

Konfigurieren von RADIUS für Windows 2008 NPS-Server - WAAS AAA

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurationsschritte](#)

[1. WAAS Central Manager](#)

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

[3. WAAS CM-Konfiguration für RADIUS-Benutzerkonten](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird das Verfahren der RADIUS-Konfiguration (Remote Authentication Dial-In User Service) für Cisco Wide Area Application Services (WAAS) und Windows 2008 R2 Network Policy Server (NPS) beschrieben.

Die WAAS-Standardkonfiguration verwendet die lokale Authentifizierung. Cisco WAAS unterstützt RADIUS und Terminal Access Controller Access Control System (TACACS+) auch für Authentication, Authorization, and Accounting (AAA). Dieses Dokument behandelt die Konfiguration nur für ein Gerät. Dies kann jedoch auch unter "Device Group" (Gerätegruppe) erfolgen. Alle Konfigurationen müssen über die grafische Benutzeroberfläche von WAAS CM angewendet werden.

Eine allgemeine WAAS-AAA-Konfiguration finden Sie im [Cisco Wide Area Application Services Configuration Guide](#) unter Configuring Administrative Login Authentication, Authorization, and Accounting.

Unterstützt von Hamilan Gnanabaskaran, Cisco TAC Engineer.

Bearbeitet von Sanaz Tayyar, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- WAAS 5.x oder 6.x
- Windows NPS-Server

- AAA - RADIUS

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer Standardkonfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Dieses Dokument kann auch mit den folgenden Hardware- und Softwareversionen angewendet werden:

- vWAAS, ISR-WAAS und alle WAAS-Appliances
- WAAS 5.x oder WAAS 6.x
- WAAS als Central Manager, Application Accelerator

Hinweis: APPNAV-XE unterstützt diese Konfiguration nicht. Router AAA leitet die Konfiguration an APPNAV-XE weiter.

Konfigurationsschritte

Diese Konfiguration muss angewendet werden:

1. WAAS Central Manager
 - 1.1 AAA RADIUS-Konfiguration
 - 1.2 Konfiguration der AAA-Authentifizierung
2. Windows 2008 R2 - NPS-Serverkonfiguration
 - 2.1 Konfiguration von RADIUS-Clients
 - 2.2 Netzwerkrichtlinienkonfiguration
3. WAAS CM-Konfiguration für RADIUS-Benutzerkonten

1. WAAS Central Manager

1.1 In WAAS Central Manager erstellt der RADIUS-Server unter **Konfigurieren > Sicherheit > AAA>RADIUS**.

Home Device Groups **Devices** AppNav Clusters Locations avalon | Logout | Help | About

CISCO Cisco Wide Area Application Services

vCM-POD4-Primary | Configure | Monitor | Admin

Devices > vCM-POD4-Primary > Configure > Security > AAA > RADIUS

RADIUS Server Settings for Central Manager, vCM-POD4-Primary Print Apply Defaults Remove Settings

RADIUS Server Settings

Time to Wait: (seconds) (1-20)

Number of Retransmits:

Shared Encryption Key:

Server 1 Name: Server 1 Port:

Server 2 Name: Server 2 Port:

Server 3 Name: Server 3 Port:

Server 4 Name: Server 4 Port:

Server 5 Name: Server 5 Port:

* To use RADIUS for Login or Configuration Authentication, please go to the Authentication Methods page.

Note: * - Required Field

1.2 Konfigurieren Sie die Authentifizierungsmethode, um RADIUS unter Konfigurieren > Sicherheit > AAA > Authentifizierungsmethoden widerzuspiegeln.

Die Methode für die primäre Authentifizierung wird als RADIUS und die sekundäre Authentifizierungsmethode als lokal ausgewählt. Im Falle eines RADIUS-Fehlers kann sich der Kunde über ein lokales Konto anmelden.

Home Device Groups **Devices** AppNav Clusters Locations avalon | Logout | Help | About

CISCO Cisco Wide Area Application Services

CM-Secondary-WAVE594 | Configure | Monitor | Admin

Devices > CM-Secondary-WAVE594 > Configure > Security > AAA > Authentication Methods

Authentication and Authorization Methods for Central Manager, CM-Seco... Print Apply Defaults Remove Settings

Authentication and Authorization Methods

Fallover to next available authentication method:

Use only local admin account to enable privilege exec level:

Authentication Login Methods: It is highly recommended to set the authentication and authorization methods in the san

Primary Login Method:

Secondary Login Method:

Tertiary Login Method:

Quaternary Login Method:

Authorization Methods:

Primary Configuration Method:

Secondary Configuration Method:

Tertiary Configuration Method:

Quaternary Configuration Method:

