Microsoft NPSによるAireOS WLCの管理アクセス

内容

概要

このドキュメントでは、Microsoft Network Policy Server(NPS)を使用してAireOS WLC GUIおよびCLIの管理アクセスを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ワイヤレスセキュリティソリューションに関する知識
- AAAおよびRADIUSの概念
- Microsoft Server 2012の基礎知識
- Microsoft NPSおよびActive Directory(AD)のインストール

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアおよびハードウェアコンポーネントに基づいています。

- 8.8.120.0のAireOSコントローラ(5520)
- Microsoft Server 2012

注：このドキュメントは、WLC管理アクセスにMicrosoftサーバで必要な設定例を読者に示すことを目的としています。このドキュメントで示す Microsoft Windows サーバの設定はラボでテスト済みで、期待通りに動作することが確認されています。設定で問題が発生した場合は、Microsoft に支援を求めてください。Cisco Technical Assistance Center(TAC)は、Microsoft Windowsサーバの設定をサポートしていません。Microsoft Windows 2012 のイン

ストール ガイドと設定ガイドは Microsoft Tech Net にあります。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

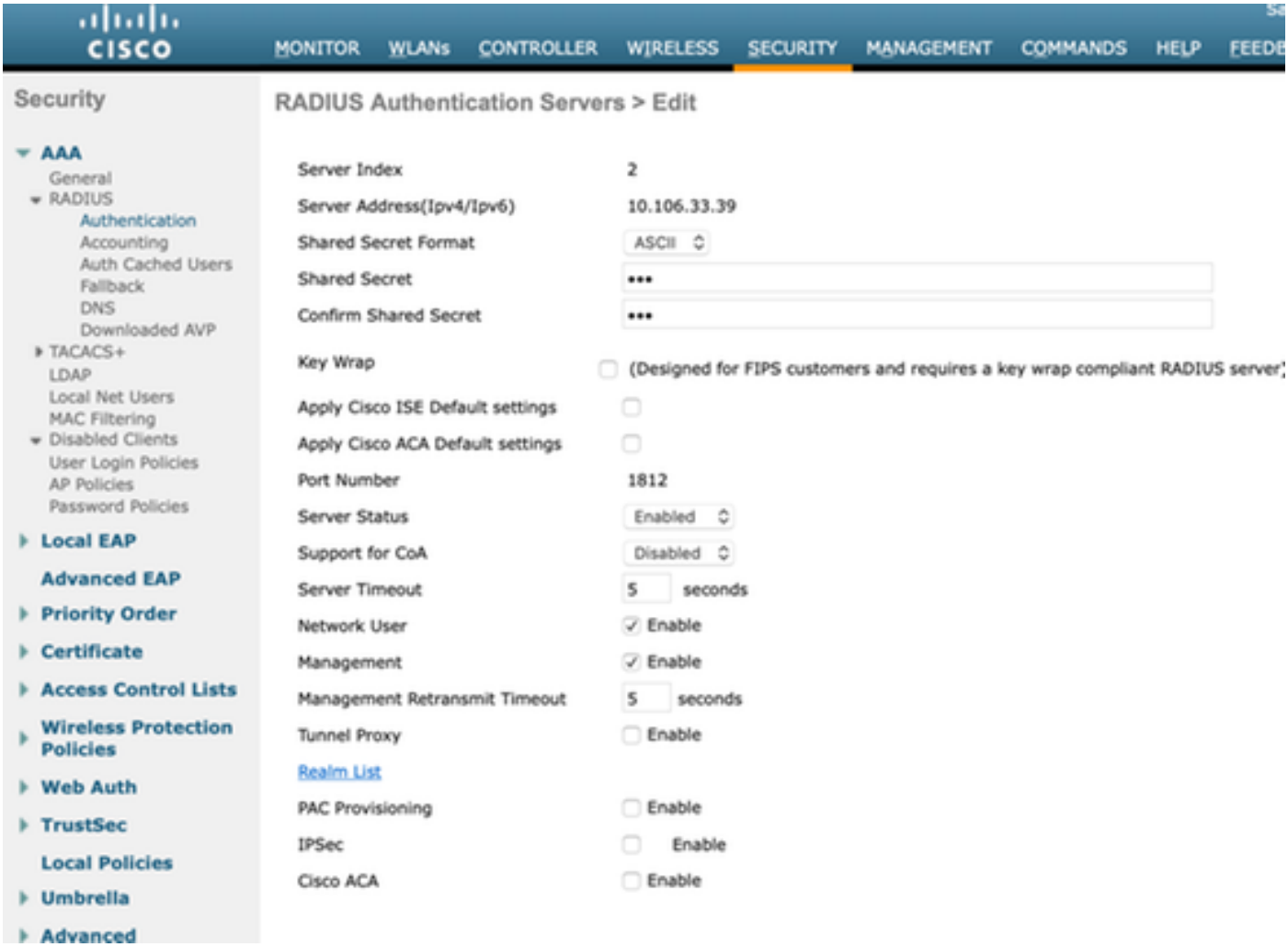
WLC CLI/GUIにアクセスすると、ユーザはログインに成功するためのクレデンシャルの入力を求められます。クレデンシャルは、ローカルデータベースまたは外部AAAサーバに対して確認できます。このドキュメントでは、外部認証サーバとしてMicrosoft NPSを使用しています。

