

RADIUS configureren voor Windows 2008 NPS-server - WAAS AAA

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratiestappen](#)

[1. WAAS Central Manager](#)

[2. Windows 2008 R2-NPS serverconfiguratie](#)

[3. WAAS CM-configuratie voor RADIUS-gebruikersrekeningen](#)

[Verificatie](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de procedure voor de RADIUS-configuratie (Remote Verificatie) van Cisco Wide Area Application Services (WAAS) en Windows 2008 R2 Network Policy Server (NPS).

Standaard WAAS-configuratie gebruikt lokale verificatie. Cisco WAAS ondersteunt RADIUS en Terminal Access Control System (TACACS+) ook voor verificatie, autorisatie en accounting (AAA). Dit document heeft alleen betrekking op de configuratie van één apparaat. Dit kan echter ook onder de apparaatgroep gebeuren. Alle configuratie moet worden toegepast via WAAS CM GUI.

De algemene WAAS AAA-configuratie wordt geleverd in de [Cisco Wide Area Application Services Configuration](#) onder het hoofdstuk Bestuurlijke Login-verificatie, autorisatie en accounting.

Bijgedragen door Hamilan Gnanabaskaran, Cisco TAC Engineer.

Bewerkt door Sanaz Tayyar, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- WAAS 5.x of 6.x
- Windows NPS-server
- AAA - RADIUS

Gebruikte componenten

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

- Cisco WAAS - Virtual Central Manager (vCM)
- WAAS 6.2.3.b
- Windows 2008 NPS

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, begonnen met een standaardconfiguratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Verwante producten

Dit document kan ook met deze hardware- en softwareversies worden toegepast:

- vWAAS, ISR-WAAS en alle WAAS-apparaten
- WAAS 5.x of WAAS 6.x
- WAAS als Central Manager, Application Accelerator

Opmerking: APPNAV-XE ondersteunt deze configuratie niet. De router AAA drukt de configuratie aan APPNAV-XE.

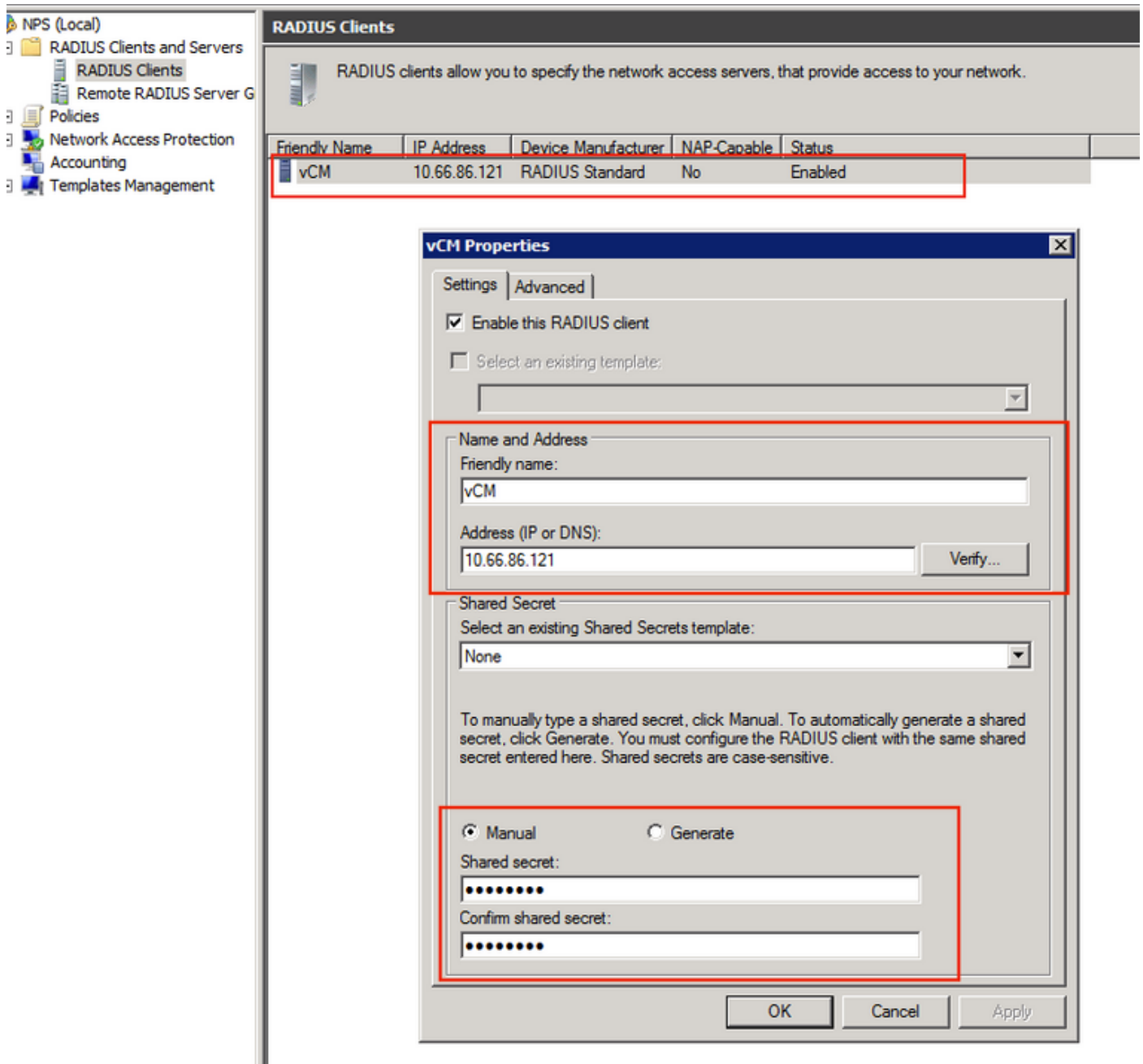
Configuratiestappen

Deze configuratie moet worden toegepast:

