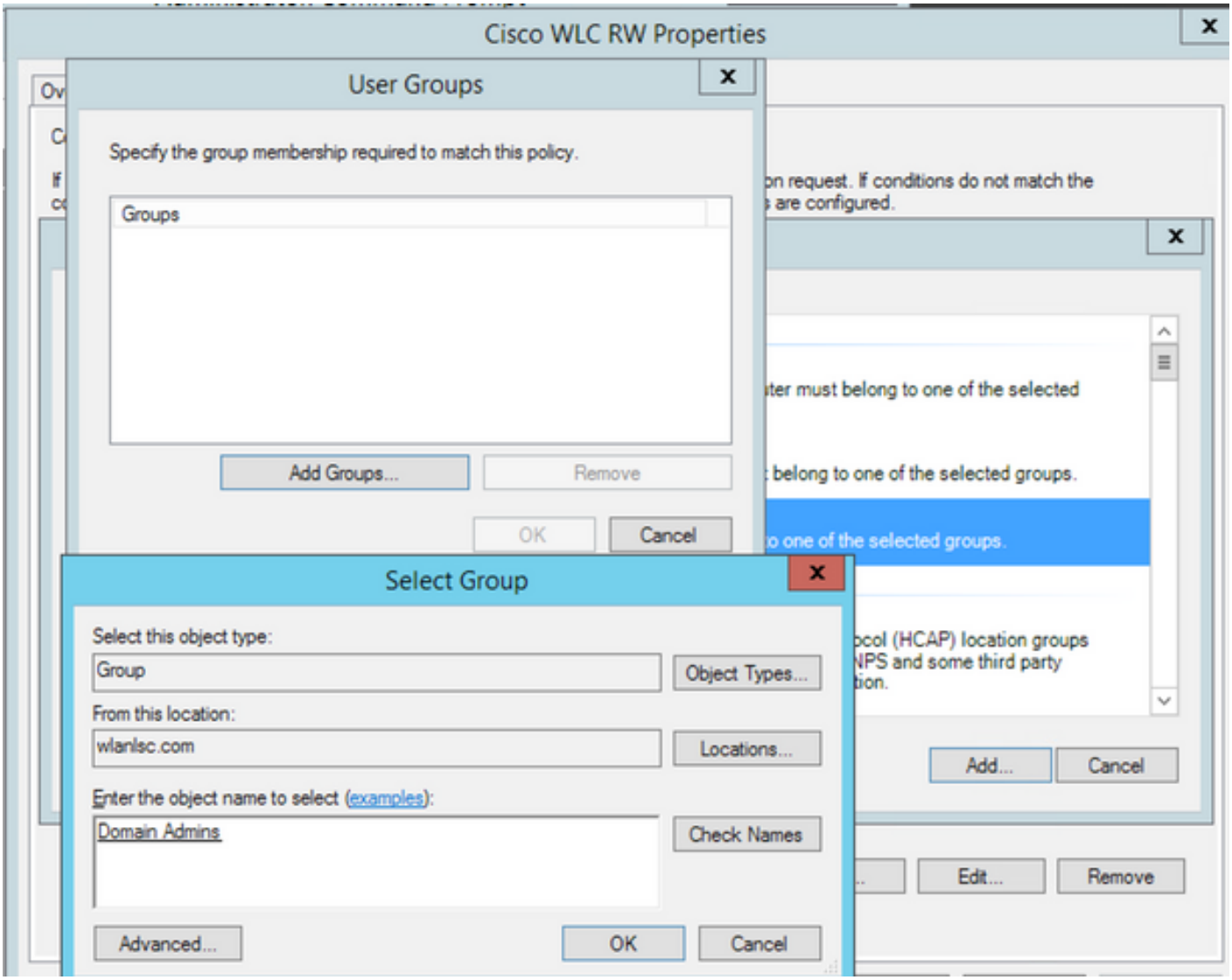
Stap 4. Navigeer naar **beleid > Netwerkbeleid**. Klik met de rechtermuisknop om een nieuw beleid toe te voegen. In dit voorbeeld wordt het beleid aangeduid als **Cisco WLC RW-**beleid wat impliceert dat het beleid wordt gebruikt om volledige (lezen-schrijven) toegang te bieden. Zorg ervoor dat het beleid is geconfigureerd zoals hier wordt getoond.