設定

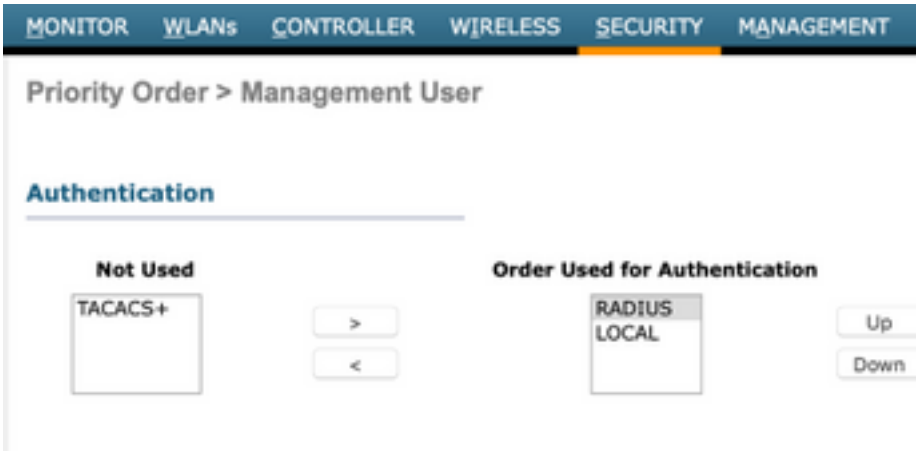
この例では、AAA(NPS)vizに2人のユーザが設定されています。**loginuser**と**adminuser**です。**loginuserは読み取り**専用アクセスを持ち、adminuserはフルアクセス**権を付与**されています。

WLC の設定

ステップ1：コントローラにRADIUSサーバを追加します。[Security] > [RADIUS] > [Authentication]**に移動します**。[新規]を**クリック**して、サーバを追加します。次の図に示**すように**、このサーバを管理アクセスに使用できるように、管理オプションが有効になっていることを確認します。



ステップ2:[Security] > **[Priority Order] > [Management User]に移動します**。認証タイプの1つとしてRADIUSが選択されていることを確認します。

