

# 通过Microsoft NPS对AireOS WLC的管理访问

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[WLC 配置](#)

[Microsoft NPS配置](#)

[验证](#)

[故障排除](#)

## 简介

本文档介绍如何通过Microsoft网络策略服务器(NPS)为AireOS WLC GUI和CLI配置管理访问。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 无线安全解决方案知识
- AAA和RADIUS概念
- Microsoft Server 2012基础知识
- 安装Microsoft NPS和Active Directory(AD)

### 使用的组件

本文档中提供的信息基于以下软件和硬件组件。

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

**注意：**本文档旨在向读者提供Microsoft服务器上WLC管理访问所需配置的示例。本文档中介绍的Microsoft Windows服务器配置已在实验室中测试，并发现可以按预期工作。如果配置有问题，请联系Microsoft获取帮助。思科技术支持中心(TAC)不支持Microsoft Windows服务器配置。Microsoft Windows 2012安装和配置指南可在Microsoft技术网上找到。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

# 背景信息

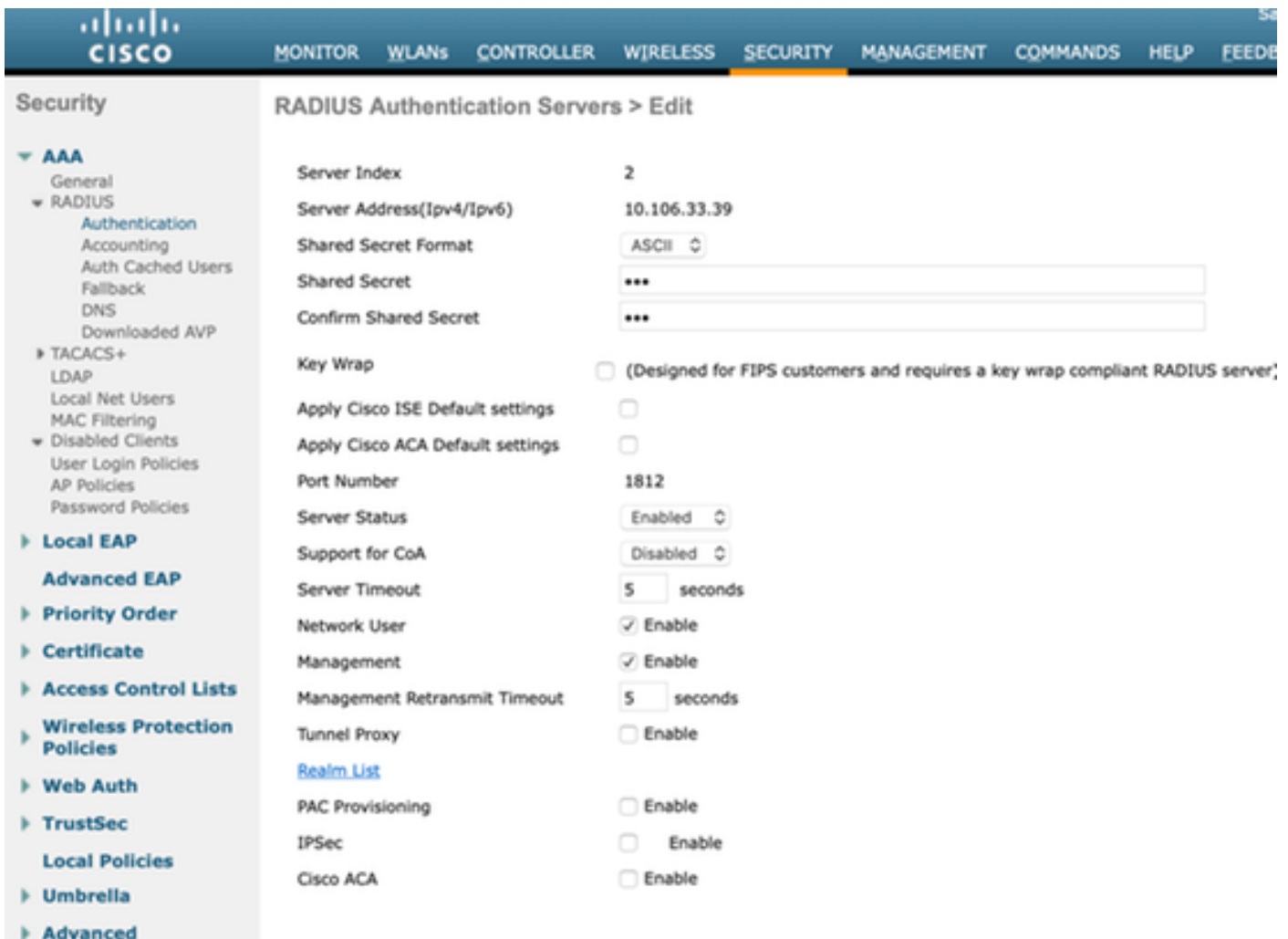
当访问WLC CLI/GUI时，系统会提示用户输入凭证以成功登录。凭证可以针对本地数据库或外部AAA服务器进行验证。在本文档中，Microsoft NPS用作外部身份验证服务器。

# 配置

在本示例中，在AAA(NPS)viz上配置了两个用户。loginuser和adminuser。loginuser只具有只读访问权限，而adminuser被授予完全访问权限。

## WLC 配置

步骤1.在控制器上添加RADIUS服务器。导航至Security > RADIUS > Authentication。单击New以添加服务器。确保management选项已启用，以便此服务器可用于管理访问，如此图所示。