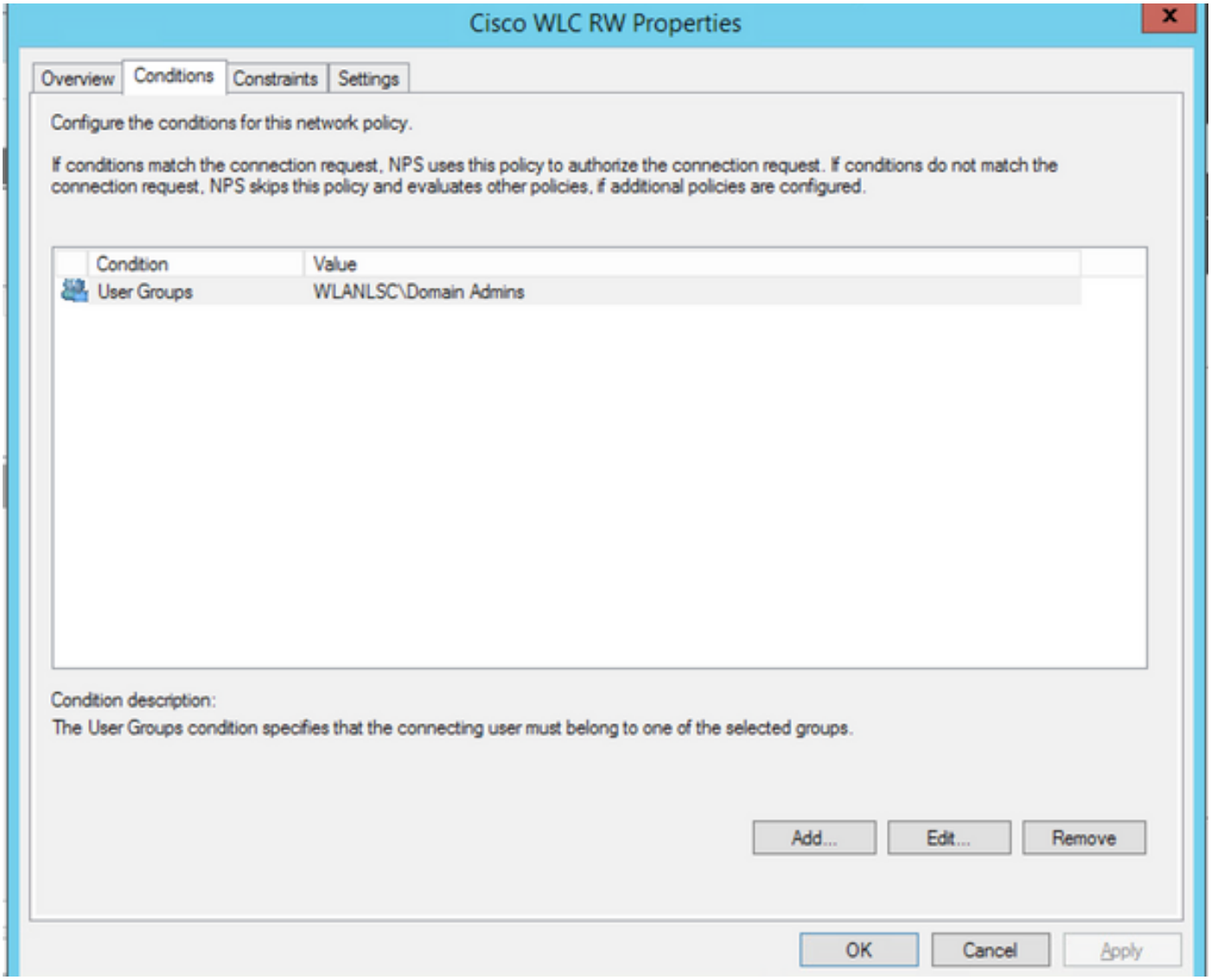
Stap 5. Onder het tabblad **Voorwaarden** klikt u op **Toevoegen**. Selecteer de **gebruikersgroepen** en klik op **Toevoegen**, zoals in de afbeelding.



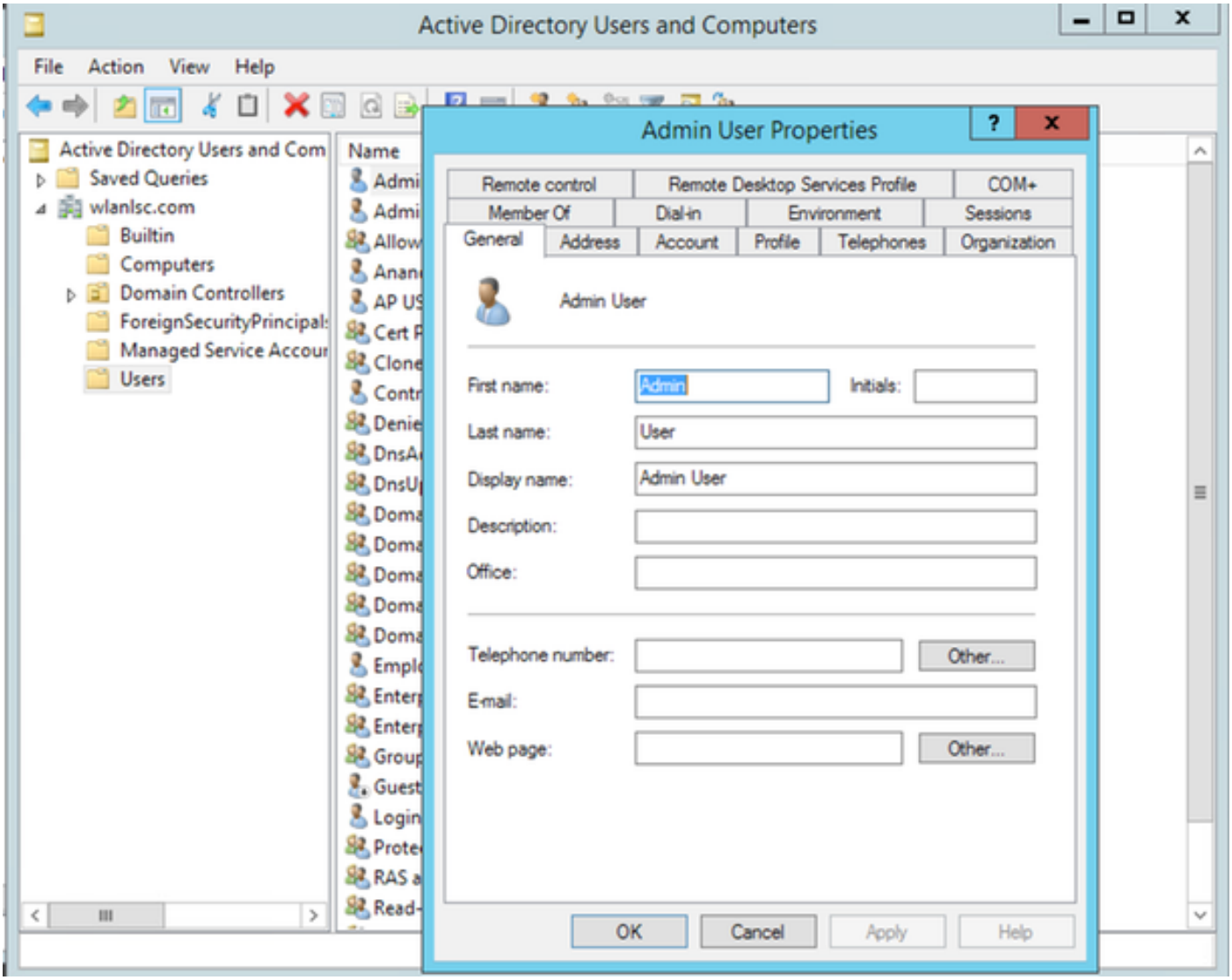
Stap 6. Klik op **Add Group** in het dialoogvenster dat nu wordt weergegeven. In het venster **Select Group** die nu wordt weergegeven, selecteert u het gewenste **doeltype** en de gewenste **locatie**. Voer de gewenste objectnaam in, zoals in de afbeelding.

