配置Windows 2008 NPS伺服器的RADIUS - WAAS AAA

目錄

簡介

本檔案介紹在Cisco廣域應用程式服務(WAAS)和Windows 2008 R2網路原則伺服器(NPS)上設定遠端驗證撥入使用者服務(RADIUS)的程式。

預設WAAS配置使用本地身份驗證。Cisco WAAS還支援RADIUS和終端訪問控制器訪問控制系統(TACACS+)進行身份驗證、授權和記帳(AAA)。 本文檔僅介紹一台裝置的配置。但是，這也可以在裝置組下完成。所有配置必須通過WAAS CM GUI應用。

一般WAAS AAA配置在Cisco廣域應用服務配置指南配置管理登入身份驗證、授權和記帳一章下提供。

作者：Hamilan Gnanabaskaran，思科TAC工程師。

由Cisco TAC工程師Sanaz Tayyar編輯。

必要條件

需求

思科建議您瞭解以下主題：

- WAAS 5.x或6.x
- Windows NPS伺服器
- AAA - RADIUS

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從預設組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

相關產品

本檔案也適用於以下硬體和軟體版本：

- vWAAS、ISR-WAAS和所有WAAS裝置
- WAAS 5.x或WAAS 6.x
- WAAS作為應用程式加速器的中央管理器

附註：APPNAV-XE不支援此配置。路由器AAA將配置推送到APPNAV-XE。

配置步驟

需要應用以下配置：

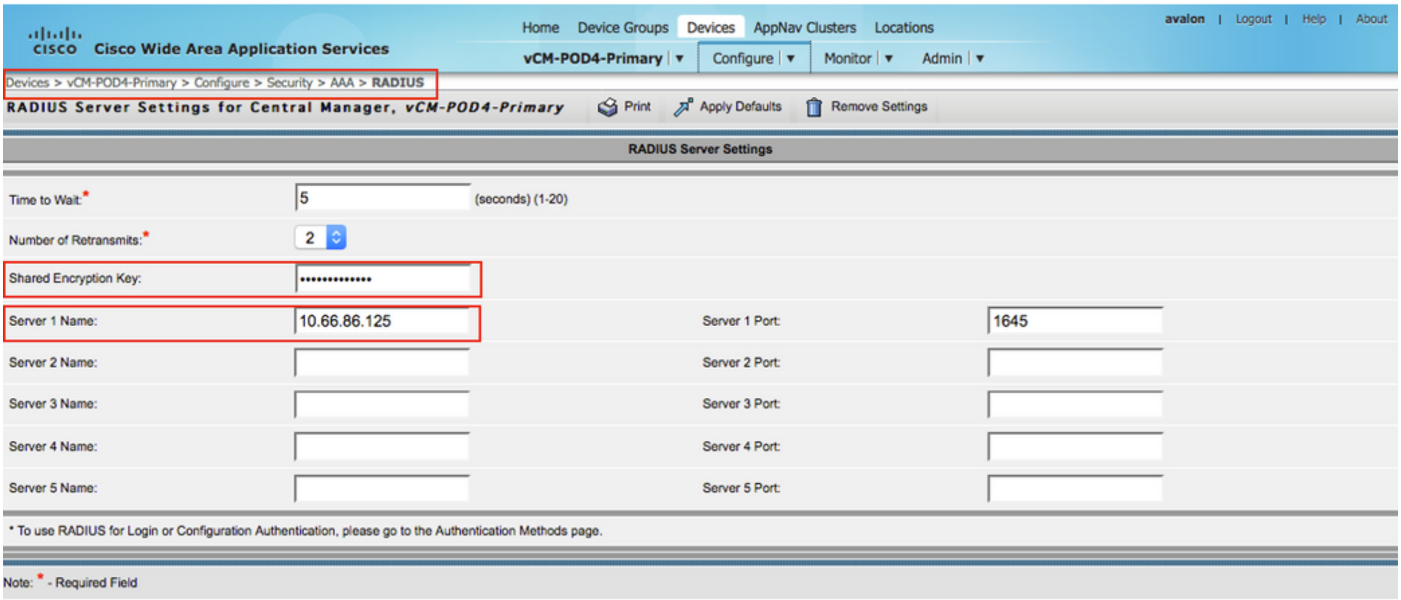
1. WAAS中央管理器
 1.1 AAA RADIUS配置
 1.2 AAA身份驗證配置

2. Windows 2008 R2 - NPS伺服器配置
 2.1 RADIUS客戶端配置
 2.2網路策略配置

3.為RADIUS使用者帳戶配置WAAS CM

1. WAAS中央管理器

1.1在WAAS Central manager中，在**Configure>Security>AAA>RADIUS**下建立RADIUS伺服器。



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

RADIUS Server Settings for Central Manager, *vCM-POD4-Primary*

RADIUS Server Settings

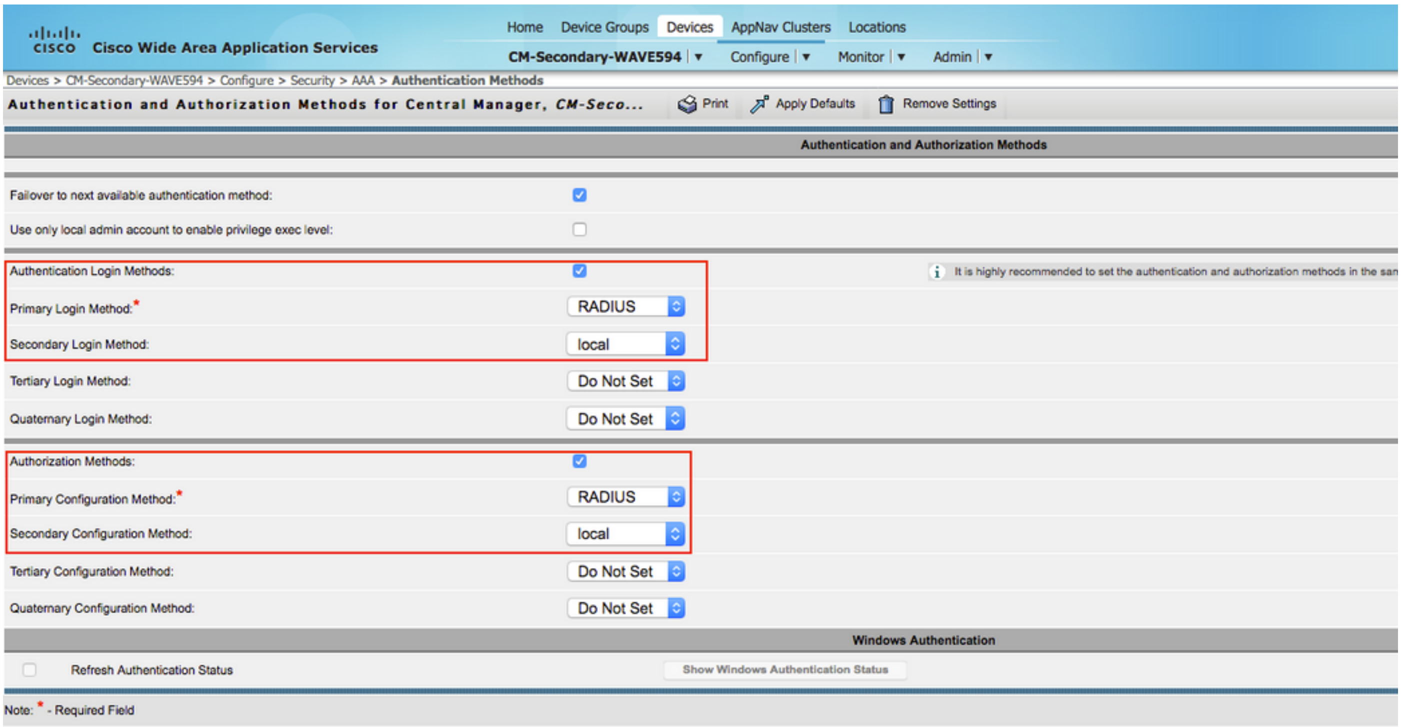
Time to Wait:*	5	(seconds) (1-20)	
Number of Retransmits:*	2		
Shared Encryption Key:	•••••••••••••		
Server 1 Name:	10.66.86.125	Server 1 Port:	1645
Server 2 Name:		Server 2 Port:	
Server 3 Name:		Server 3 Port:	
Server 4 Name:		Server 4 Port:	
Server 5 Name:		Server 5 Port:	