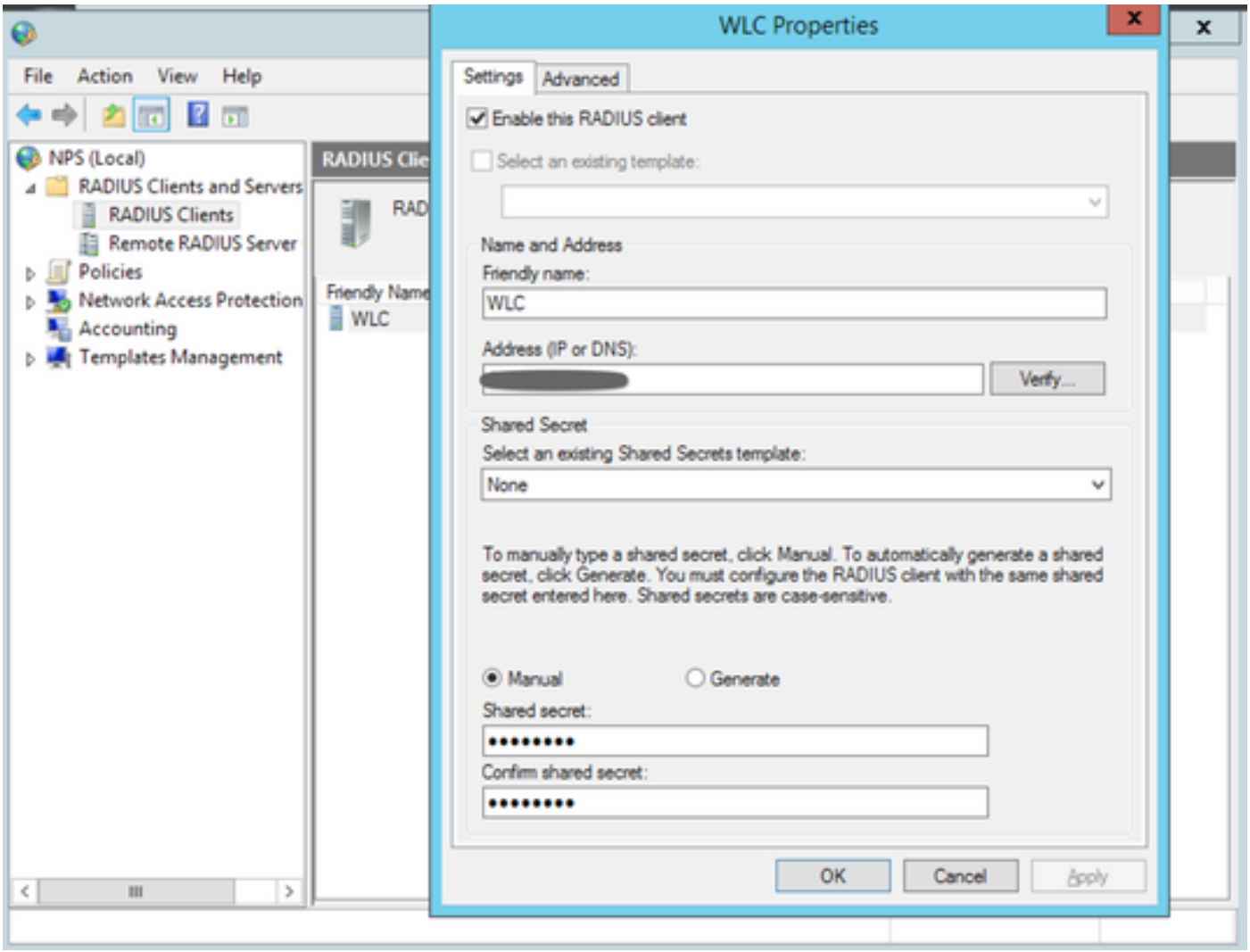


注：認証順序でRADIUSが最初の優先順位として選択されている場合、ローカルクレデンシャルはRADIUSサーバに到達できない場合にのみ認証に使用されます。RADIUSが2番目の優先順位として選択されている場合、RADIUSクレデンシャルは最初にローカルデータベースに対して確認され、次に設定済みのRADIUSサーバに対して確認されます。