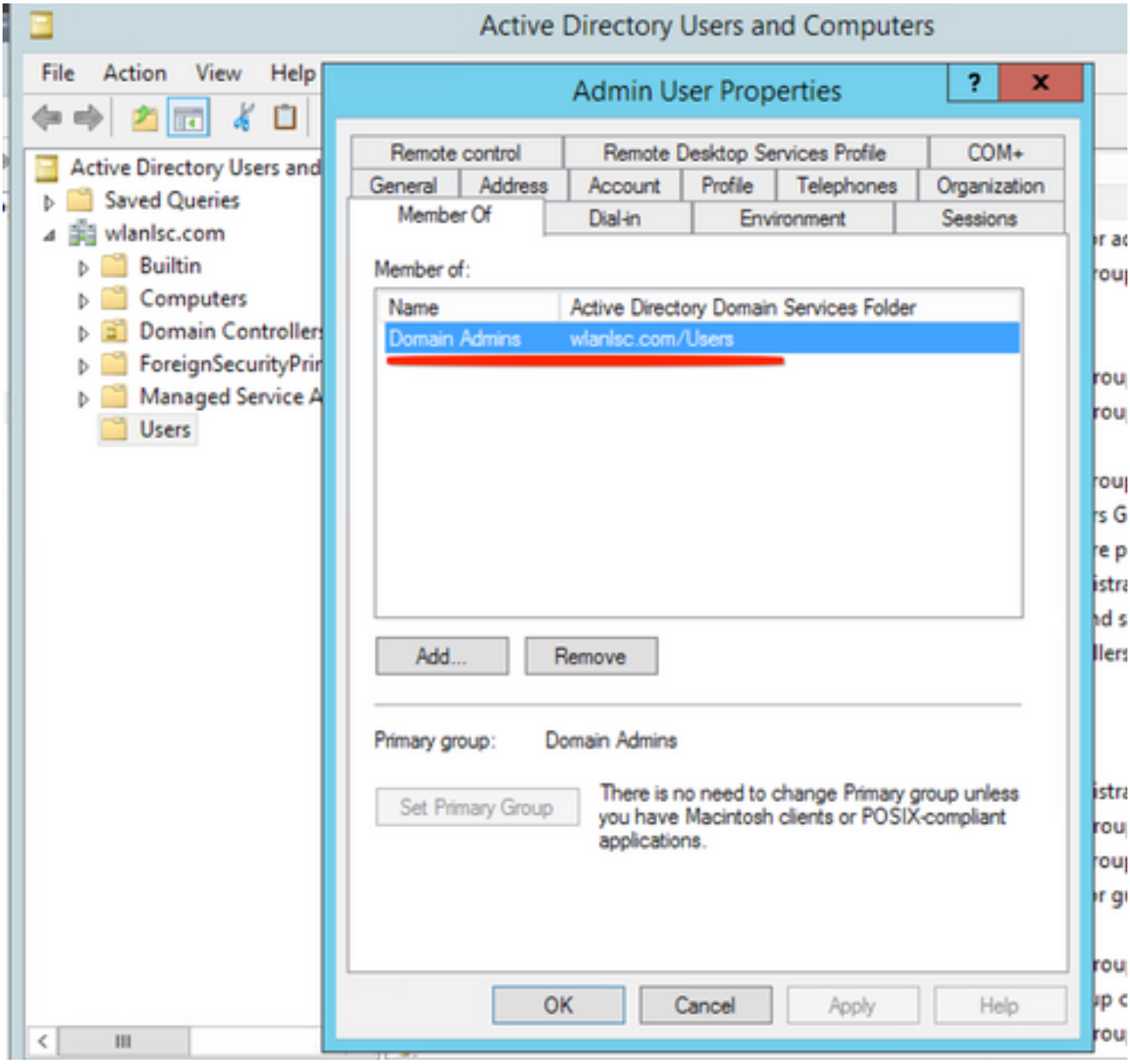


De conditie, indien correct toegevoegd, moet eruit zien zoals hier getoond wordt.