1. WAAS Central Manager
 - 1.1 AAA RADIUS-configuratie
 - 1.2 AAA-verificatie-configuratie
2. Windows 2008 R2 - NPS serverconfiguratie
 - 2.1 Configuratie van RADIUS-clients
 - 2.2 Configuratie van netwerkbeleid
3. WAAS CM-configuratie voor RADIUS-gebruikersrekeningen

1. WAAS Central Manager

1.1 Maak in WAAS Central Manager de RADIUS-server onder **Configuration>Security>AAA>RADIUS**.



2.2 Voer in de Windows 2008 R2 - NPS server een netwerkbeleid in om de WAAS-apparaten aan te passen en verificatie mogelijk te maken.

Network Policy Server

File Action View Help

NPS (Local)

- RADIUS Clients and Servers
 - RADIUS Clients
 - Remote RADIUS Server G
- Policies
 - Connection Request Poli
 - Network Policies
 - Health Policies
- Network Access Protection
 - System Health Validators
 - Remediation Server Group
- Accounting
- Templates Management

Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
POLICY_WAAS	Enabled	1	Grant Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified
Connections to other access servers	Enabled	999999	Deny Access	Unspecified

POLICY_WAAS

Conditions - If the following conditions are met:

Condition	Value
Client Friendly Name	vCM
Windows Groups	ANS0\WAAS

Settings - Then the following settings are applied:

Setting	Value
Cisco-AV-Pair	shell:priv-lvl=15
Extended State	<Blank>
Access Permission	Grant Access
Authentication Method	Unencrypted authentication (PAP, SPAP)
NAP Enforcement	Allow full network access
Update Noncompliant Clients	True
Service-Type	Administrative
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

In het LAB moeten deze parameters worden geselecteerd onder **NPS >beleid>Netwerkbeleid**.

POLICY_WAAS Properties

Overview | Conditions | Constraints | Settings

Policy name:

Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

Policy enabled

Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

Grant access. Grant access if the connection request matches this policy.

Deny access. Deny access if the connection request matches this policy.

Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .

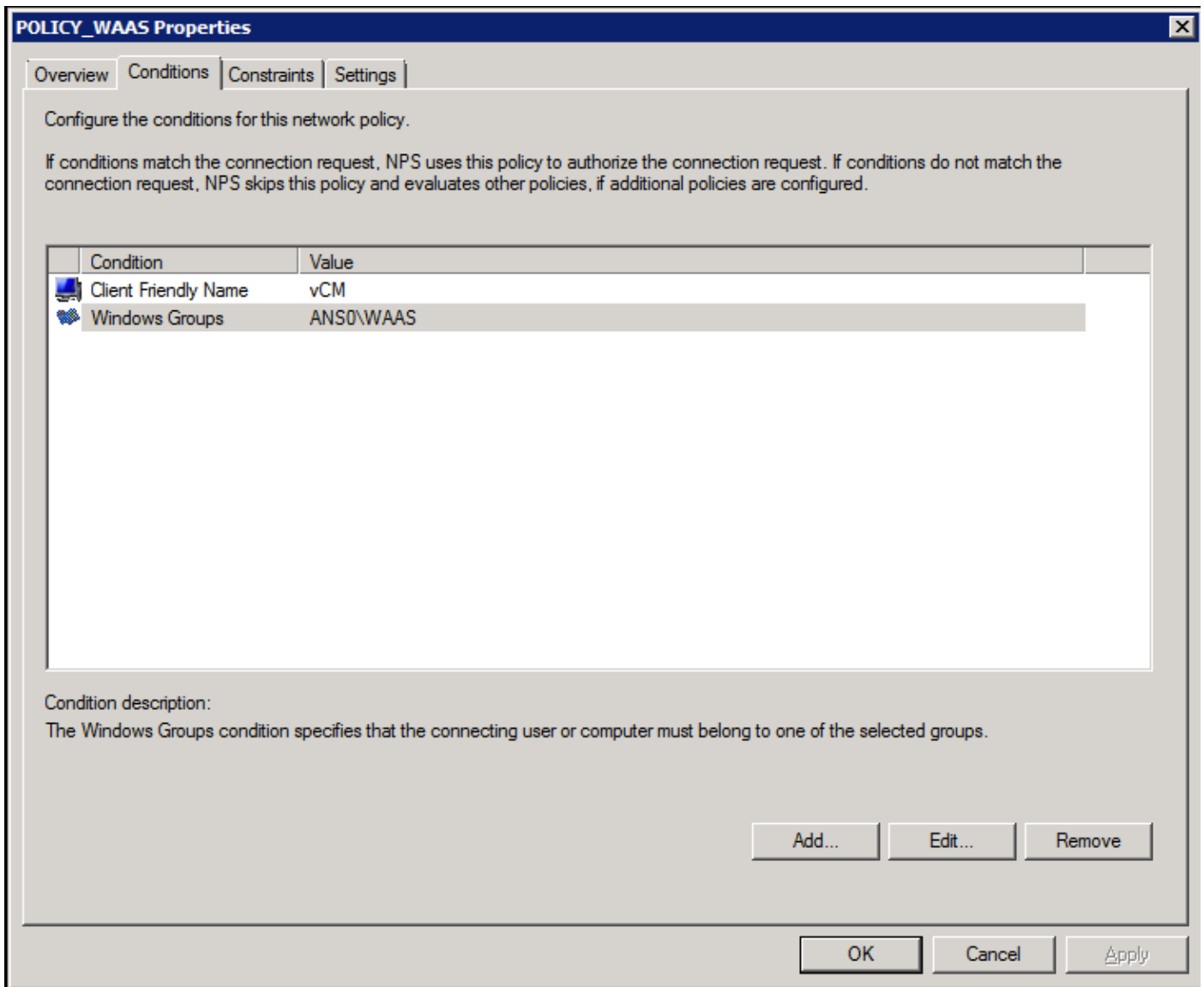
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:

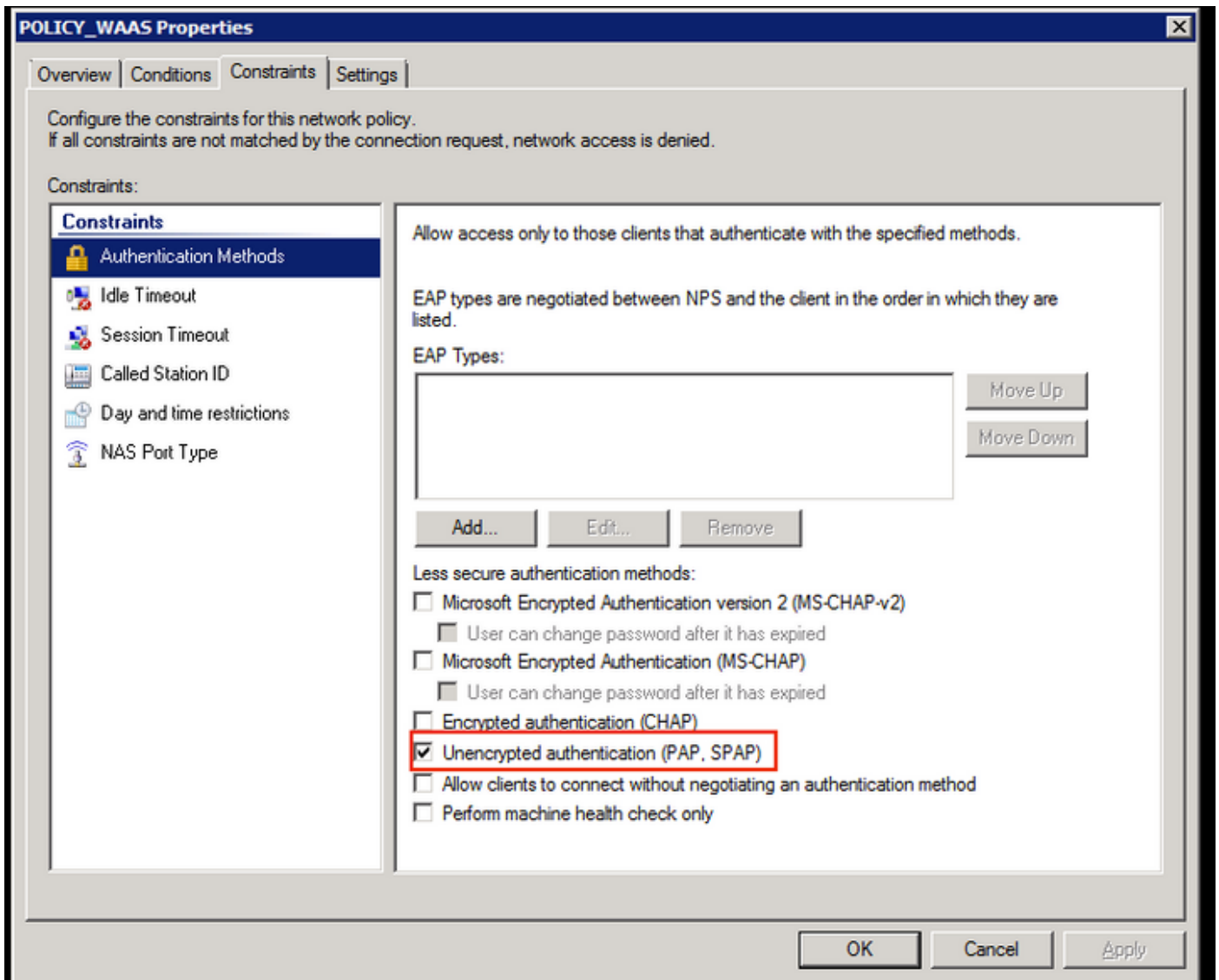
Vendor specific:

OK Cancel Apply

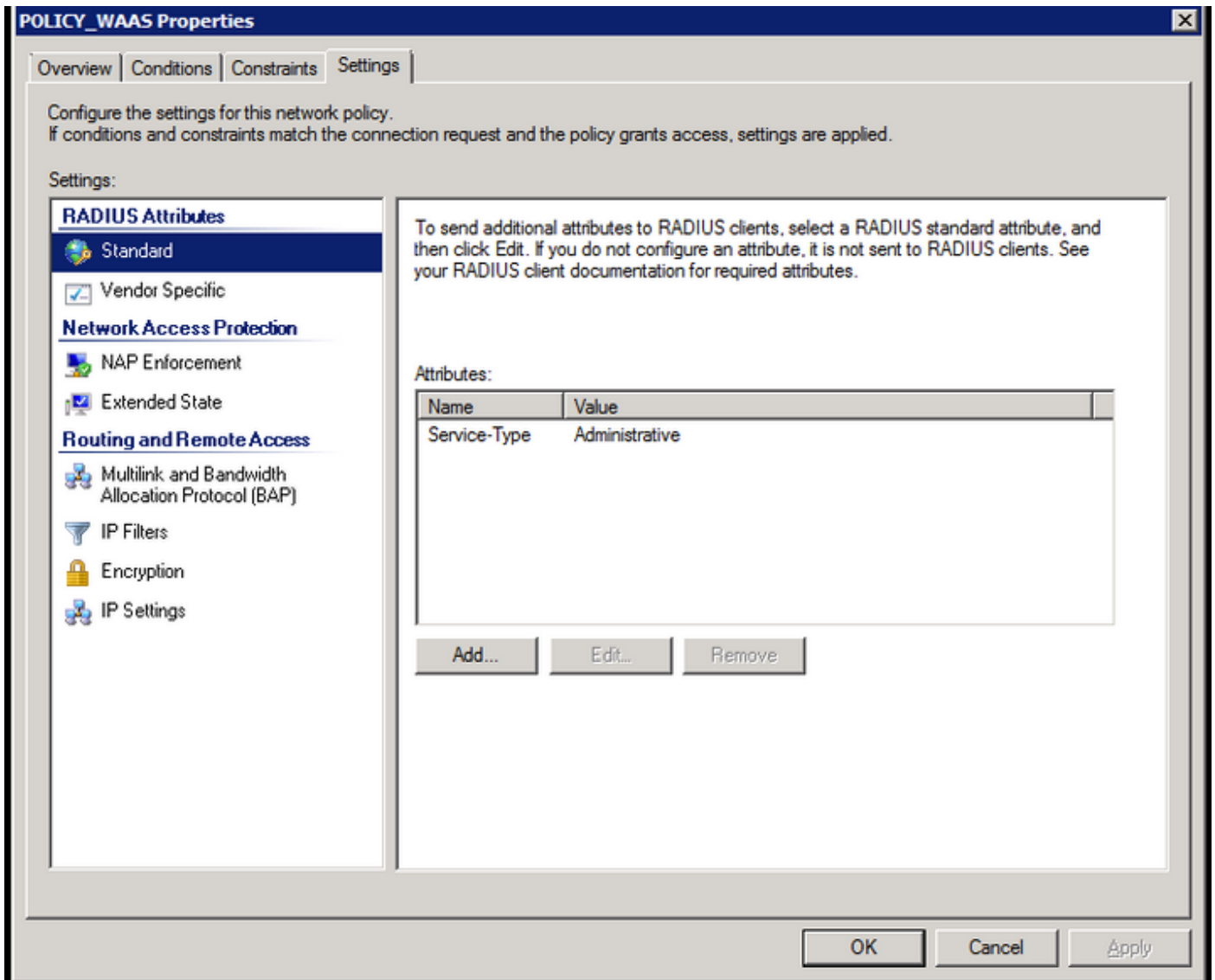
De conditionering kan worden aangepast aan de naam van de klant Radius. Andere methoden kunnen worden gebruikt zoals IP adres.