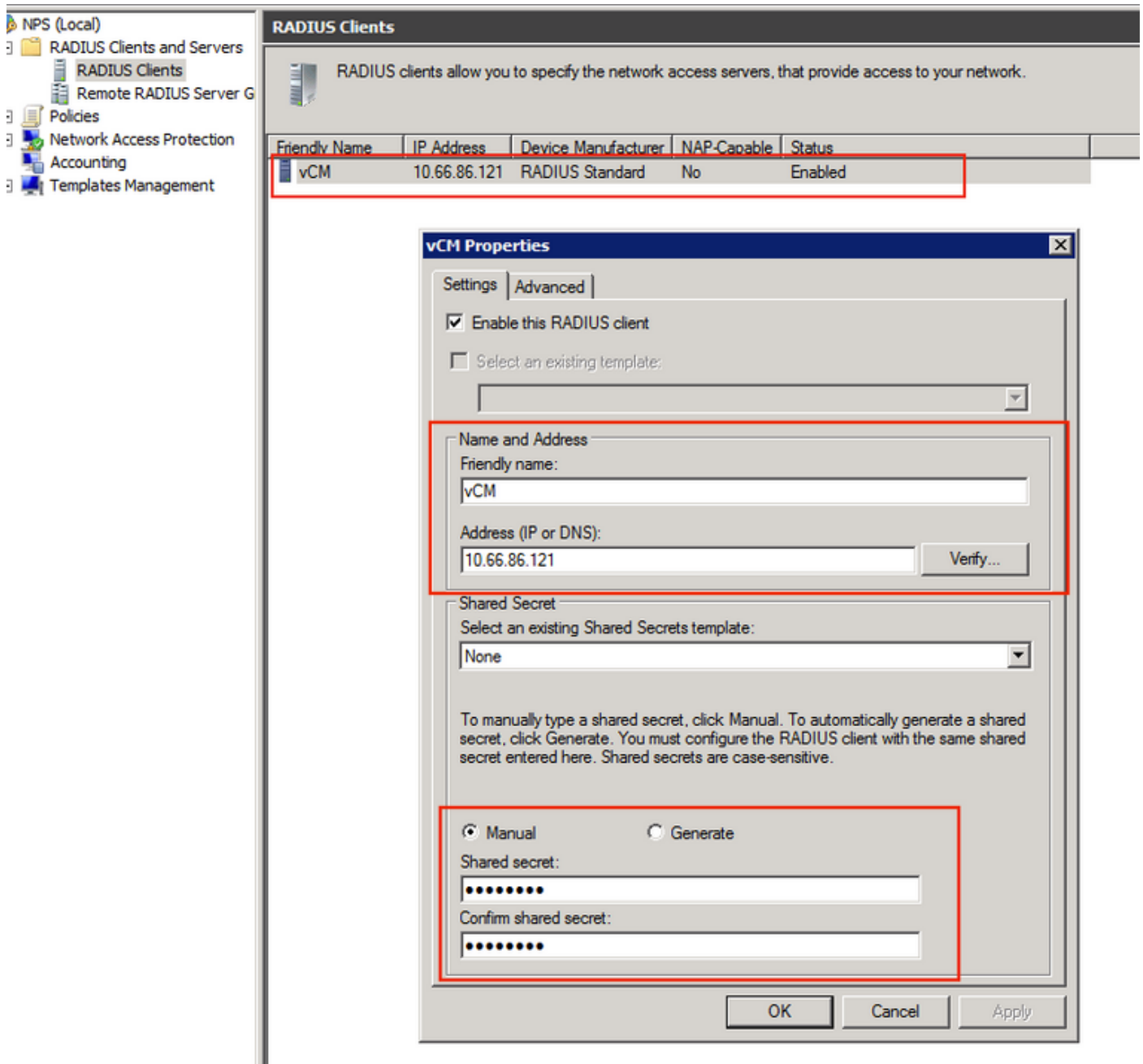
Windows Authentication

Refresh Authentication Status

Note: * - Required Field

2. Windows 2008 R2 - NPS-Serverkonfiguration

2.1 Erstellen Sie im Windows 2008 R2 - NPS-Server die WAAS-Geräte-IP als RADIUS-Client.



2.2 Erstellen Sie im Windows 2008 R2 - NPS-Server eine Netzwerkrichtlinie, die den WAAS-Geräten entspricht und eine Authentifizierung zulässt.

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

Im LAB müssen diese Parameter unter NPS > Policies > Network Policy (NPS > Richtlinien > Netzwerkrichtlinie) ausgewählt werden.

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 .

