通過Microsoft NPS對AireOS WLC的管理訪問

目錄

簡介

本文說明如何通過Microsoft網路策略伺服器(NPS)為AireOS WLC GUI和CLI配置管理訪問。

必要條件

需求

思科建議您瞭解以下主題：

- 無線安全解決方案知識
- AAA和RADIUS概念
- Microsoft Server 2012基礎知識
- 安裝Microsoft NPS和Active Directory(AD)

採用元件

本文檔中提供的資訊基於以下軟體和硬體元件。

- 8.8.120.0上的AireOS控制器(5520)
- Microsoft Server 2012

附註：本文旨在為讀者提供在Microsoft伺服器上進行WLC管理訪問所需的配置示例。本文檔中介紹的Microsoft Windows伺服器配置已在實驗室中經過測試，發現可以按預期工作。如果配置有問題，請與Microsoft聯絡以獲得幫助。思科技術支援中心(TAC)不支援Microsoft Windows伺服器配置。Microsoft Windows 2012安裝及設定指南可在Microsoft Tech Net上找到。

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已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

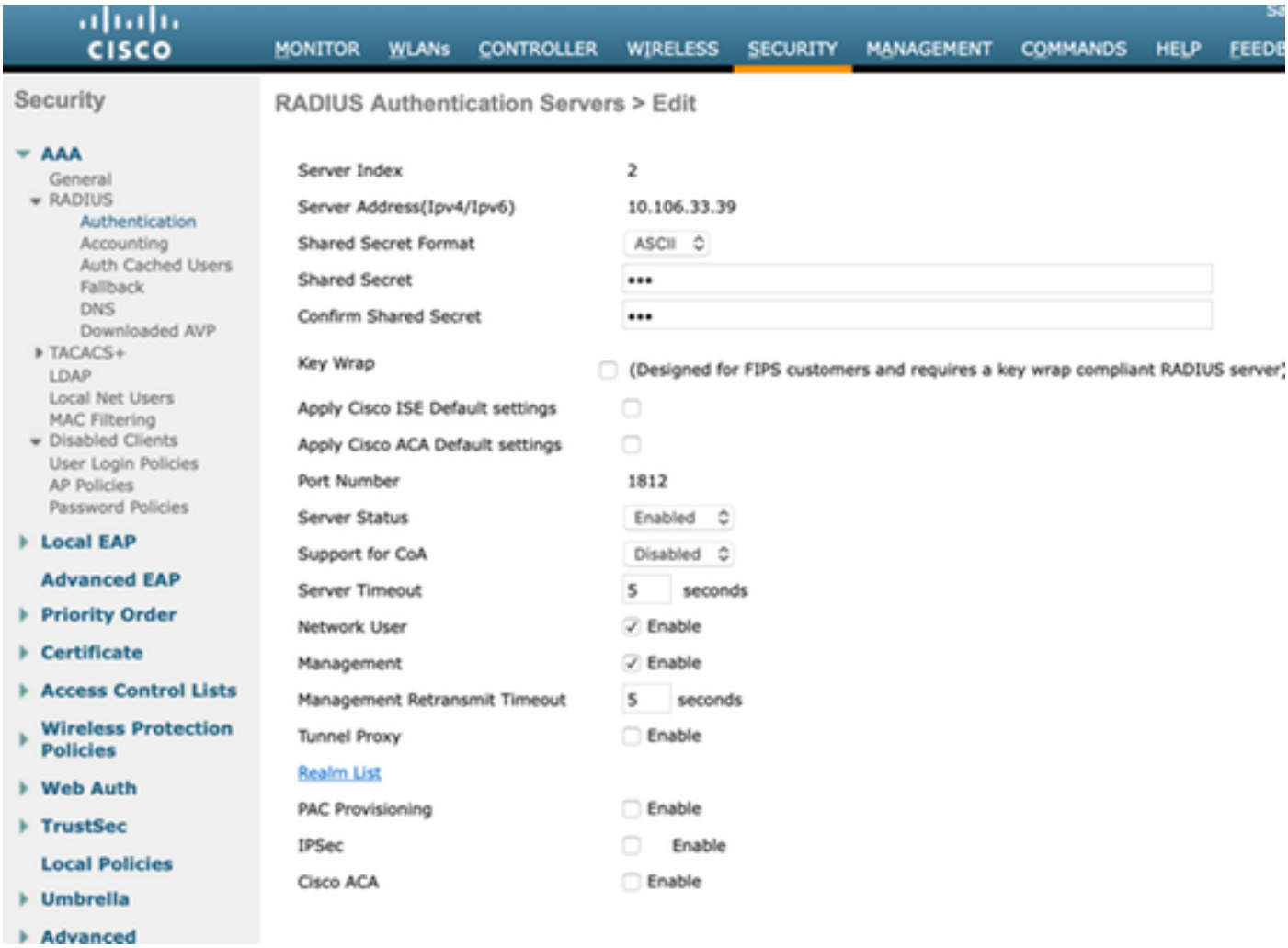
訪問WLC CLI/GUI時，系統會提示使用者輸入憑證以成功登入。可以針對本地資料庫或外部AAA伺服器驗證憑證。在本文檔中，Microsoft NPS用作外部身份驗證伺服器。

組態

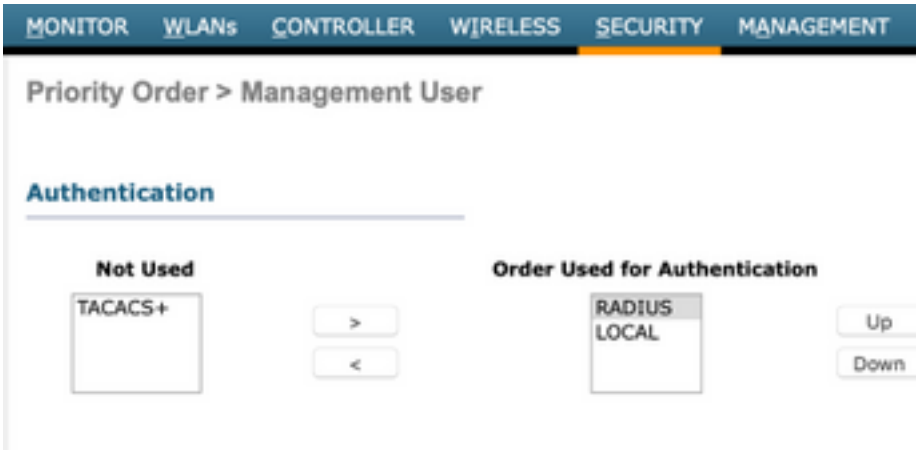
在本範例中，在AAA(NPS)上設定兩個使用者，即**loginuser**和**adminuser**。**loginuser**只有只讀訪問許可權，而adminuser**獲得完**整訪問許可權。

WLC組態

步驟1.在控制器上新增RADIUS伺服器。導覽至**Security > RADIUS > Authentication**。按一下**New**新增伺服器。確保啟用了**management**選項，以便此伺服器可用於管理訪問，如下圖所示。