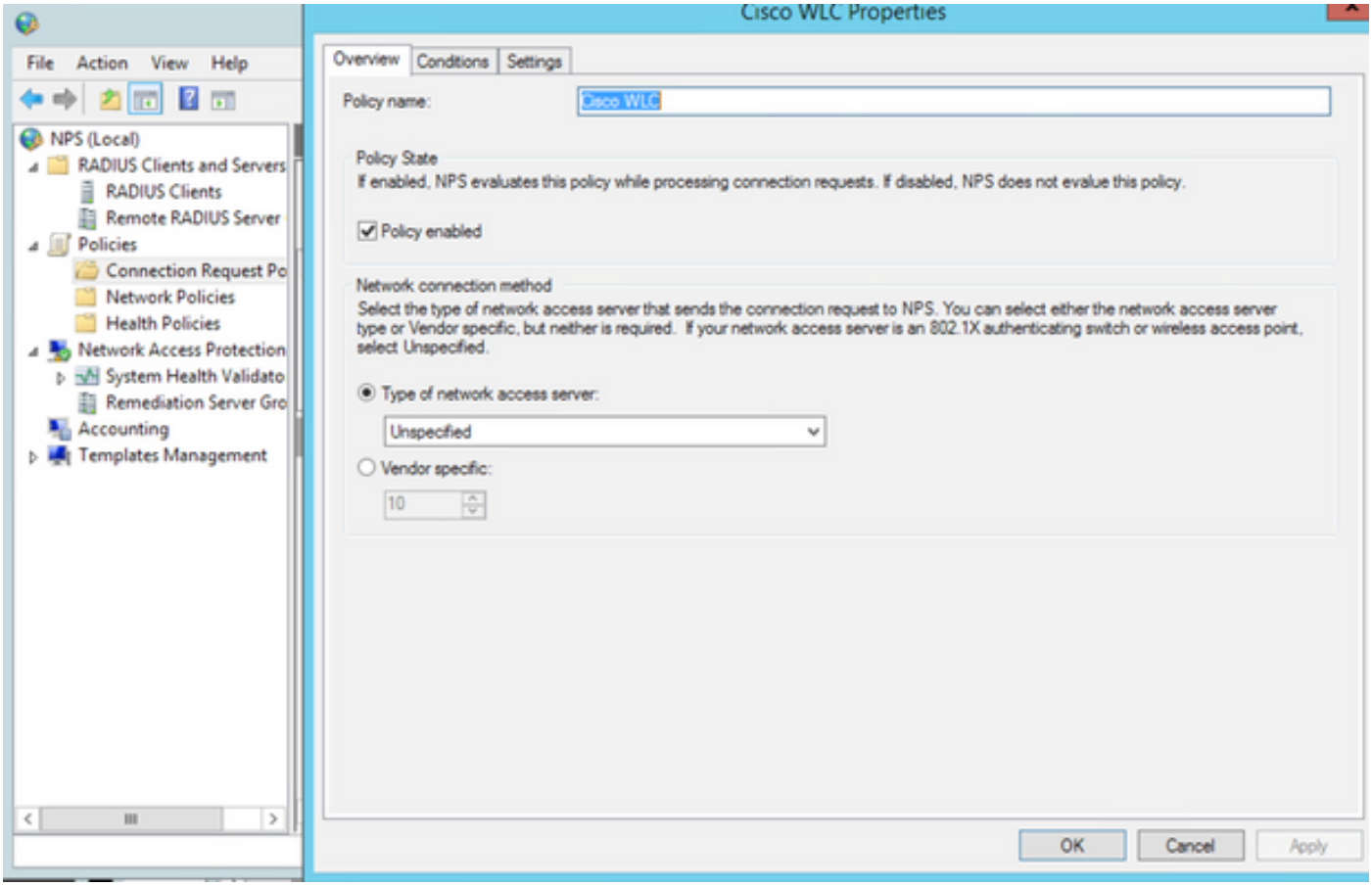
Microsoft NPSの構成

ステップ1: Microsoft NPSサーバーを開きます。[Radius Clients]を右クリックします。[New]をクリックして、WLCをRADIUSクライアントとして追加します。

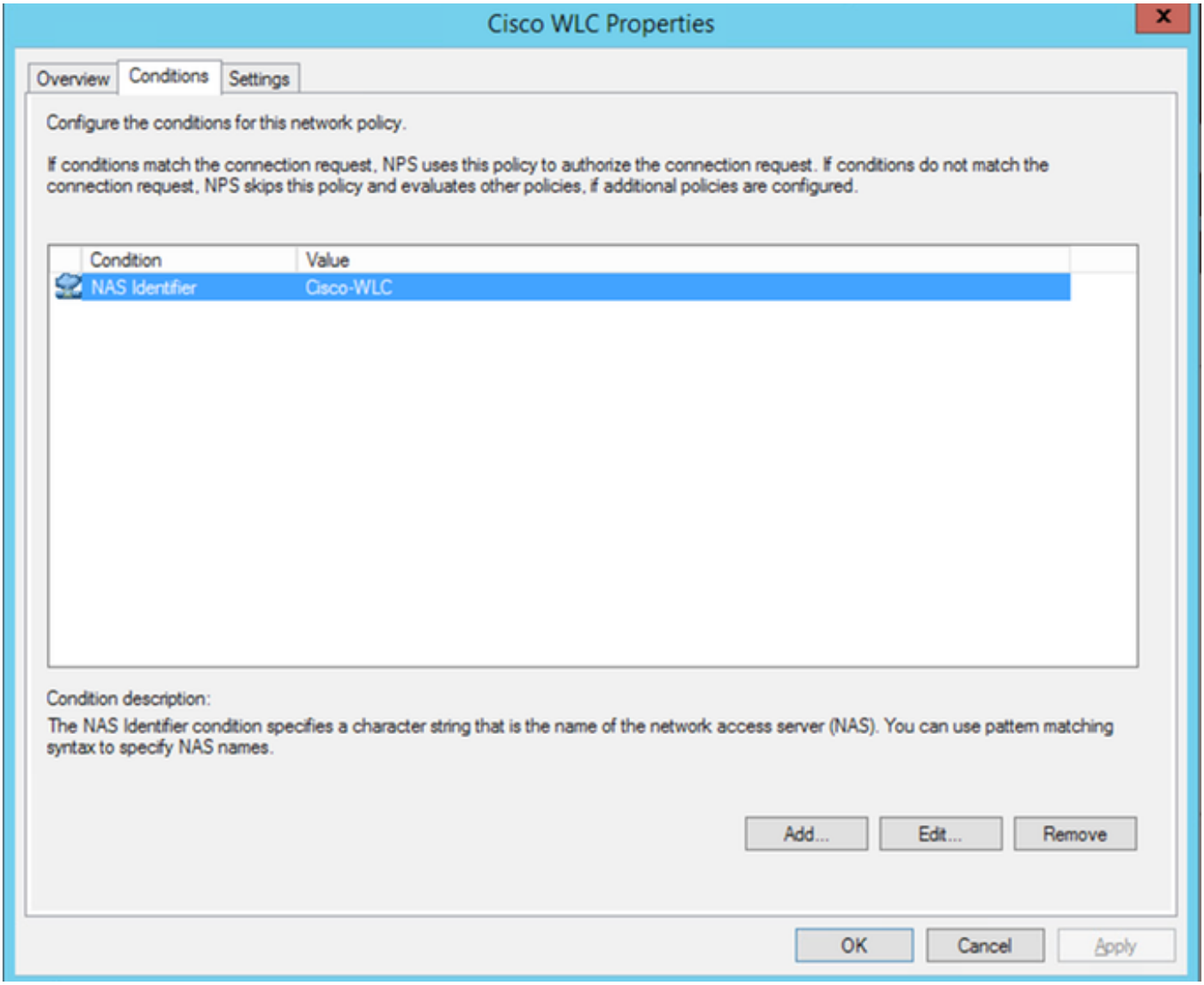
必要な詳細を入力します。RADIUSサーバの追加時に、コントローラに設定されている共有秘密と同じであることを確認してください。