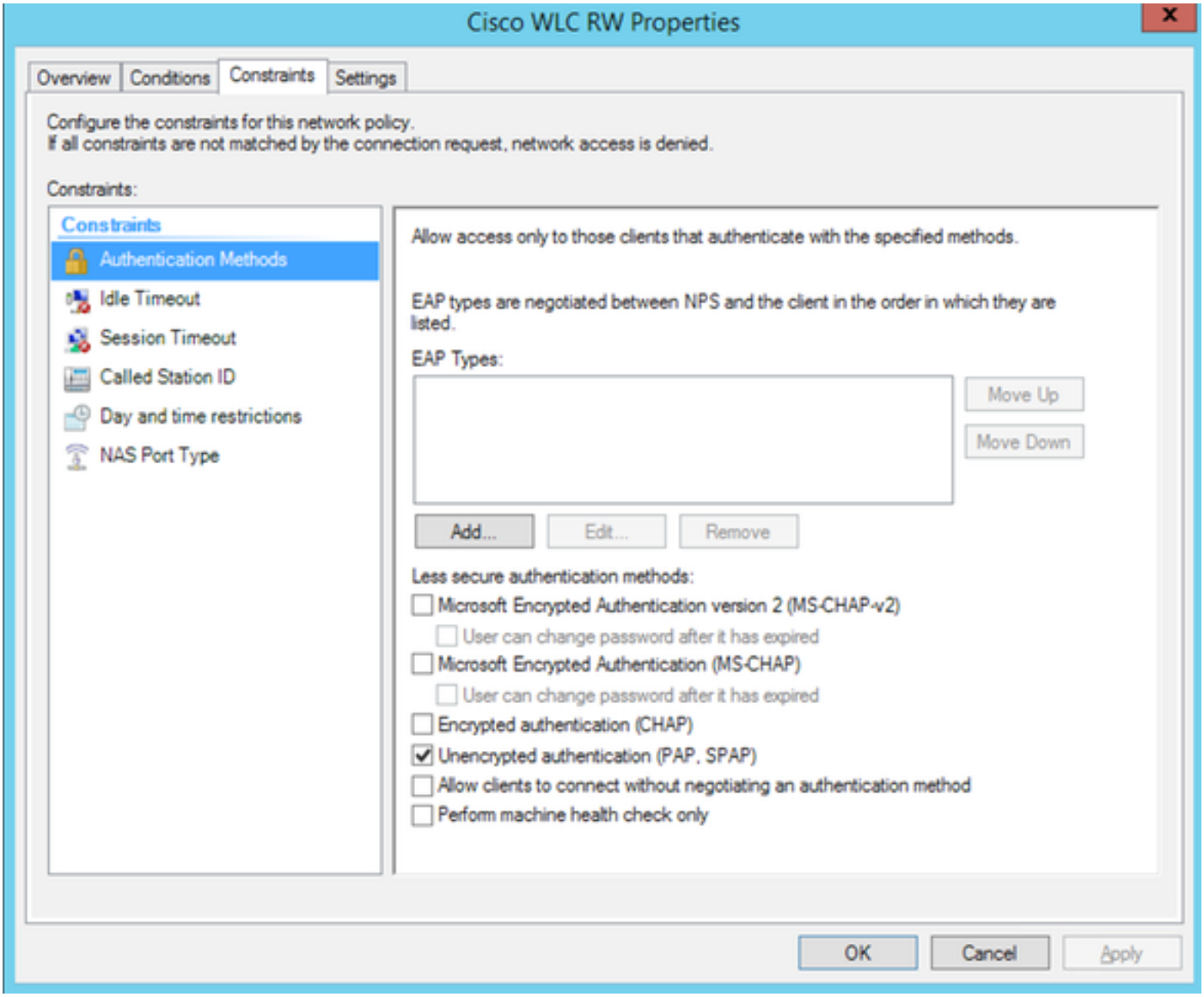


Opmerking: Wilt u te weten komen waar de locatie en de objectnaam zijn, dan opent u de actieve directory en zoekt u de gewenste gebruikersnaam. In dit voorbeeld bestaat **Domain Admins** uit gebruikers die volledige toegang krijgen. **beheerder** maakt deel uit van deze objectnaam.

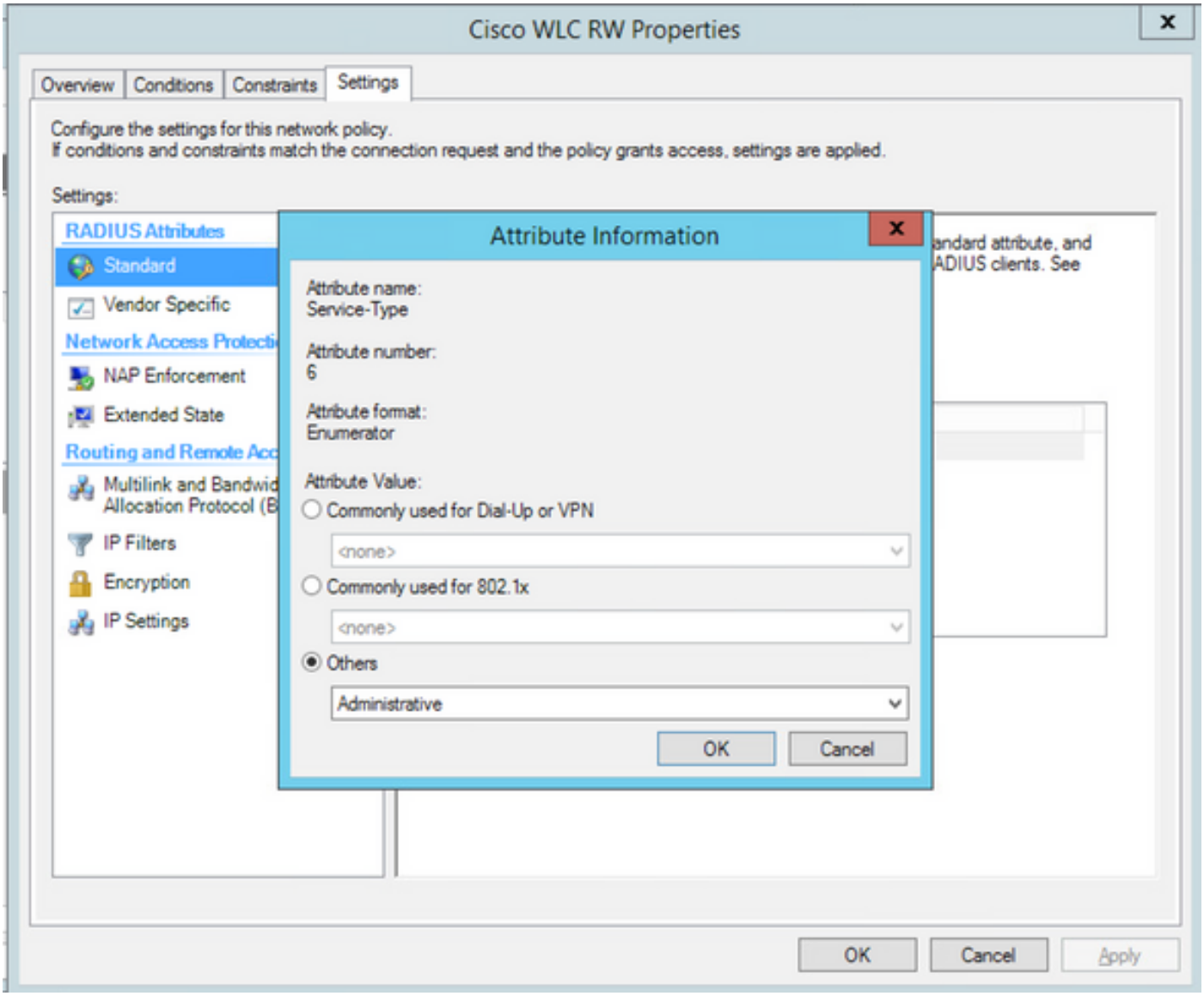

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
wlanlsc.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name
Admin User Properties
Remote control
Remote Desktop Services Profile
COM+
Member Of
Dial-in
Environment
Sessions
General
Address
Account
Profile
Telephones
Organization
Admin User
First name:
Admin
Initials:
Last name:
User
Display name:
Admin User
Description:
Office:
Telephone number:
Other...
E-mail:
Web page:
Other...
OK
Cancel
Apply
Help