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

Note: * - Required Field

1.2在**Configure>Security>AAA>Authentication Methods**下**配置身份驗證方法以反映RADIUS。**

選擇主要身份驗證方法作為RADIUS，選擇輔助身份驗證方法作為本地。因此，發生RADIUS故障時，客戶可透過本機帳戶登入。



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

Authentication and Authorization Methods for Central Manager, *CM-Seco...*

Authentication and Authorization Methods

Failover to next available authentication method:	☑
Use only local admin account to enable privilege exec level:	□
Authentication Login Methods:	☑
Primary Login Method:*	RADIUS
Secondary Login Method:	local
Tertiary Login Method:	Do Not Set
Quaternary Login Method:	Do Not Set
Authorization Methods:	☑
Primary Configuration Method:*	RADIUS
Secondary Configuration Method:	local
Tertiary Configuration Method:	Do Not Set
Quaternary Configuration Method:	Do Not Set

It is highly recommended to set the authentication and authorization methods in the san

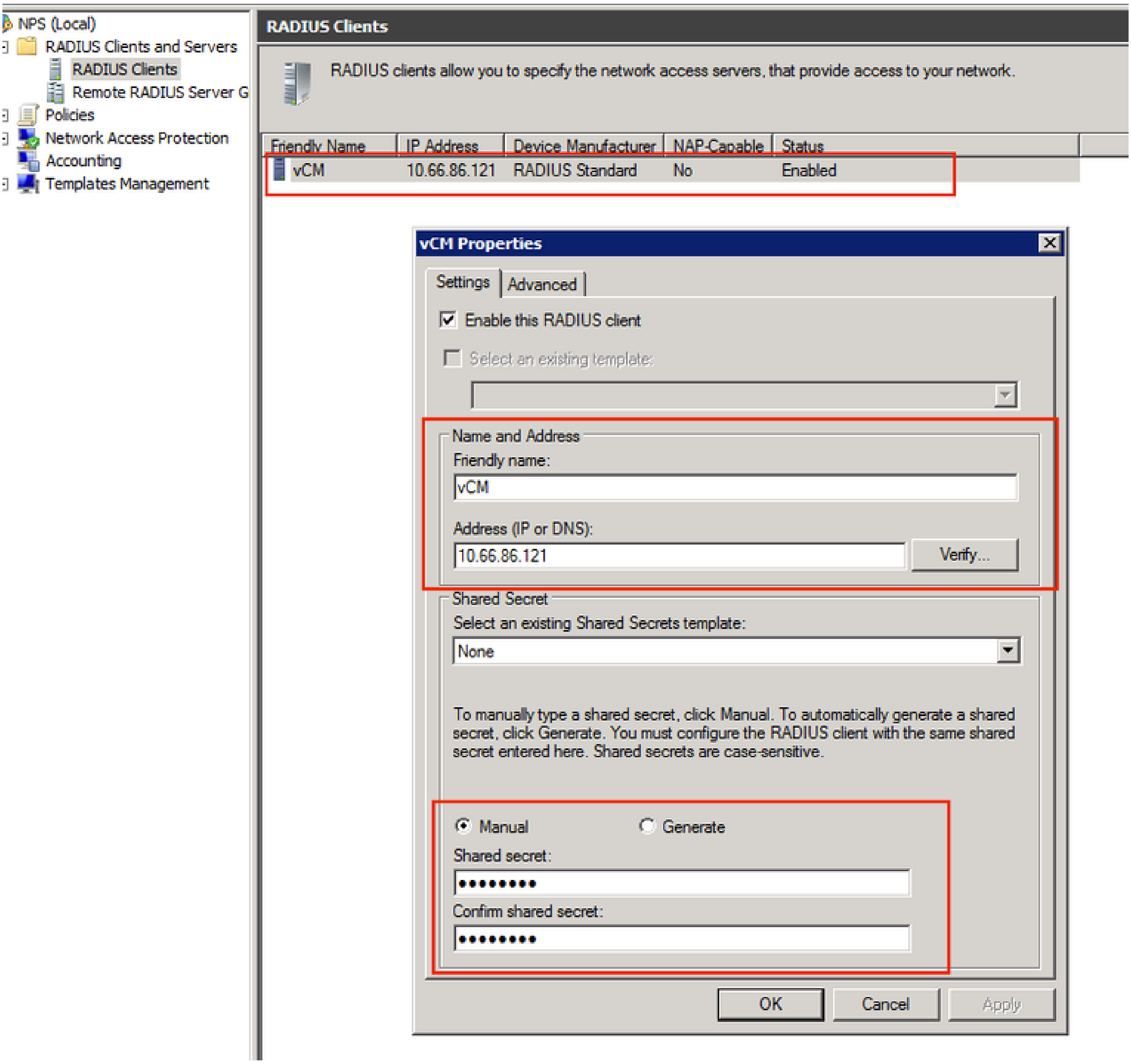
Windows Authentication

□ Refresh Authentication Status

Note: * - Required Field

2. Windows 2008 R2 -NPS伺服器配置

2.1在Windows 2008 R2 - NPS伺服器中，建立WAAS裝置IP作為RADIUS客戶端。



RADIUS Clients

RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
vCM	10.66.86.121	RADIUS Standard	No	Enabled