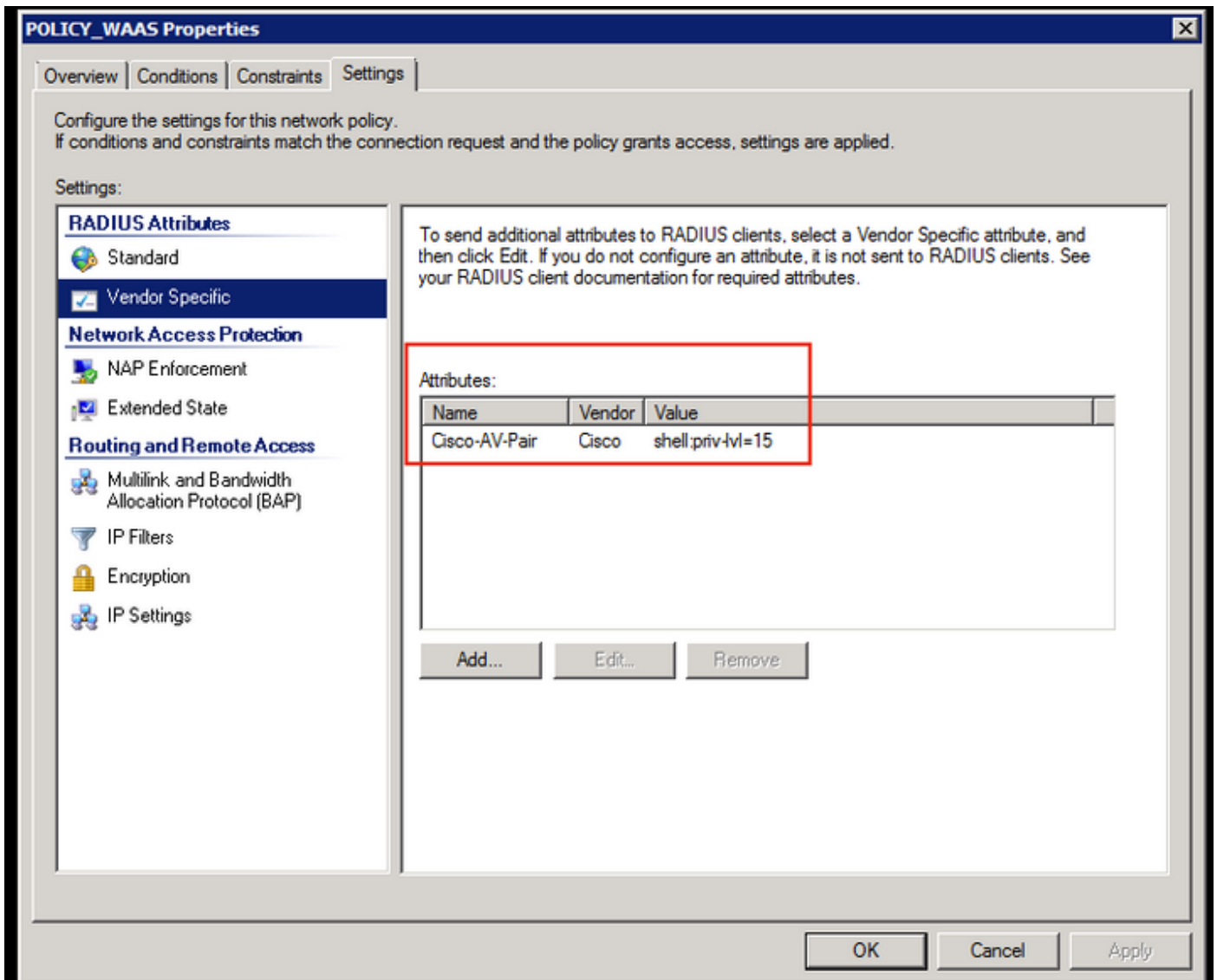
Verificatiemethoden als niet-versleutelde verificatie (PAP, SPAP).



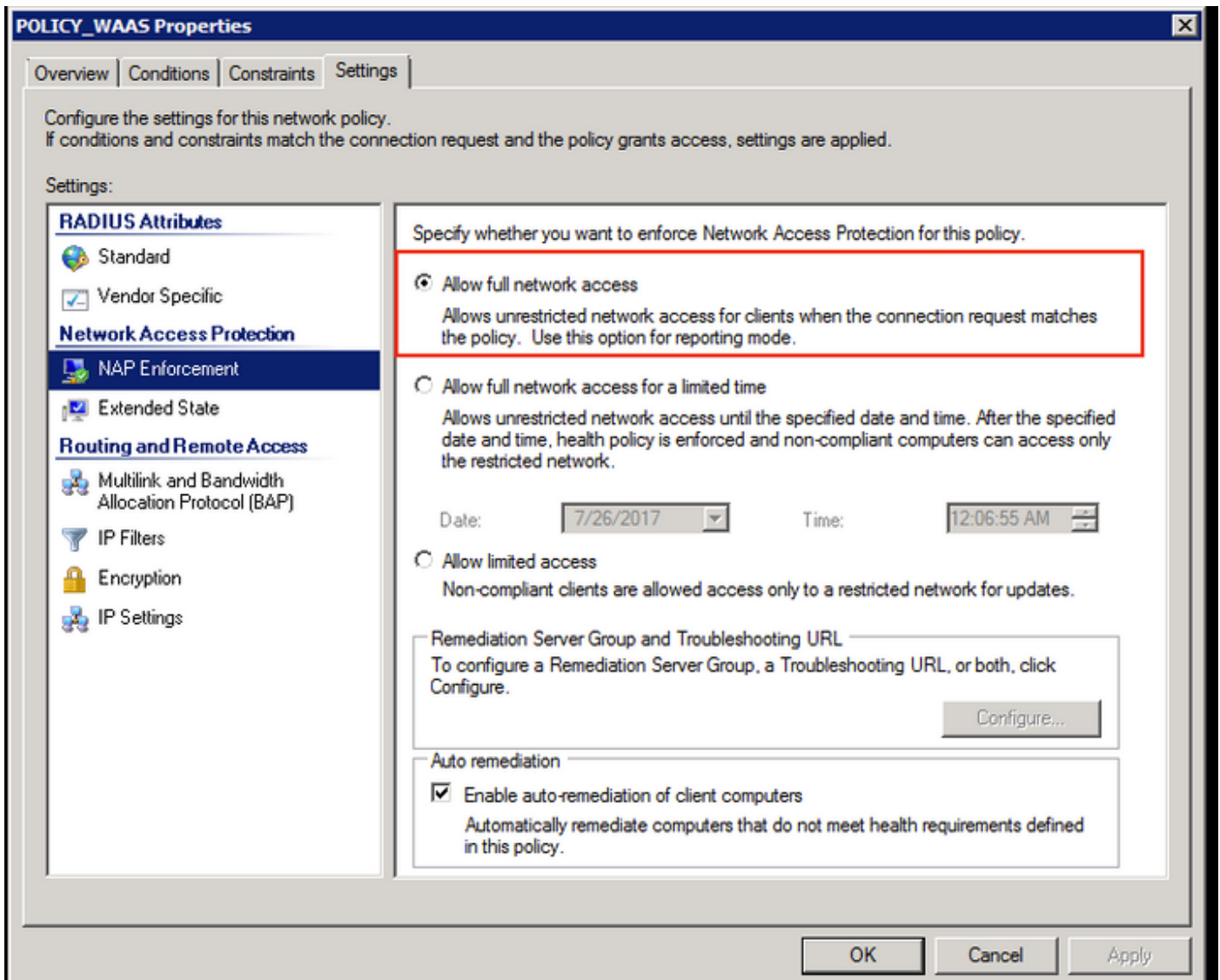
Service-type als administratief.



