Management Access for AireOS WLC through Microsoft NPS

Contents

Introduction

This document describes how to configure management access for AireOS WLC GUI and CLI through the Microsoft Network Policy Server (NPS).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Wireless Security Solutions
- AAA and RADIUS concepts
- Basic knowledge of Microsoft Server 2012
- Installation of Microsoft NPS and Active Directory (AD)

Components Used

The information provided in this document is based on the following software and hardware components.

- AireOS controller (5520) on 8.8.120.0
- Microsoft Server 2012

  Note: This document is intended to give the readers an example of the configuration required on a Microsoft server for WLC management access. The Microsoft Windows server configuration presented in this document has been tested in the lab and found to work as expected. If you have trouble with the configuration, contact Microsoft for help. The Cisco Technical Assistance Center (TAC) does not support the Microsoft Windows server

configuration. Microsoft Windows 2012 installation and configuration guides can be found on Microsoft Tech Net.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

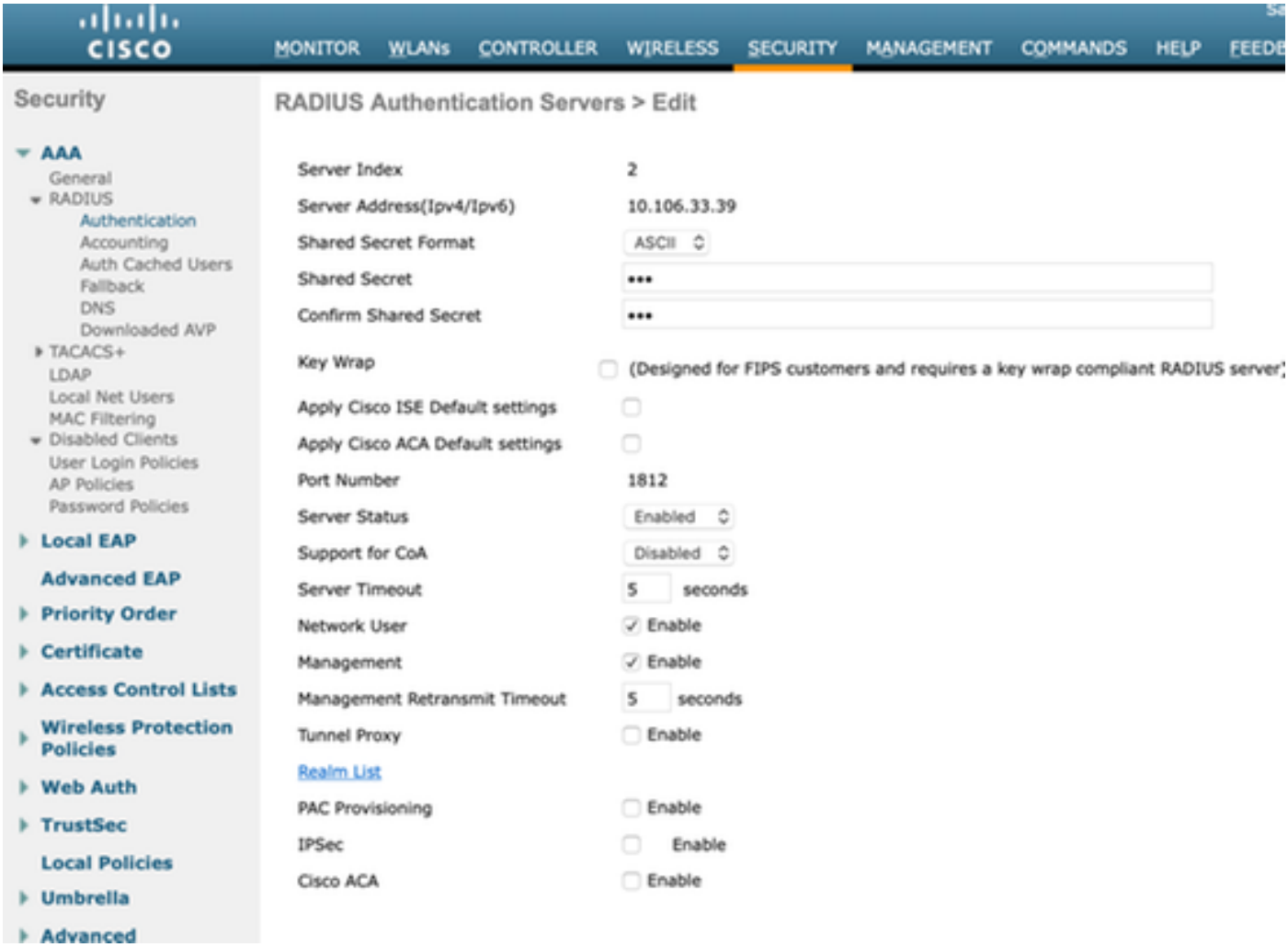
When WLC CLI/GUI is accessed, the user is prompted to enter the credentials to successfully log in. The credentials can be verified against either a local database or an external AAA server. In this document, Microsoft NPS is being used as the external authentication server.

Configurations

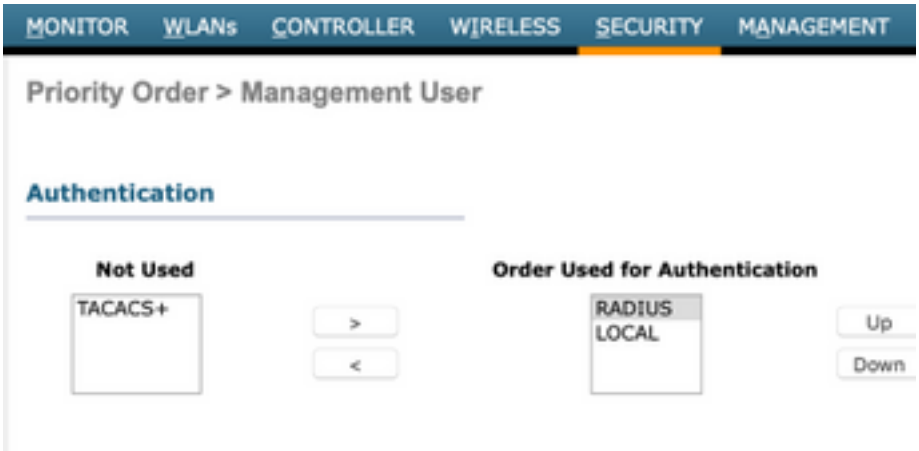
In this example, two users are configured on the AAA (NPS) viz. **loginuser** and **adminuser**. **loginuser** has just the read-only access while **adminuser** is granted full access.

WLC Configuration

Step 1. Add the RADIUS server on the controller. Navigate to **Security > RADIUS > Authentication**. Click **New** to add the server. Ensure **management** option is enabled so that this server can be used for management access, as shown in this image.



Step 2. Navigate to **Security > Priority Order > Management User**. Ensure that the RADIUS is selected as one of the authentication types.