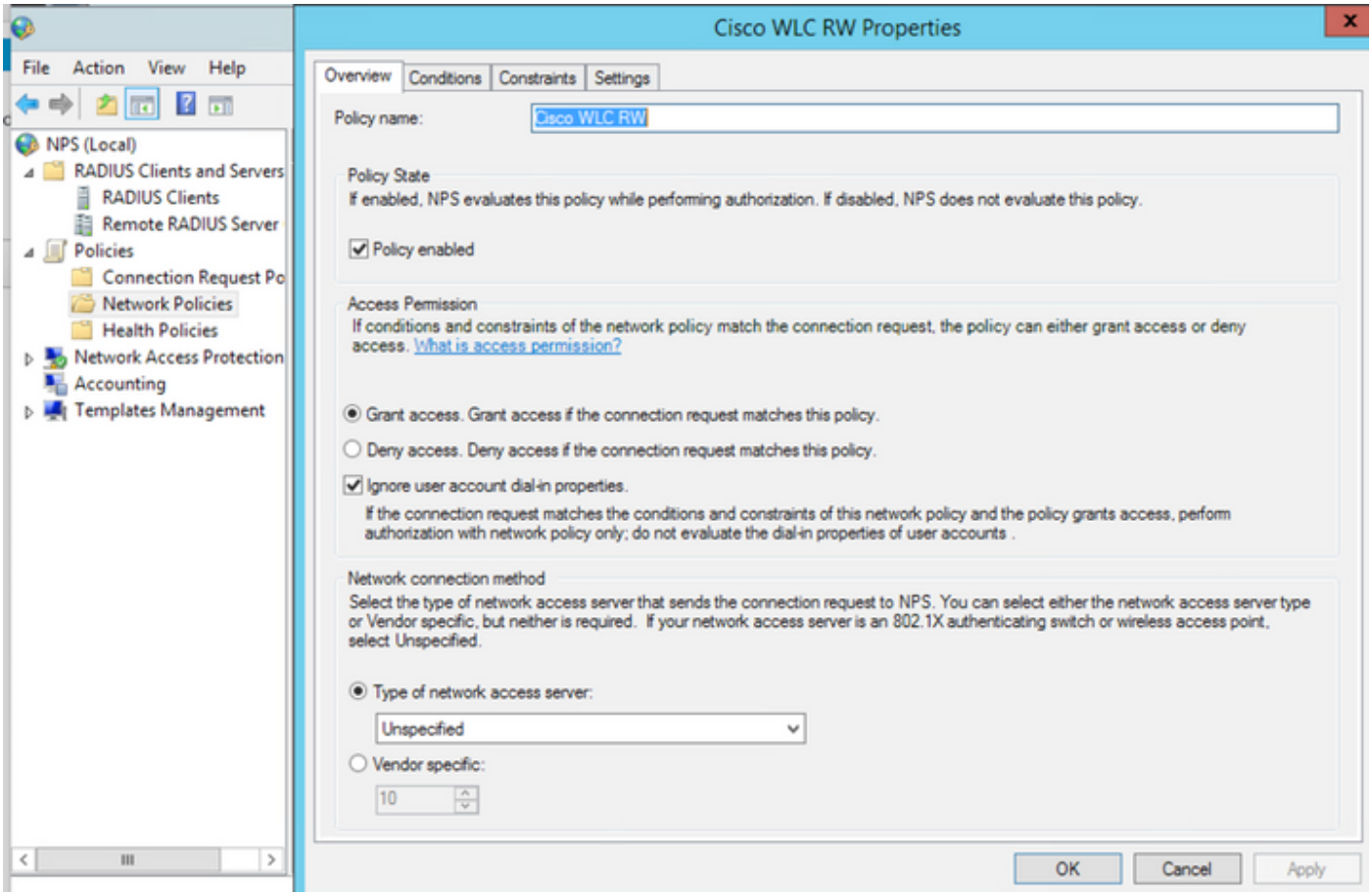
ステップ2:[Policies] > [**Connection Request Policies]に移動します。**右クリックして新しいポリシーを追加します（図を参照）。