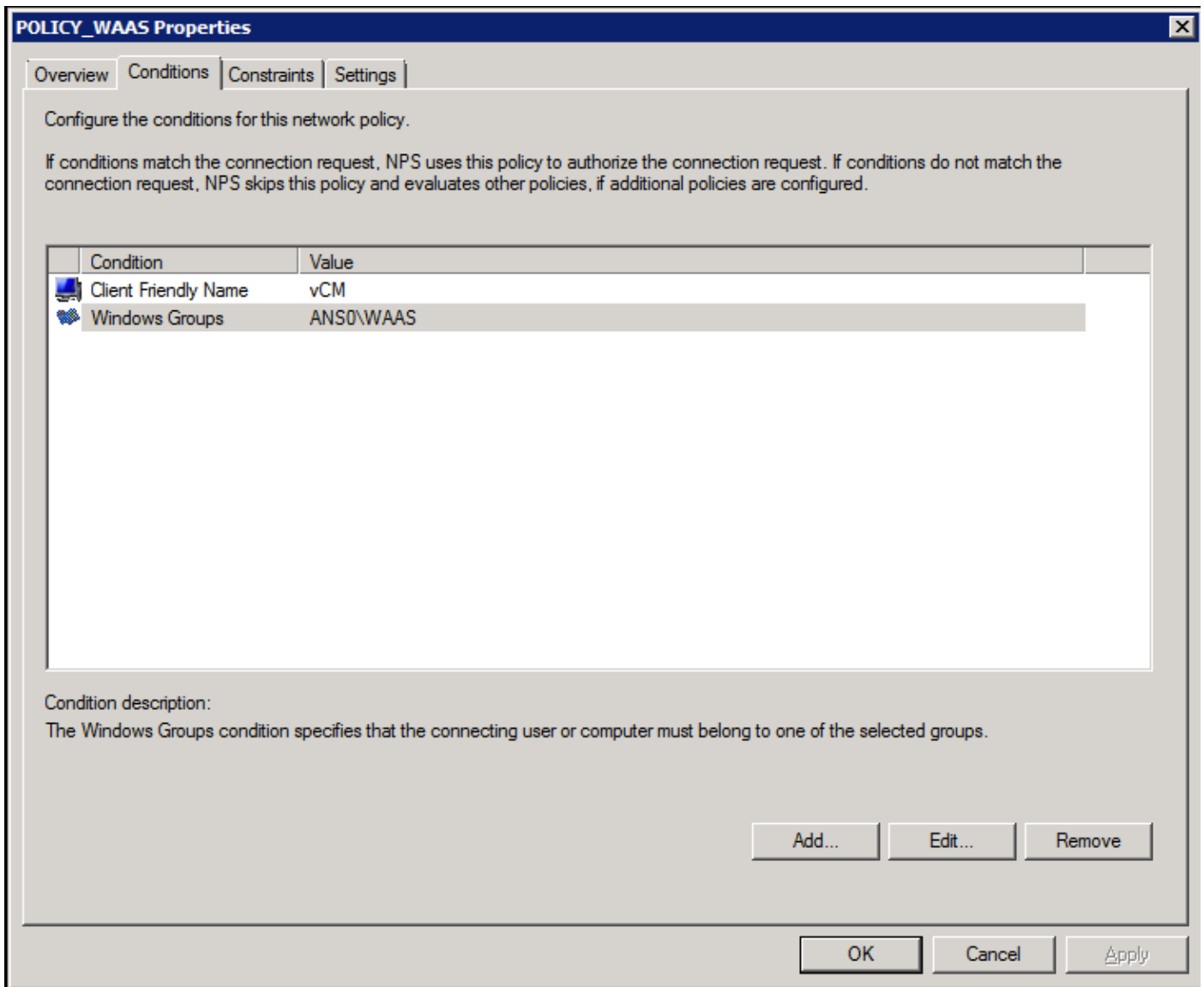
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select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

Type of network access server:

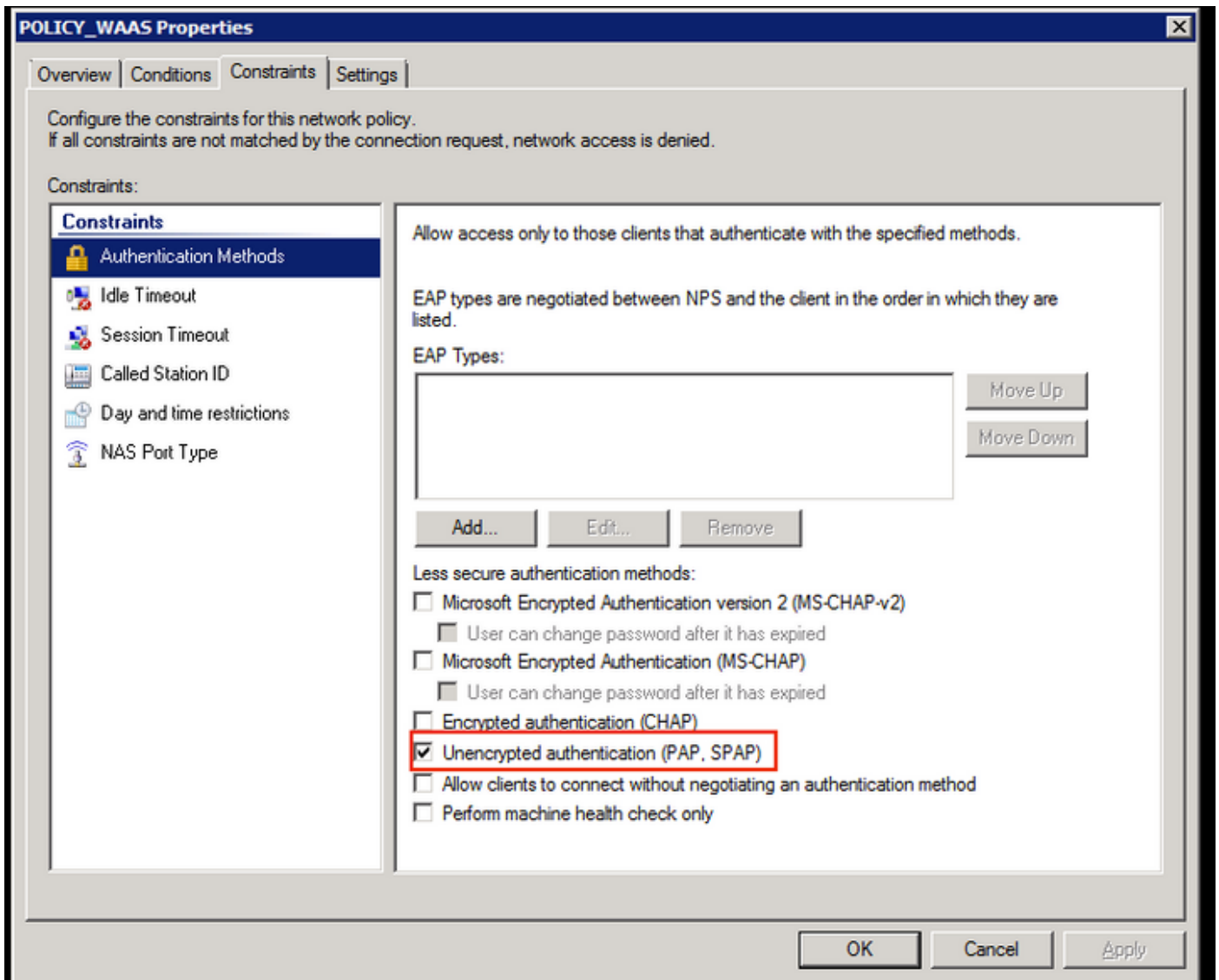
Vendor specific:

OK Cancel Apply

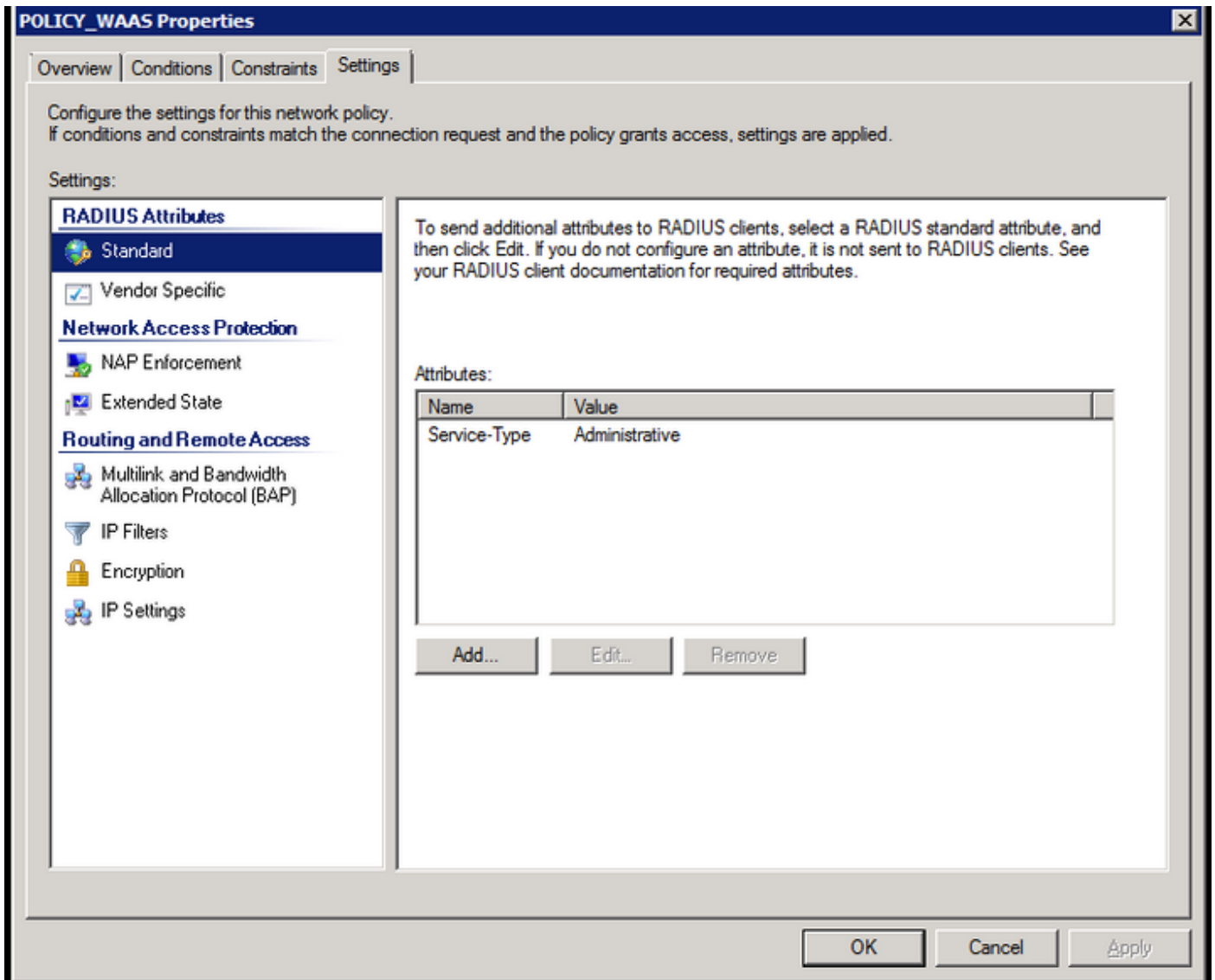
Bedingung kann mit Radius Client Friendly Name abgeglichen werden. Es können andere Methoden verwendet werden, z. B. die IP-Adresse.