步骤2.导航至“安全”>“优先级订单”>“管理用户”。确保RADIUS被选作身份验证类型之一。

Priority Order > Management User

Authentication

Not Used: TACACS+

Order Used for Authentication: RADIUS LOCAL

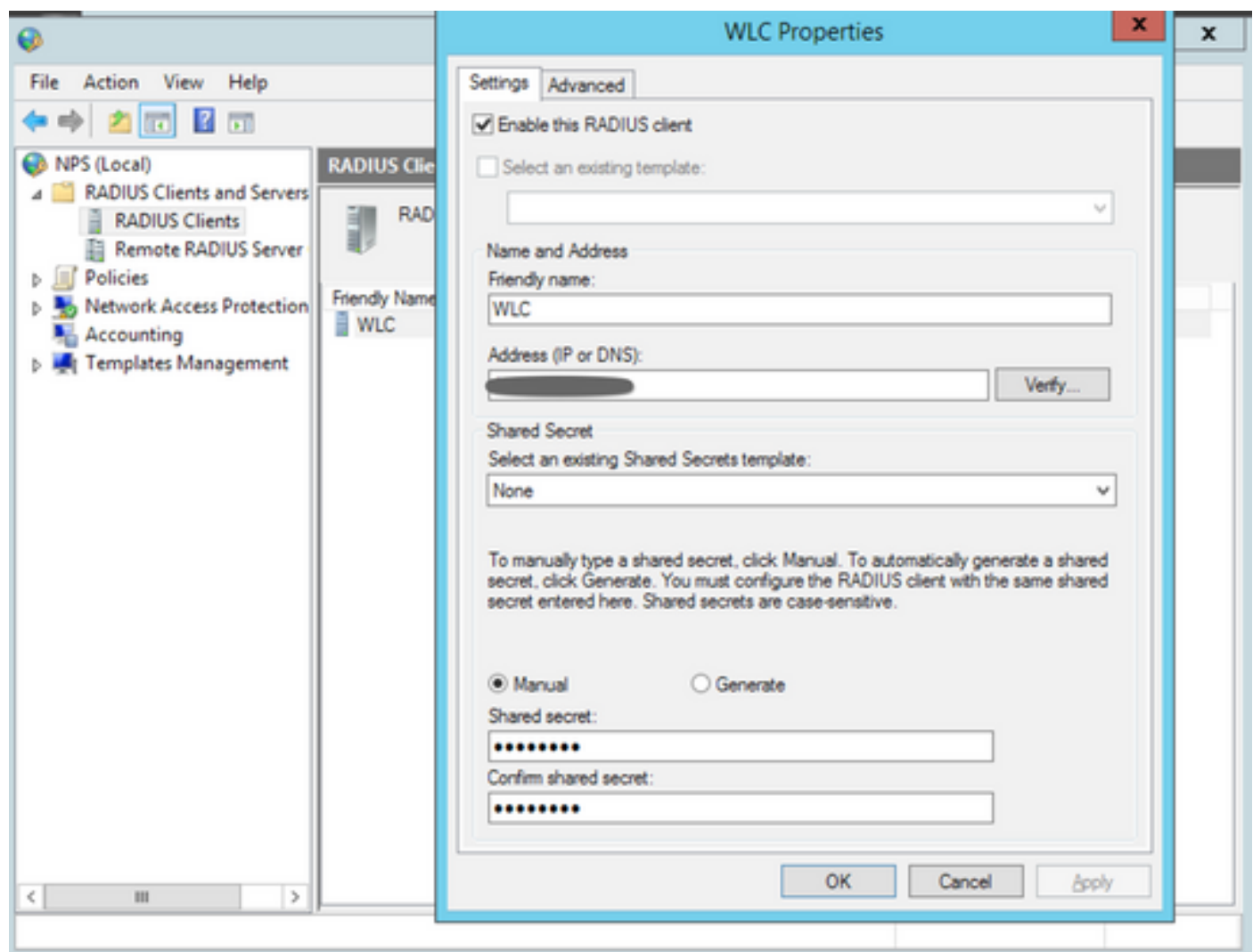
Buttons: >, <, Up, Down

**注意：**如果选择RADIUS作为身份验证顺序中的第一个优先级，则仅当RADIUS服务器无法访问时，本地凭证才用于身份验证。如果选择RADIUS作为第二优先级，则首先根据本地数据库验证RADIUS凭证，然后根据已配置的RADIUS服务器检查。