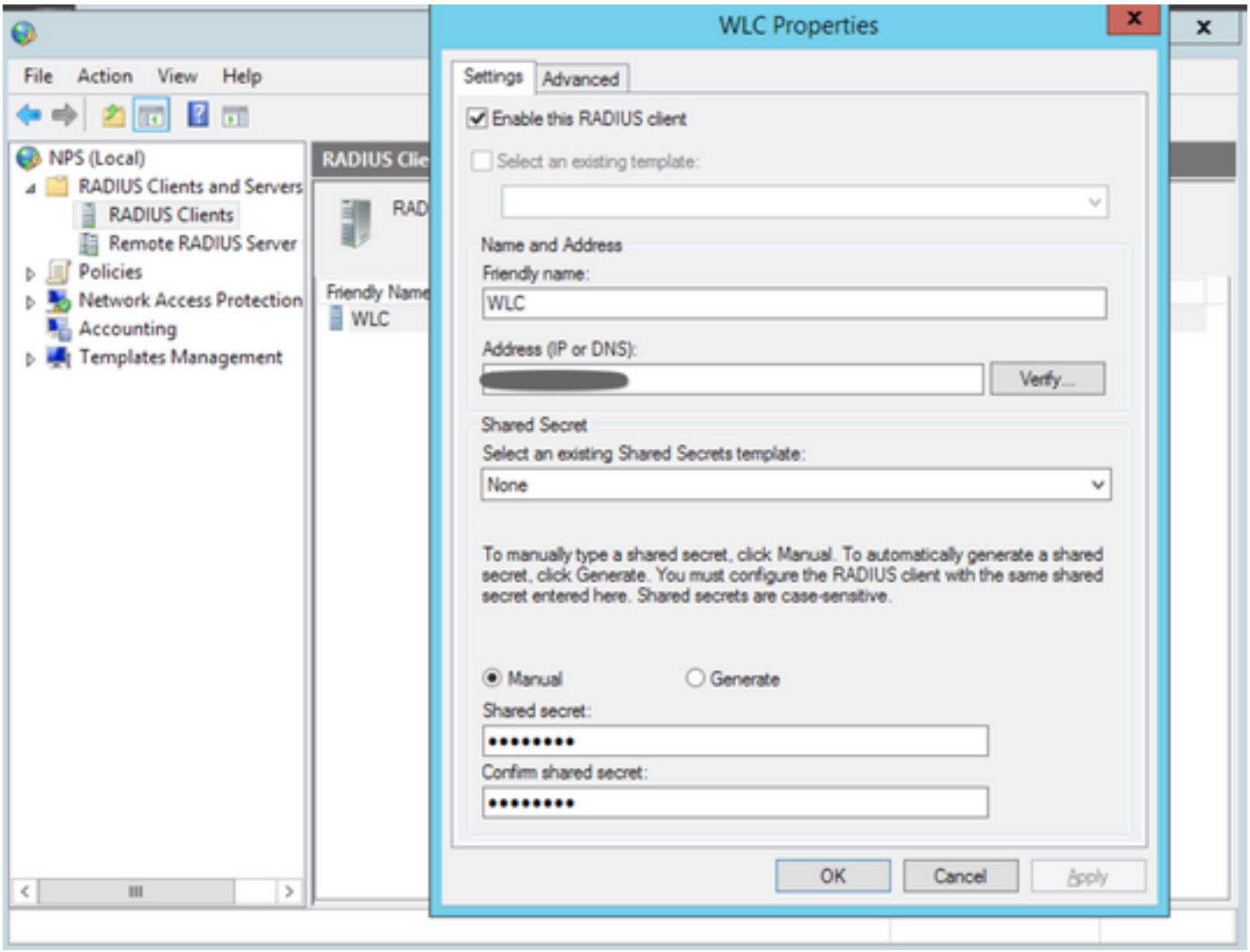


> **Note**: If RADIUS is selected as the first priority in the authentication order, local credentials will be used for authentication only if the RADIUS server is unreachable. If RADIUS is selected as a second priority, the RADIUS credentials will be first verified against the local database and then, checked against the configured RADIUS servers.

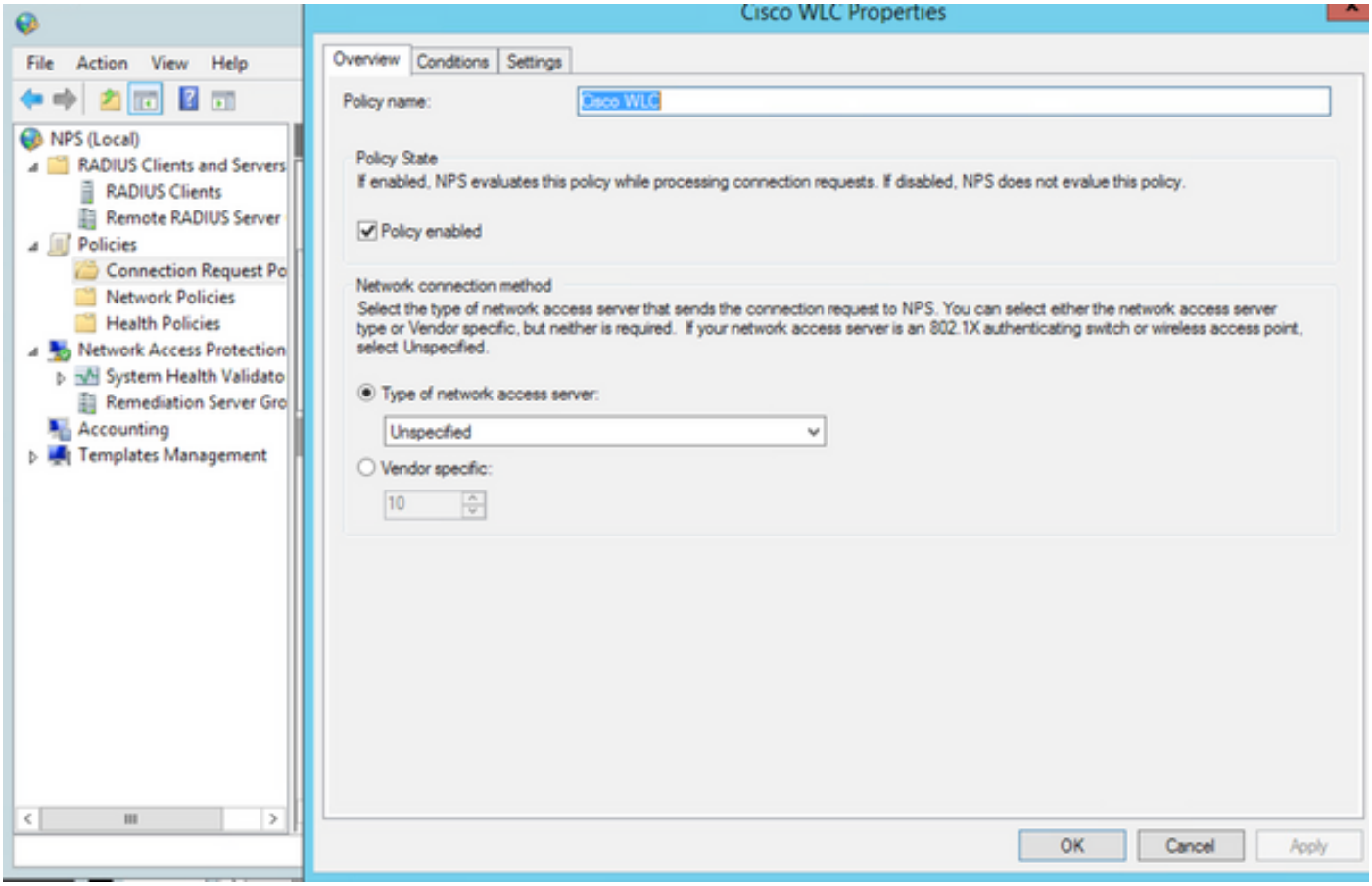
Microsoft NPS Configuration

Step 1. Open the Microsoft NPS server. Right-click on **Radius Clients**. Click **New** to add the WLC as the RADIUS client.