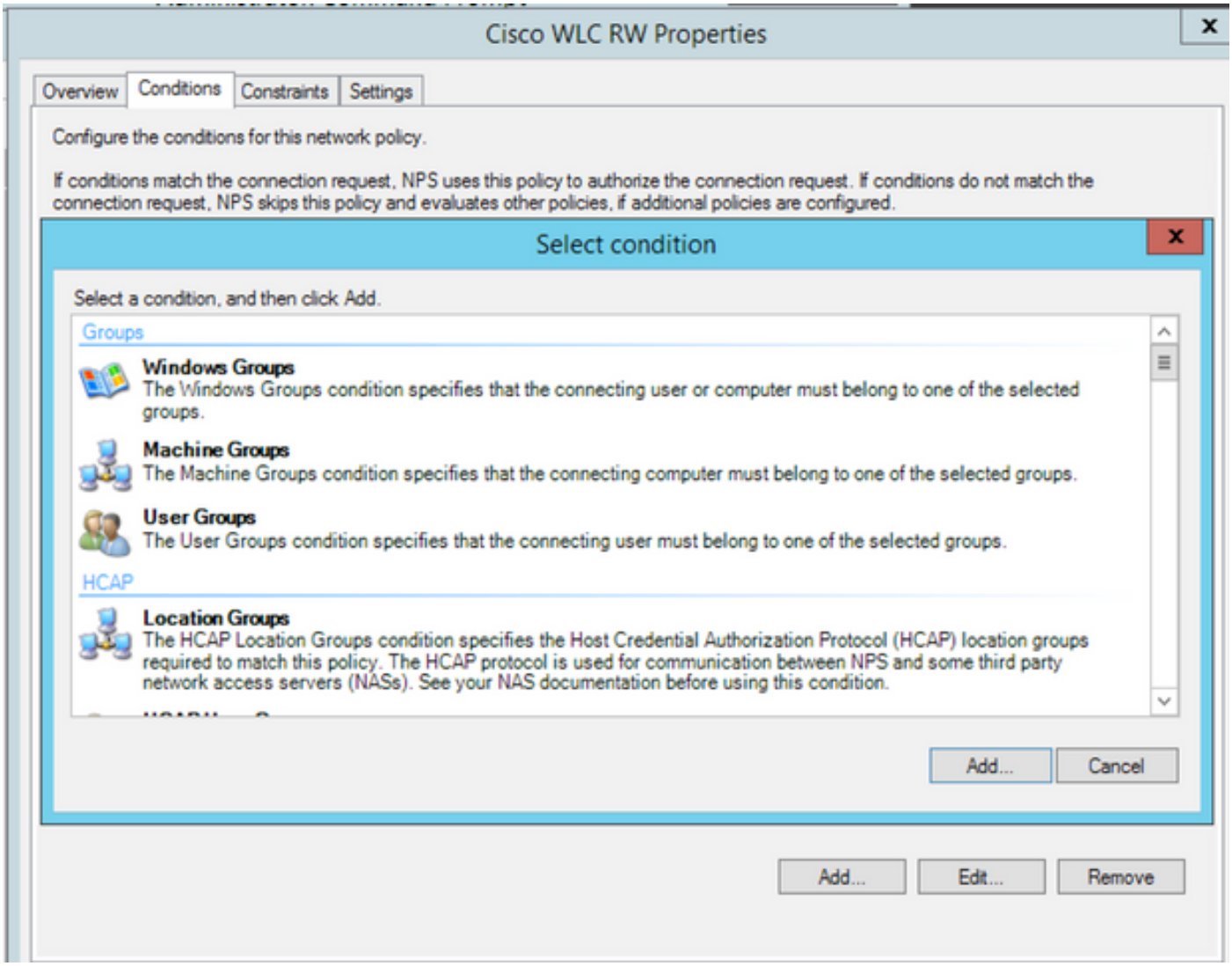
ステップ3:[Conditions]タブで、新しい条件として[NAS Identifier]を選択します。プロンプトが表示されたら、図に示すように、コントローラのホスト名を値として入力します。