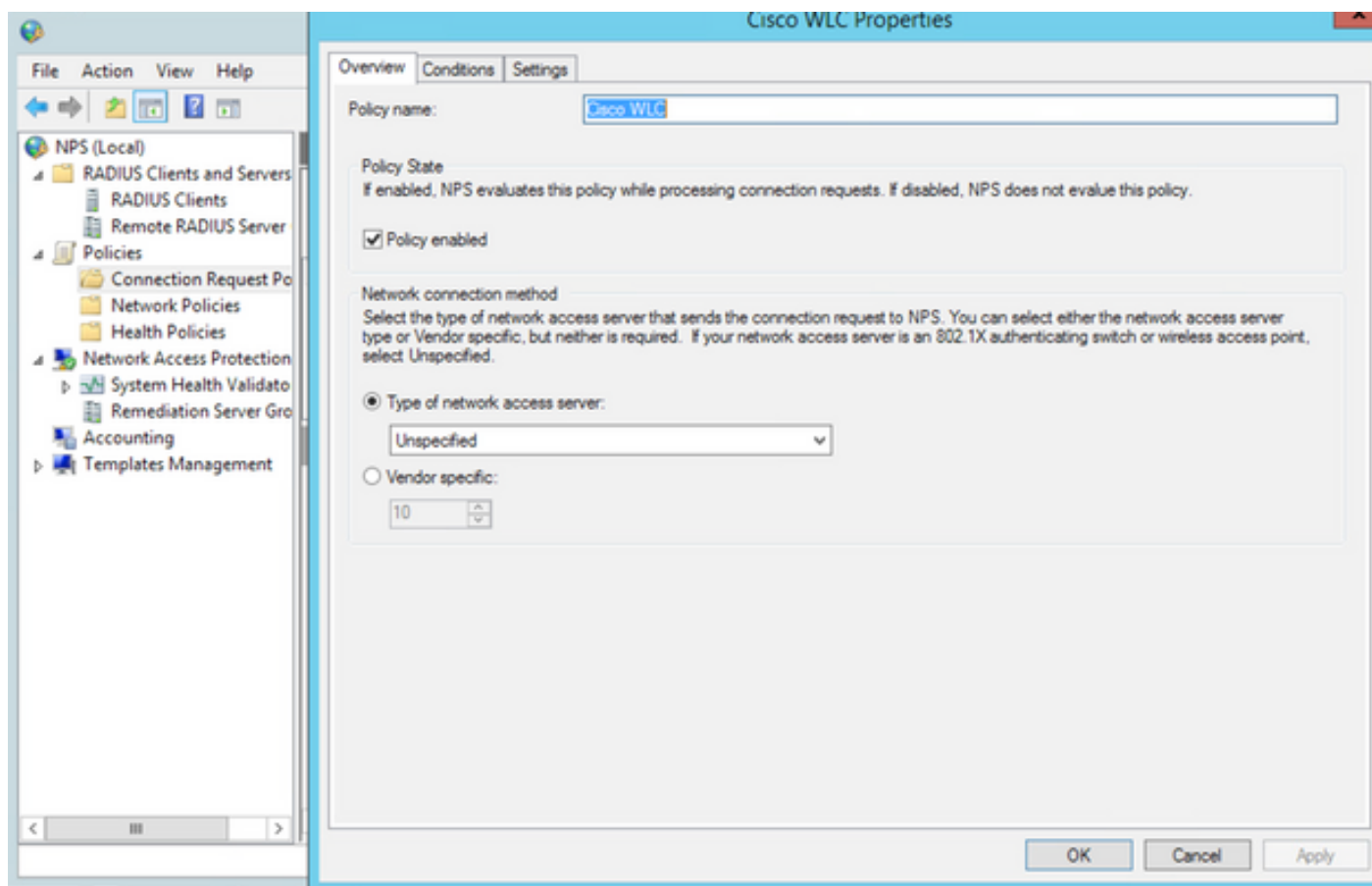
### Microsoft NPS配置

步骤1.打开Microsoft NPS服务器。右键单击“Radius Clients(Radius客户端)”。单击New将WLC添加为RADIUS客户端。

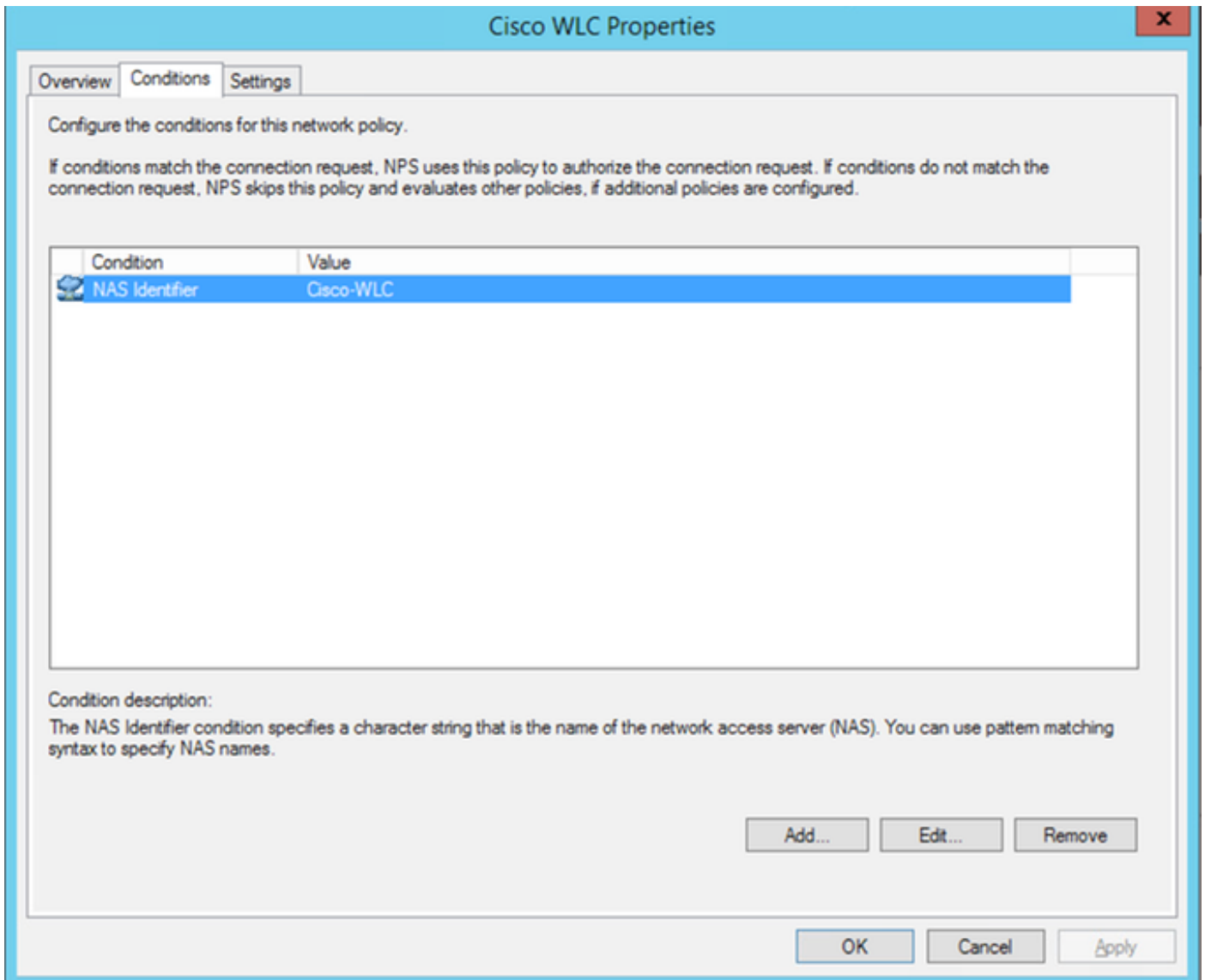
输入所需的详细信息。请确保在添加RADIUS服务器时共享密钥与控制器上配置的密钥相同。



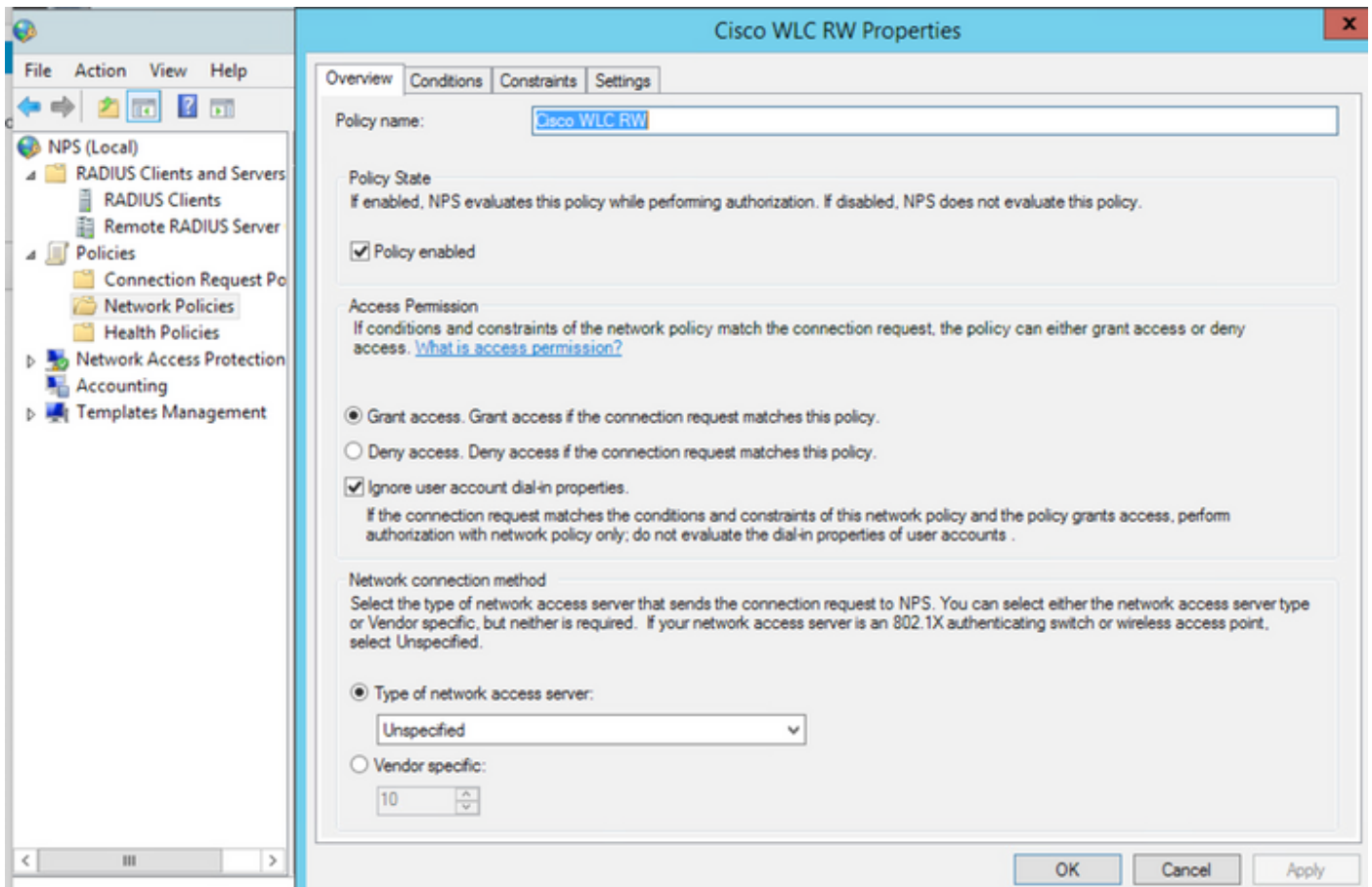
步骤2. 导航至Policies > Connection Request Policies。右键点击以添加新策略，如图所示。