specifieke eigenschap van de verkoper als Cisco-AV-air (Shell:priv-lvl=15).



Geef volledige netwerktoegang toe.

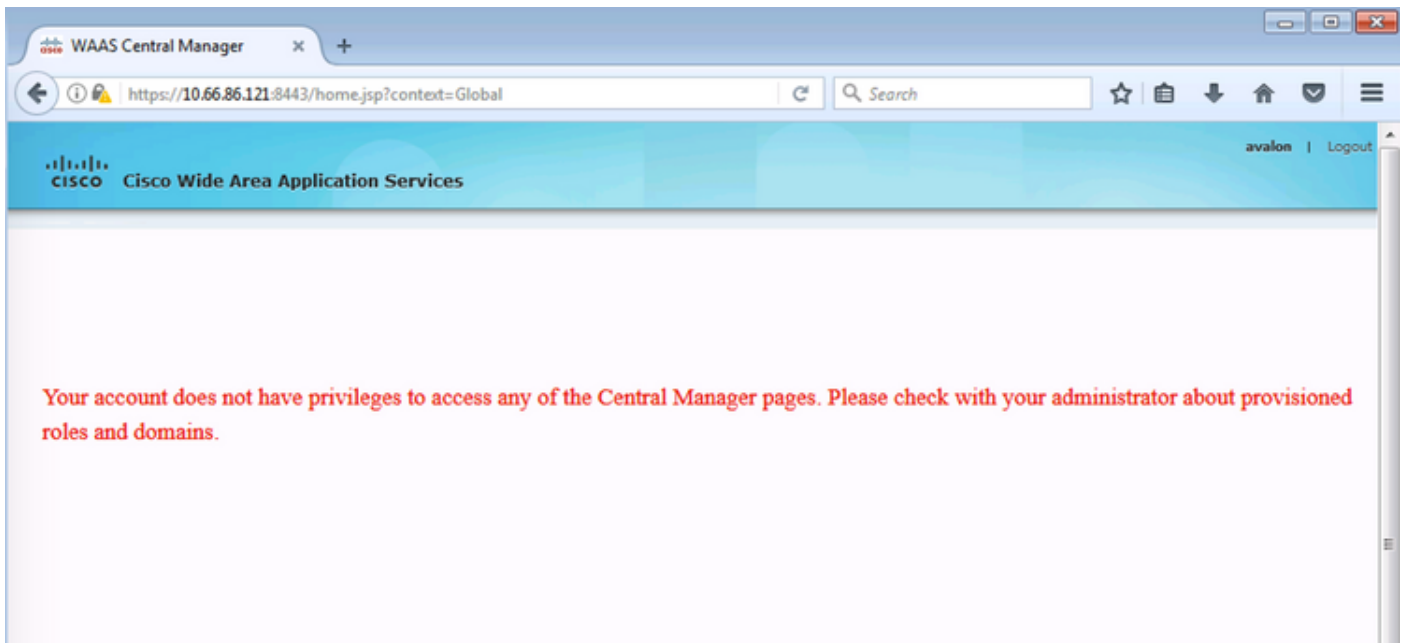


3. WAAS CM-configuratie voor RADIUS-gebruikersrekeningen

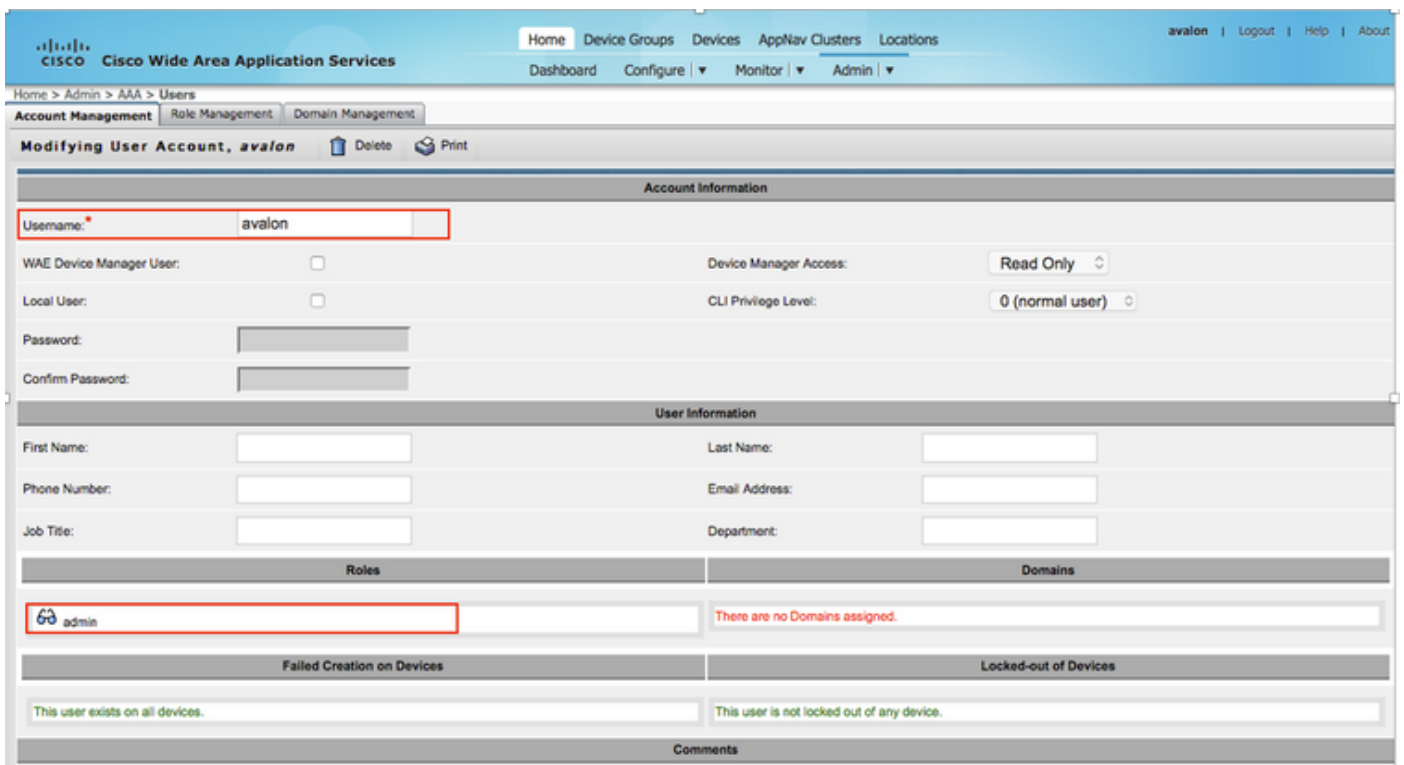
Het configureren van een gebruiker in RADIUS met voorkeursniveau 15 of 1 geeft niet de toegang tot WAAS CM GUI. De CMS database behoudt een lijst met gebruikers, rollen en domeinen gescheiden van de externe AAA-server.