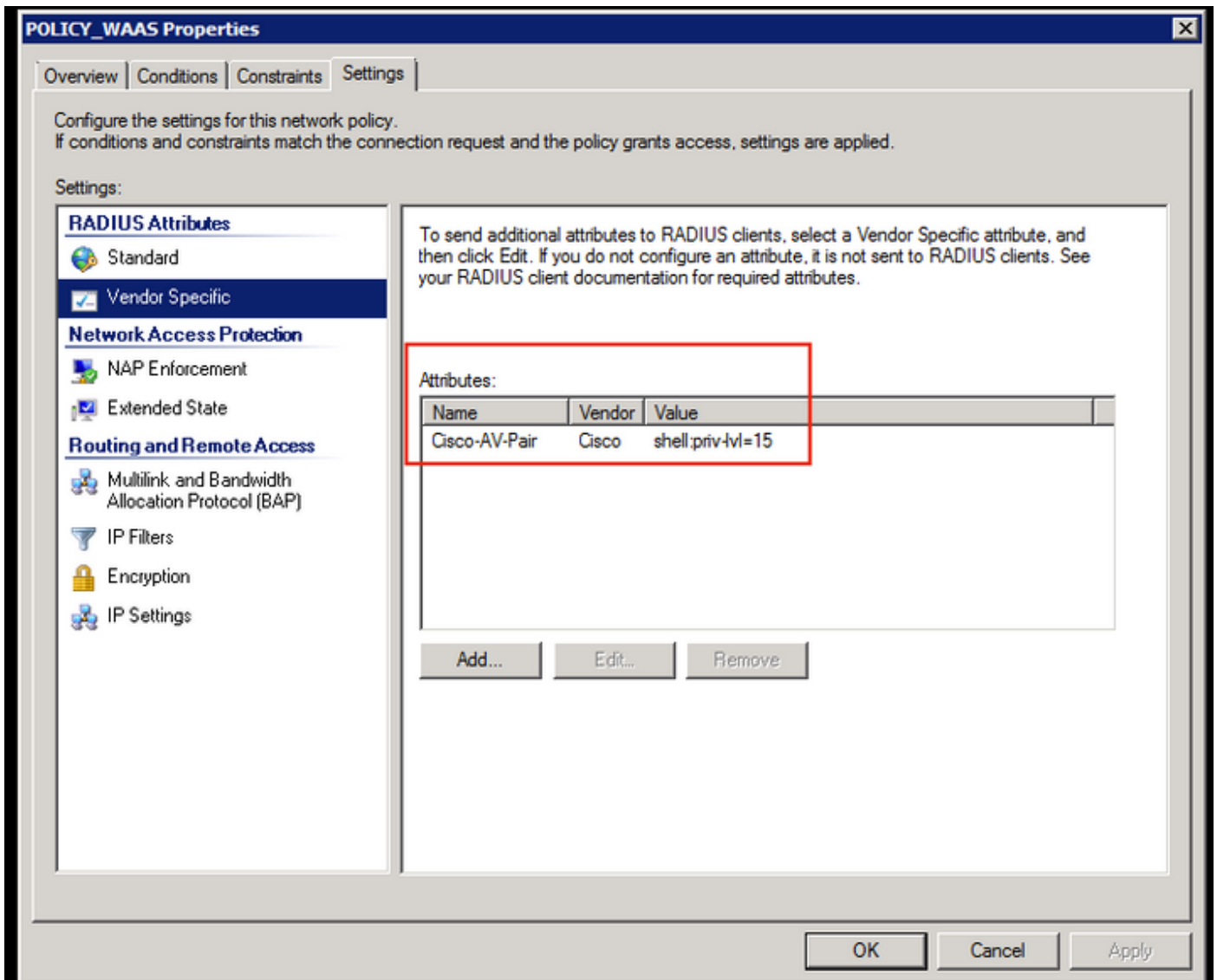
Authentifizierungsmethoden als unverschlüsselte Authentifizierung (PAP, SPAP).



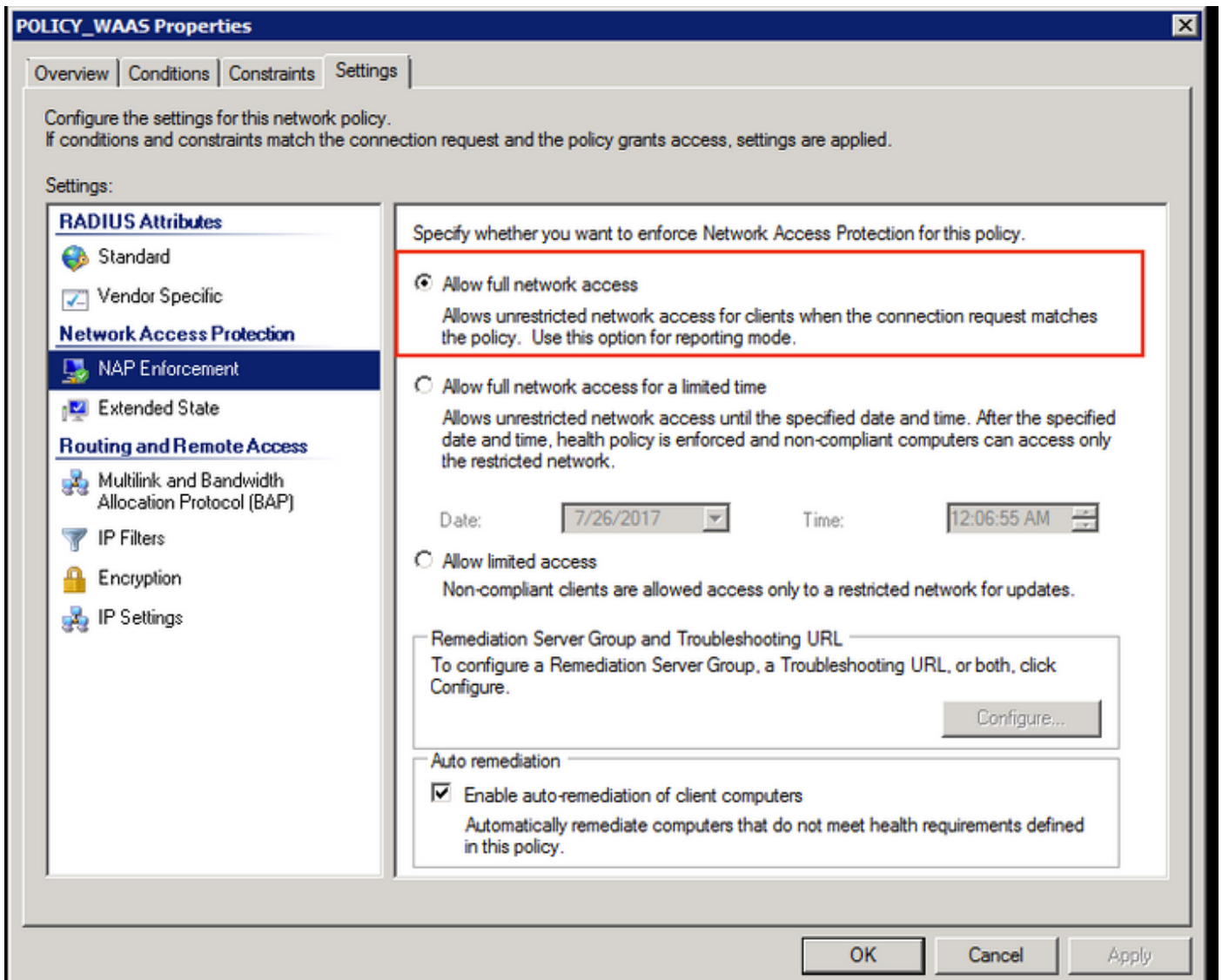
Servicetyp als "Verwaltung".