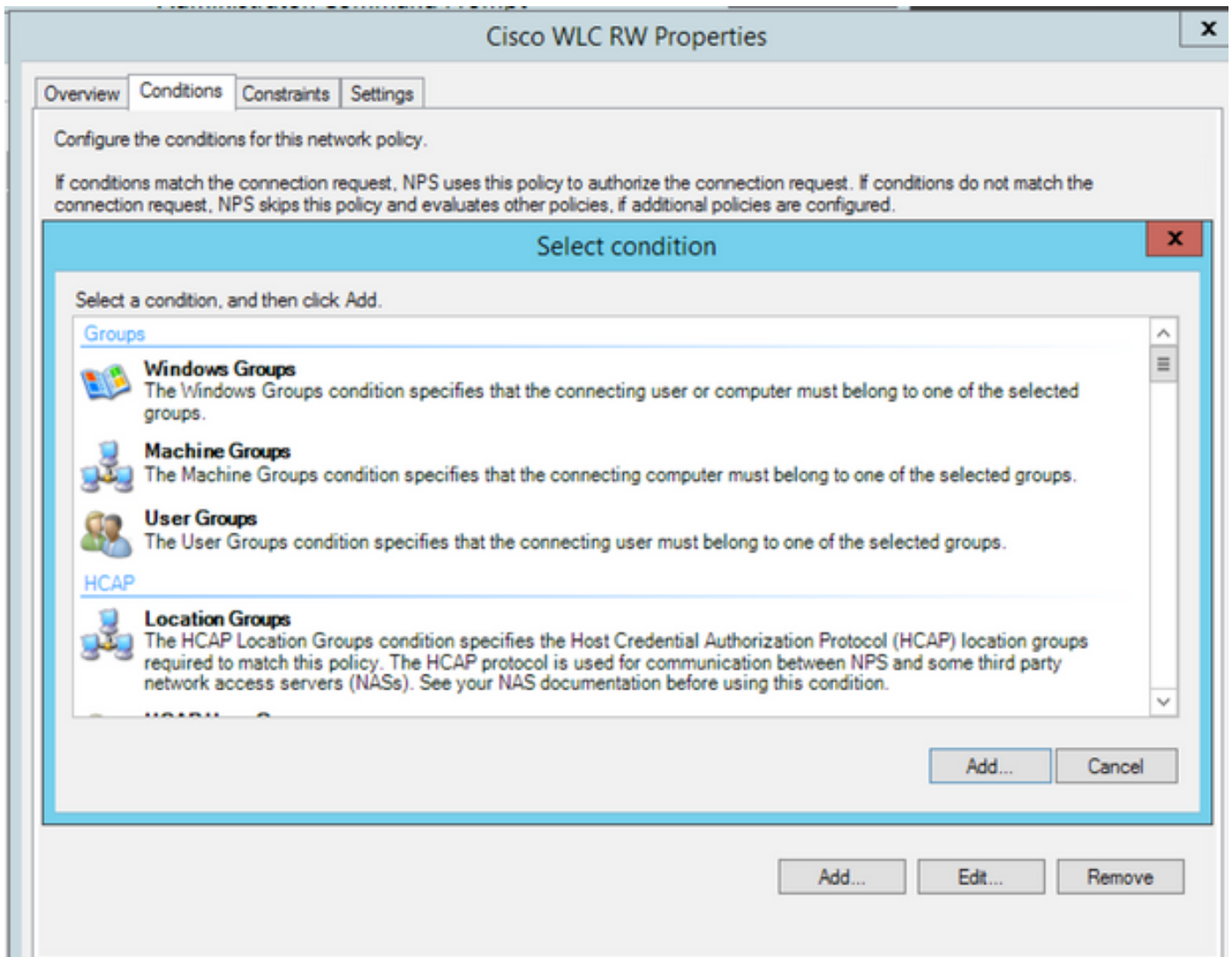
步骤3. 在“条件”选项卡下，选择NAS标识符作为新条件。出现提示时，输入控制器的主机名作为值，如图所示。



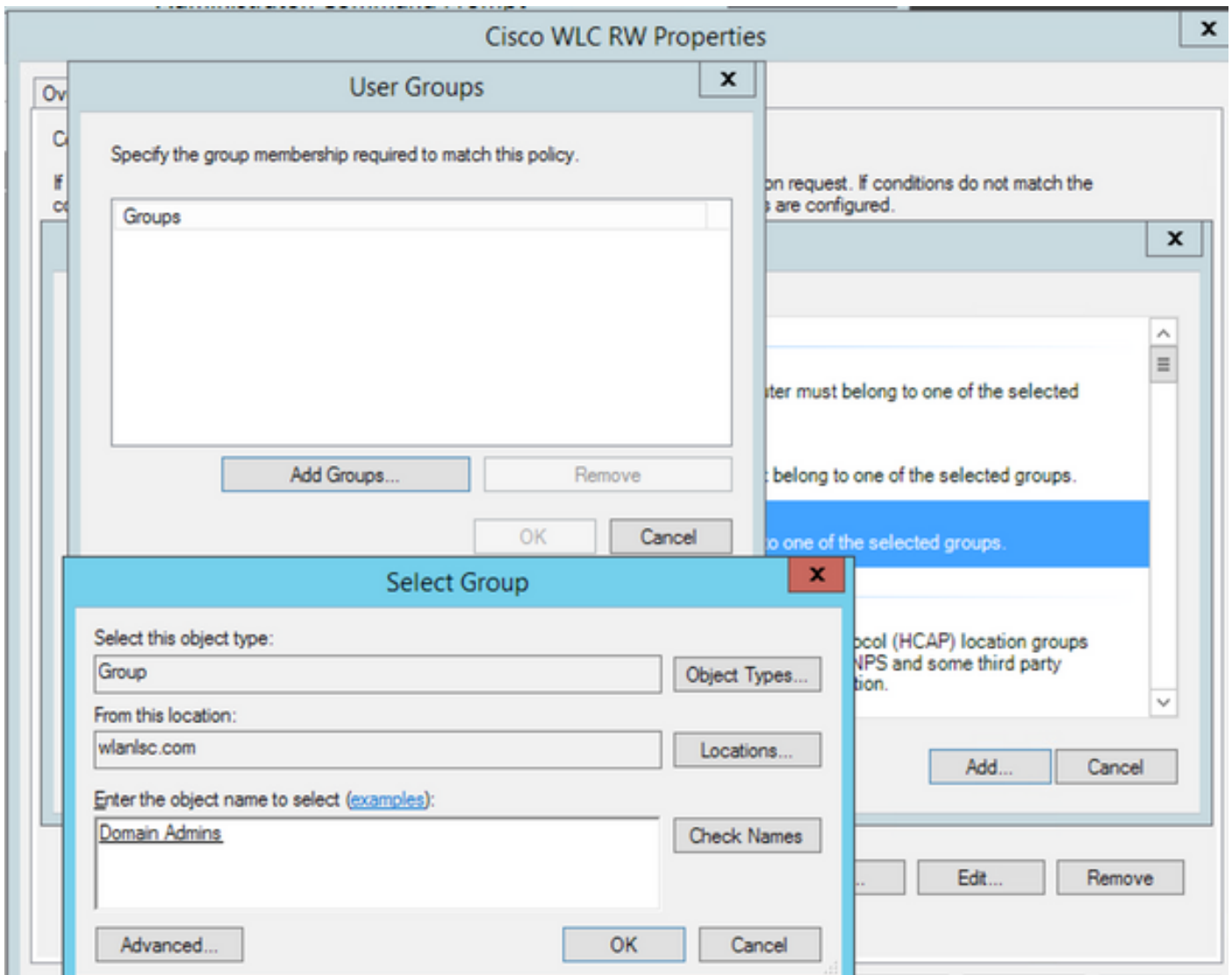
步骤4. 导航至 Policies > Network Policies。右键单击以添加新策略。在本示例中，策略名为 Cisco WLC RW，这意味着策略用于提供完全（读写）访问。确保策略配置如下所示。