Na het correct configureren van de externe AAA-server om een gebruiker te authentifieren moet de CM GUI zijn ingesteld om die gebruiker de noodzakelijke rollen en domeinen te geven om binnen de CM GUI te werken.

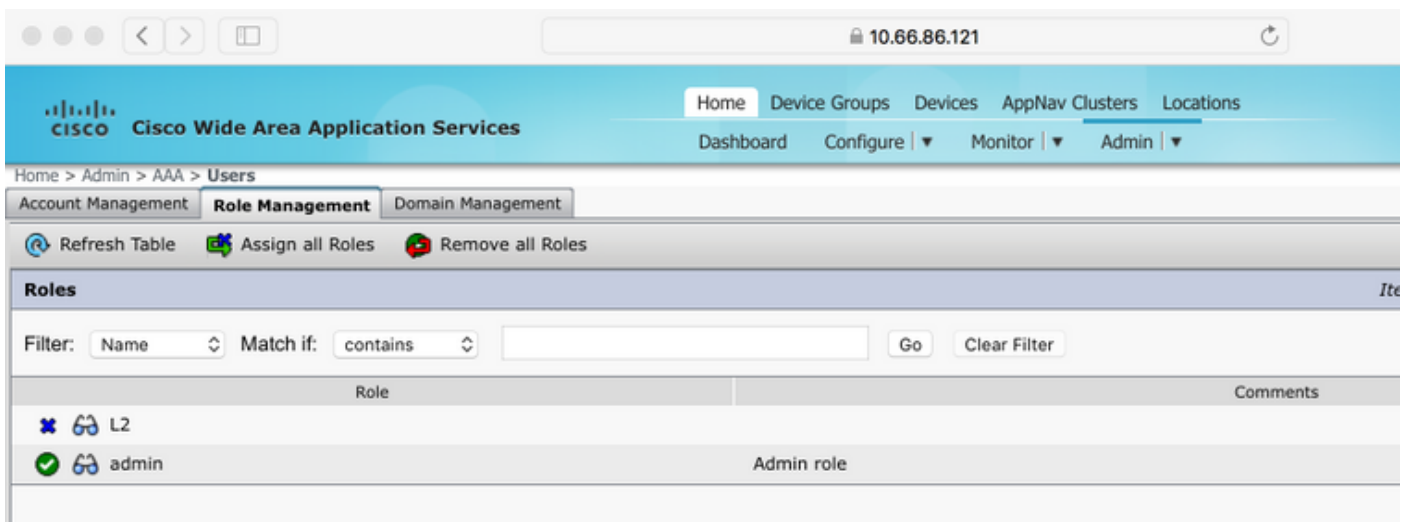
Als de RADIUS-gebruiker niet onder gebruiker in de CM staat, heeft de account van Uw account geen rechten op toegang tot een van de pagina's van de Central Manager. Controleer met de beheerder of de rollen en domeinen waarvoor u een provisioning hebt ingesteld. Deze message wordt weergegeven.