vCM Properties

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: vCM

Address (IP or DNS): 10.66.86.121

Shared Secret

Select an existing Shared Secrets template: None

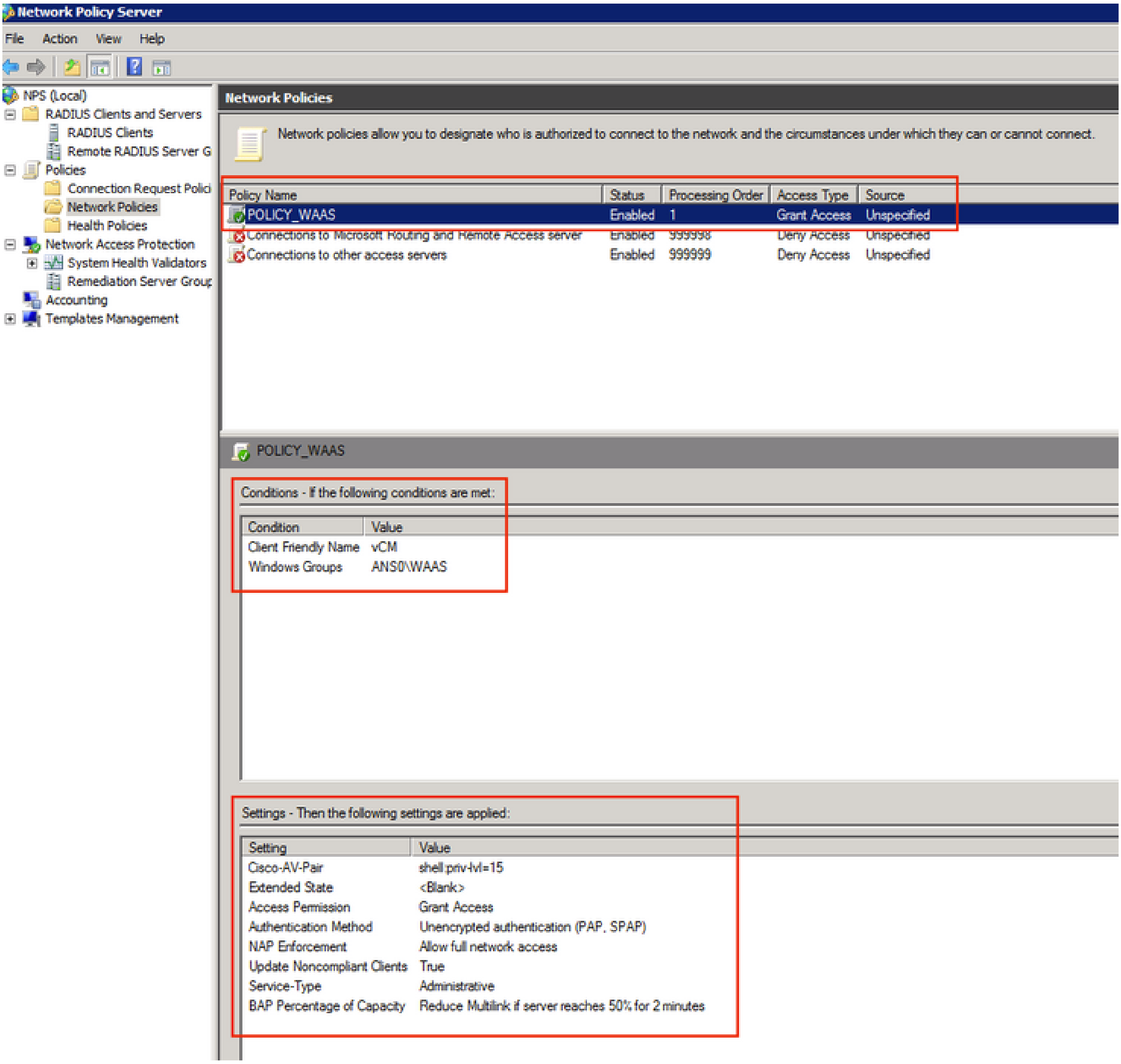
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••

Confirm shared secret: ••••••••

2.2在Windows 2008 R2 - NPS伺服器中，建立與WAAS裝置匹配的網路策略並允許身份驗證。



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

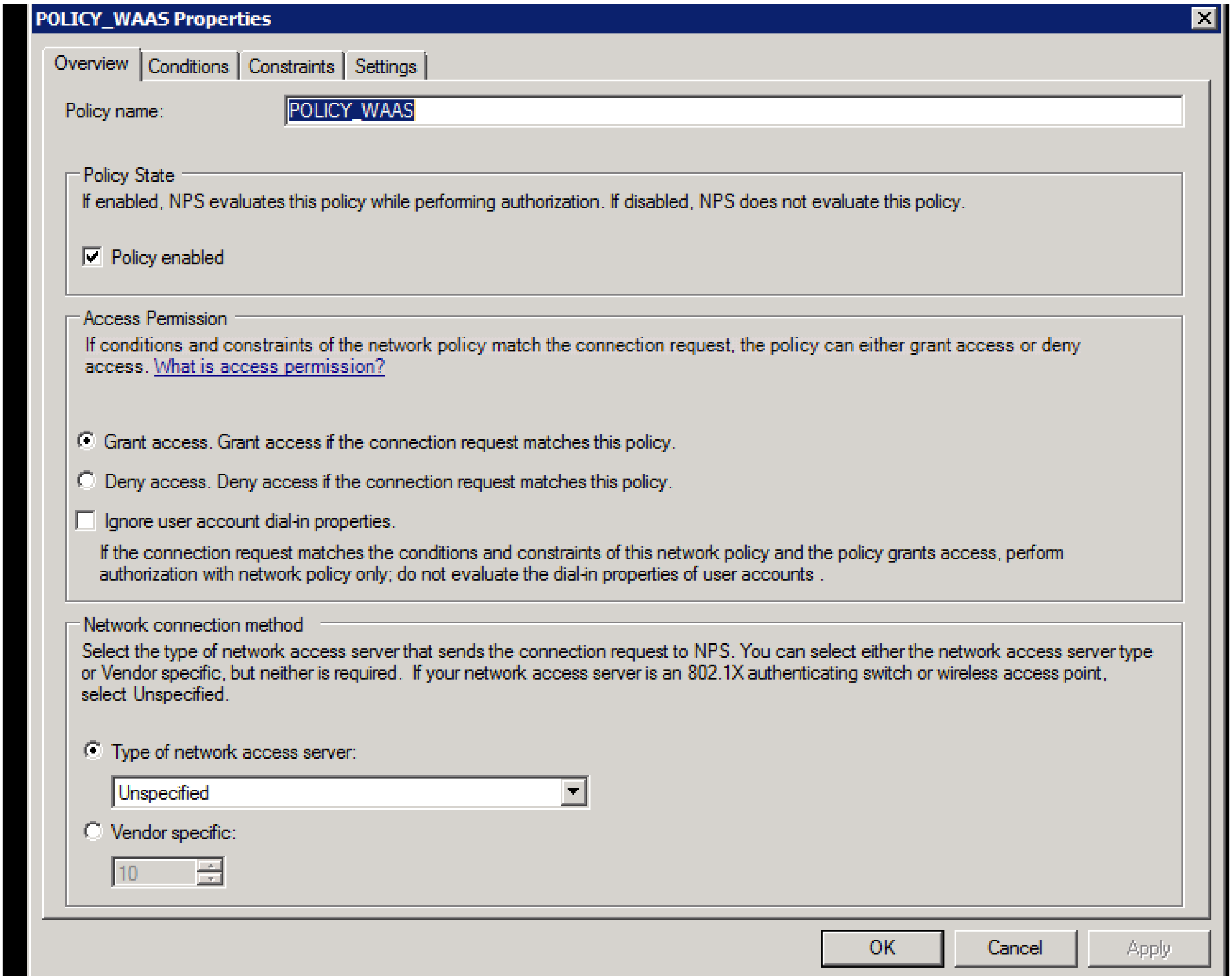
Conditions - If the following conditions are met:

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

在實驗室中，必須在NPS >Policies>Network Policy下選擇這些引數。



POLICY_WAAS Properties

Policy name: POLICY_WAAS

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.