步驟2.定位至**安全性>優先順序順序>管理使用者**。確保RADIUS被選為其中一個身份驗證型別。

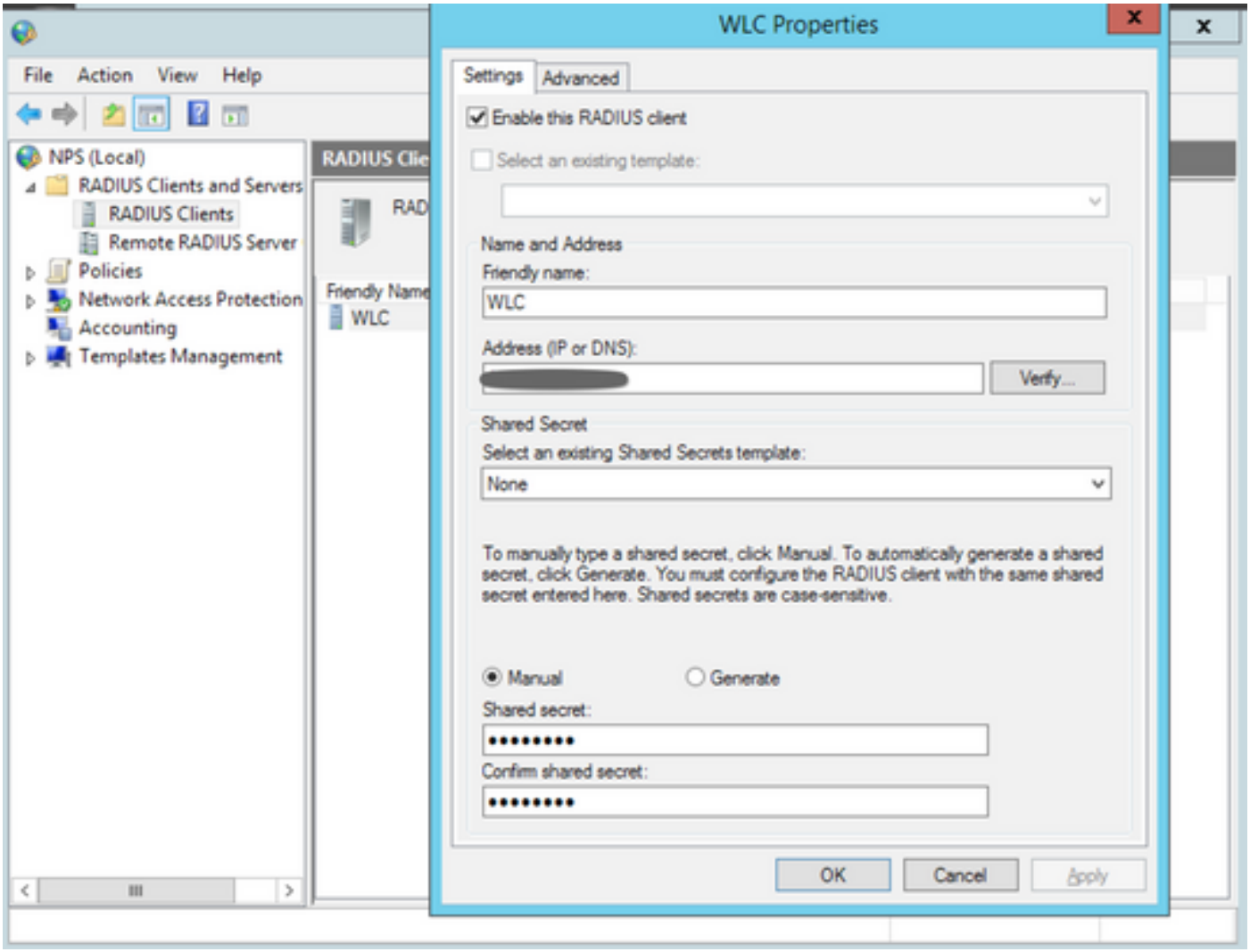


附註：如果選擇RADIUS作為身份驗證順序中的第一個優先順序，則只有在RADIUS伺服器無法訪問時，才會使用本地憑據進行身份驗證。如果選擇RADIUS作為第二個優先順序，將首先針對本地資料庫驗證RADIUS憑證，然後針對配置的RADIUS伺服器進行檢查。