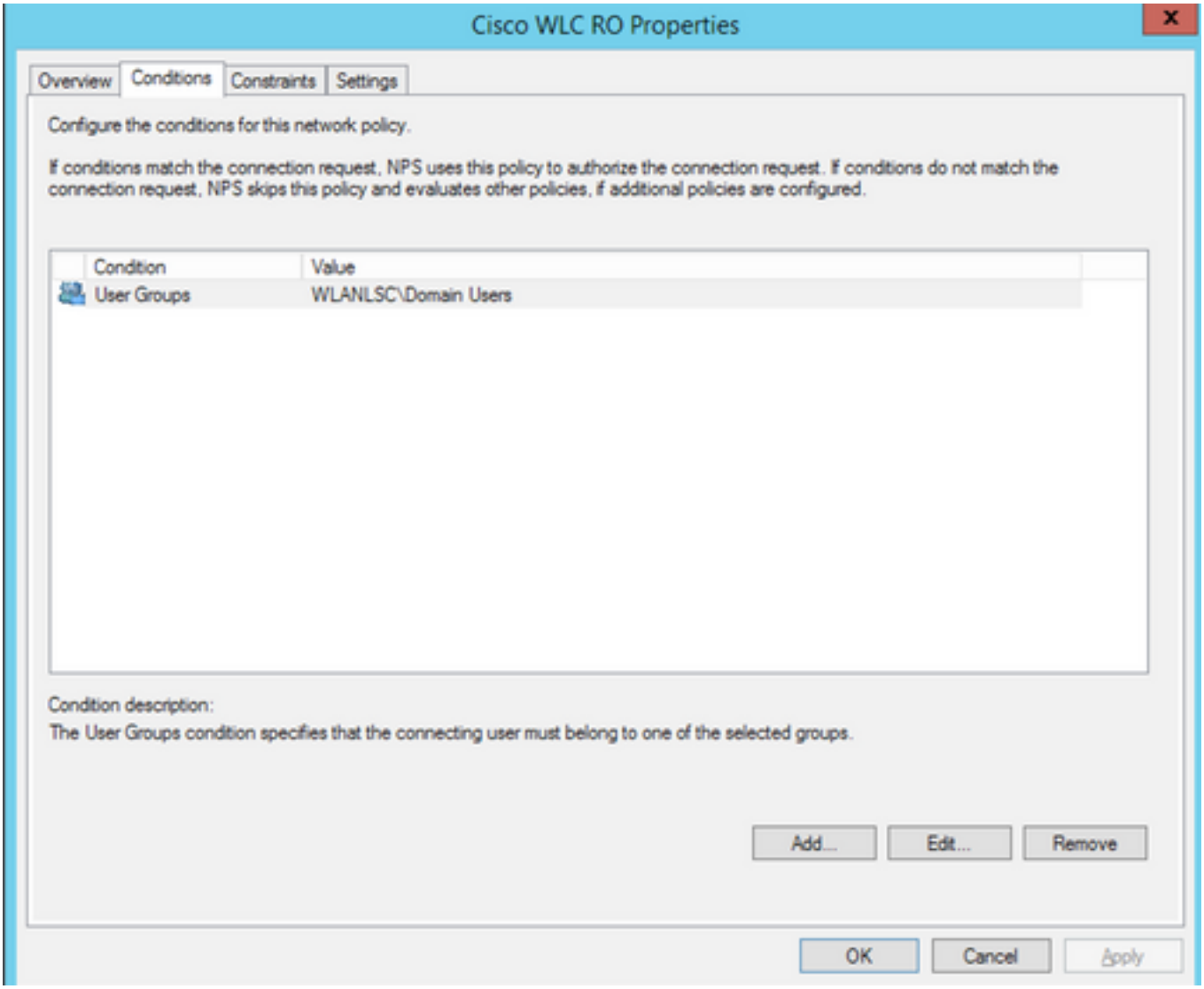
Stap 7. Onder het tabblad **Beperkingen**, navigeer naar **Verificatiemethoden** en controleer of alleen **niet-versleutelde verificatie** is ingeschakeld.