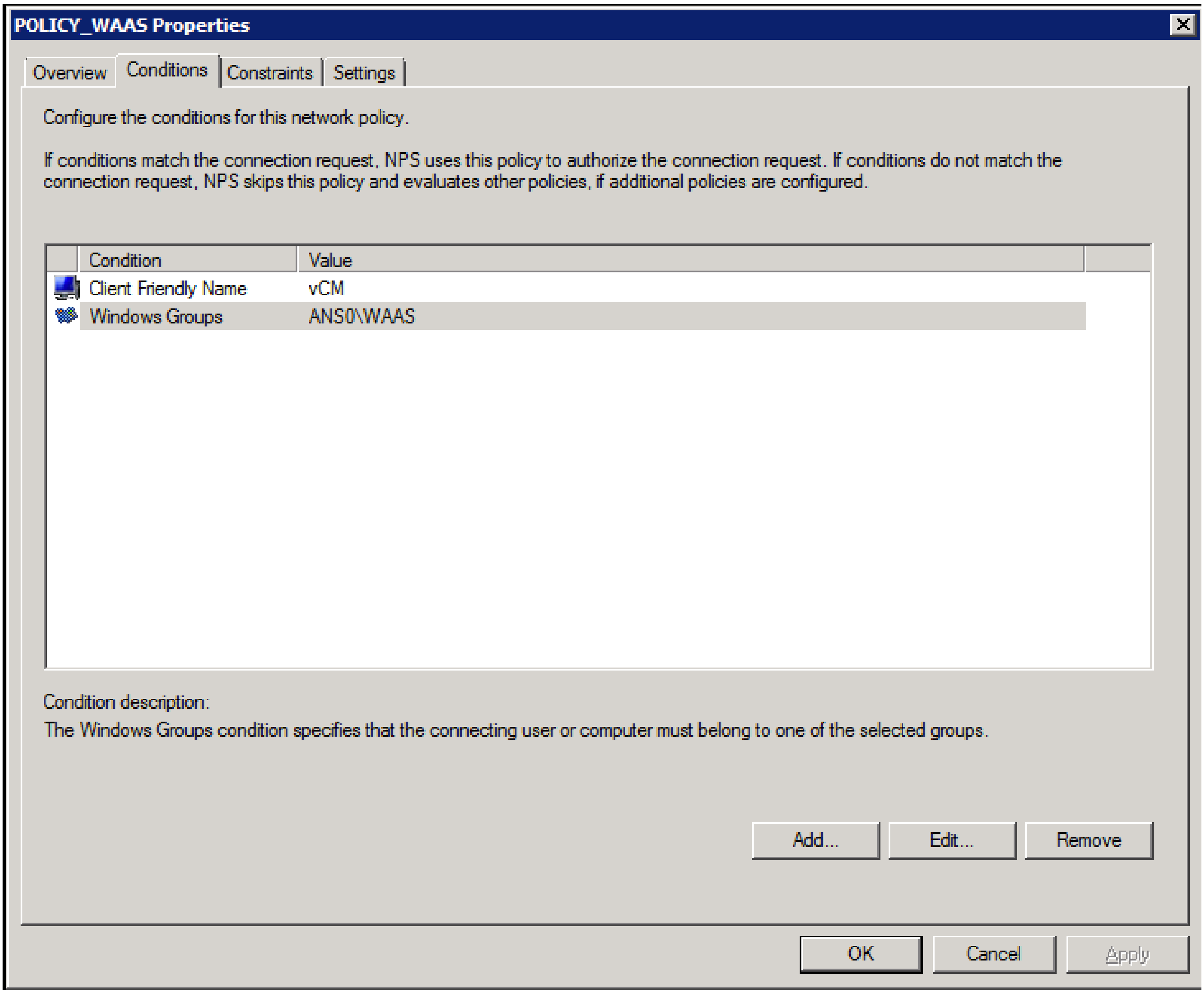
● Type of network access server:

Unspecified

○ Vendor specific:

10

條件可以與Radius使用者端友好名稱相匹配。也可以使用其它方法，例如IP地址。



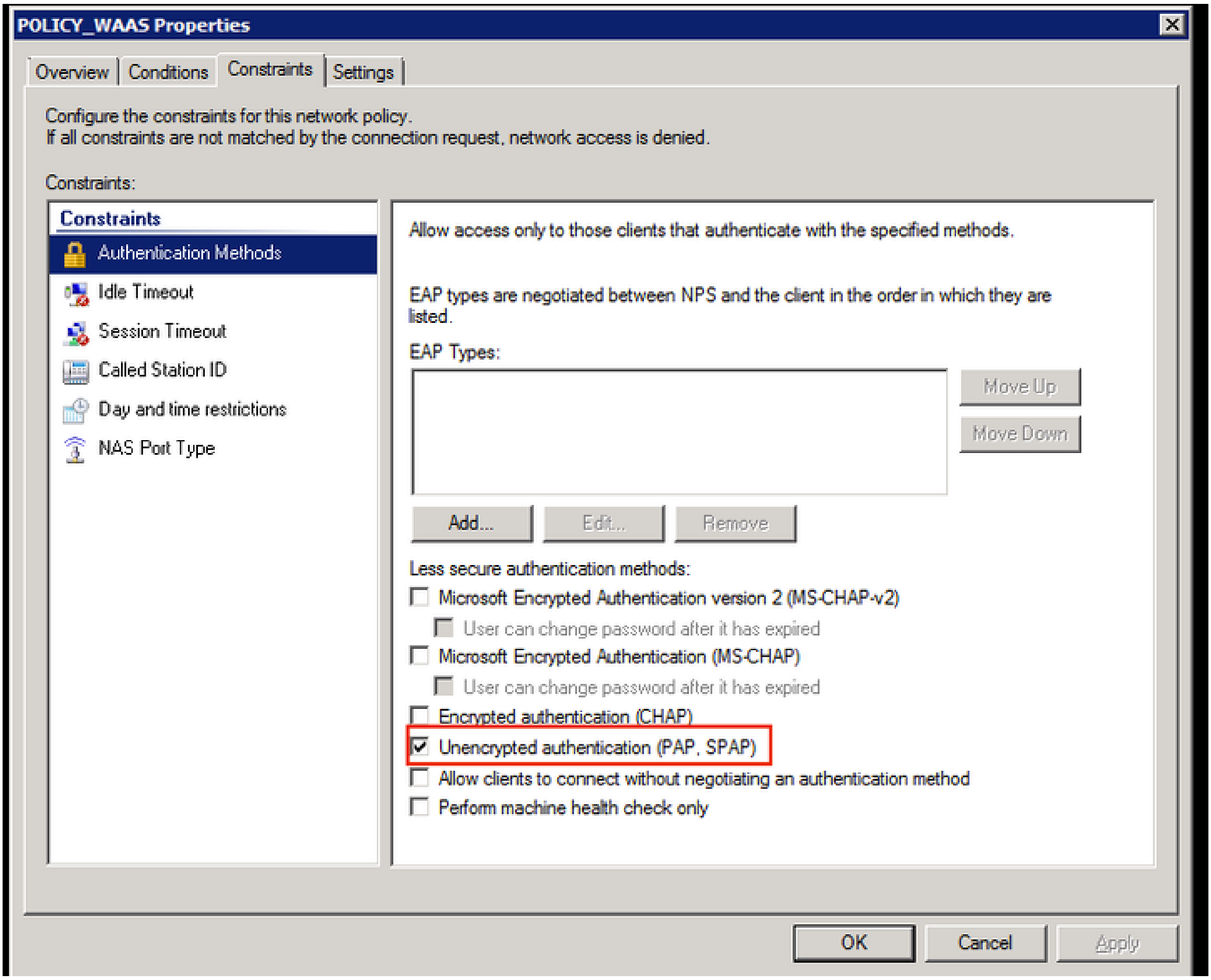
Configure the conditions for this network policy.