Herstellerspezifisches Attribut als Cisco-AV-Paar (Shell:priv-lvl=15).



Vollständigen Netzwerkzugriff zulassen.

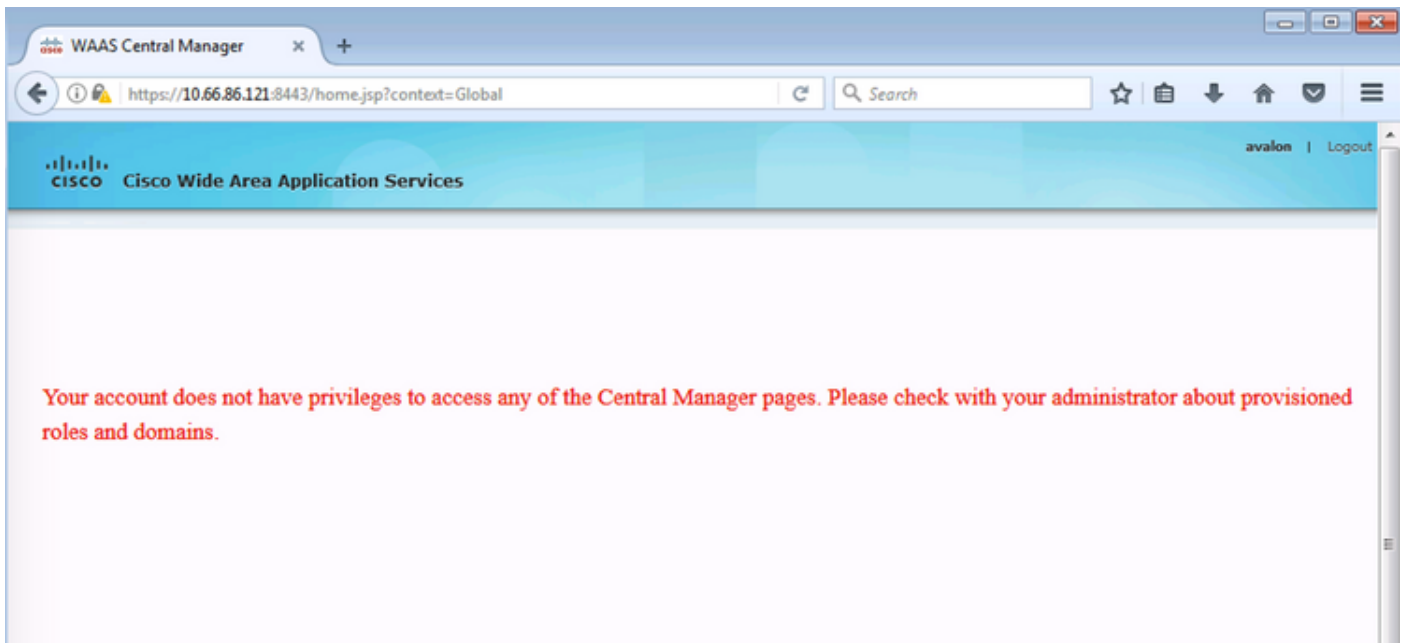


3. WAAS CM-Konfiguration für RADIUS-Benutzerkonten

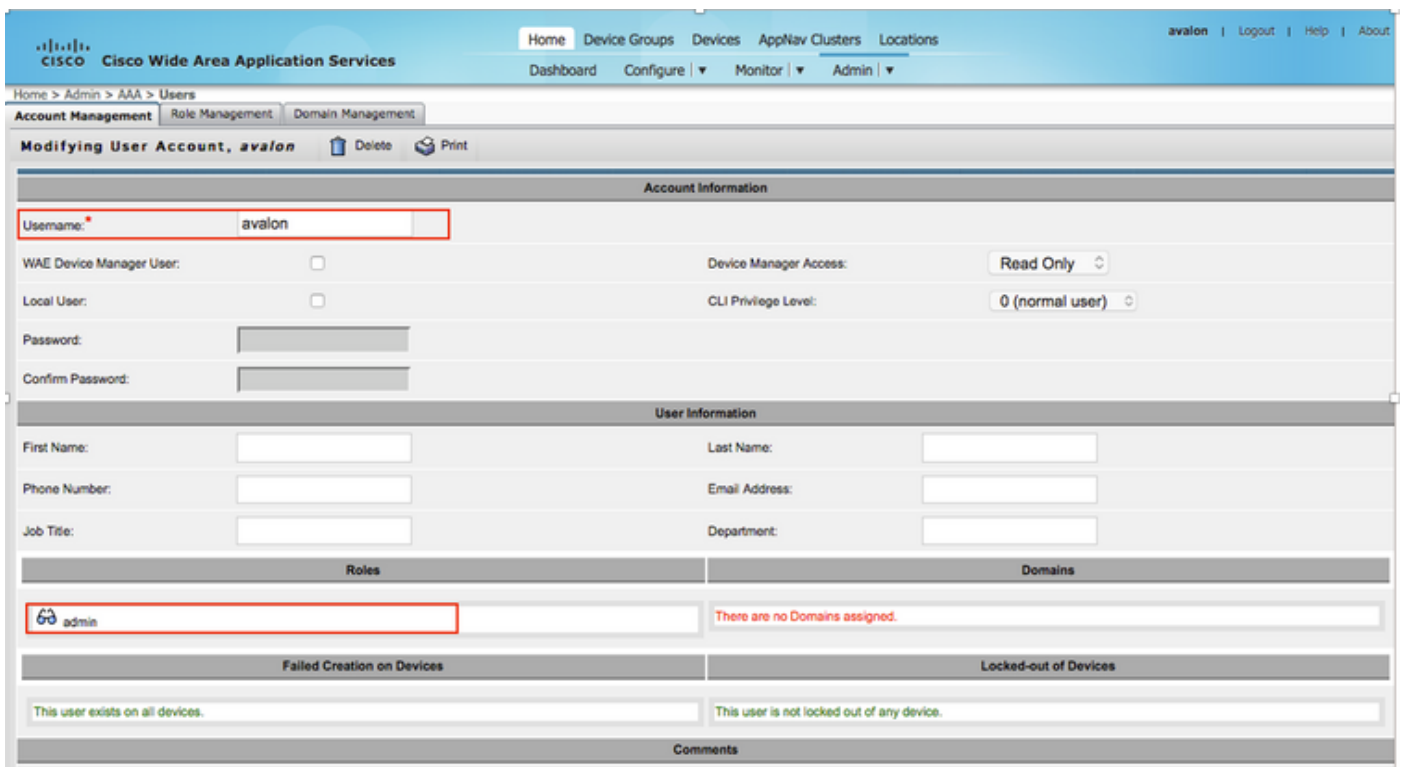
Wenn Sie einen Benutzer in RADIUS mit der Berechtigungsstufe 15 oder 1 konfigurieren, ist der Zugriff auf die grafische Benutzeroberfläche von WAAS CM nicht möglich. Die CMS-Datenbank verwaltet eine Liste von Benutzern, Rollen und Domänen, die vom externen AAA-Server getrennt sind.