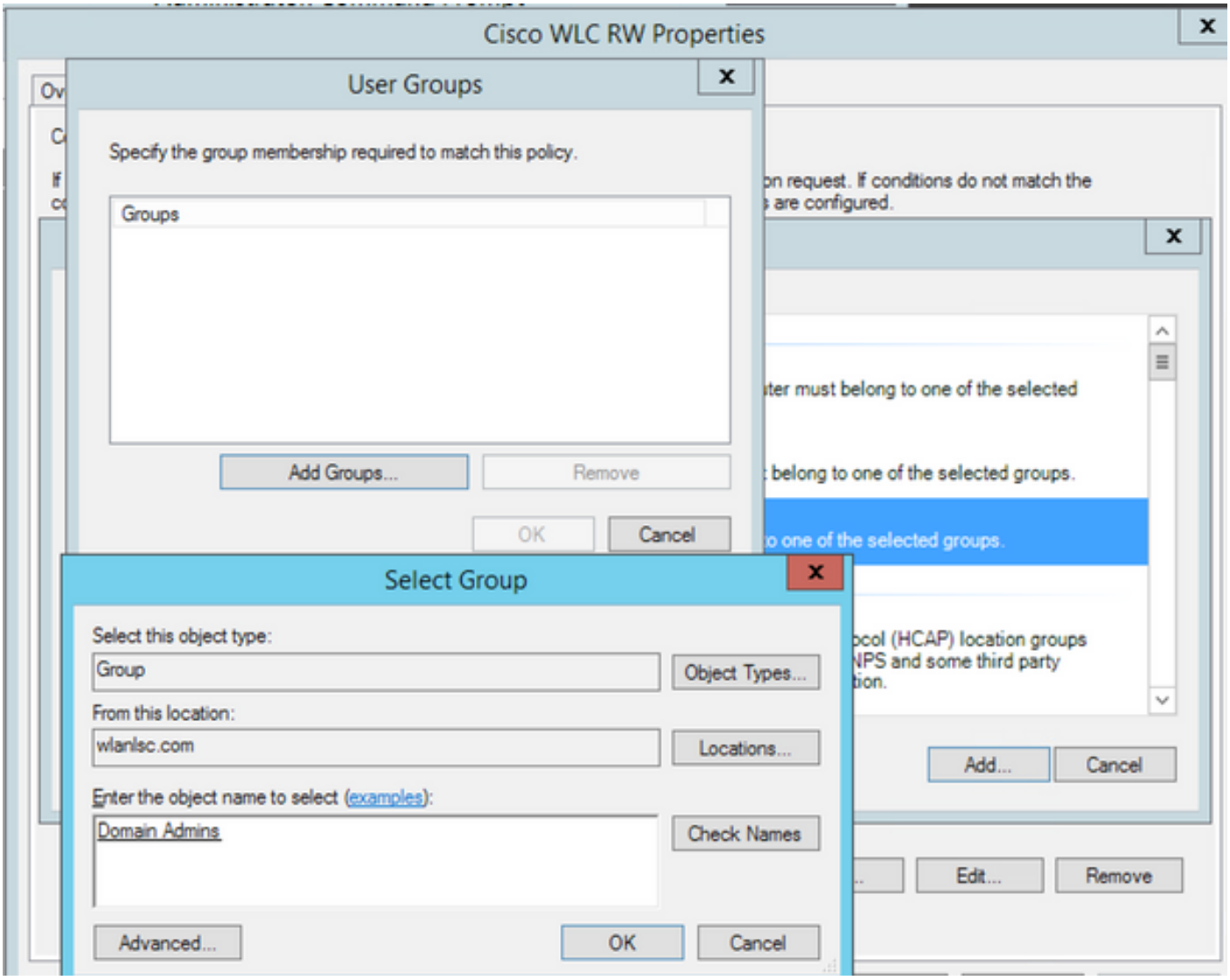
ステップ4:[Policies] > **[Network Policies]に移動します**。右クリックして新しいポリシーを追加します。この例では、ポリシーの名前は**Cisco WLC RW**です。これは、ポリシーがフル（読み取り/書き込み）アクセスを提供するために使用されていることを意味します。ポリシーが次のように設定されていることを確認します。