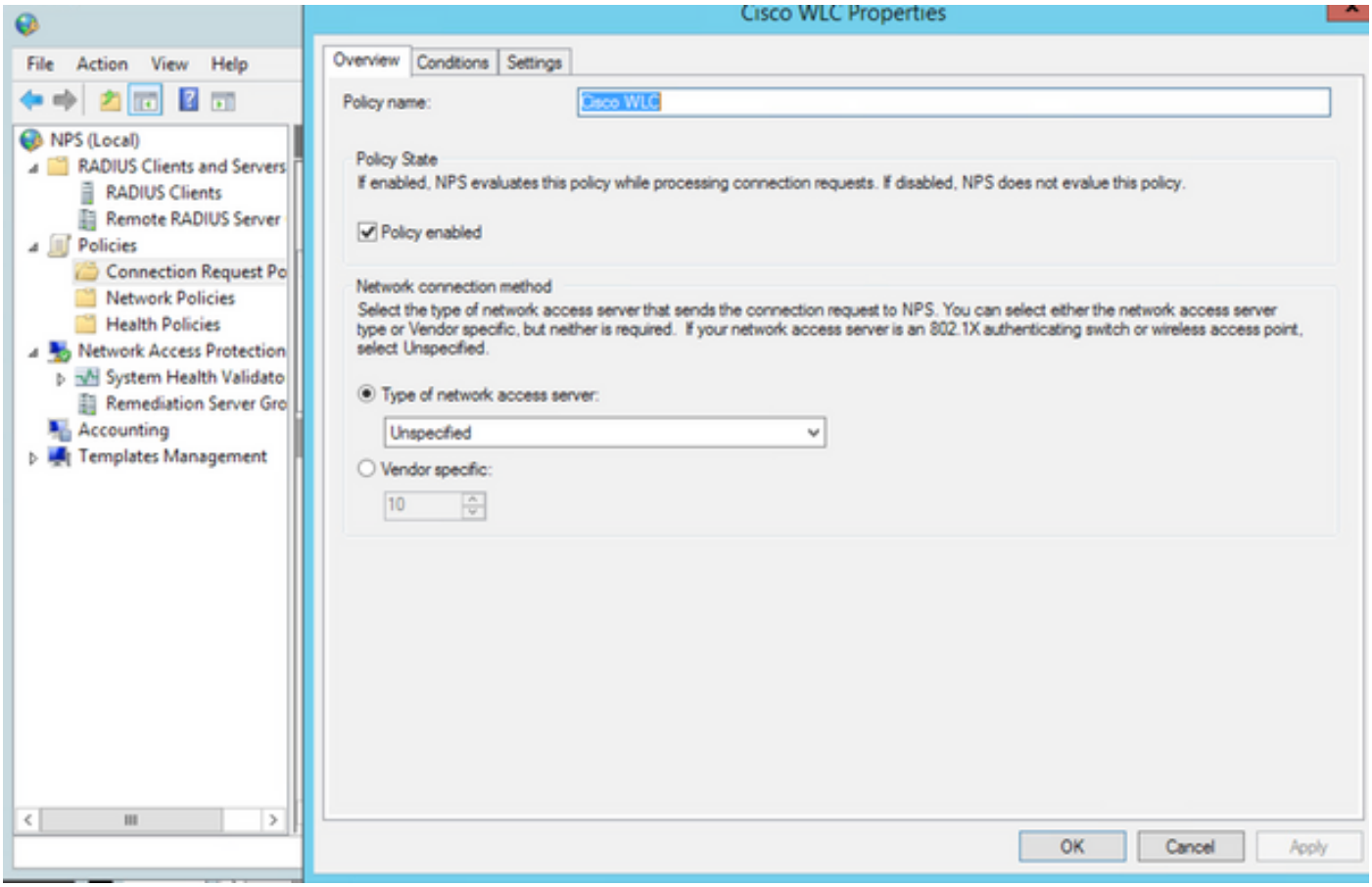
Microsoft NPS配置

步驟1.開啟Microsoft NPS伺服器。按一下右鍵**Radius Clients**。按一下「**New**」，將WLC新增為RADIUS使用者端。

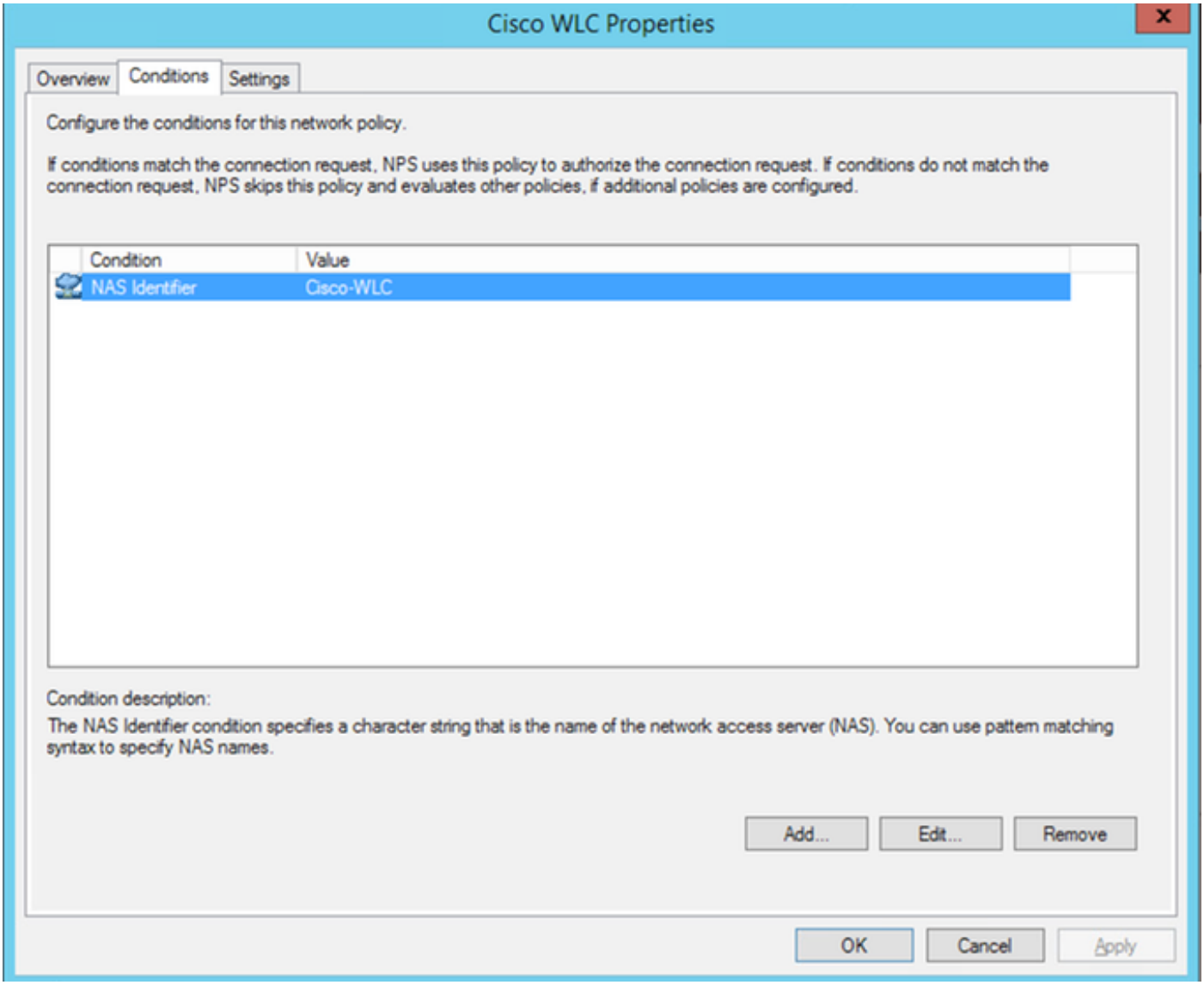
輸入所需的詳細資訊。請確認增加RADIUS伺服器時，共用密碼與控制器上設定的密碼相同。



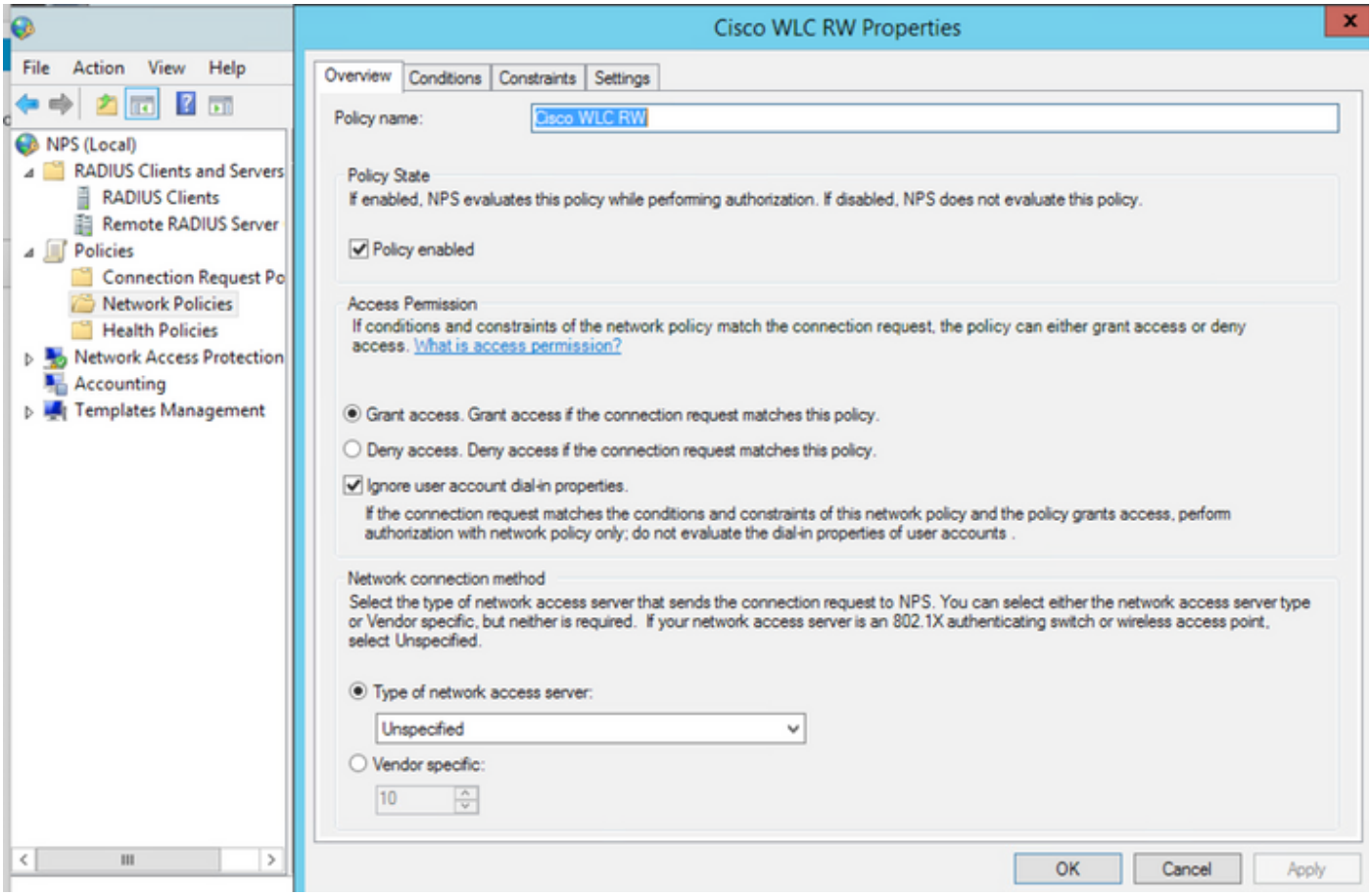
步驟2.導航到**Policies > Connection Request Policies**。按一下右鍵可新增新策略，如下圖所示。