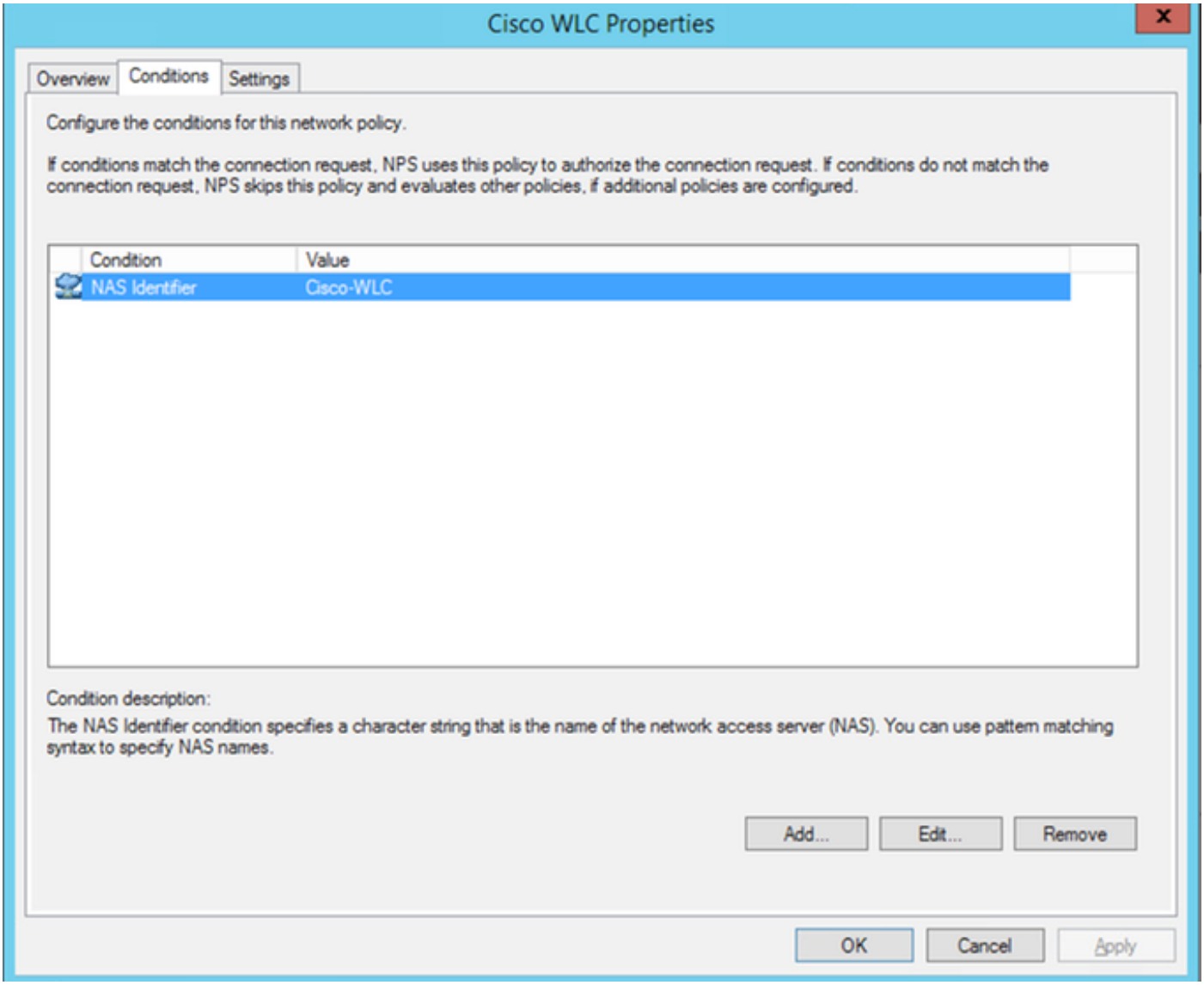
Enter the required details. Please ensure that the shared secret is the same as the one configured on the controller while the RADIUS server is added.



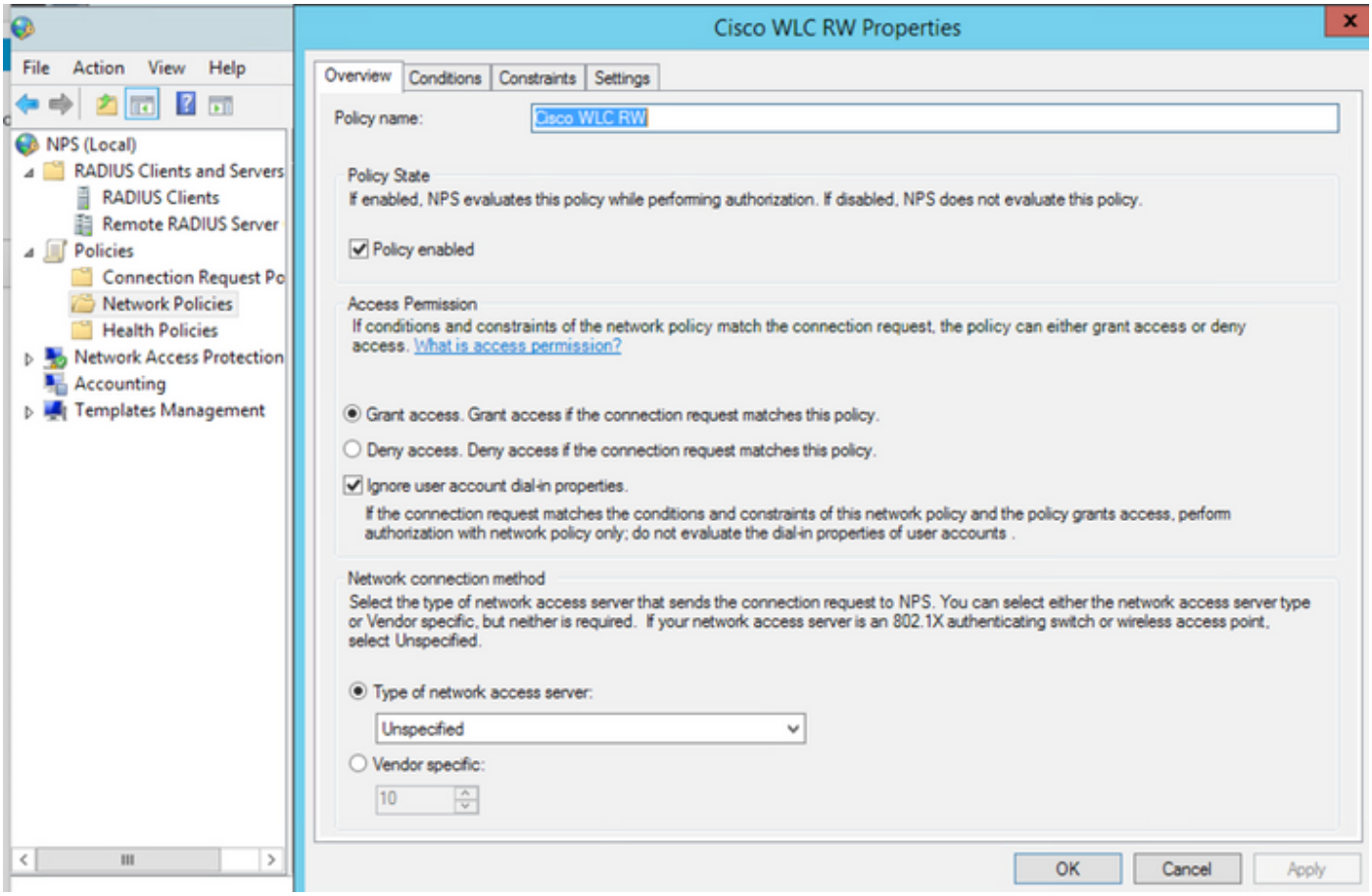
Step 2. Navigate to **Policies > Connection Request Policies**. Right-click to add a new policy, as shown in the image.