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
Client Friendly Name	vCM
Windows Groups	ANS0\WAAS

Condition description:
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

驗證方法為非加密驗證(PAP、SPAP)。



POLICY_WAAS Properties

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Allow access only to those clients that authenticate with the specified methods.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

☐ User can change password after it has expired

☐ Microsoft Encrypted Authentication (MS-CHAP)

☐ User can change password after it has expired

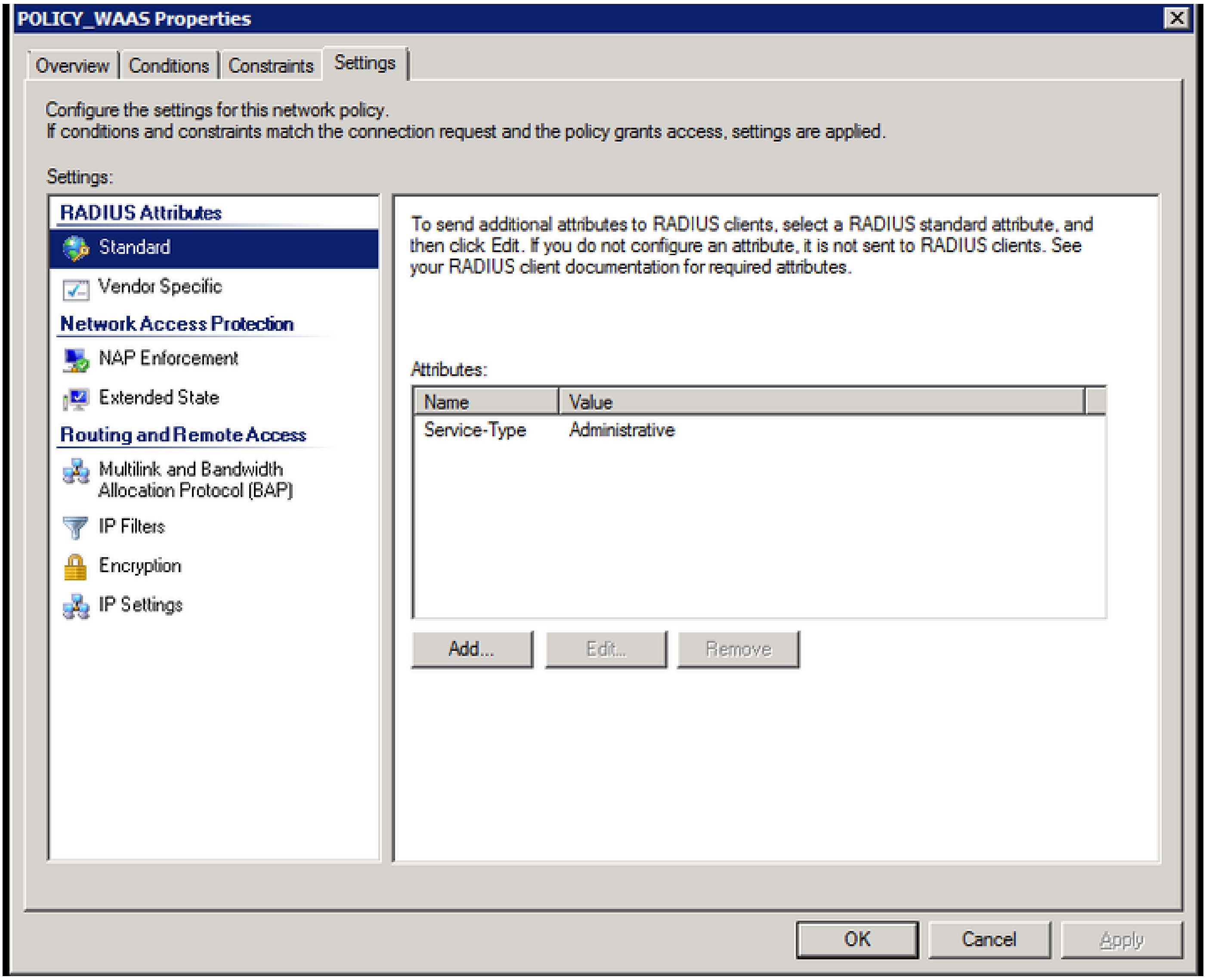
☐ Encrypted authentication (CHAP)

☑ Unencrypted authentication (PAP, SPAP)

☐ Allow clients to connect without negotiating an authentication method

☐ Perform machine health check only

Service-Type（管理）。



POLICY_WAAS Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

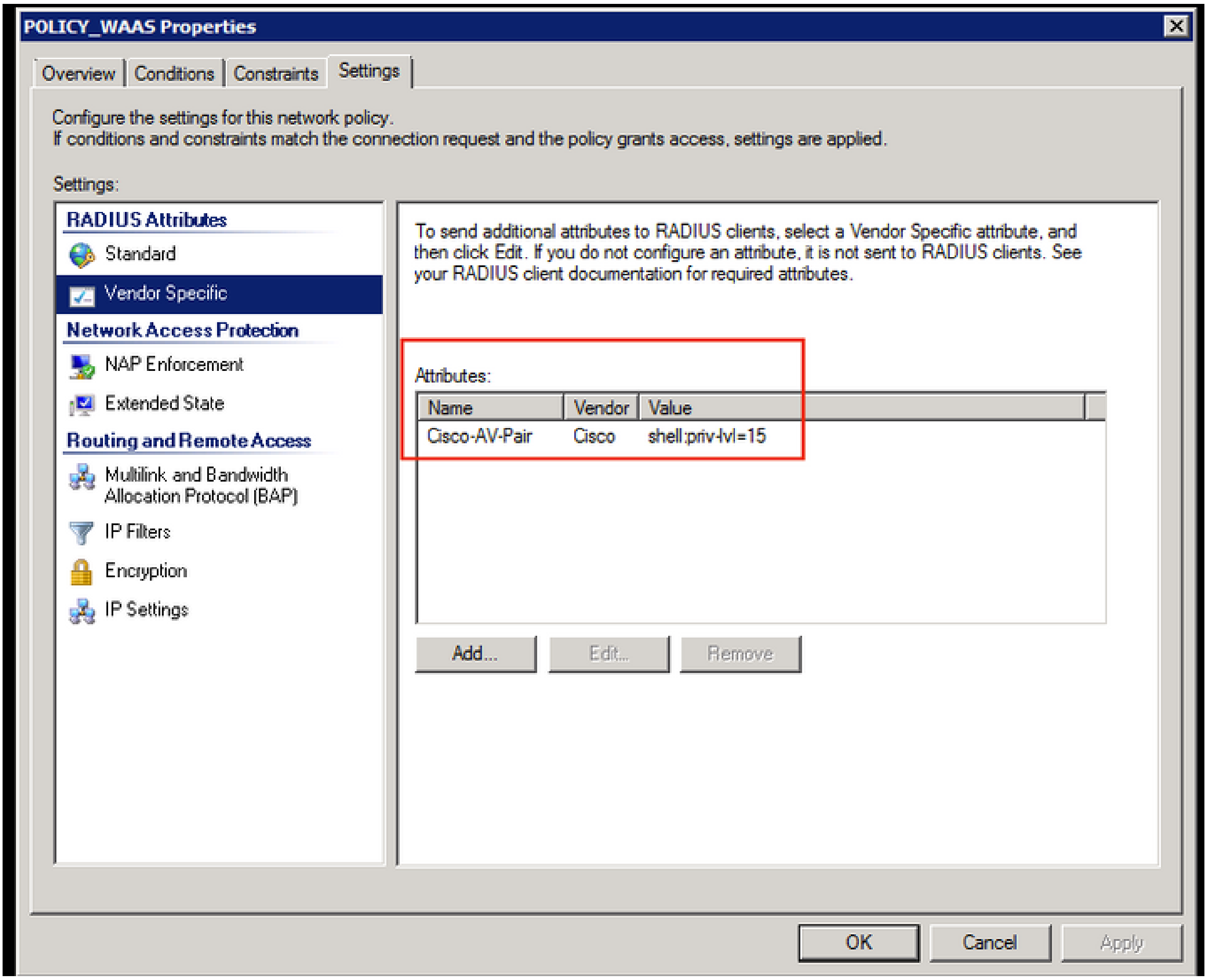
Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Service-Type	Administrative