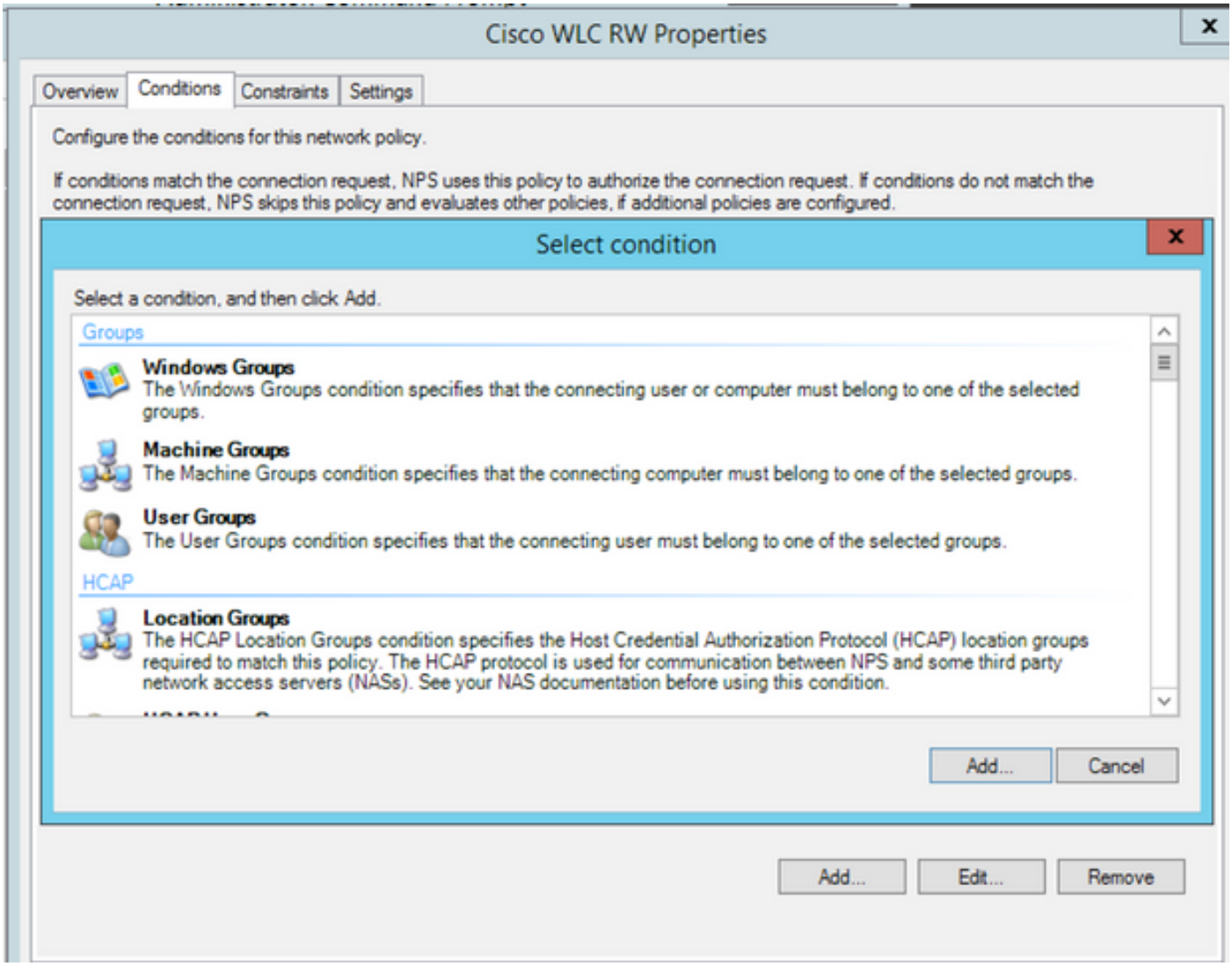
步驟3.在**Conditions**頁籤下，選擇**NAS Identifier**作為新條件。出現提示時，輸入控制器的主機名作為值，如下圖所示。



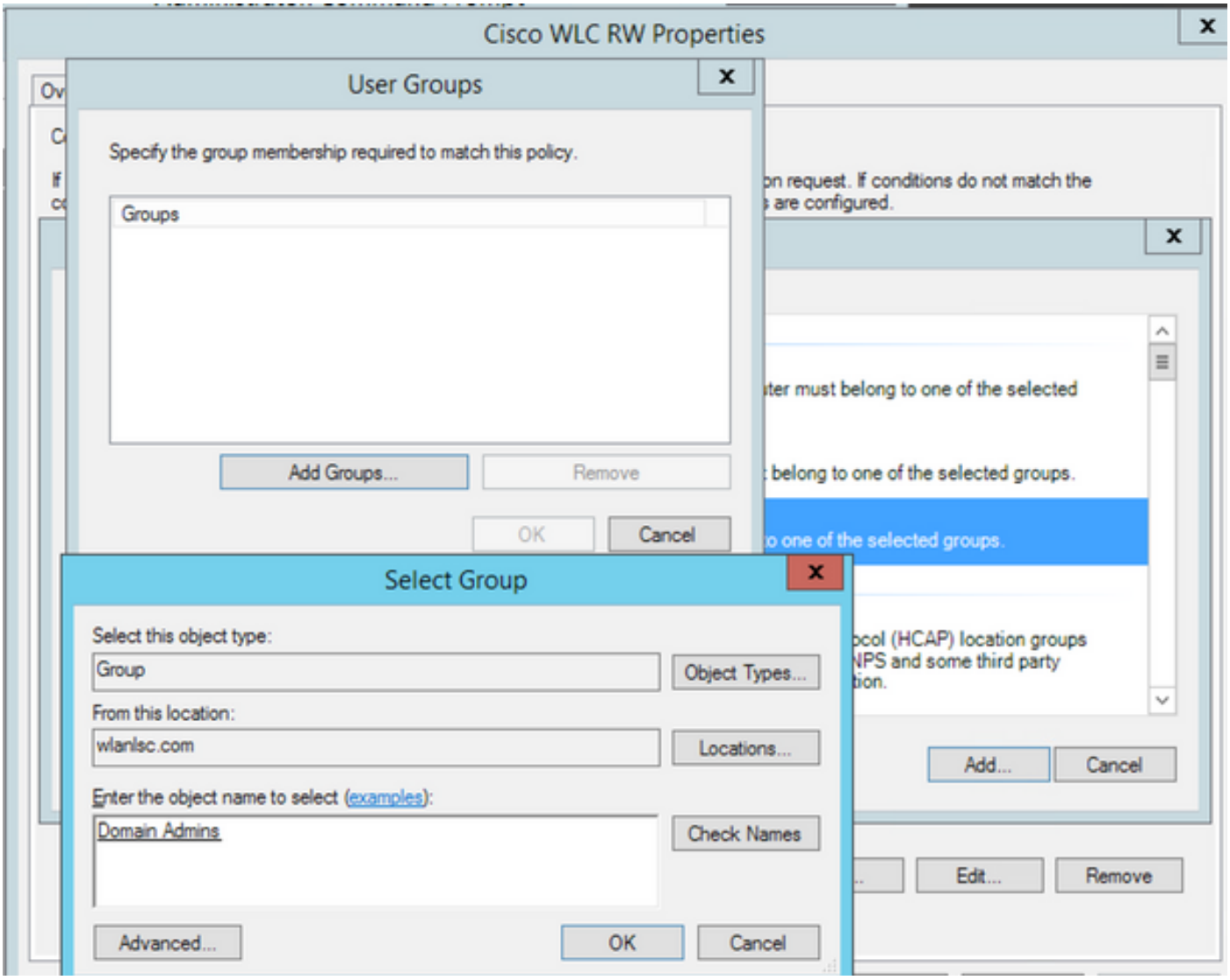
步驟4.導覽至**Policies > Network Policies**。按一下右鍵可新增新策略。在本例中，策略名稱為**Cisco WLC RW**，這表示策略用於提供完全（讀取/寫入）訪問許可權。確保策略配置如圖所示。