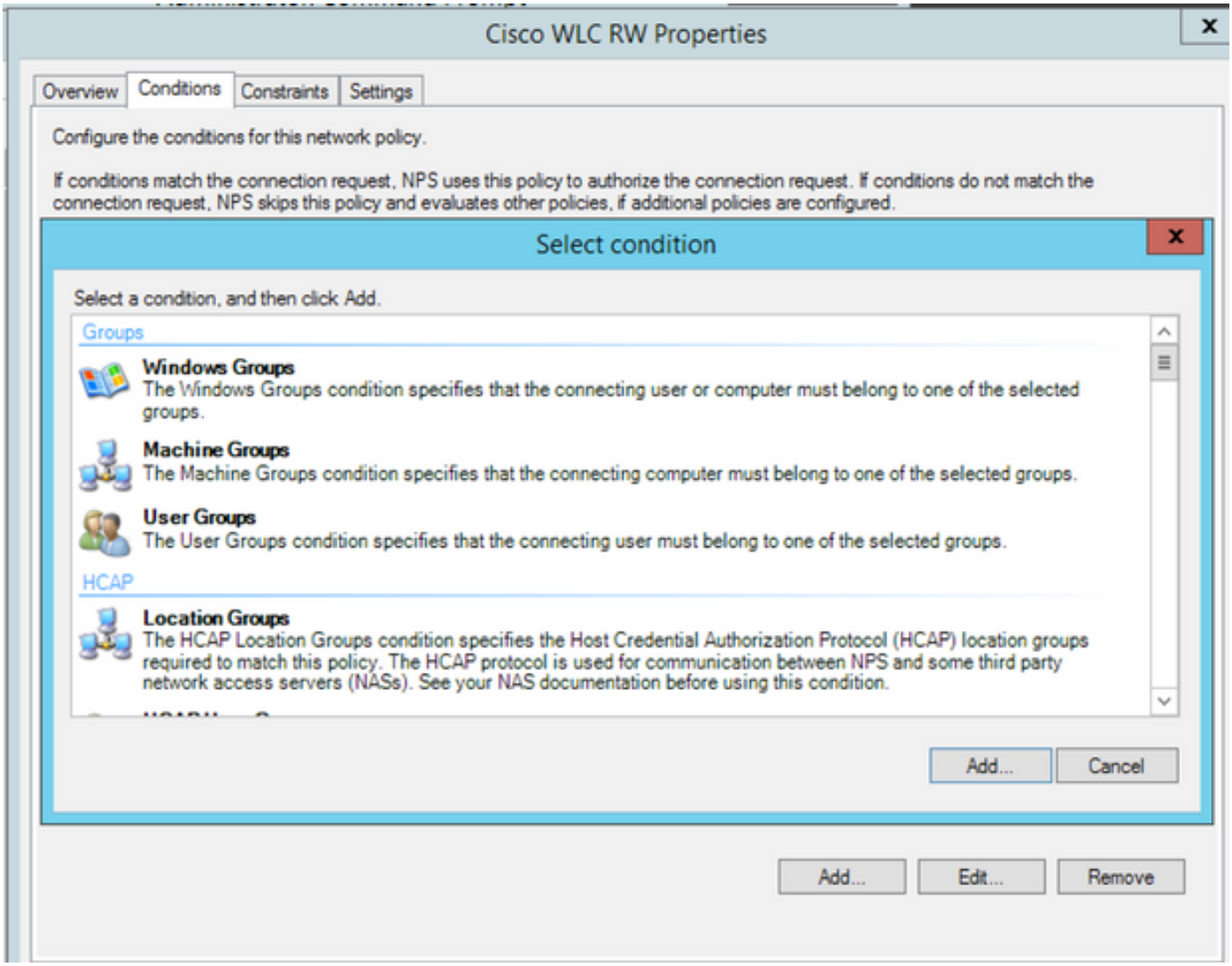
Step 3. Under the **Conditions** tab, select **NAS Identifier** as the new condition. When prompted, enter the hostname of the controller as the value, as shown in the image.



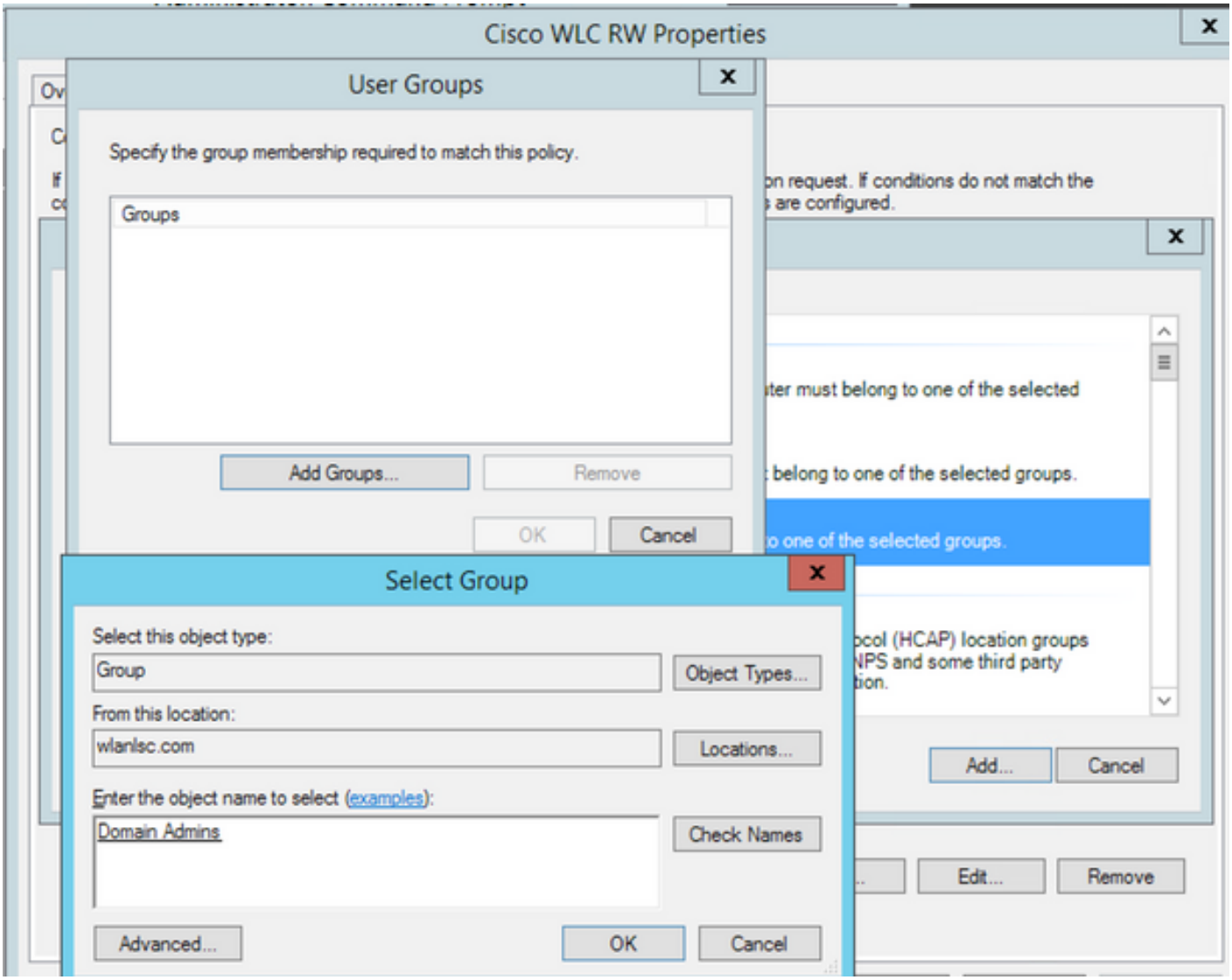
Step 4. Navigate to **Policies > Network Policies**. Right-click to add a new policy. In this example, the policy is named **Cisco WLC RW** which implies that the policy is used to provide full (read-write) access. Ensure that the policy is configured as shown here.