步骤5.在“条件”选项卡下，单击“添加”。选择用户组，然后单击添加，如图所示。

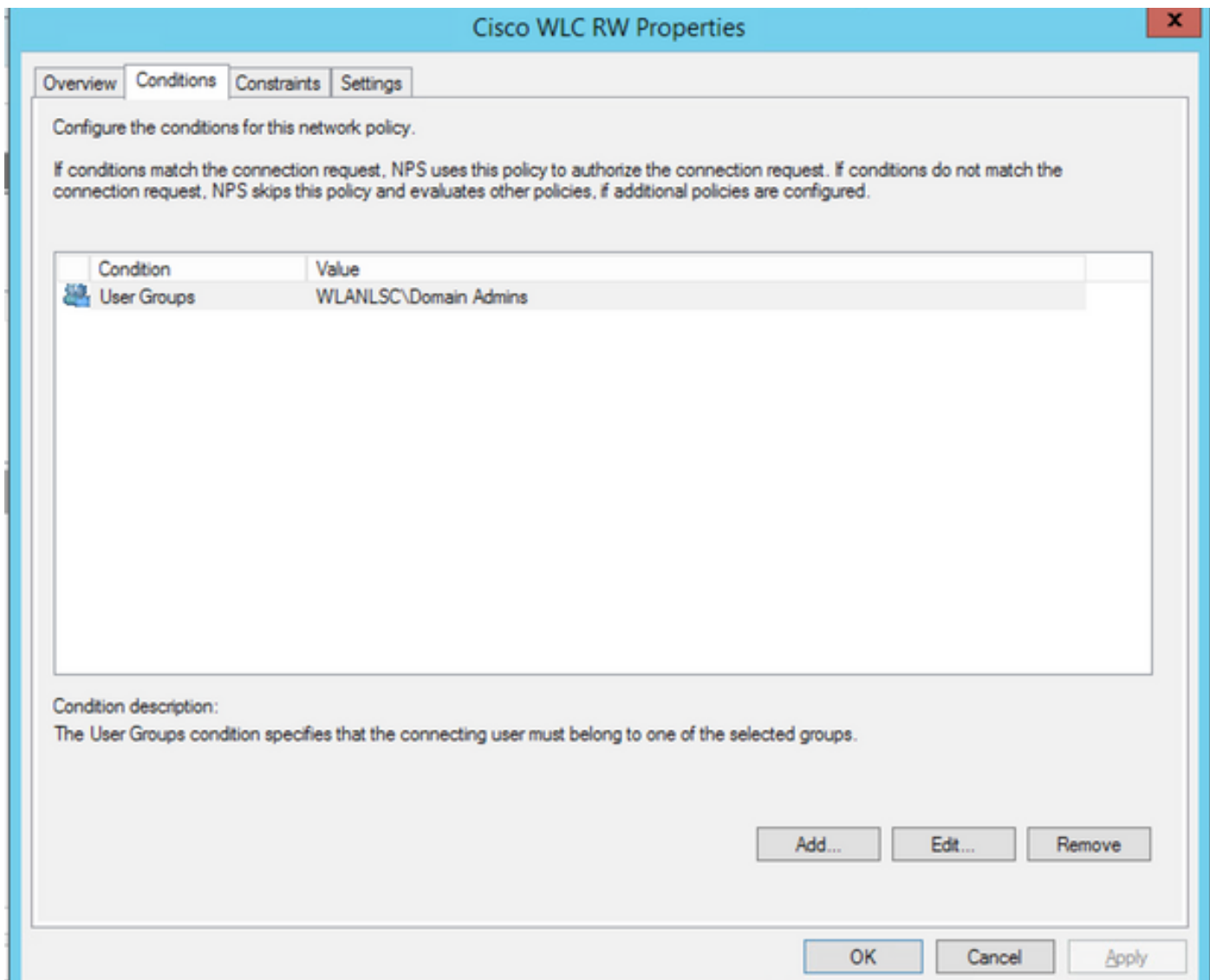


步骤6.在显示的对话框中单击“添加组”。在显示的“选择组”窗口中，选择所需的对象类型和位置，并输入所需的对象名称，如图所示。

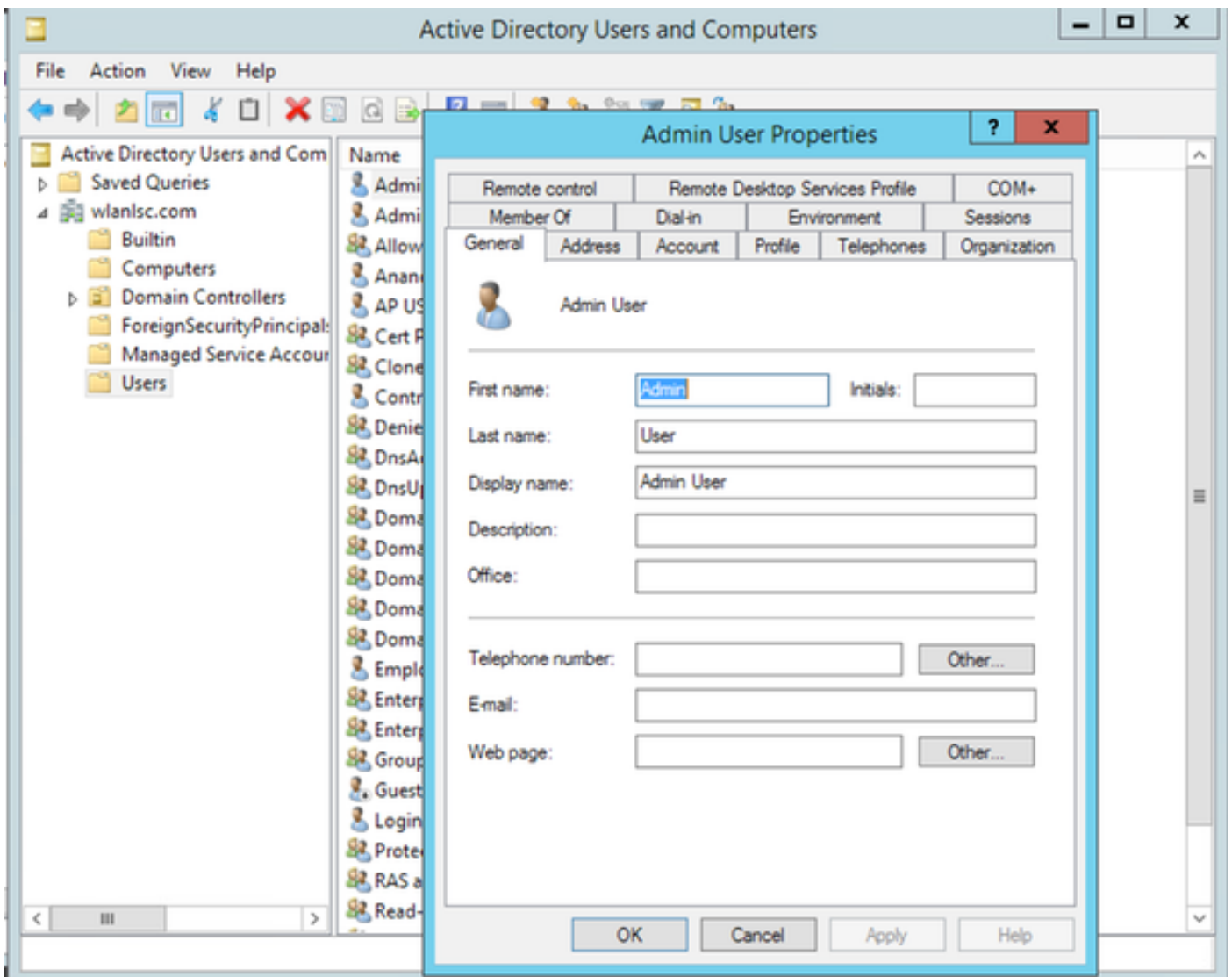


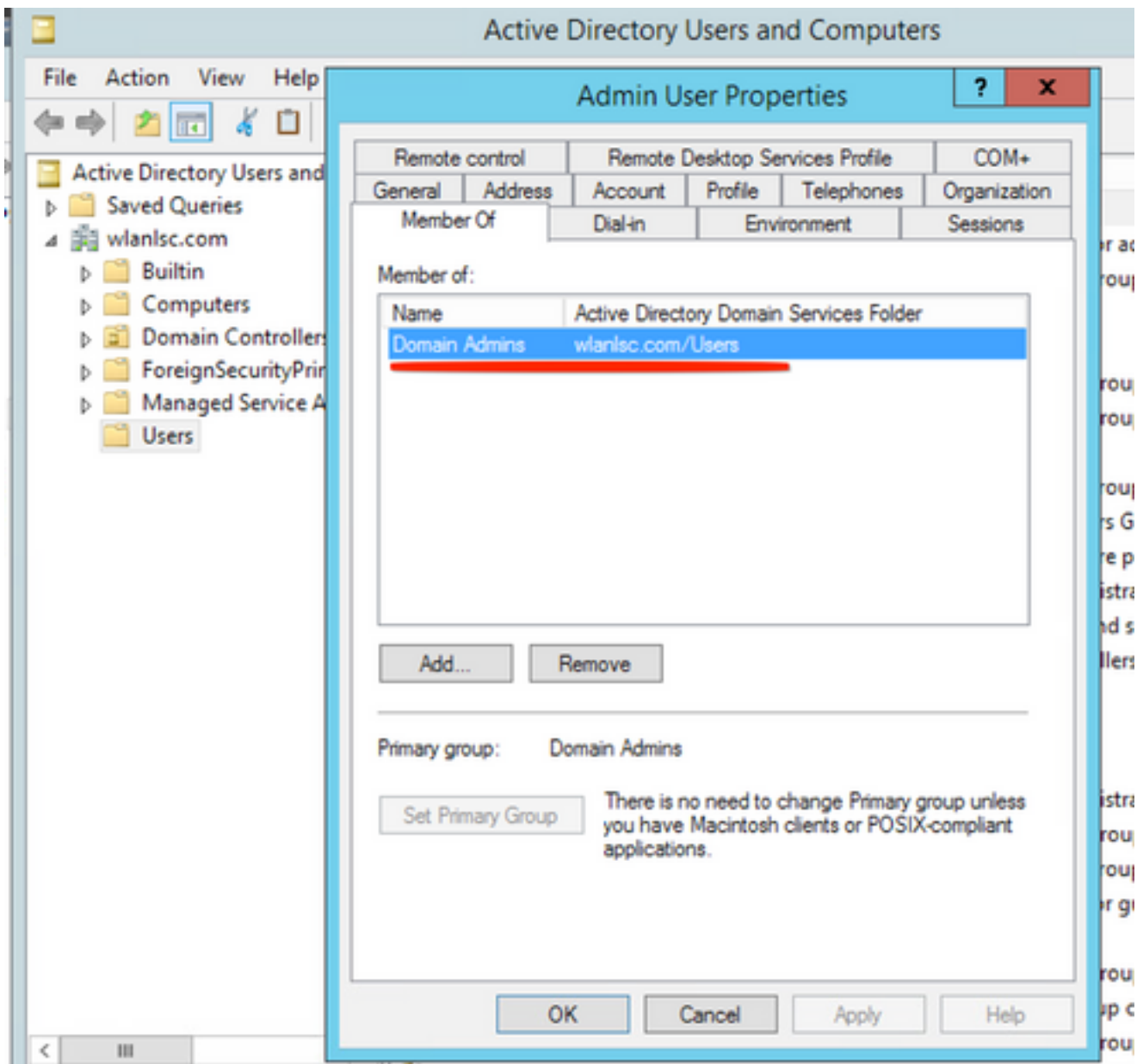
如果添加正确，应如下所示。



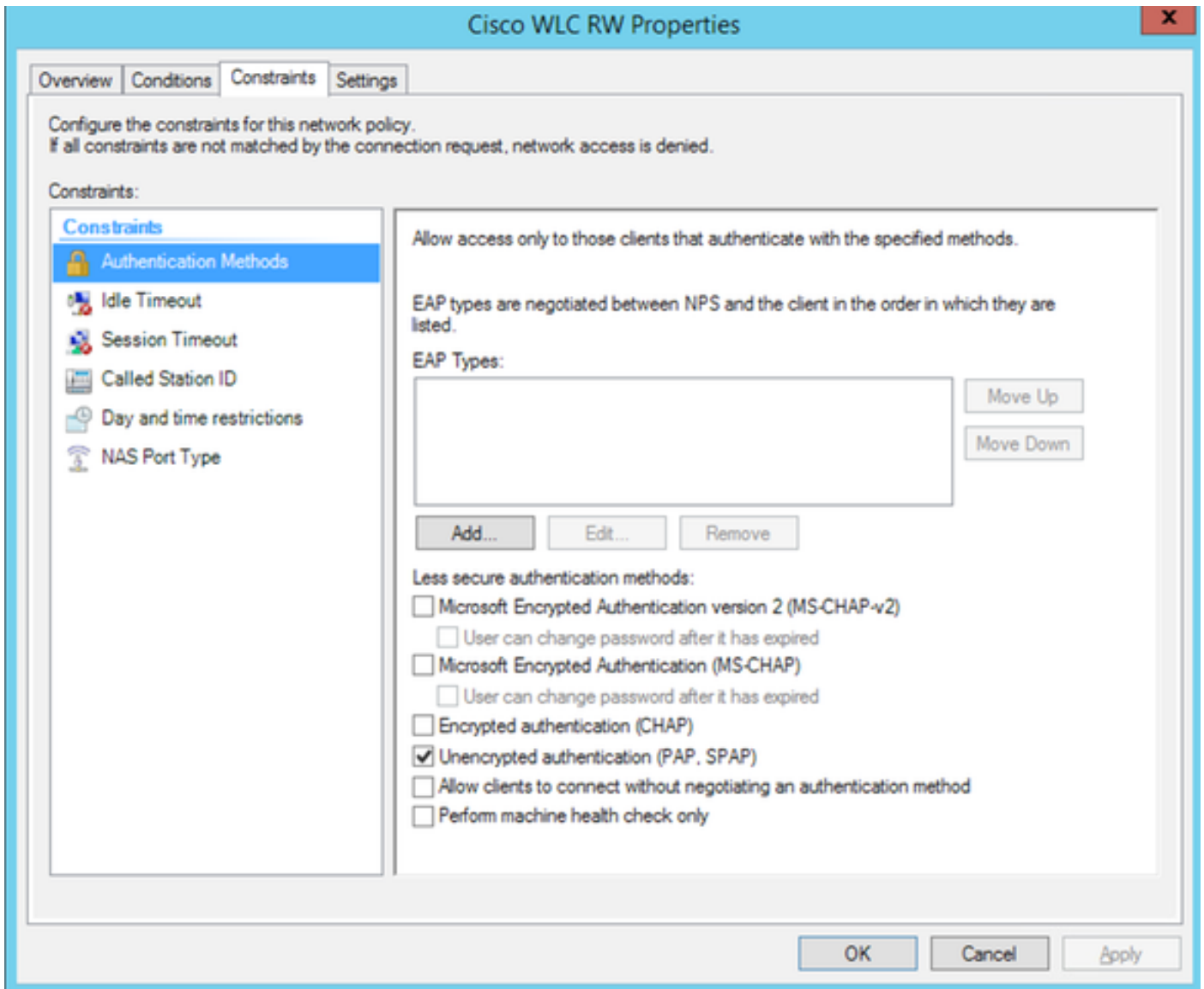