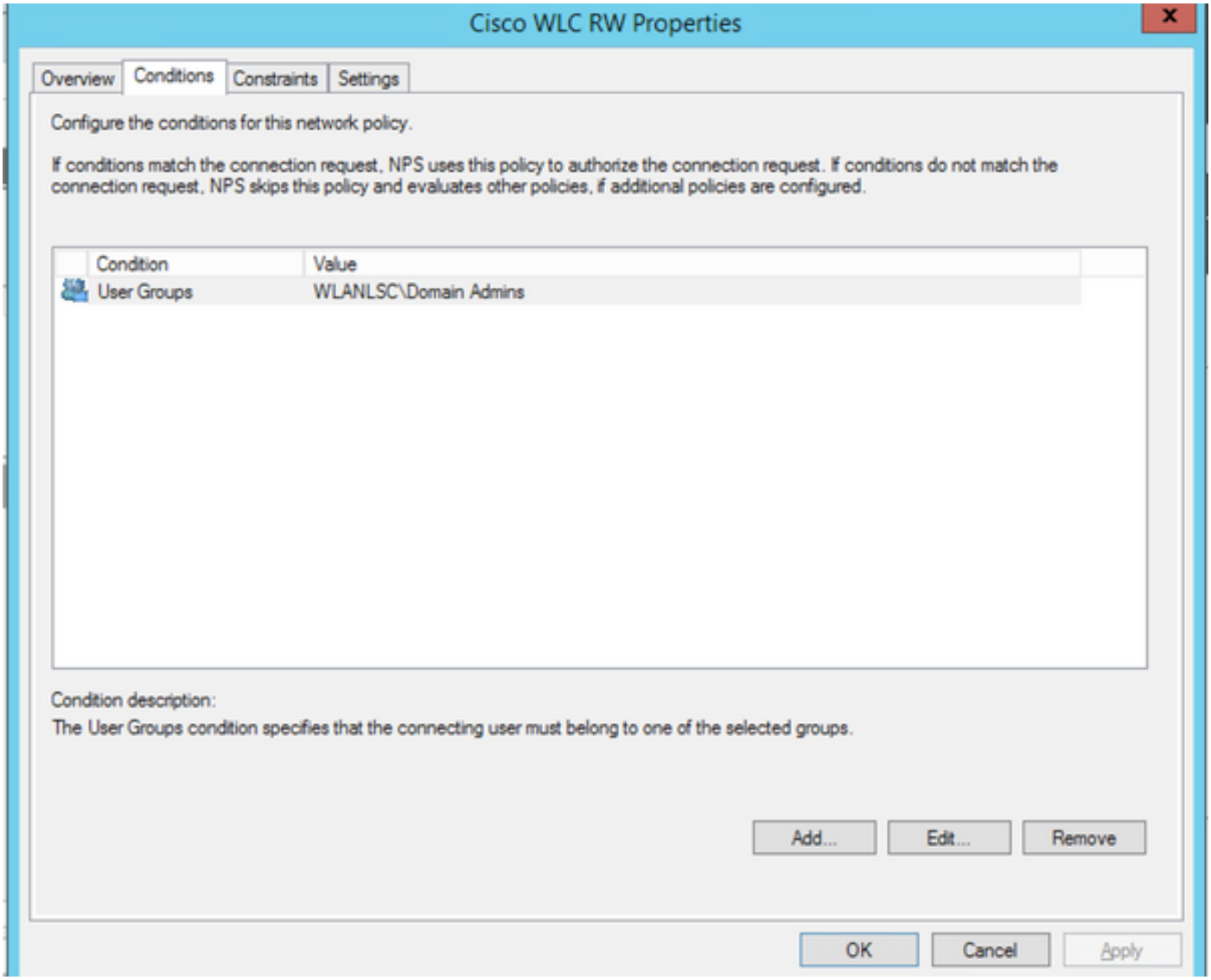
步驟5.在**Conditions**索引標籤下，按一下**Add**。選擇**User groups**，然後按一下**Add**，如下圖所示。



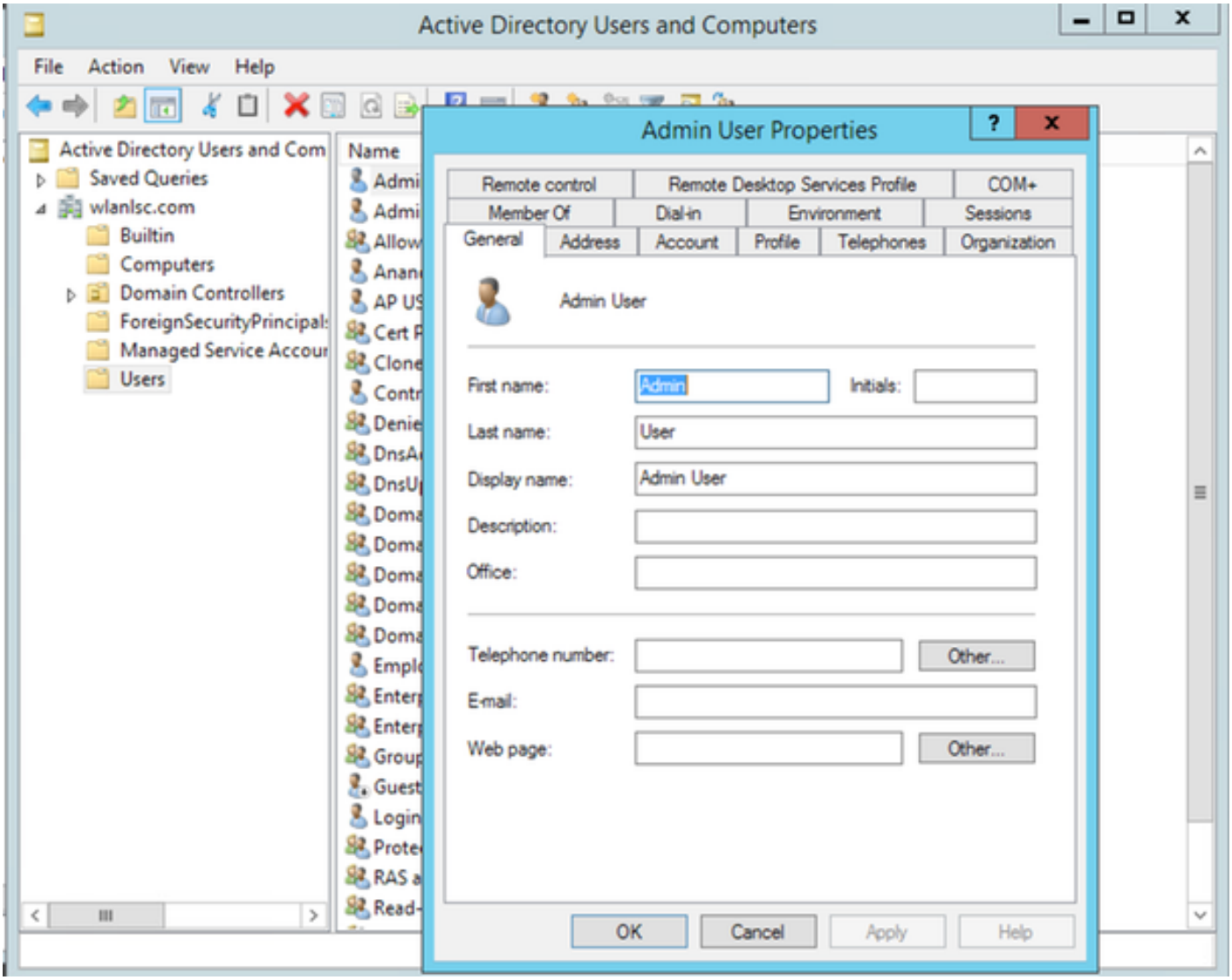
步驟6.在出現的對話方塊中按一下Add Groups。在出現的**選擇組**視窗中，選擇所需的**對象型別**和**位置**，然後輸入所需的對象名稱，如下圖所示。