Cisco-AV-Pair形式的供應商特定屬性(Shell:priv-lvl=15)。



POLICY_WAAS Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

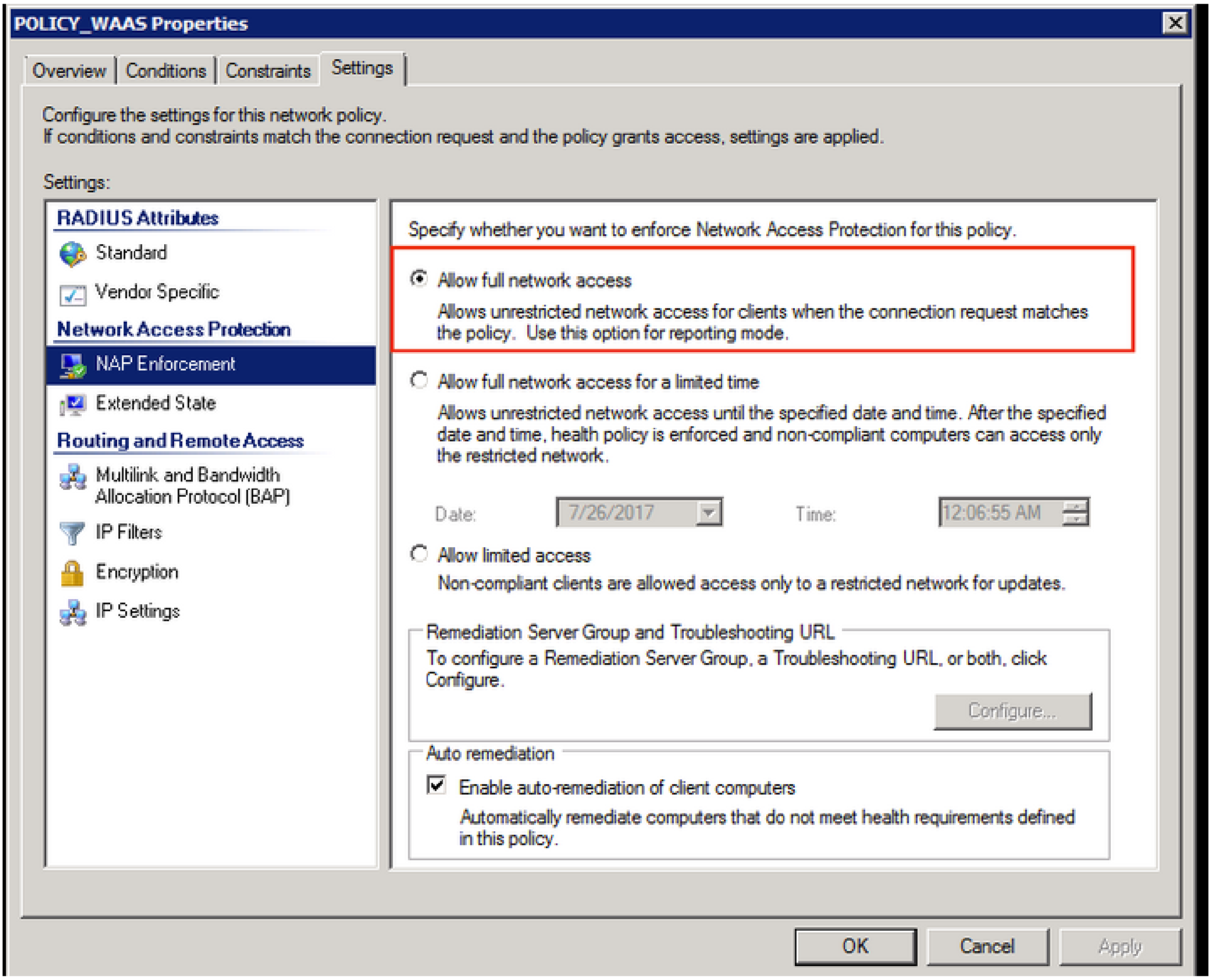
Settings:

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Cisco-AV-Pair	Cisco	shell:priv-lvl=15

允許完全網路訪問。



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

Specify whether you want to enforce Network Access Protection for this policy.

● Allow full network access

Allows unrestricted network access for clients when the connection request matches the policy. Use this option for reporting mode.

○ Allow full network access for a limited time

Allows unrestricted network access until the specified date and time. After the specified date and time, health policy is enforced and non-compliant computers can access only the restricted network.

Date: 7/26/2017 Time: 12:06:55 AM

○ Allow limited access

Non-compliant clients are allowed access only to a restricted network for updates.

Remediation Server Group and Troubleshooting URL

To configure a Remediation Server Group, a Troubleshooting URL, or both, click Configure.