**注意：**要查找位置和对象名称的详细信息，请打开Active Directory并查找所需的用户名。在本示例中，**域管理员**由获得完全访问权限的用户组成。**adminuser**是此对象名称的一部分。

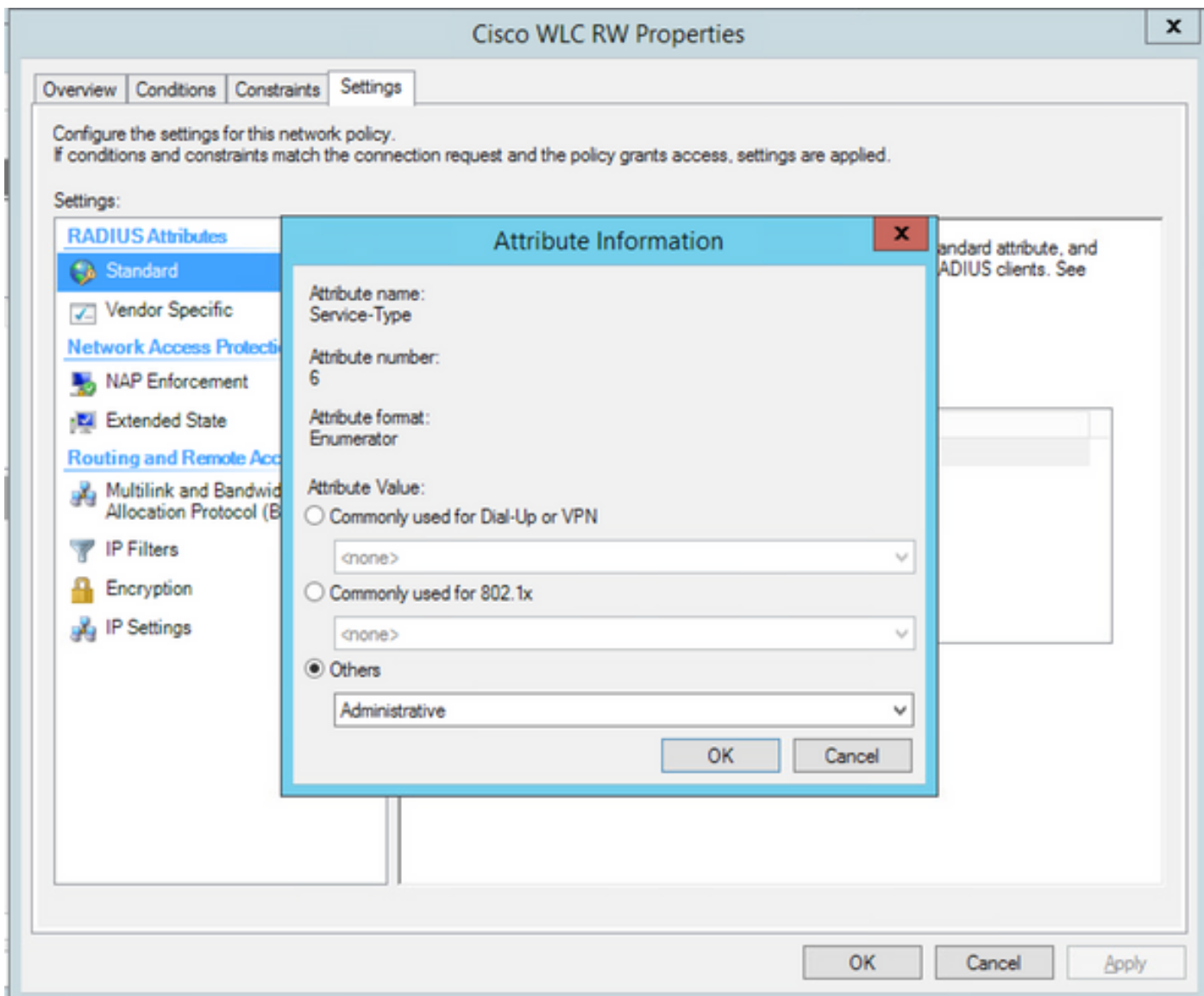




步骤7.在“约束”选项卡下，导航至“身份验证方法”，并确保仅选中未加密的身份验证。



步骤8.在“设置”选项卡下，导航至“RADIUS属性”>“标准”。单击Add以添加新属性Service-Type。