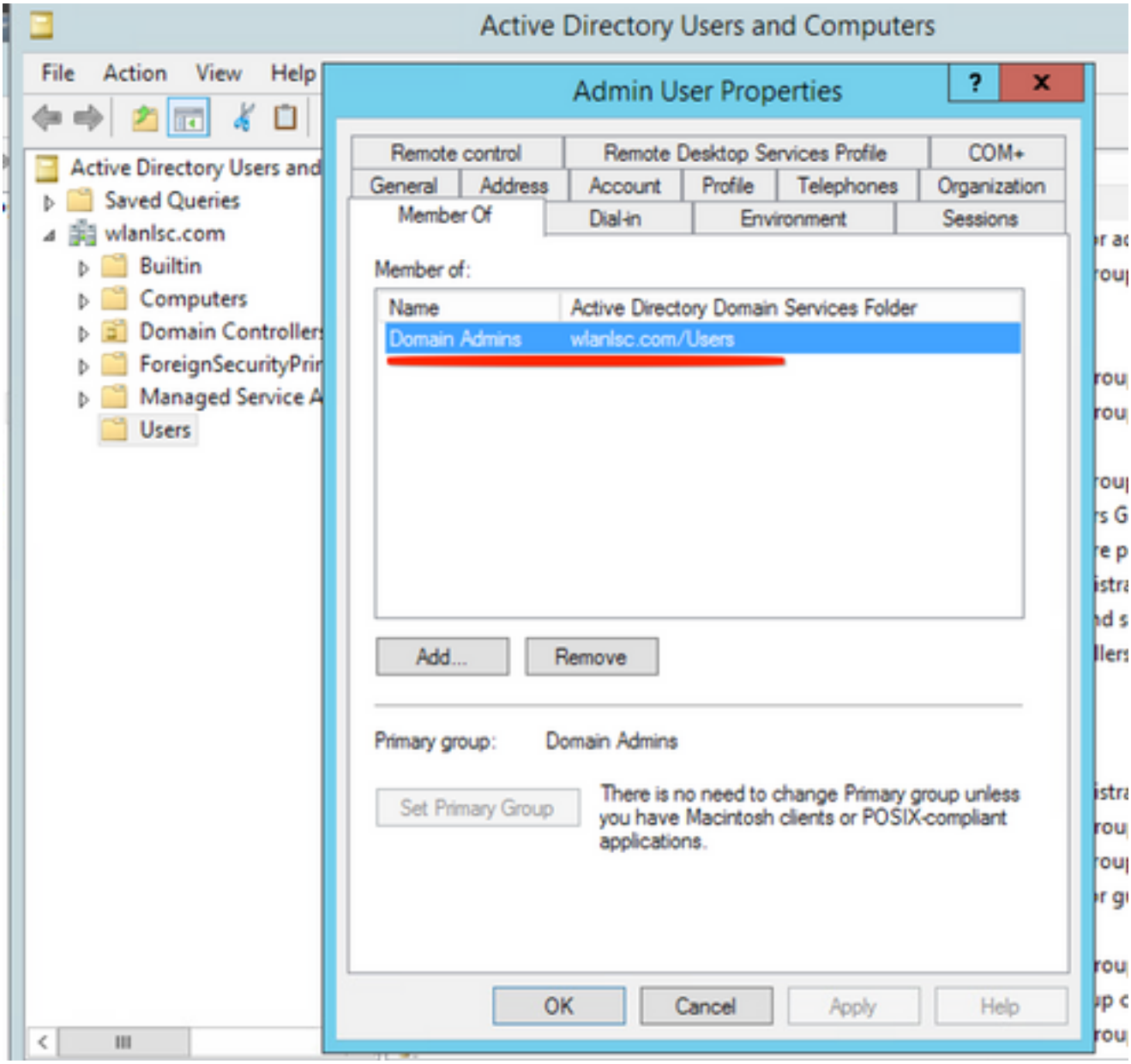


如果條件新增正確，應如下所示。

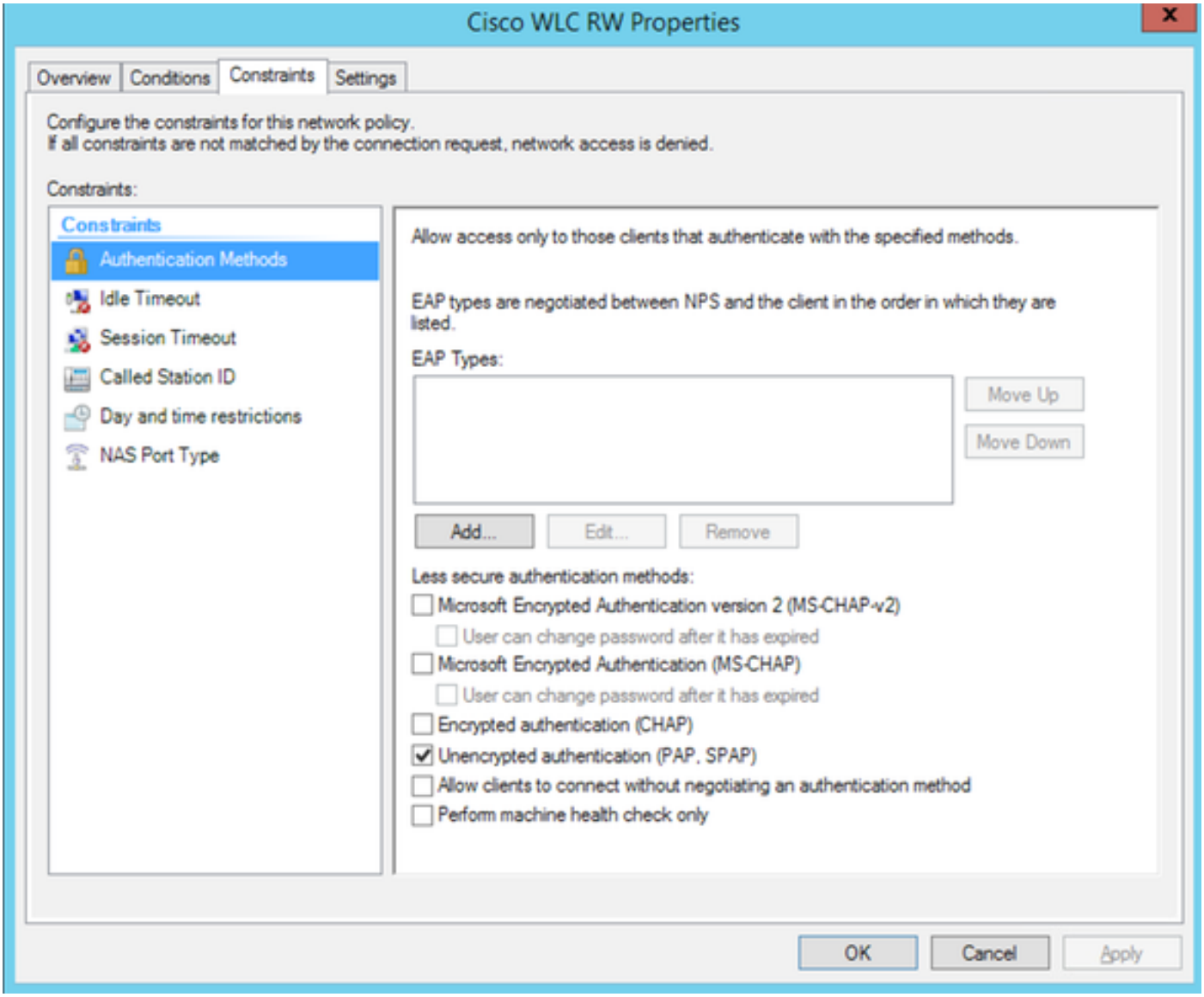


附註：要瞭解位置和對象名稱的詳細資訊，請開啟Active Directory並查詢所需的使用者名稱。在本示例中，**域管理員**由具有完全訪問許可權的使用者組成。**adminuser是**此對象名稱的一部分。