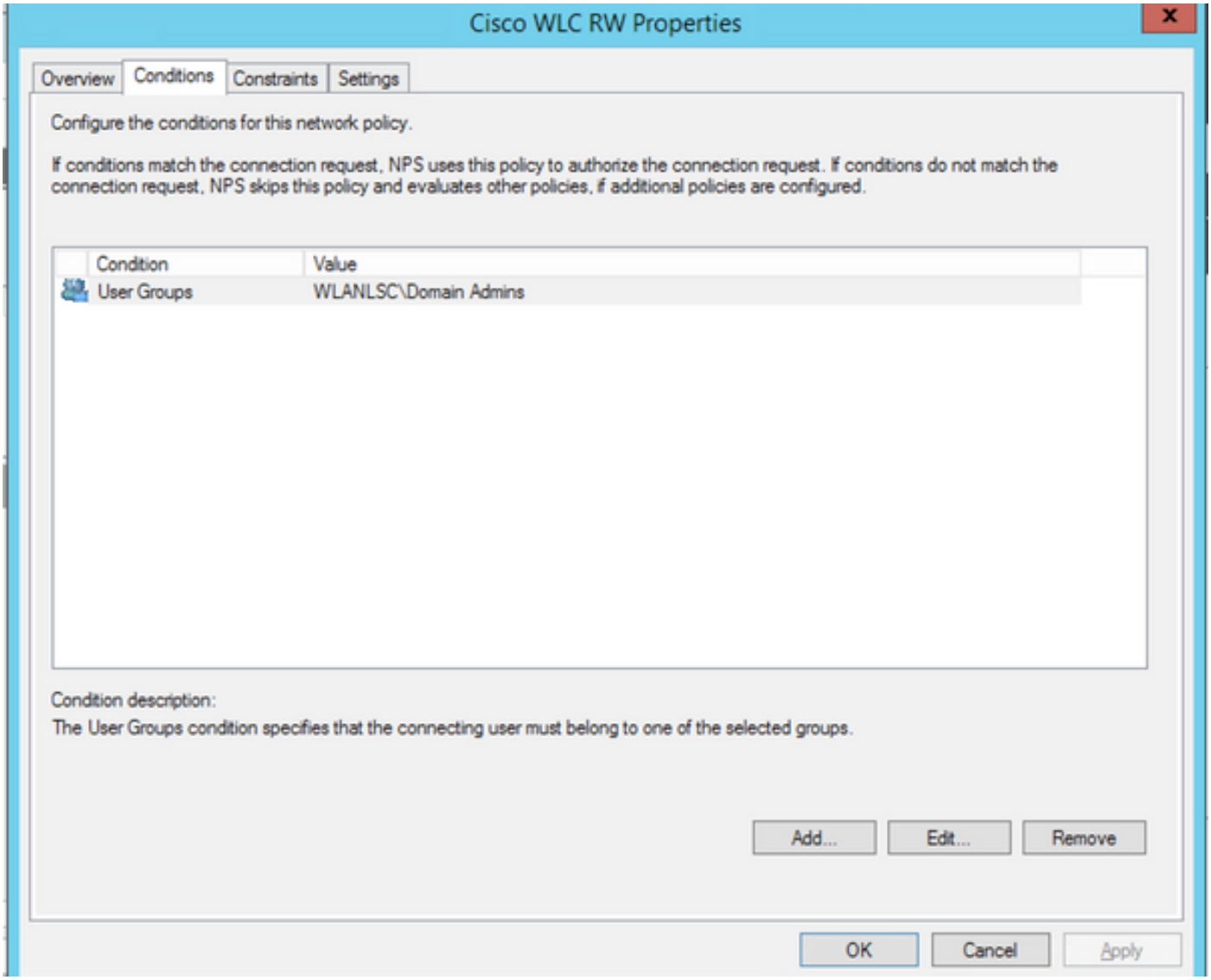
Step 5. Under the **Conditions** tab, click **Add**. Select the **User groups** and click **Add**, as shown in the image.



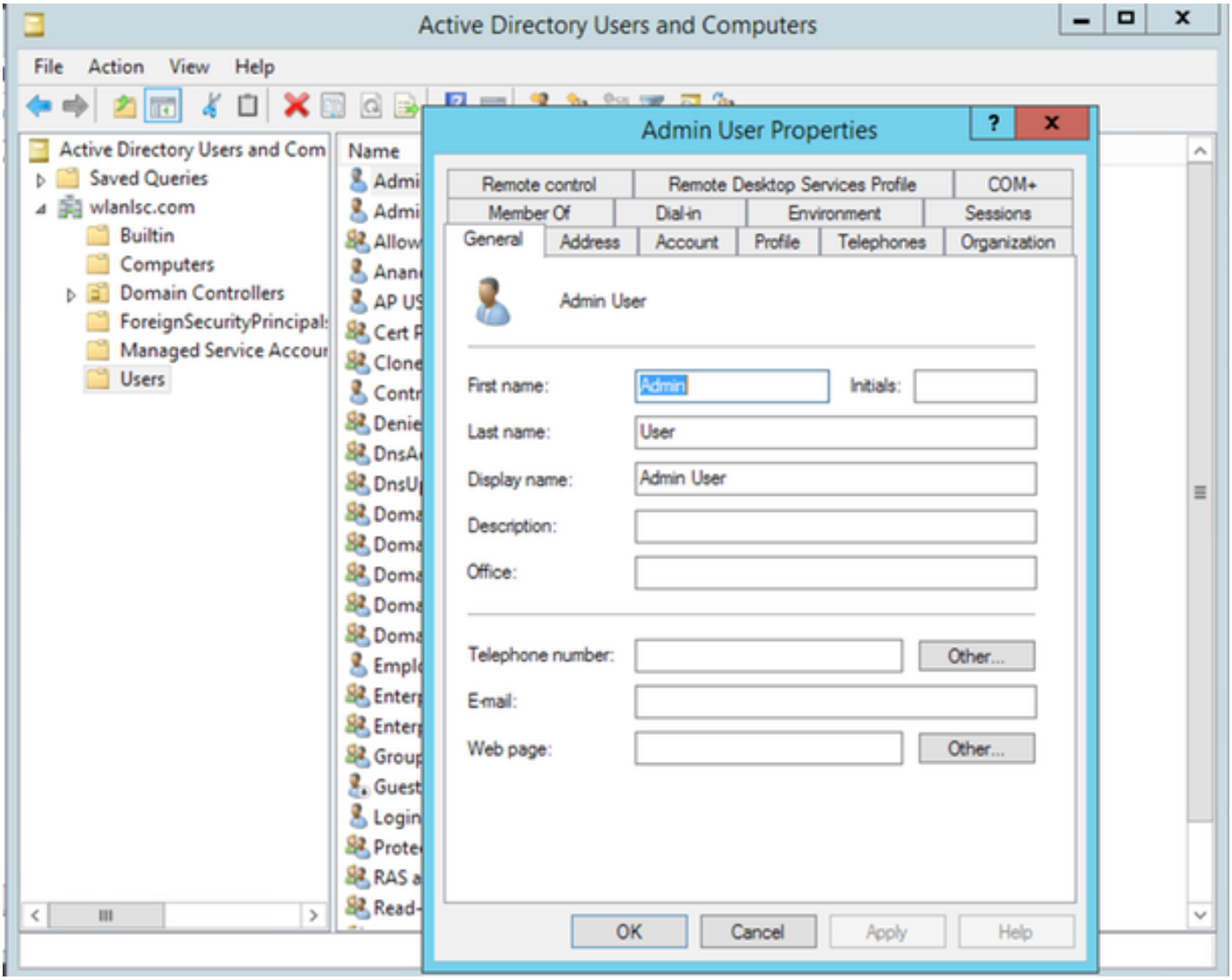
Step 6. Click on **Add Groups** on the dialog box that appears. On the **Select Group** window that appears, select the desired **object type** and **location** and enter the required object name, as shown in the image.