从下拉菜单中，选择Administrative以提供对映射到此策略的用户的完全访问权限。单击应用保存更改，如图所示。




**注意：**如果要为特定用户提供只读访问权限，请从下拉列表中选择NAS-Prompt。在本示例中，创建另一个名为Cisco WLC RO的策略，以在域用户对象名下为用户提供只读访问权限。

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...

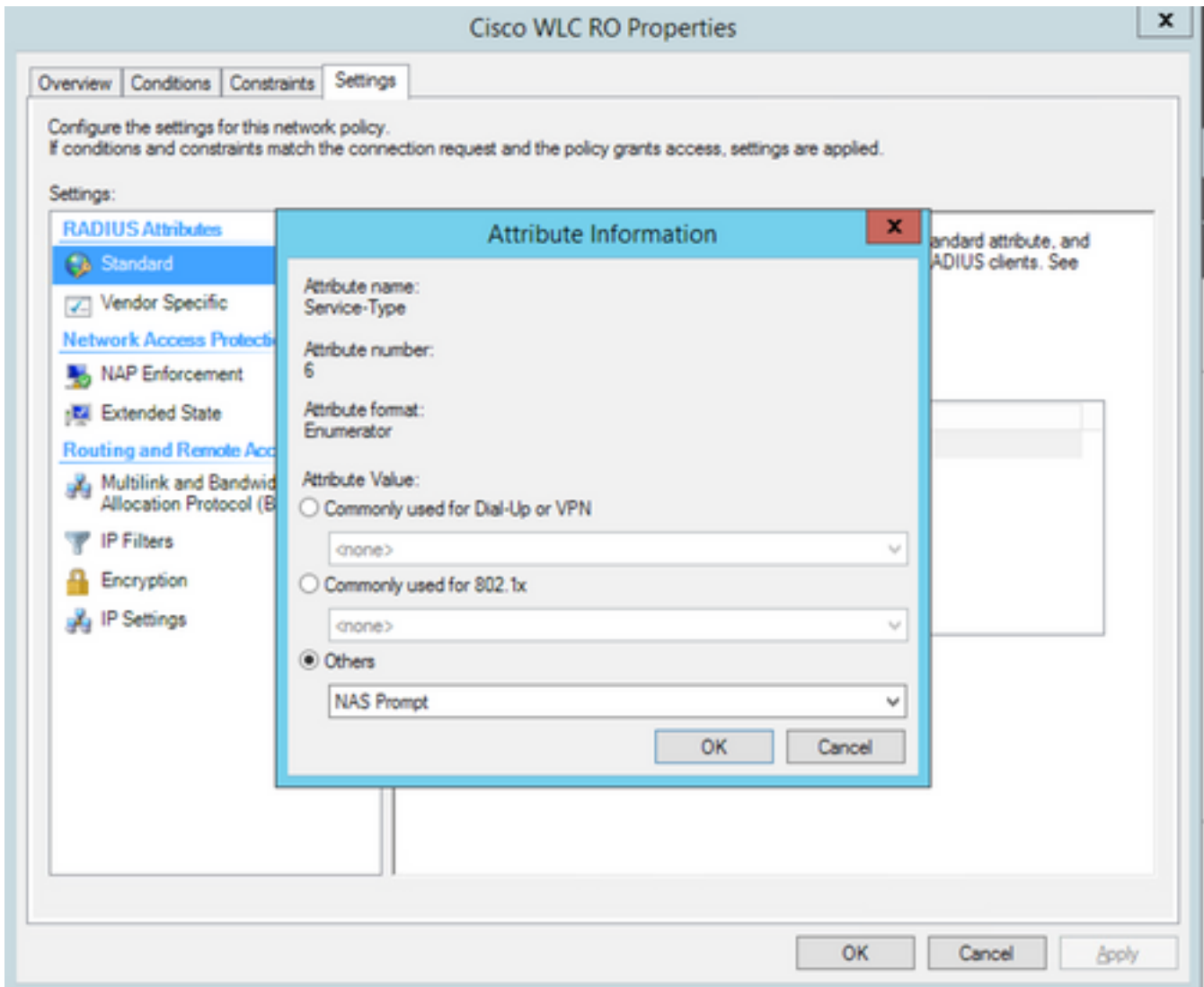
Edit...