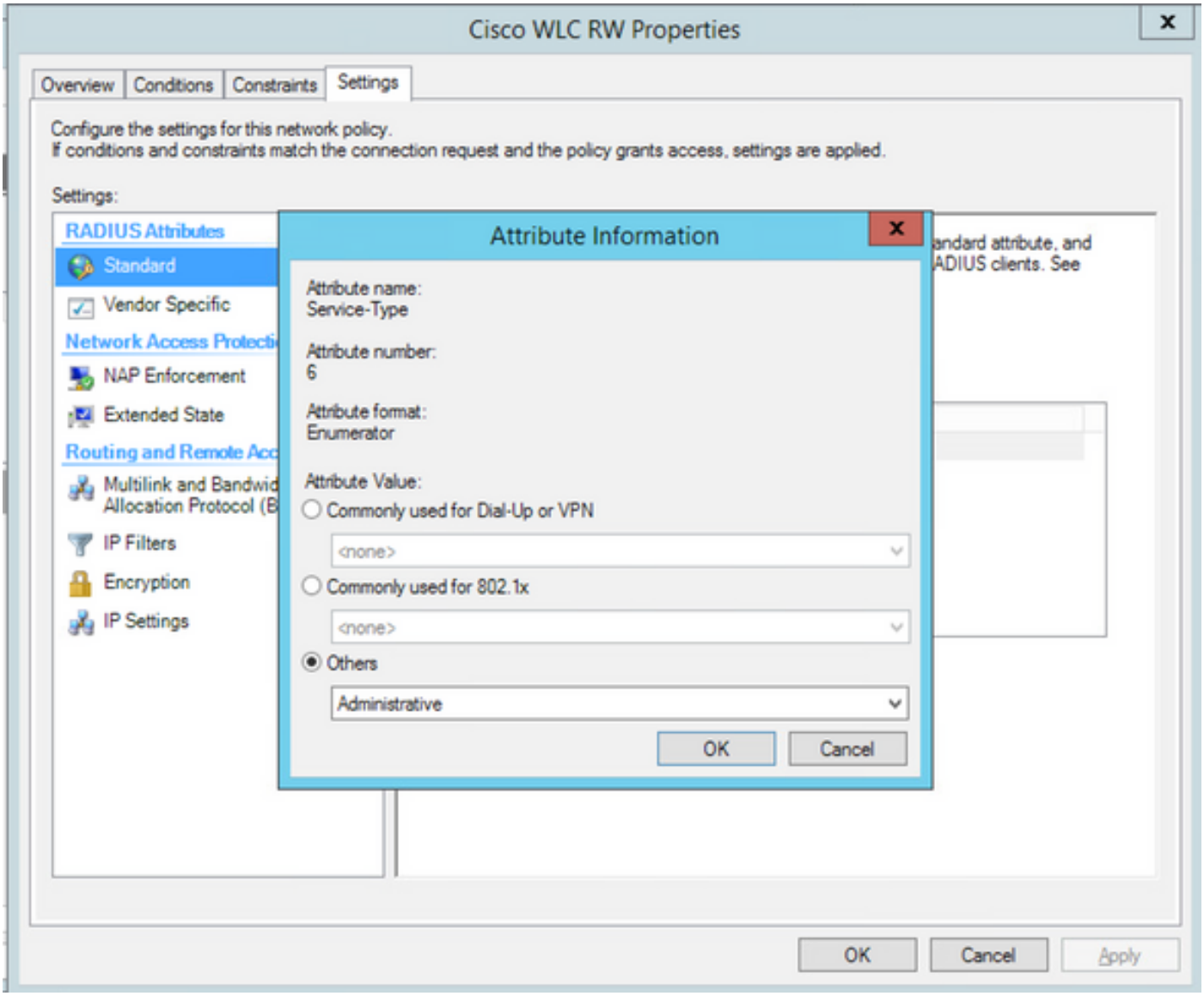

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
wlanlsc.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name
Admin User Properties
Remote control
Remote Desktop Services Profile
COM+
Member Of
Dial-in
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



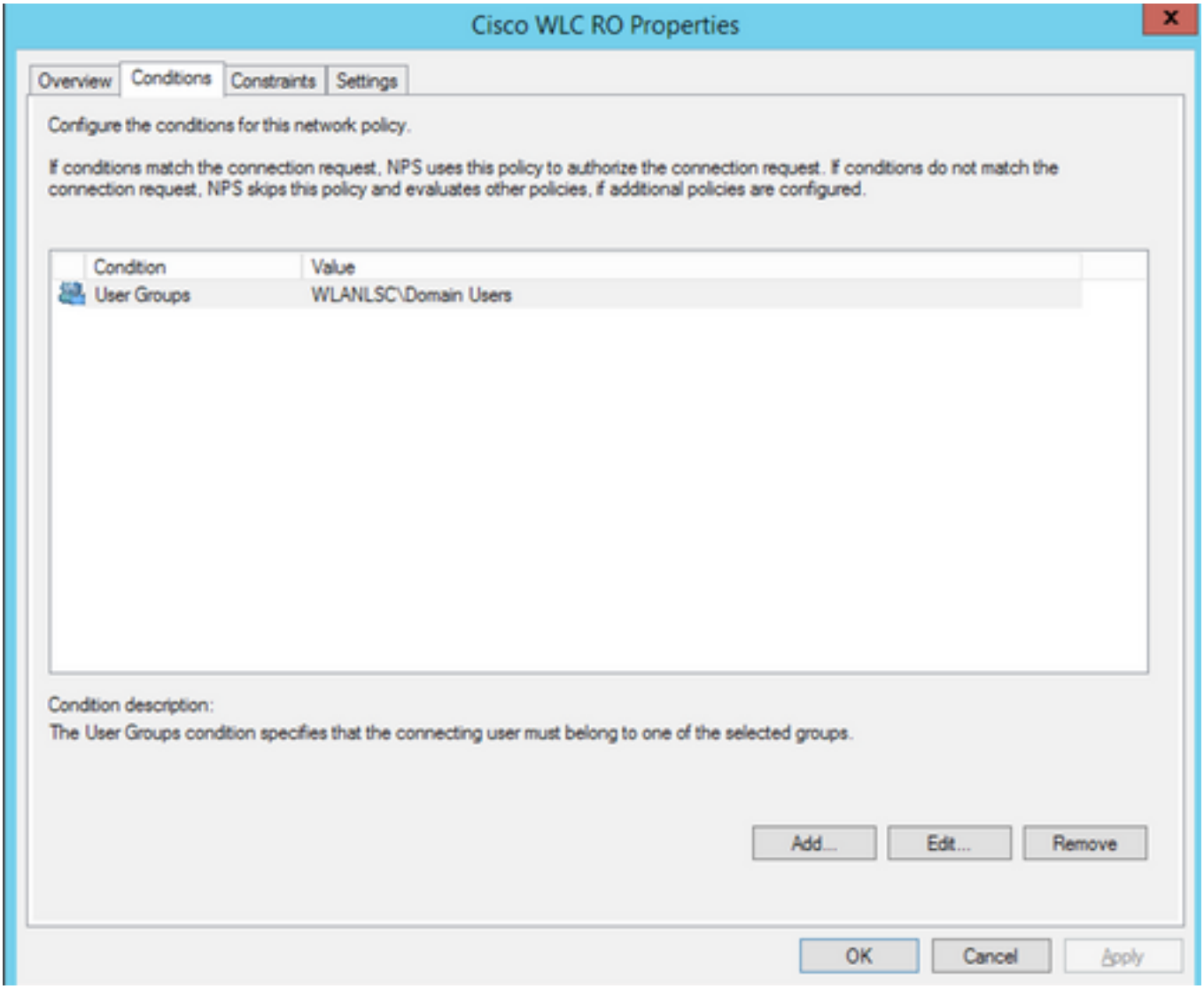
步驟7.在Constraints索引標籤下，導覽至Authentication Methods，並確保僅勾選未加密的驗證。