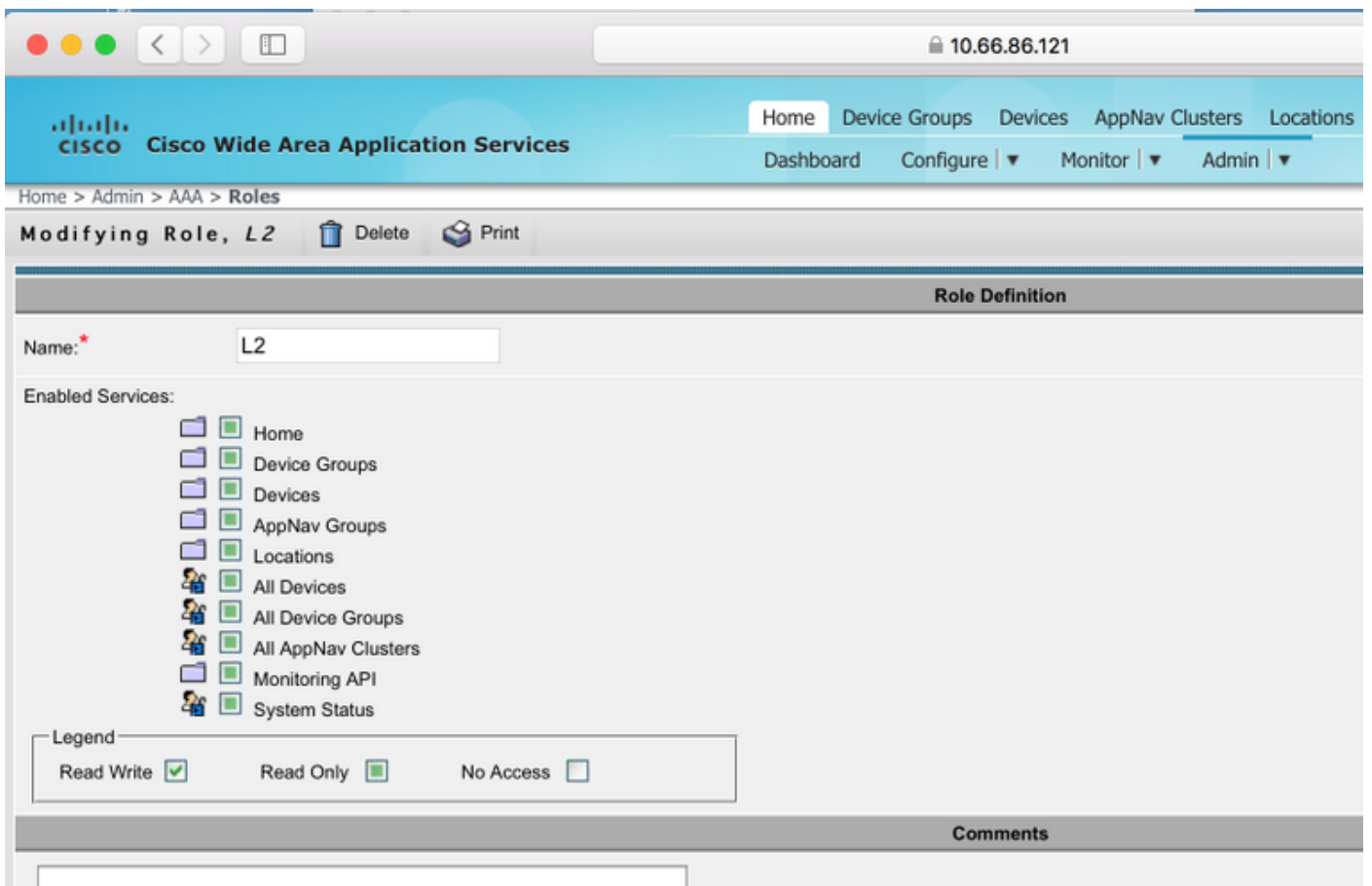
Configuratie van de lokale gebruikersnaam onder WAAS CM zonder wachtwoord.



Gebruikersnaam moet zich binden met de juiste rollen onder Rol Management voor elke gebruiker.



Als de gebruiker alleen-lezen of een beperkte toegang nodig heeft, kan dit onder een rolverdeling worden ingesteld.



Verificatie

In de WAAS-apparaten wordt deze configuratie geduwd.

Straalserver-toets ***

Straal-server host 10.66.86.125 poorten en 1645

!

Lokale inlognaam voor verificatie: secundair

authenticatie loginstraal mogelijk

authenticatie lokale configuratie mogelijk

authenticatieconversiegeleiding mogelijk maken primaire authenticatie faalt-over server-onbereikbaar

De [Cisco CLI Analyzer](#) ([alleen geregistreeerde](#) klanten) ondersteunt bepaalde **show**-opdrachten. Gebruik de Cisco CLI Analyzer om een analyse van de opdrachtoutput te bekijken.

- **Verificatie** - Verificatie configureren

Problemen oplossen

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

- Controleer de Windows-domeinlogs
- **#debug aaa autorisatie** van WAAS CM CLI

Gerelateerde informatie

- [RADIUS-serververificatie configureren op WAAS](#)
- [Network Policy Server is van toepassing op Windows Server 2008](#)