Auto remediation

☑ Enable auto-remediation of client computers

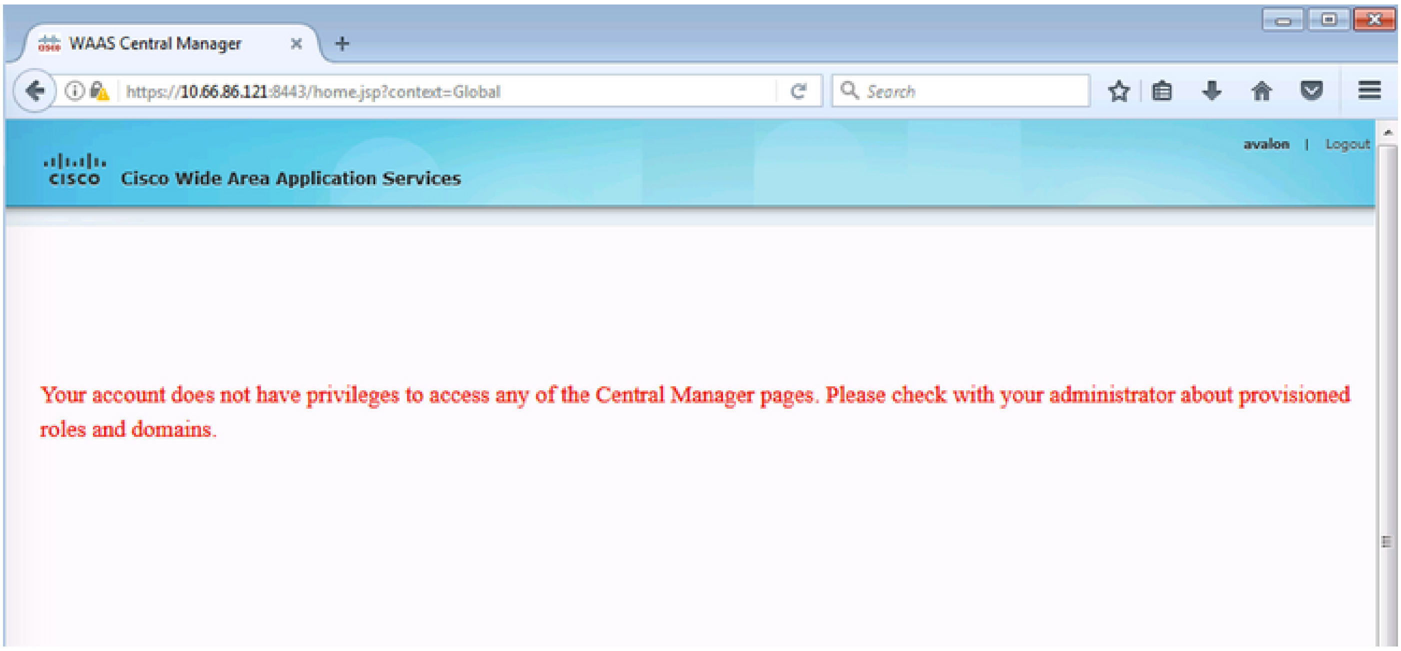
Automatically remediate computers that do not meet health requirements defined in this policy.

3.為RADIUS使用者帳戶配置WAAS CM

在RADIUS中為使用者配置許可權級別15或1，不提供對WAAS CM GUI的訪問。CMS資料庫維護獨立於外部AAA伺服器的使用者、角色和域清單。

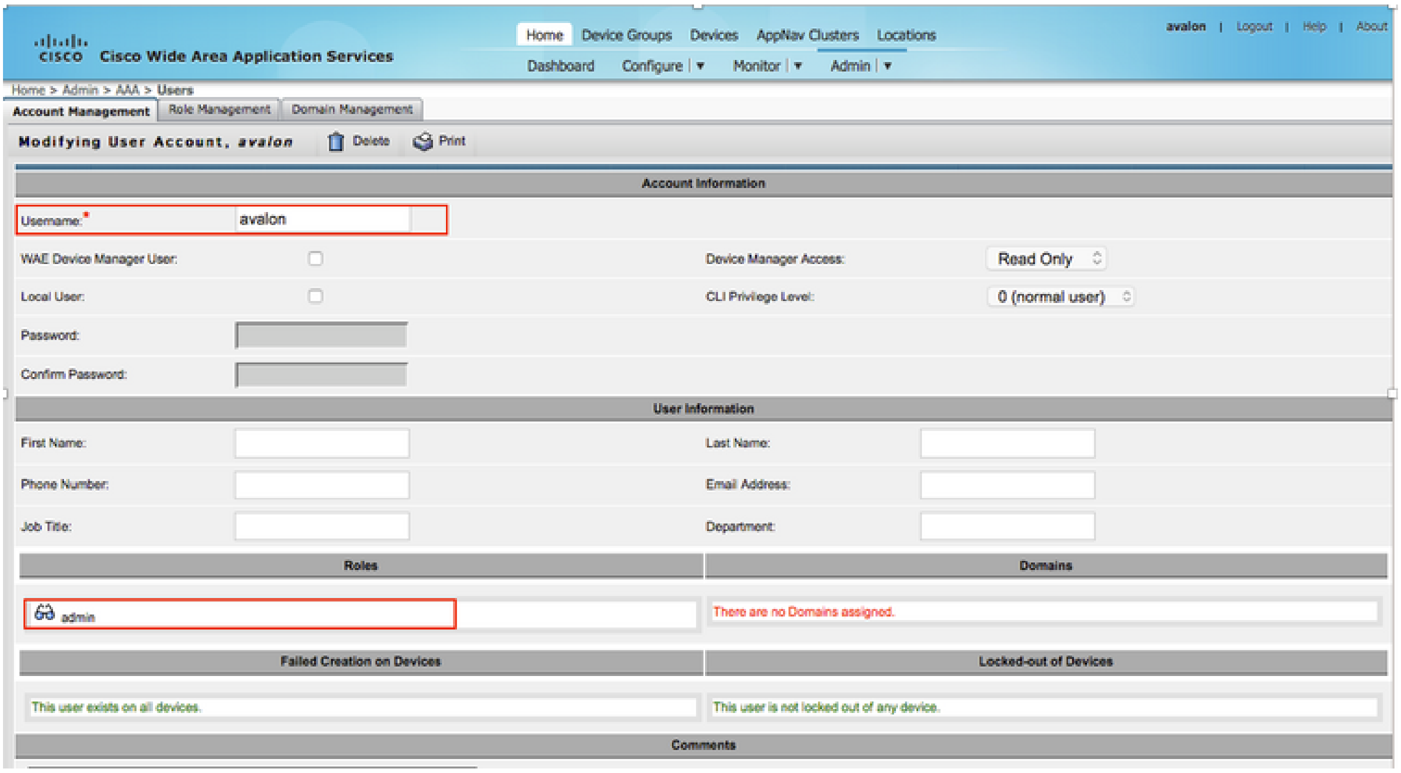
在對外部AAA伺服器進行正確配置以驗證使用者之後，必須配置CM GUI，以便為使用者在CM GUI中工作提供必要的角色和域。

如果RADIUS使用者不在CM under user下，則使用該使用者登入GUI時，您的帳戶沒有訪問任何**Central Manager頁面的許可權。請向您的管理員諮詢已設定的角色和域**。將顯示此消息。


WAAS Central Manager
https://10.66.86.121:8443/home.jsp?context=Global
Search
Cisco Wide Area Application Services
avalon | Logout

Your account does not have privileges to access any of the Central Manager pages. Please check with your administrator about provisioned roles and domains.