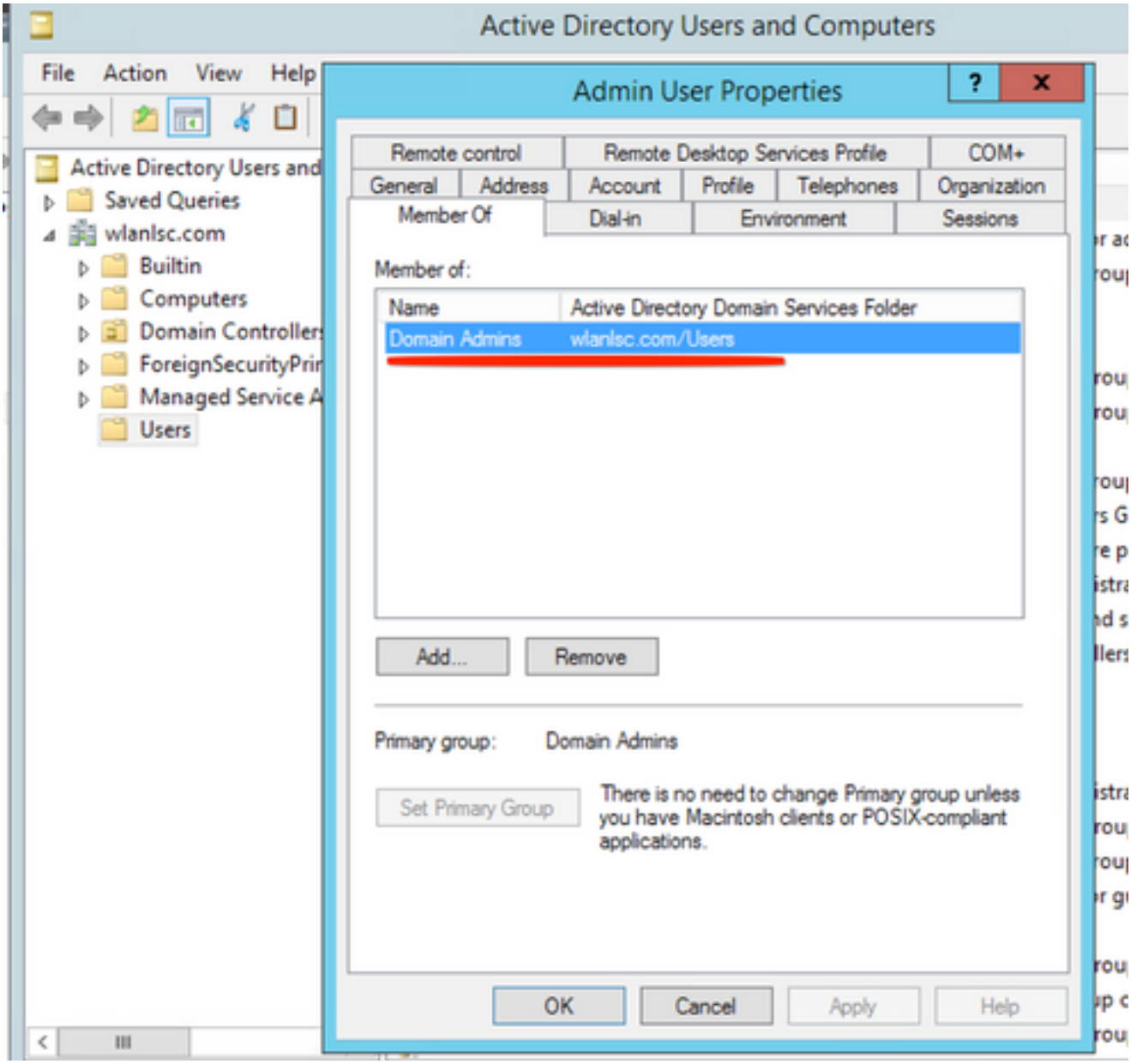


The condition, if added correctly, should look as shown here.

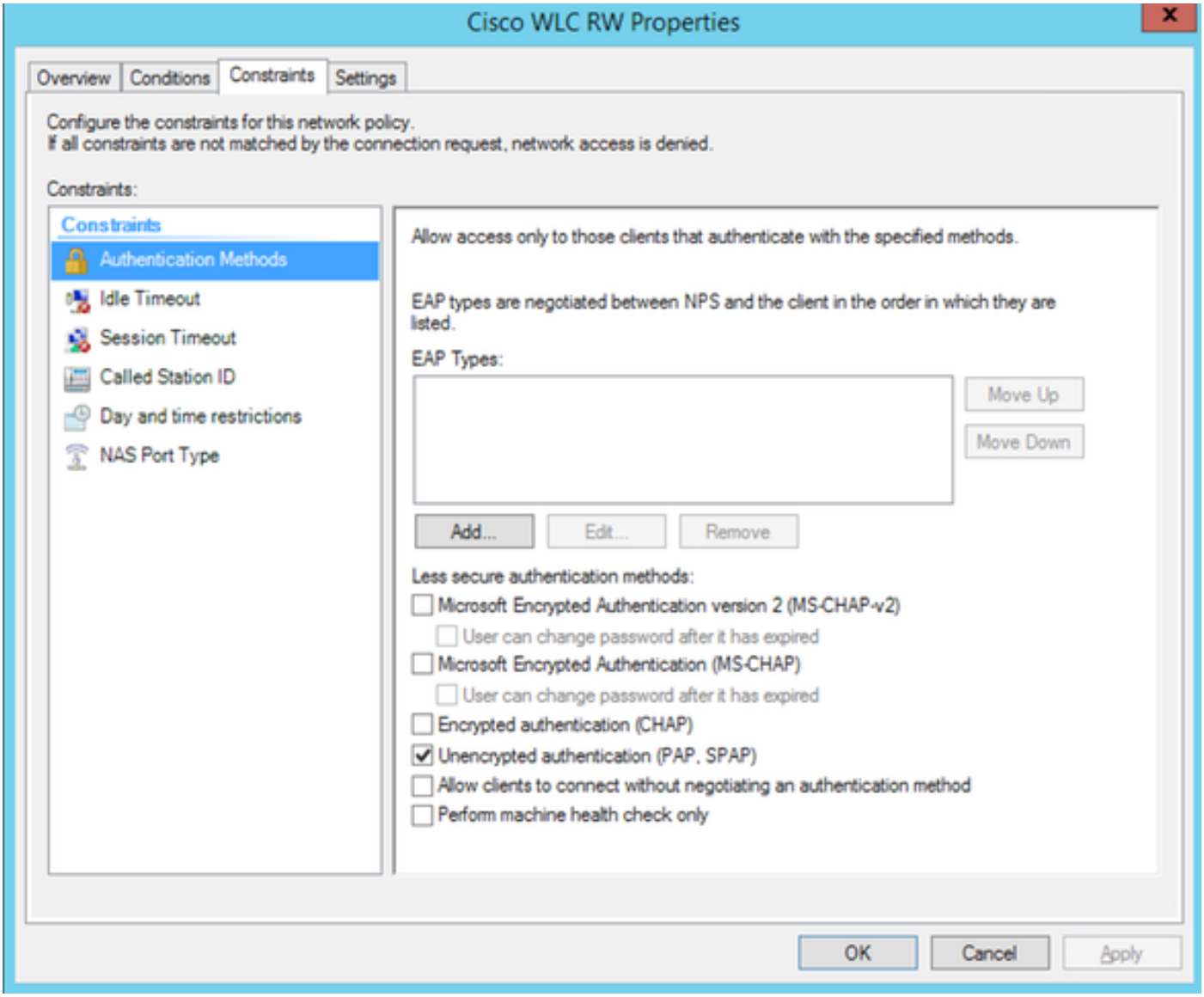


Note: To find out the location and object name details, open the active directory and look for the desired username. In this example, **Domain Admins** consists of users who are given full access. **adminuser** is part of this object name.