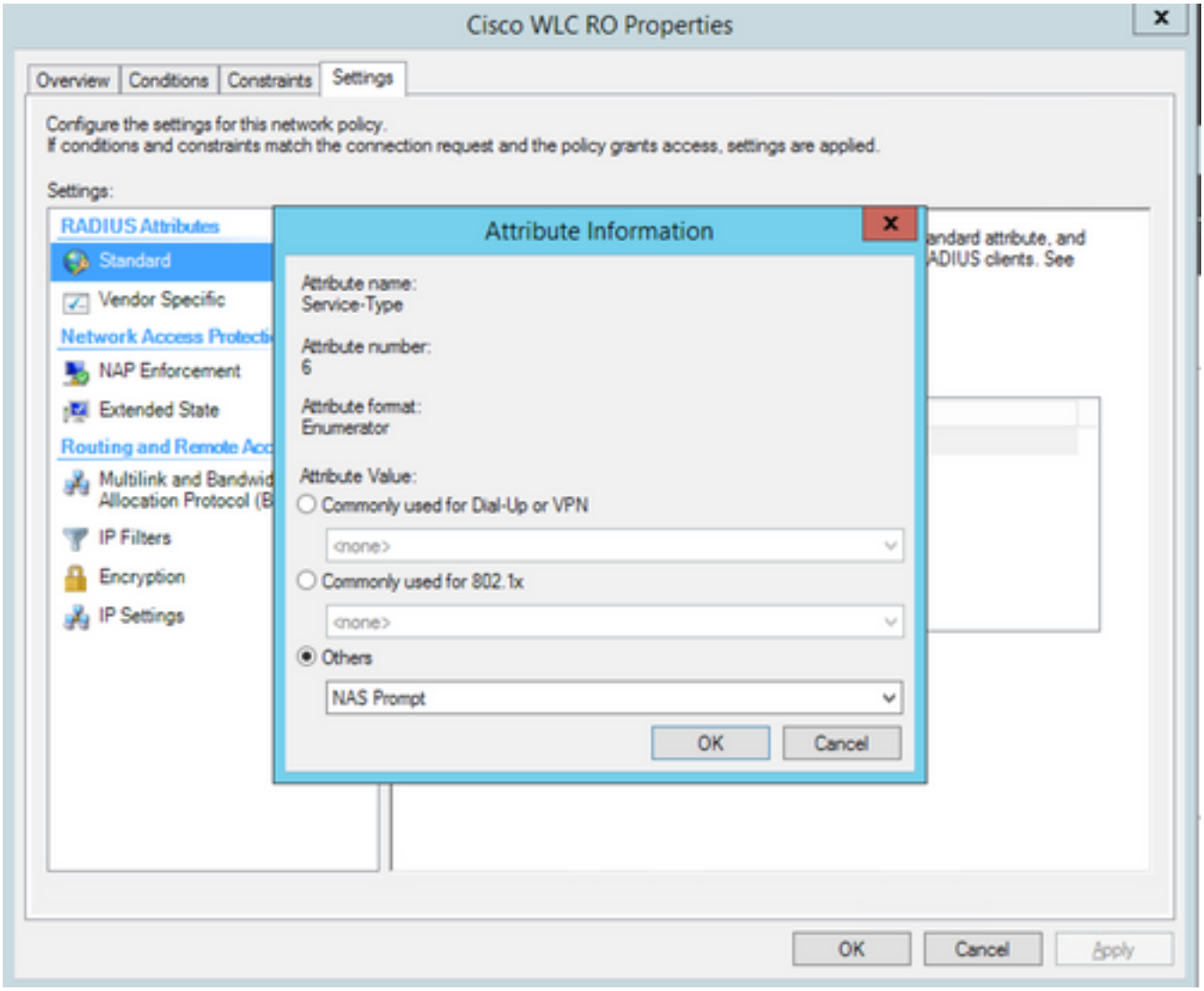


Stap 8. Onder het tabblad **Instellingen** navigeren naar **RADIUS-kenmerken > Standaard**. Klik op **Add** om een nieuwe eigenschap, **Service-type,** toe te voegen. Selecteer in het vervolgkeuzemenu de optie **Administratief** om volledige toegang te bieden tot de gebruikers die aan dit beleid zijn toegewezen. Klik op Toepassen om de wijzigingen op te slaan, zoals in de afbeelding wordt weergegeven.



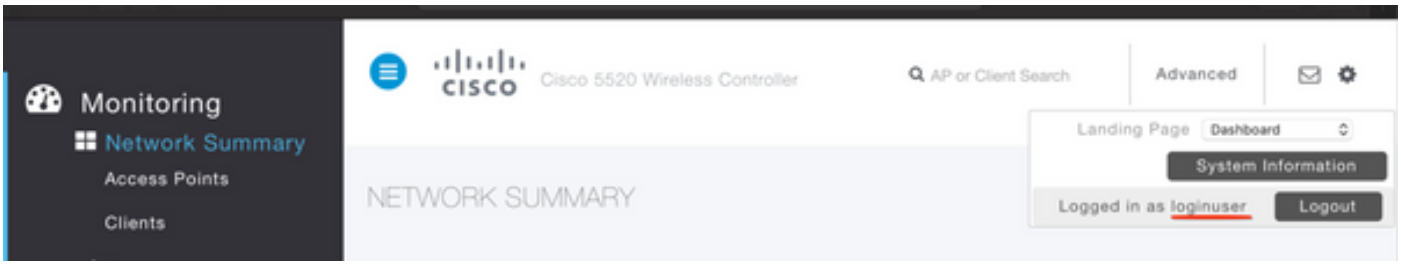
Opmerking: Als u alleen-lezen toegang wilt geven aan bepaalde gebruikers, selecteert u NAS-prompt in de vervolgkeuzelijst. In dit voorbeeld wordt een ander beleid met de naam **Cisco WLC RO** gecreëerd om alleen-lezen toegang te bieden aan gebruikers onder de objectnaam **Domain Gebruikers**.