Nach der korrekten Konfiguration des externen AAA-Servers für die Benutzerauthentifizierung muss die CM-GUI so konfiguriert werden, dass diesem Benutzer die Rollen und Domänen zugewiesen werden, die für die Arbeit in der CM-GUI erforderlich sind.

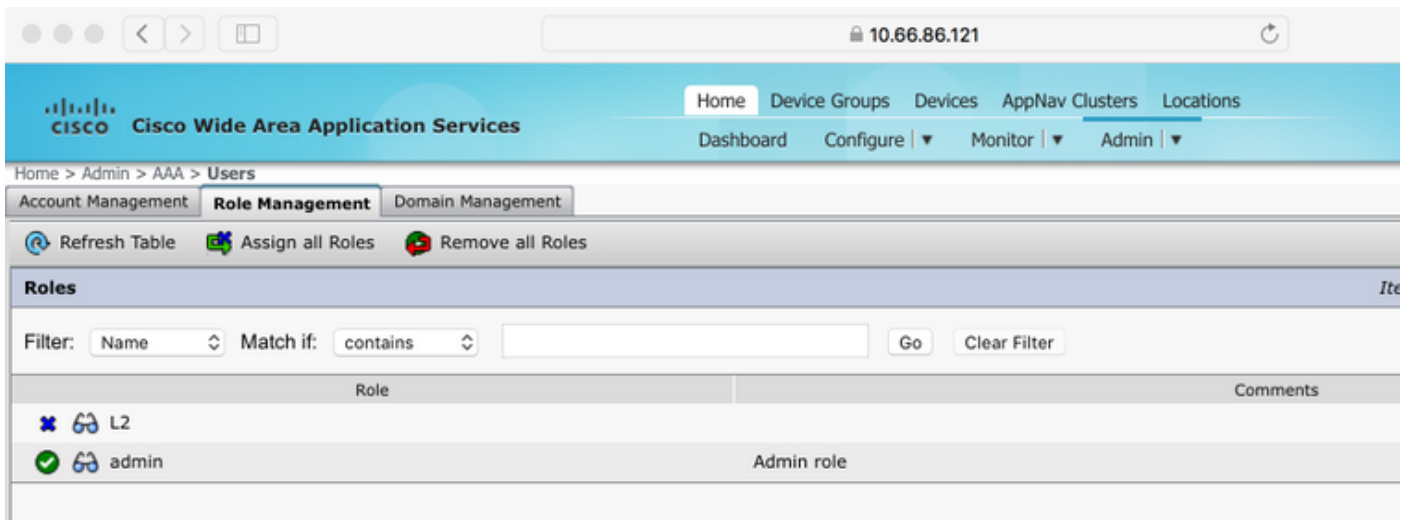
Wenn sich der RADIUS-Benutzer nicht im CM unter dem Benutzer befindet, **hat Ihr Konto keine Berechtigungen für den Zugriff auf eine der Seiten des zentralen Managers, wenn Sie sich bei diesem Benutzer in der GUI anmelden.** Bitte erkundigen Sie sich bei Ihrem Administrator nach den bereitgestellten Rollen und Domänen. Diese Message wird angezeigt.