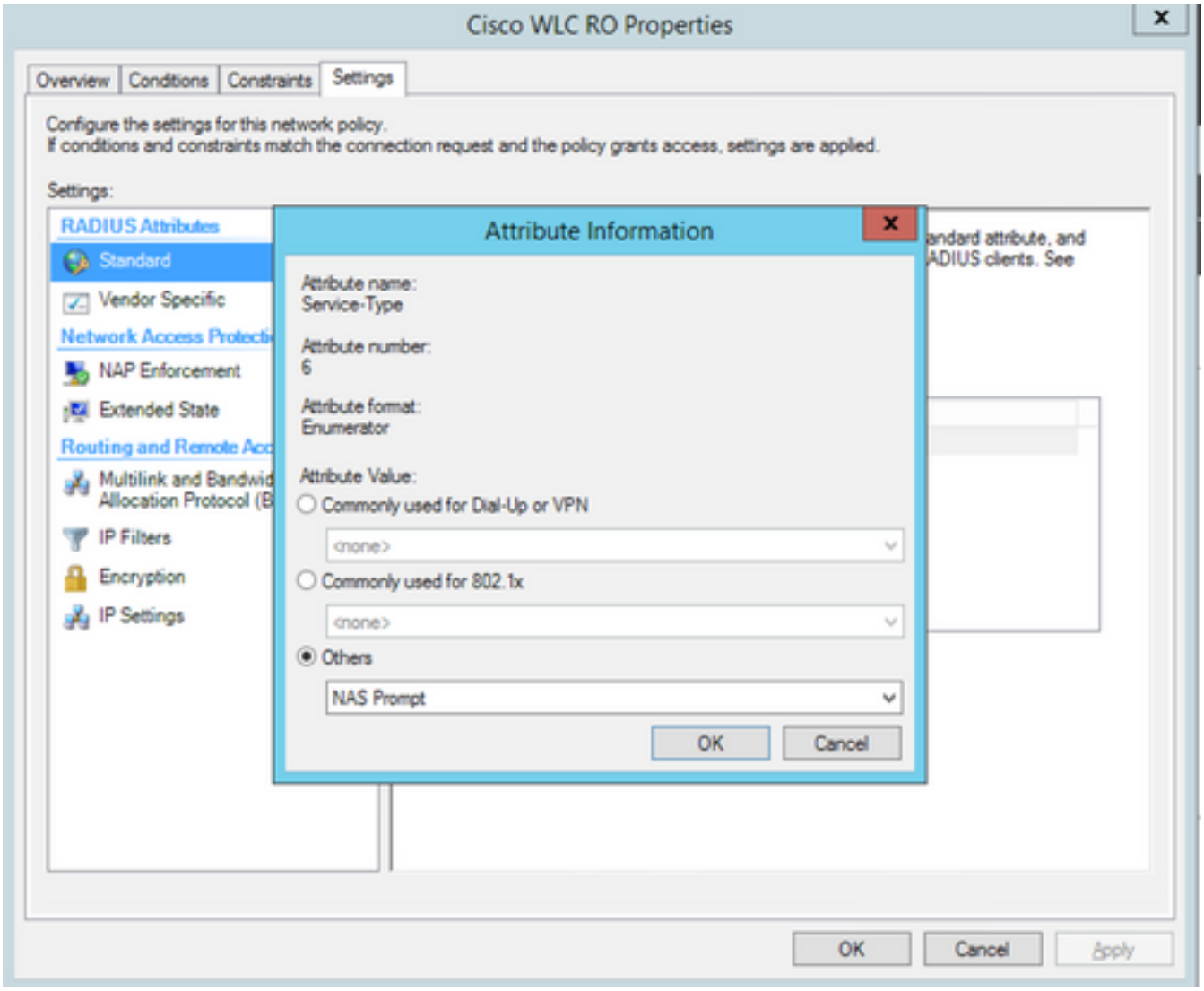


步驟8.在**Settings**索引標籤下，導覽至**RADIUS Attributes > Standard**。按一下**Add**以新增新屬性**Service-Type**。從下拉選單中，選擇**Administrative**，以提供對對映到此策略的使用者的完全訪問許可權。按一下「Apply」以儲存變更，如下圖所示。



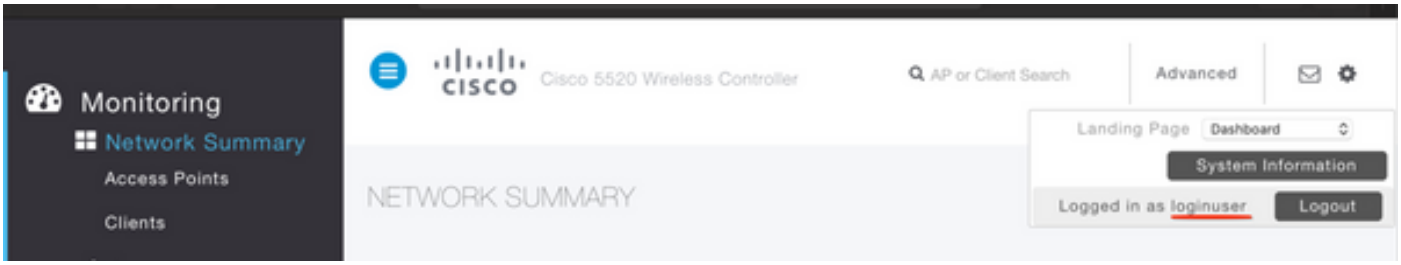
附註：如果要為特定使用者提供只讀訪問許可權，請從下拉選單中選擇NAS-Prompt。在本示例中，建立了名為**Cisco WLC RO**的另一個策略，以便在**Domain Users**對象名稱下為使用者提供只讀訪問許可權。

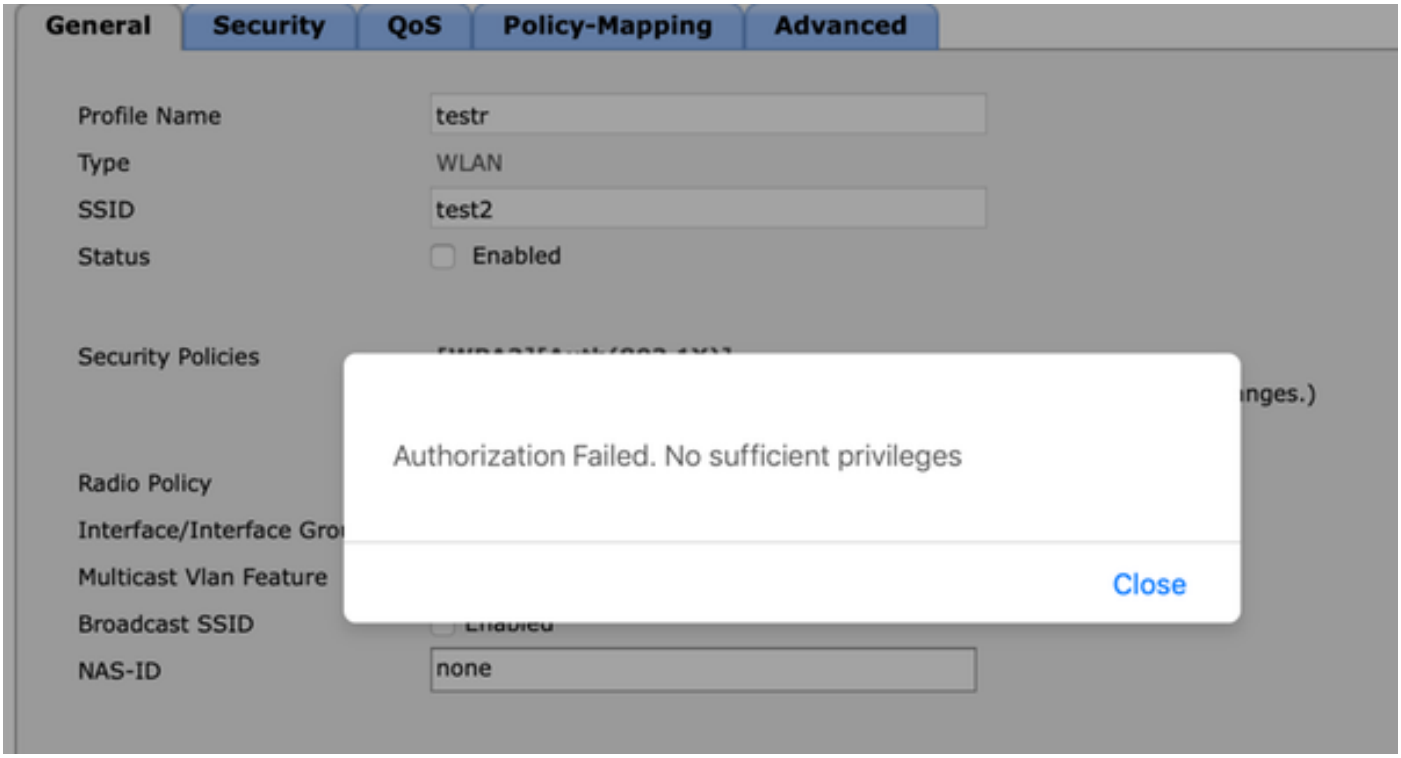

Cisco WLC RO Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates 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



驗證

1.使用loginuser憑據時，不允許使用者配置控制器上的任何更改。

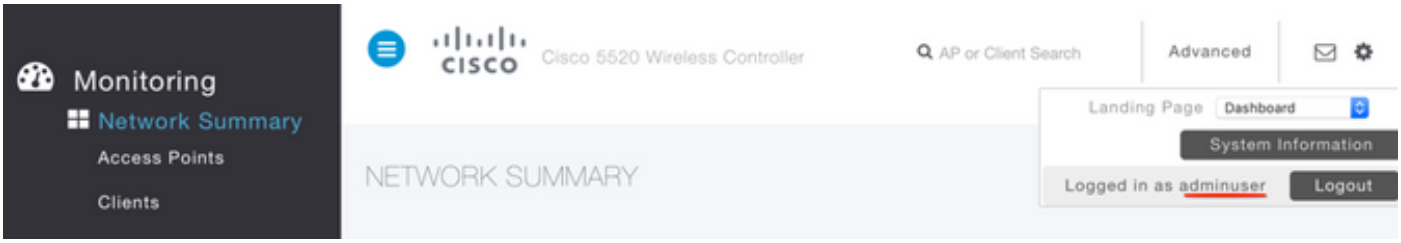




從**debug aaa all enable**中，您可以看到授權響應中的service-type屬性的值為7，該值對應於NAS-prompt。

```
*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.使用**adminuser**憑據時，使用者應具有與**administrative**對應的**service-type** value 6的完全訪問許可權。




```
*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)
```

疑難排解

若要對透過NPS對WLC的管理存取進行排解疑難，請執行**debug aaa all enable**指令。

1.此處顯示了使用不正確憑證時的日誌。

```
*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.將service-type與Administrative(value=6)或NAS-prompt(value=7)以外的值一起使用時的日誌顯示如下。在這種情況下，即使身份驗證成功，登入也會失敗。

```
*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
```