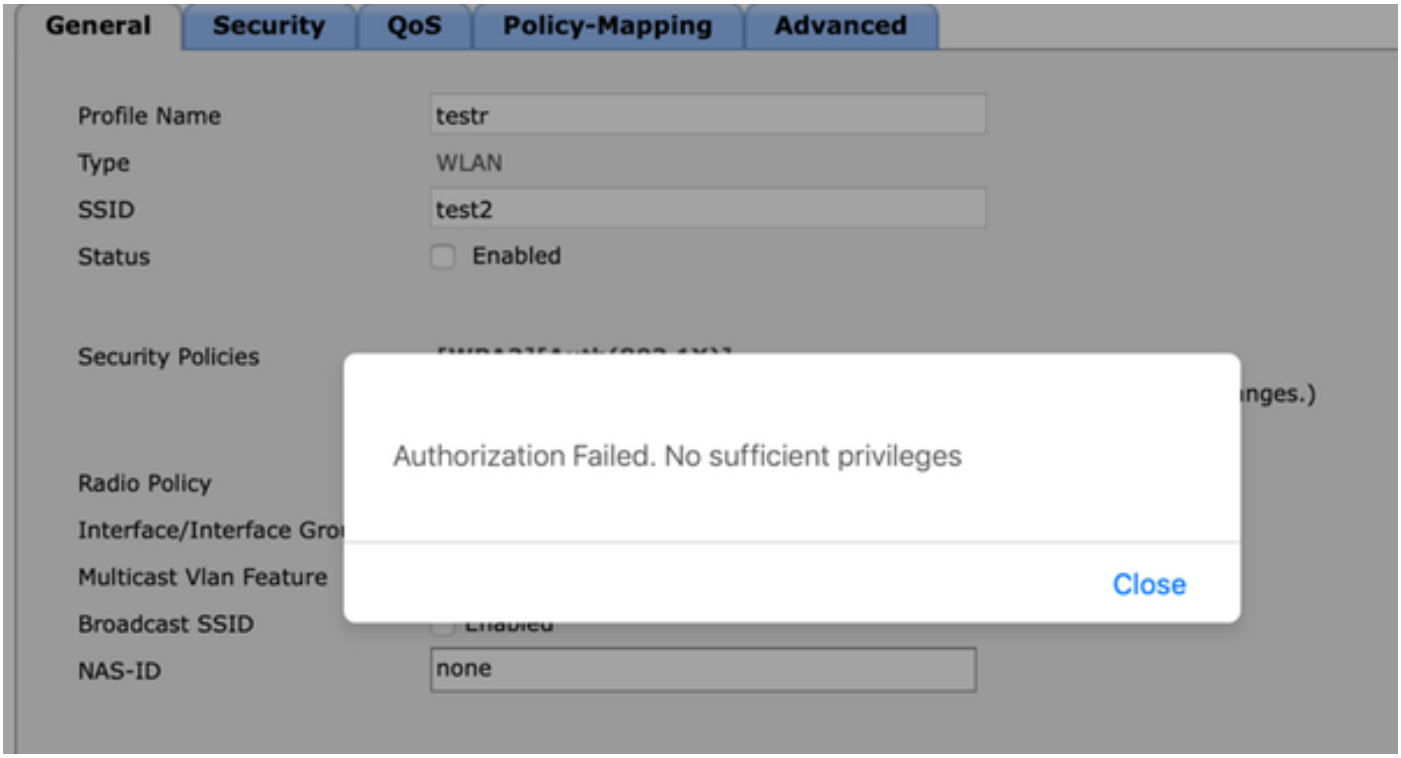

Cisco WLC RO Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
User Groups
WLANLSC\Domain Users
Condition description:
The User Groups condition specifies that the connecting user must belong to one of the selected groups.
Add...
Edit...
Remove
OK
Cancel
Apply



Verifiëren

1. Wanneer inloggebruikersreferenties worden gebruikt, mag de gebruiker geen wijzigingen op de controller configureren.

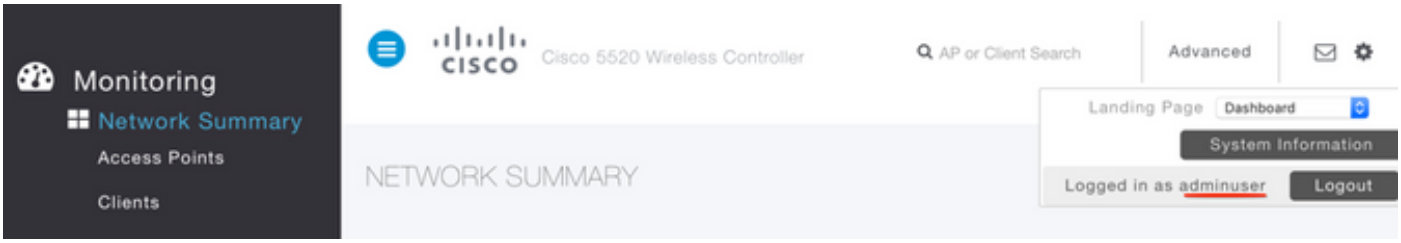




Van **debug a allen toelaten**, kunt u zien dat de waarde van de eigenschap servicetype in autorisatie 7 is die aan NAS-prompt correspondeert.

```
*aaaQueueReader: Dec 07 22:20:14.664: 30:01:00:00:00:00 Successful transmission of
Authentication Packet (pktId 14) to 10.106.33.39:1812 from server queue 0, proxy state
30:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:20:14.664: 00000000: 01 0e 00 48 47 f8 f3 5c 58 46 98 ff 8e f8 20 7a
...HG..\XF.....z
*aaaQueueReader: Dec 07 22:20:14.664: 00000010: f6 a1 f1 d1 01 0b 6c 6f 67 69 6e 75 73 65 72 02
......loginuser.
*aaaQueueReader: Dec 07 22:20:14.664: 00000020: 12 c2 34 69 d8 72 fd 0c 85 aa af 5c bd 76 96 eb
..4i.r.....\.v..
*aaaQueueReader: Dec 07 22:20:14.664: 00000030: 60 06 06 00 00 00 07 04 06 0a 6a 24 31 20 0b 43
`.........j$1..C
*aaaQueueReader: Dec 07 22:20:14.664: 00000040: 69 73 63 6f 2d 57 4c 43 isco-WLC
:
:
*radiusTransportThread: Dec 07 22:20:14.668: 30:01:00:00:00:00 Access-Accept received from
RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:14
*radiusTransportThread: Dec 07 22:20:14.668: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:20:14.668: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Dec 07 22:20:14.668: structureSize.............................304
*radiusTransportThread: Dec 07 22:20:14.668:
protocolUsed.................................0x00000001
*radiusTransportThread: Dec 07 22:20:14.668:
proxyState...................................30:01:00:00:00:00-00:00
*radiusTransportThread: Dec 07 22:20:14.668: Packet contains 2 AVPs:
*radiusTransportThread: Dec 07 22:20:14.668: AVP[01] Service-
Type.............................0x00000007 (7) (4 bytes)
*radiusTransportThread: Dec 07 22:20:14.668: AVP[02]
Class.................................DATA (44 bytes)
```