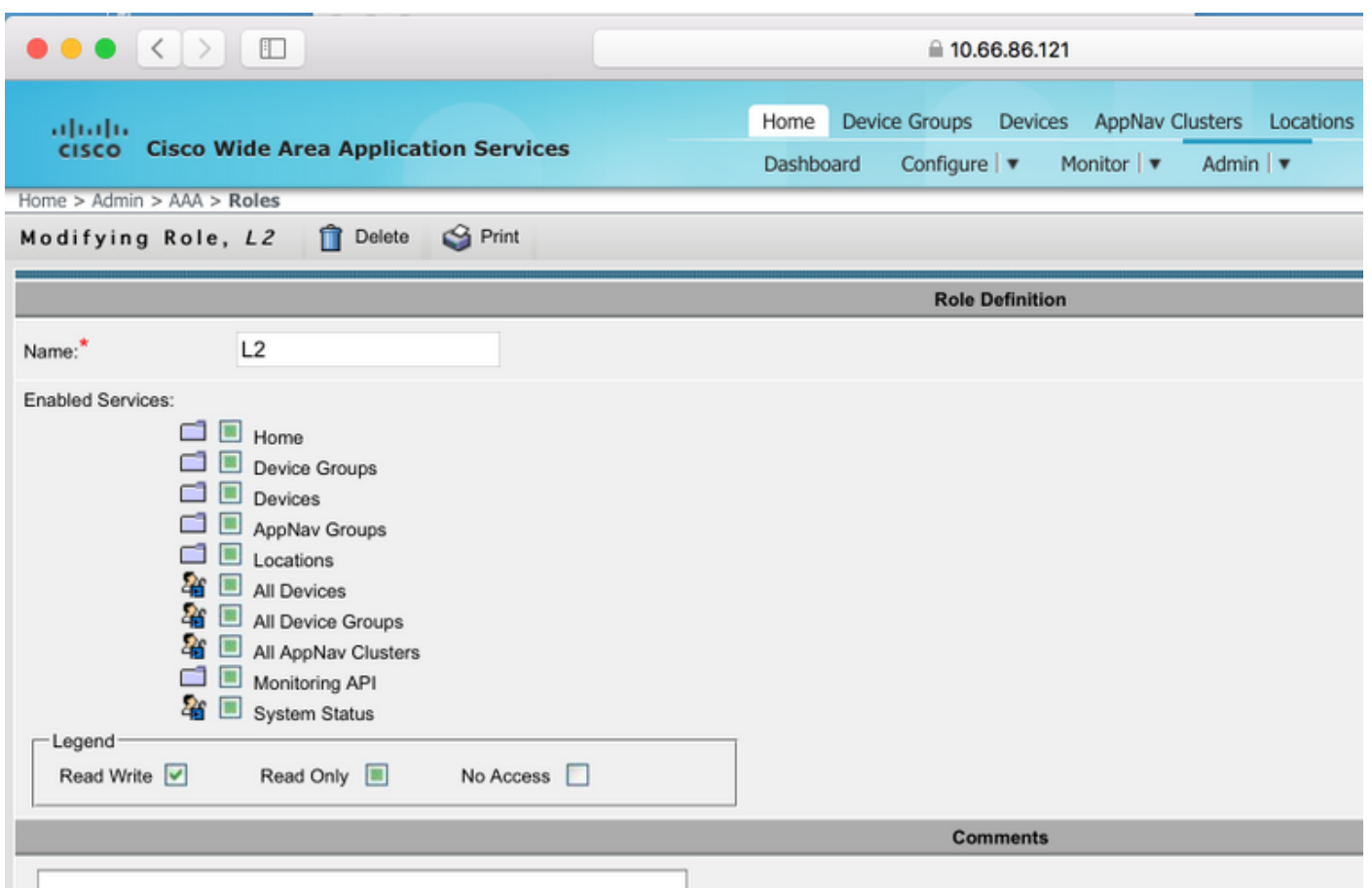
Konfiguration eines lokalen Benutzernamens unter WAAS CM ohne Kennwort.



Benutzername muss für jeden Benutzer mit den richtigen Rollen unter Rollenverwaltung verknüpft werden.



Wenn der Benutzer nur Lesezugriff oder eingeschränkten Zugriff benötigt, kann dies unter Rollen konfiguriert werden.



Überprüfung

Auf den WAAS-Geräten wird diese Konfiguration weitergeleitet.

Radius-Server-Schlüssel ****

RADIUS-Server-Host 10,66,86.125 Authentifizierungsport 1645

!

Authentifizierung Anmeldung lokal aktivieren sekundäre

Authentifizierungs-Anmelderadius aktiviert primär

Authentifizierung Konfiguration lokal aktivieren sekundäre

Authentifizierungskonfigurationsradius enable primary
Authentifizierung nicht erreichbar über Server

Der [Cisco CLI Analyzer](#) (nur [registrierte](#) Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie den Cisco CLI Analyzer, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

- **Authentifizierung:** Authentifizierung konfigurieren

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- Überprüfen Sie die Windows-Domänenprotokolle
- **#debugaa-Autorisierung** von der WAAS CM-CLI

Zugehörige Informationen

- [Konfigurieren der Authentifizierungseinstellungen des RADIUS-Servers in WAAS](#)
- [Network Policy Server gilt für Windows Server 2008](#)