Remove

OK

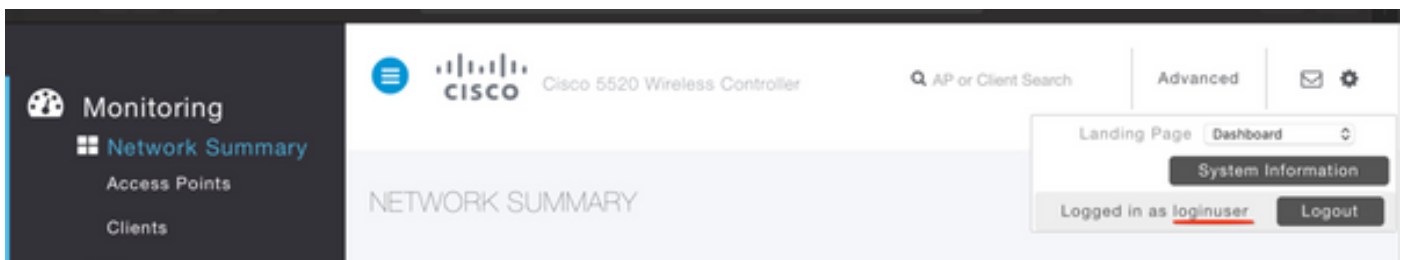
Cancel

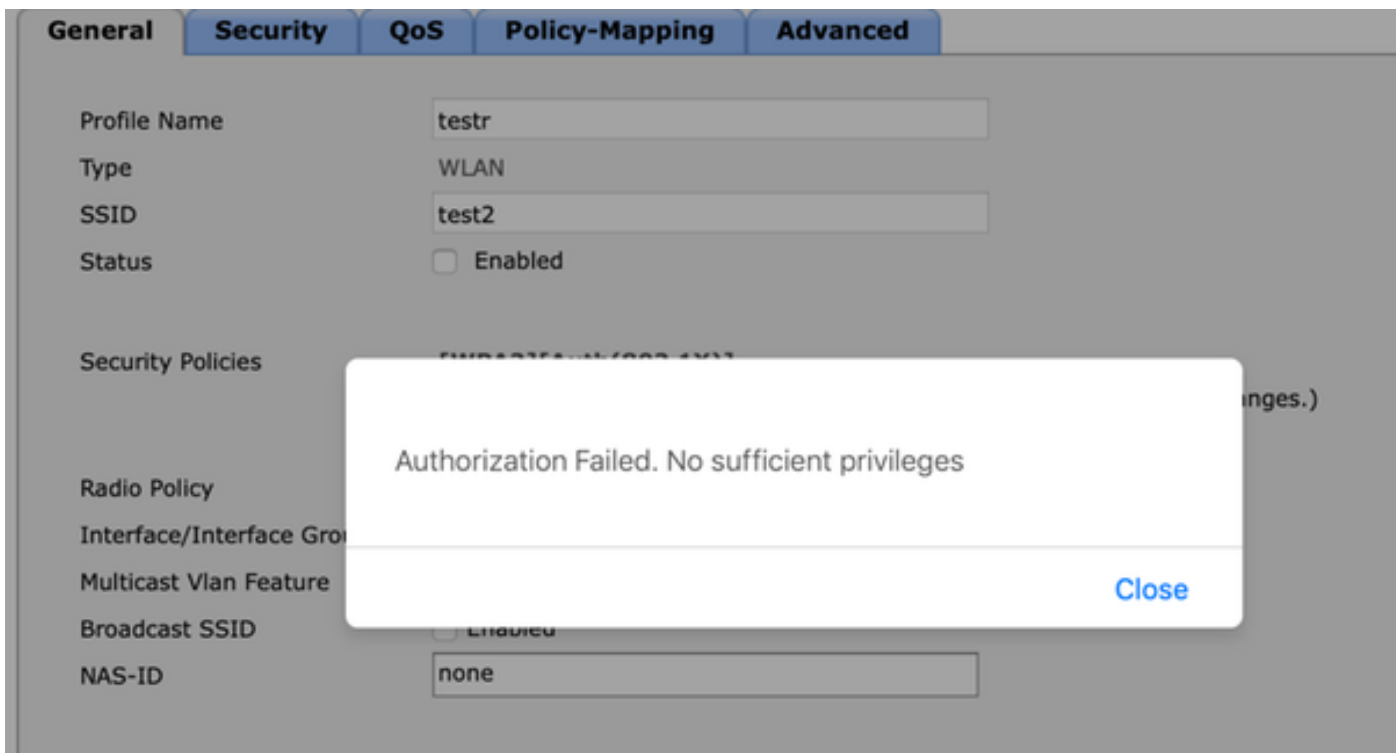
Apply



## 验证

1.使用登录用户凭据时，不允许用户在控制器上配置任何更改。



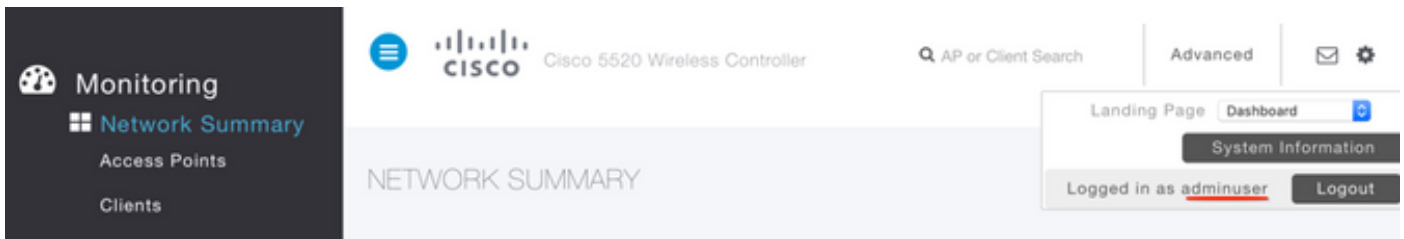


从debug aaa all enable中，您可以看到授权响应中service-type属性的值为7，与NAS提示符对应。

```
*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凭据时，用户应具有服务类型值6的完全访问权限，该值与管理相对应。





```
*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)
```

## 故障排除

要排除通过NPS对WLC的管理访问故障，请运行debug aaa all enable命令。

1.此处显示了使用不正确凭据时的日志。

```
*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: 0x7fbaebef860
*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.当service-type与Administrative(value=6)或NAS-prompt(value=7)以外的值一起使用时，如下所示。在这种情况下，即使身份验证成功，登录也会失败。

```
*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
```