2. Wanneer de gebruikersreferenties worden gebruikt, moet de gebruiker volledige toegang hebben met **servicetype** waarde 6, hetgeen overeenkomt met **administratieve gegevens**.




```
*aaaQueueReader: Dec 07 22:14:27.439: AuthenticationRequest: 0x7fba240c2f00
*aaaQueueReader: Dec 07 22:14:27.439: Callback.....................................0xa3c13ccb70
*aaaQueueReader: Dec 07 22:14:27.439:
proxyState.....................................2E:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:14:27.439: Packet contains 5 AVPs:
*aaaQueueReader: Dec 07 22:14:27.439: AVP[01] User-Name.............................adminuser
(9 bytes)
*aaaQueueReader: Dec 07 22:14:27.439: AVP[04] Nas-Ip-
Address.........................0x0a6a2431 (174728241) (4 bytes)
*aaaQueueReader: Dec 07 22:14:27.439: AVP[05] NAS-Identifier.........................Cisco-WLC
(9 bytes)
:
:
*radiusTransportThread: Dec 07 22:14:27.442: 2e:01:00:00:00:00 Access-Accept received from
RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:13
*radiusTransportThread: Dec 07 22:14:27.442: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:14:27.442: structureSize.............................304
*radiusTransportThread: Dec 07 22:14:27.442:
protocolUsed.................................0x00000001
*radiusTransportThread: Dec 07 22:14:27.442:
proxyState.....................................2E:01:00:00:00:00-00:00
*radiusTransportThread: Dec 07 22:14:27.442: AVP[01] Service-
Type.............................0x00000006 (6) (4 bytes)
*radiusTransportThread: Dec 07 22:14:27.442: AVP[02]
Class.....................................DATA (44 bytes)
```

Problemen oplossen

Om de toegang tot WLC van het probleemoplossingsbeheer door NPS te toegang hebben, **kan** de run **debug a.u.** opdracht uitvoeren.

1. De logbestanden waarin onjuiste referenties worden gebruikt, worden hier weergegeven.

```
*aaaQueueReader: Dec 07 22:36:39.753: 32:01:00:00:00:00 Successful transmission of
Authentication Packet (pktId 15) to 10.106.33.39:1812 from server queue 0, proxy state
32:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:36:39.753: 00000000: 01 0f 00 48 b7 e4 16 4d cc 78 05 32 26 4c ec 8d
...H...M.x.2&L..
*aaaQueueReader: Dec 07 22:36:39.753: 00000010: c7 a0 5b 72 01 0b 6c 6f 67 69 6e 75 73 65 72 02
..[r..loginuser.
*aaaQueueReader: Dec 07 22:36:39.753: 00000020: 12 03 a7 37 d4 c0 16 13 fc 73 70 df 1f de e3 e4
...7.....sp.....
*aaaQueueReader: Dec 07 22:36:39.753: 00000030: 32 06 06 00 00 00 07 04 06 0a 6a 24 31 20 0b 43
2.........j$1..C
*aaaQueueReader: Dec 07 22:36:39.753: 00000040: 69 73 63 6f 2d 57 4c 43 isco-WLC
*aaaQueueReader: Dec 07 22:36:39.753: 32:01:00:00:00:00 User entry not found in the Local FileDB
for the client.
*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Counted 0 AVPs (processed 20
bytes, left 0)
*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Access-Reject received from
```

```
RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:15
*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Did not find the macaddress to be
deleted in the RADIUS cache database
*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Returning AAA Error
'Authentication Failed' (-4) for mobile 32:01:00:00:00:00 serverIdx 1
*radiusTransportThread: Dec 07 22:36:39.763: AuthorizationResponse: 0x7fbaebebf860
*radiusTransportThread: Dec 07 22:36:39.763: structureSize.............................136
*radiusTransportThread: Dec 07 22:36:39.763: resultCode.................................-4
*radiusTransportThread: Dec 07 22:36:39.763:
protocolUsed.............................0xffffffff
*radiusTransportThread: Dec 07 22:36:39.763: Packet contains 0 AVPs:
*emWeb: Dec 07 22:36:39.763: Authentication failed for loginuser
```

2. De logboeken bij gebruik van het servicetype met een andere waarde dan **administratief (waarde=6)** of **NAS-prompt (waarde=7)** worden als volgt weergegeven. In dat geval, mislukt de inlognaam, zelfs als de verificatie lukt.

```
*aaaQueueReader: Dec 07 22:46:31.849: AuthenticationRequest: 0x7fba240c56a8
*aaaQueueReader: Dec 07 22:46:31.849: Callback.....................................0xa3c13ccb70
*aaaQueueReader: Dec 07 22:46:31.849: protocolType.................................0x00020001
*aaaQueueReader: Dec 07 22:46:31.849:
proxyState.....................................39:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:46:31.849: Packet contains 5 AVPs:
*aaaQueueReader: Dec 07 22:46:31.849: AVP[01] User-Name.............................adminuser
(9 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[02] User-Password............................[...]
*aaaQueueReader: Dec 07 22:46:31.849: AVP[03] Service-
Type............................0x00000007 (7) (4 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[04] Nas-Ip-
Address............................0x0a6a2431 (174728241) (4 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[05] NAS-Identifier.........................Cisco-WLC
(9 bytes)
:
:
*radiusTransportThread: Dec 07 22:46:31.853: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:46:31.853: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Dec 07 22:46:31.853: structureSize.............................304
*radiusTransportThread: Dec 07 22:46:31.853: resultCode.................................0
*radiusTransportThread: Dec 07 22:46:31.853:
protocolUsed.............................0x00000001
*radiusTransportThread: Dec 07 22:46:31.853: Packet contains 2 AVPs:
*radiusTransportThread: Dec 07 22:46:31.853: AVP[01] Service-
Type............................0x00000001 (1) (4 bytes)
*radiusTransportThread: Dec 07 22:46:31.853: AVP[02]
Class.................................DATA (44 bytes)
*emWeb: Dec 07 22:46:31.853: Authentication succeeded for adminuser
```