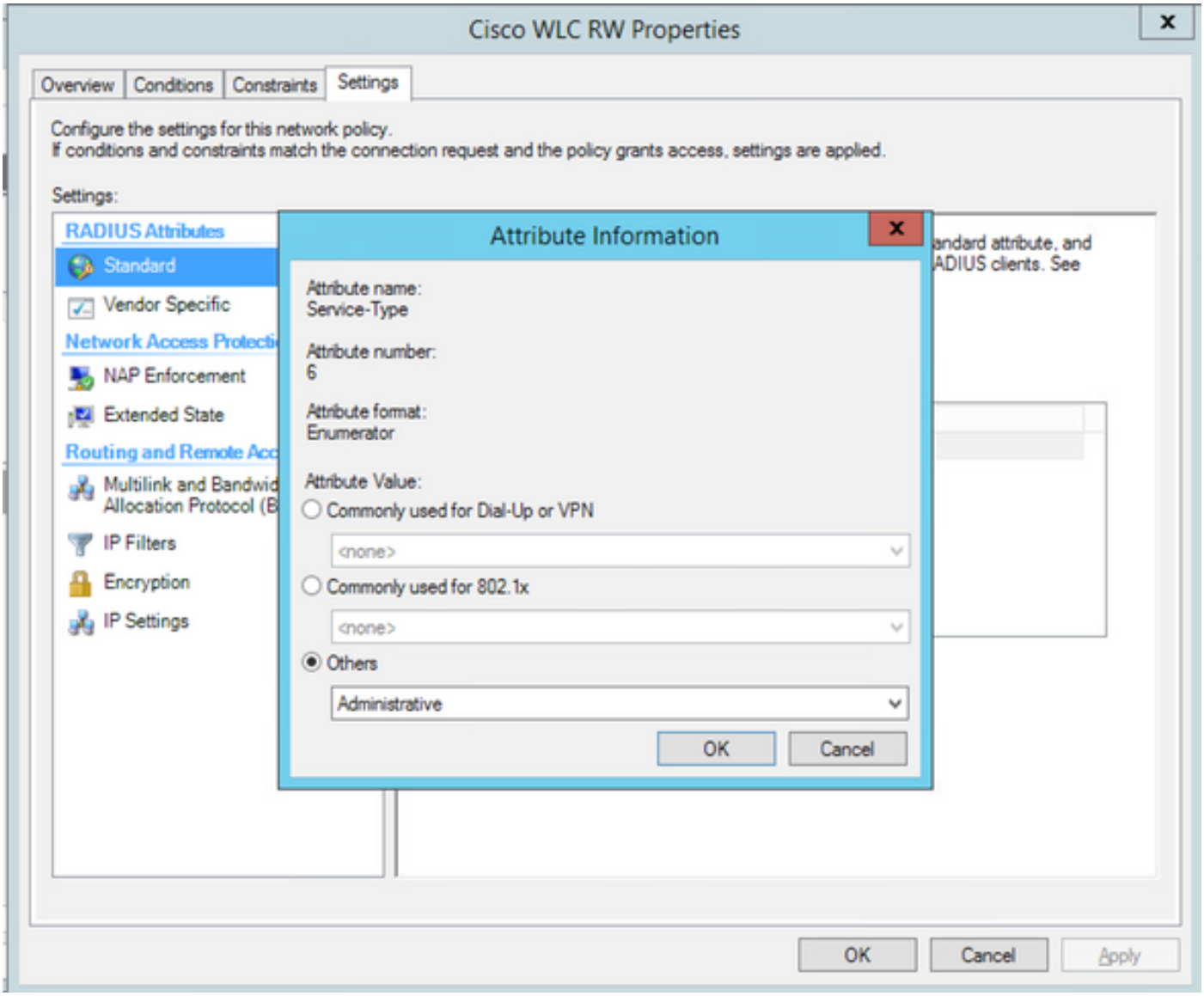

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
wlanlsc.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name
Admin User Properties
Remote control
Remote Desktop Services Profile
COM+
Member Of
Dial-in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



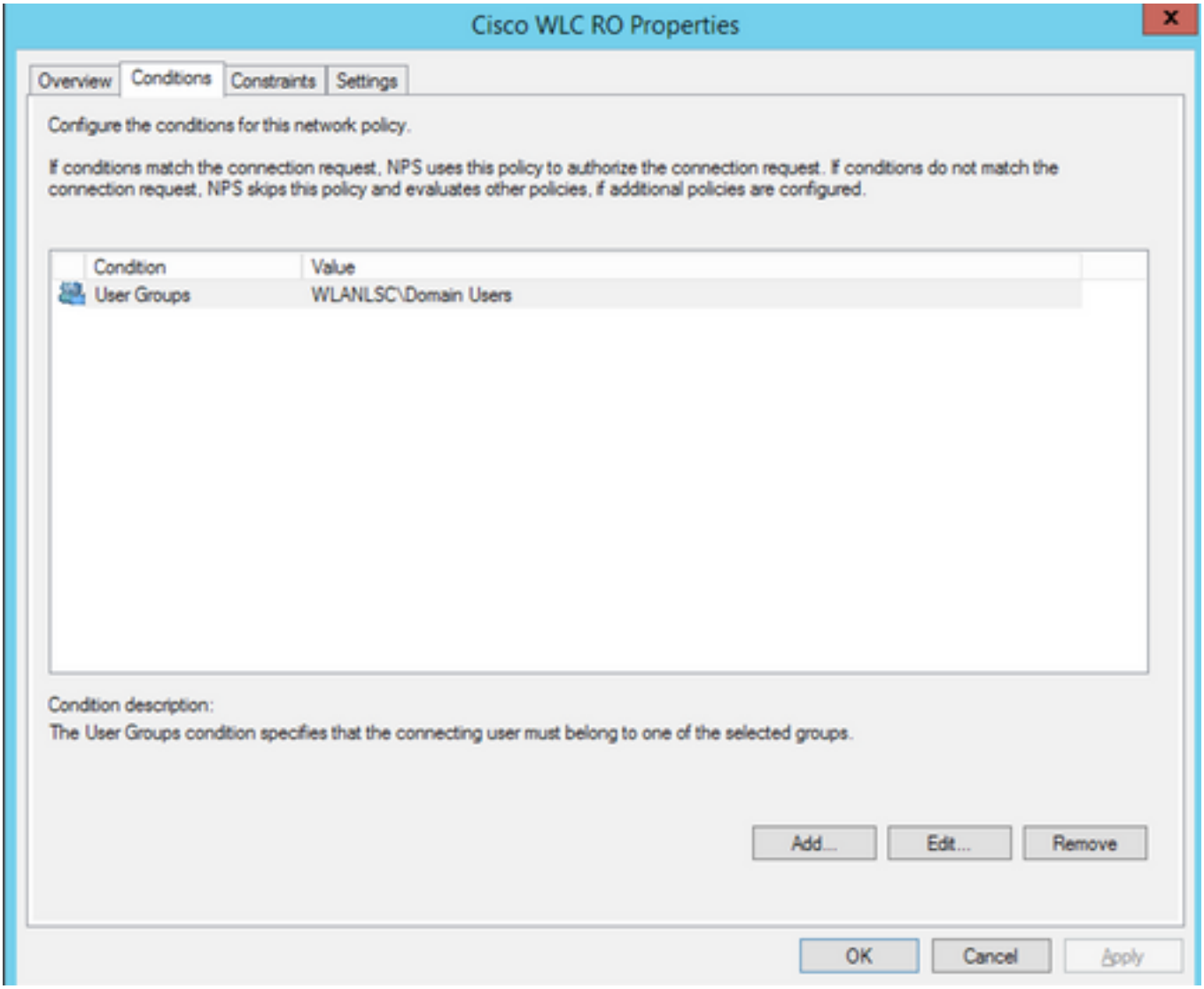
Step 7. Under the **Constraints** tab, navigate to **Authentication Methods** and ensure only **unencrypted authentication** is checked.