在WAAS CM下配置本地使用者名稱，無需密碼。



Modifying User Account, avalon

Account Information

Username:*	avalon		
WAE Device Manager User:	□	Device Manager Access:	Read Only
Local User:	□	CLI Privilege Level:	0 (normal user)
Password:			
Confirm Password:			

User Information

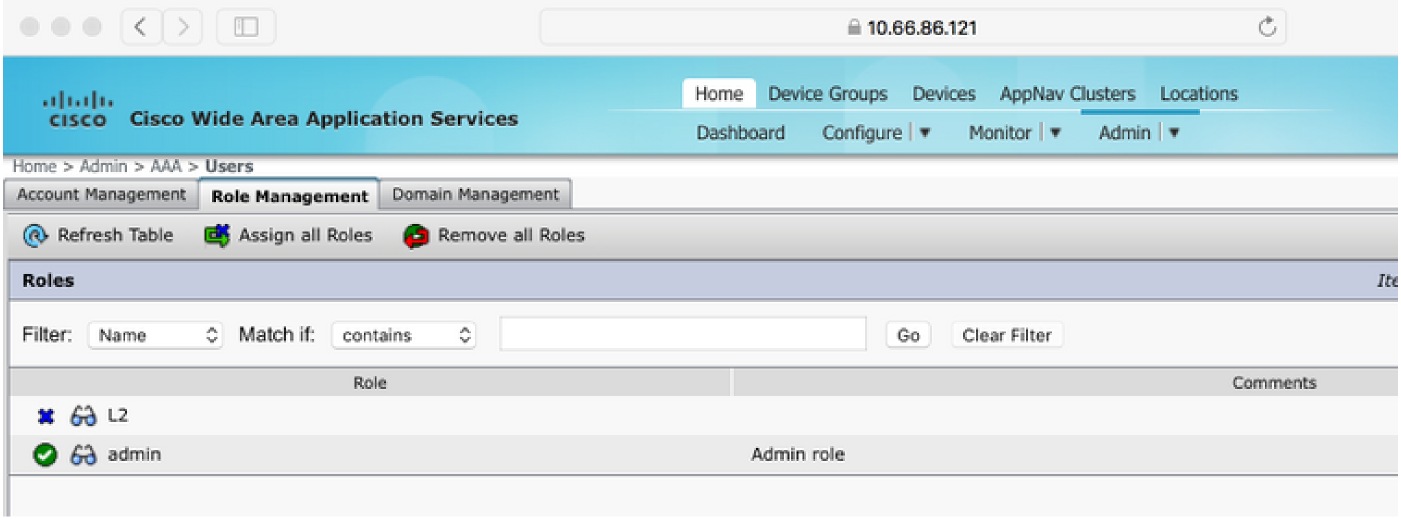
First Name:		Last Name:	
Phone Number:		Email Address:	
Job Title:		Department:	

Roles	Domains
admin	There are no Domains assigned.

Failed Creation on Devices	Locked-out of Devices
This user exists on all devices.	This user is not locked out of any device.

Comments

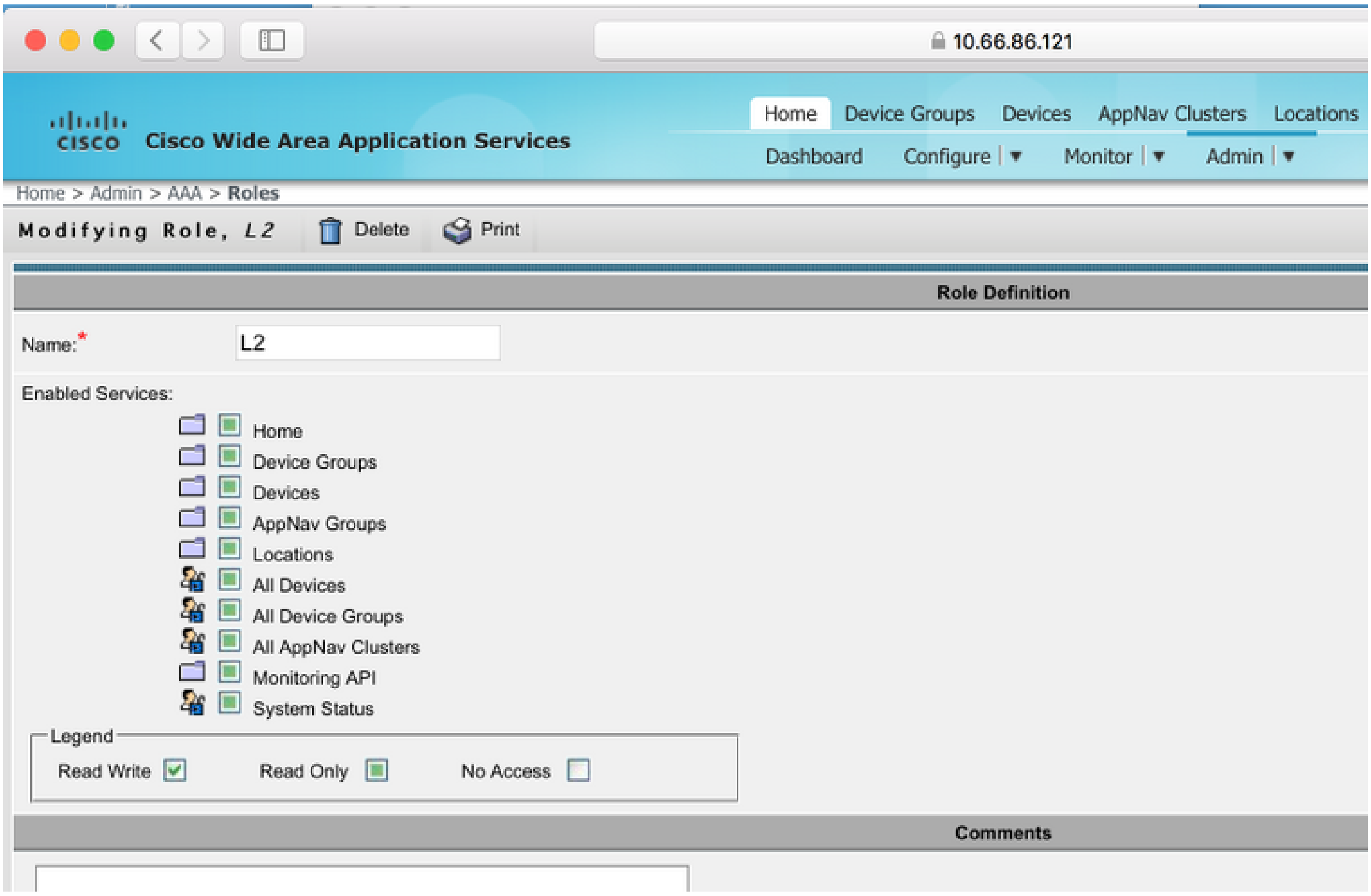
對於每個使用者，使用者名稱必須與角色管理下的正確角色繫結。



Filter: Name Match if: contains Go Clear Filter

Role	Comments
L2	
admin	Admin role

如果使用者需要具有只讀訪問許可權或受限訪問許可權，可以在角色下配置該許可權。



Modifying Role, L2

Role Definition

Name:* L2

Enabled Services:

- 🟩 Home
- 🟩 Device Groups
- 🟩 Devices
- 🟩 AppNav Groups
- 🟩 Locations
- 🟩 All Devices
- 🟩 All Device Groups
- 🟩 All AppNav Clusters
- 🟩 Monitoring API
- 🟩 System Status

Legend
Read Write ☑ Read Only 🟩 No Access □

Comments

驗證

在WAAS裝置中推送此配置。

```
radius-server key ****
radius-server host 10.66.86.125 auth-port 1645
!
authentication login local enable secondary
驗證登入radius enable primary
身份驗證配置local enable secondary
身份驗證配置radius enable primary
```

身份驗證故障轉移伺服器無法訪問

Cisco CLI Analyzer（僅供已註冊客戶使用）支援某些 **show 指令。**使用 Cisco CLI Analyzer 檢視 show 指令輸出的分析。

- **authentication** — 配置身份驗證

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

- 檢查Windows域日誌
- #**debug aaa authorization** from WAAS CM CLI

相關資訊

- 在WAAS上配置RADIUS伺服器身份驗證設定
- 網路策略伺服器適用於Windows Server 2008