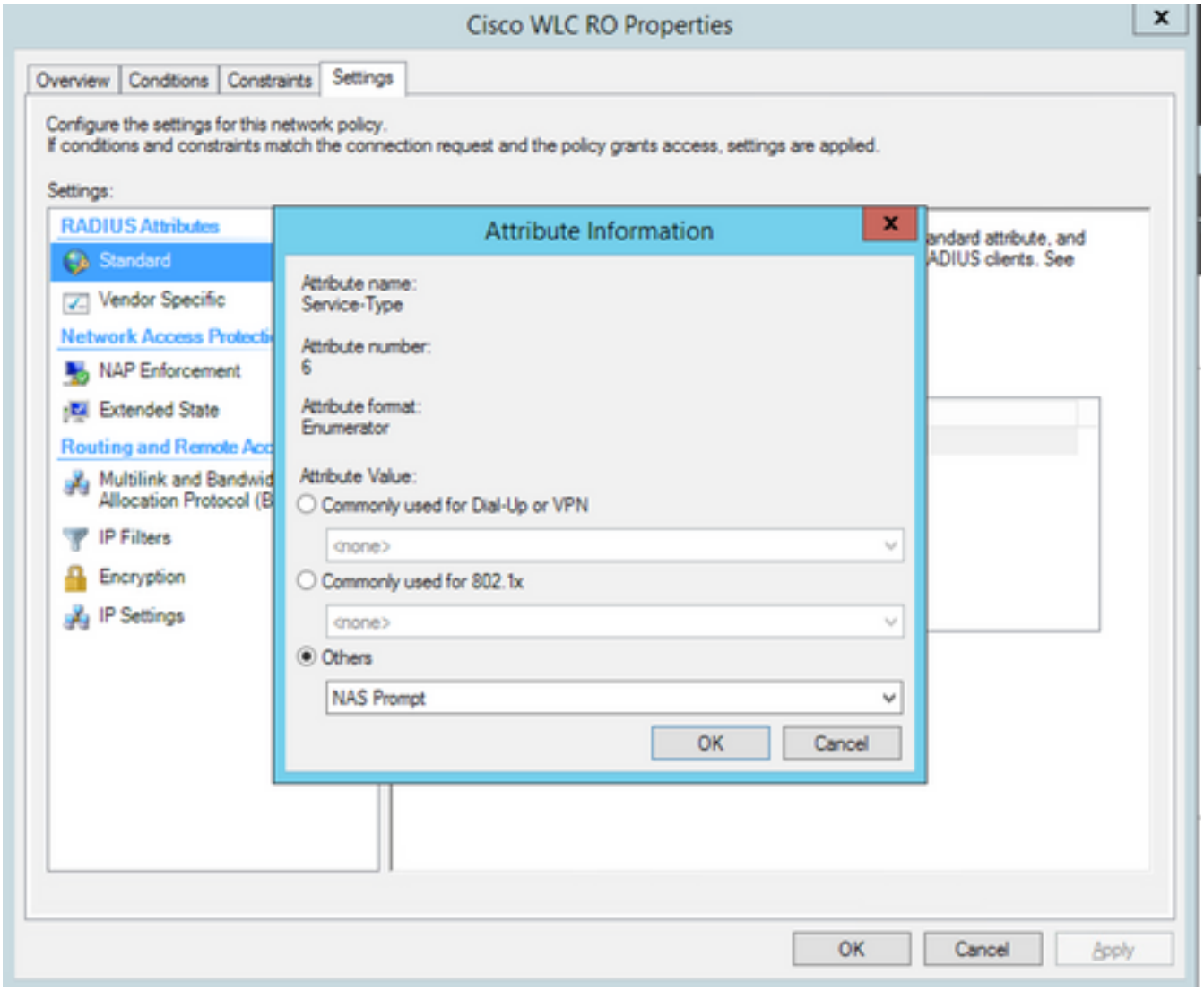


Step 8. Under the **Settings** tab, navigate to **RADIUS Attributes > Standard**. Click **Add** to add a new attribute, **Service-Type**. From the drop-down menu, select **Administrative** to provide full access to the users mapped to this policy. Click on Apply to save the changes, as shown in the image.



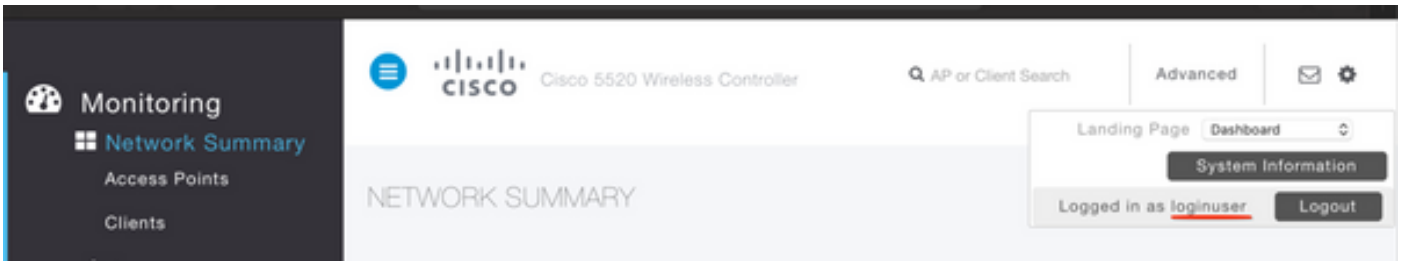
Note: If you want to give read-only access to specific users, select NAS-Prompt from the drop-down. In this example, another policy named **Cisco WLC RO** is created to provide read-only access to users under **Domain Users** object name.

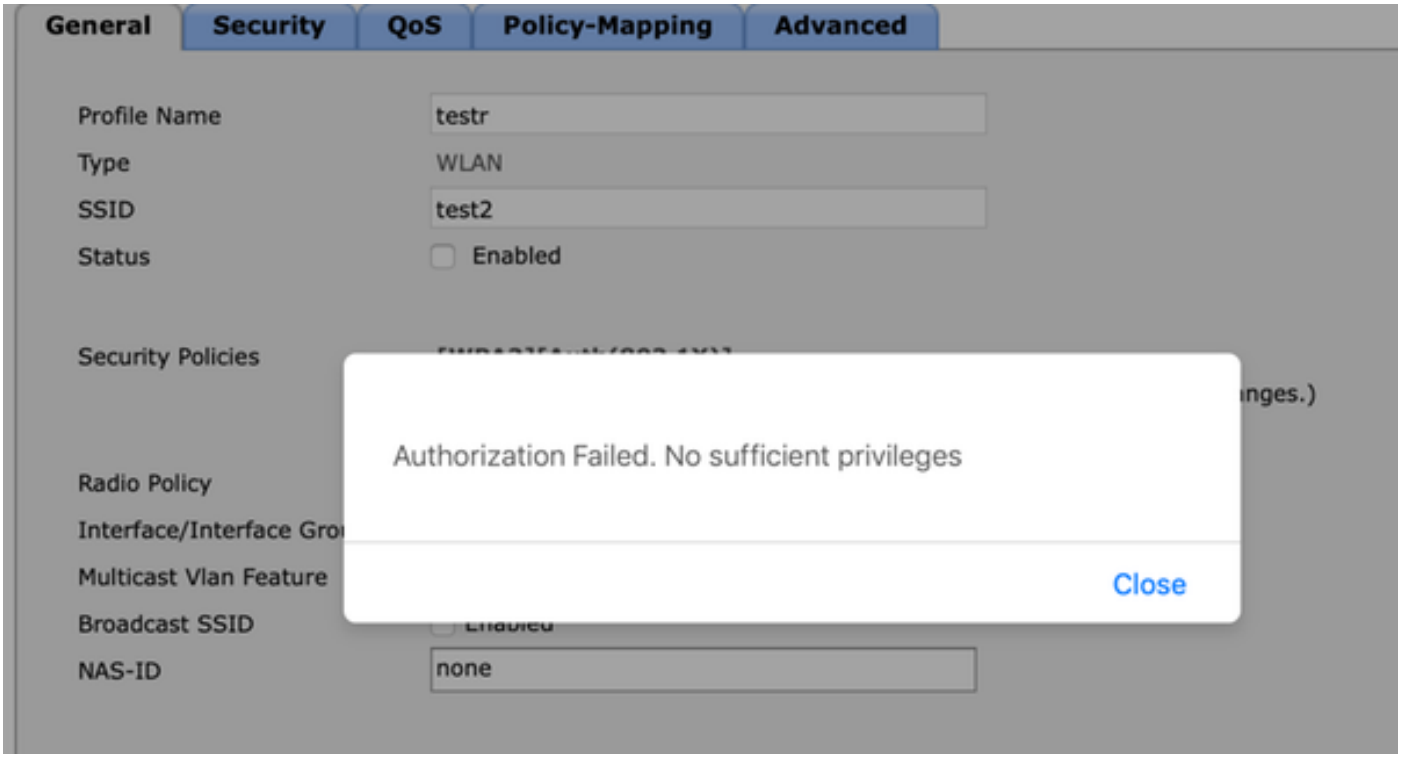

Cisco WLC RO Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates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



Verify

1. When **loginuser** credentials are used, the user is not allowed to configure any changes on the controller.

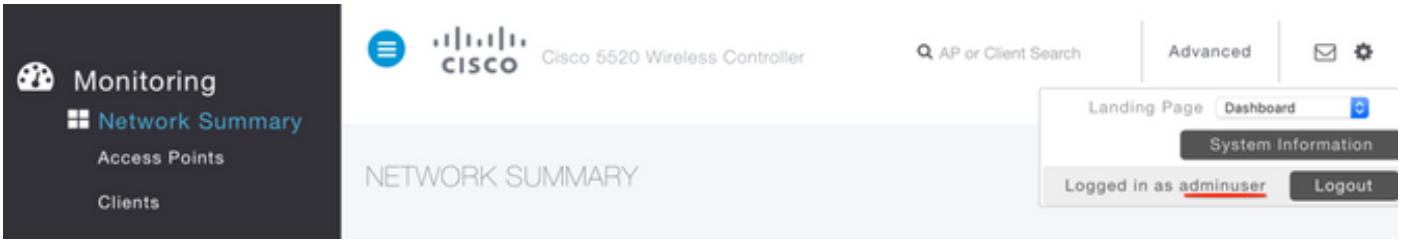




From **debug aaa all enable**, you can see that the service-type attribute's value in authorization response is 7 which corresponds to NAS-prompt.

```
*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. When **adminuser** credentials are used, the user should have full access with **service-type** value 6, which corresponds to **administrative**.




```
*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)
```

Troubleshoot

In order to troubleshoot management access to WLC through NPS, run **debug aaa all enable** command.

1. The logs when incorrect credentials are used is shown here.

```
*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. The logs when service-type is used with a value other than **Administrative (value=6)** or **NAS-prompt (value=7)** is shown as follows. In such a case, login fails even if authentication succeeds**.**

```
*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
```