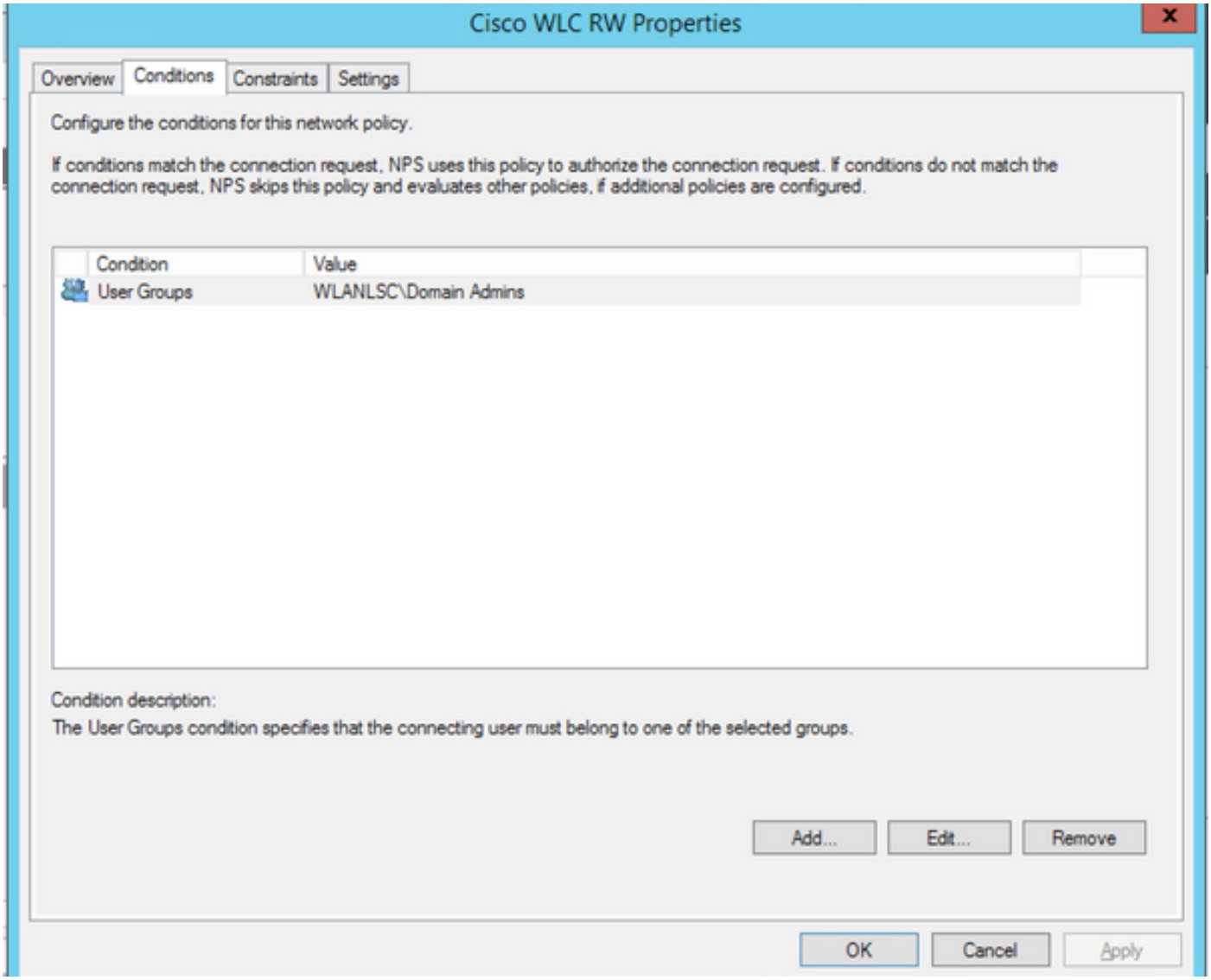
ステップ5:[Conditions]タブで[Add]をクリックします。図に示すように、[User groups]を選択し、[Add]をクリックします。



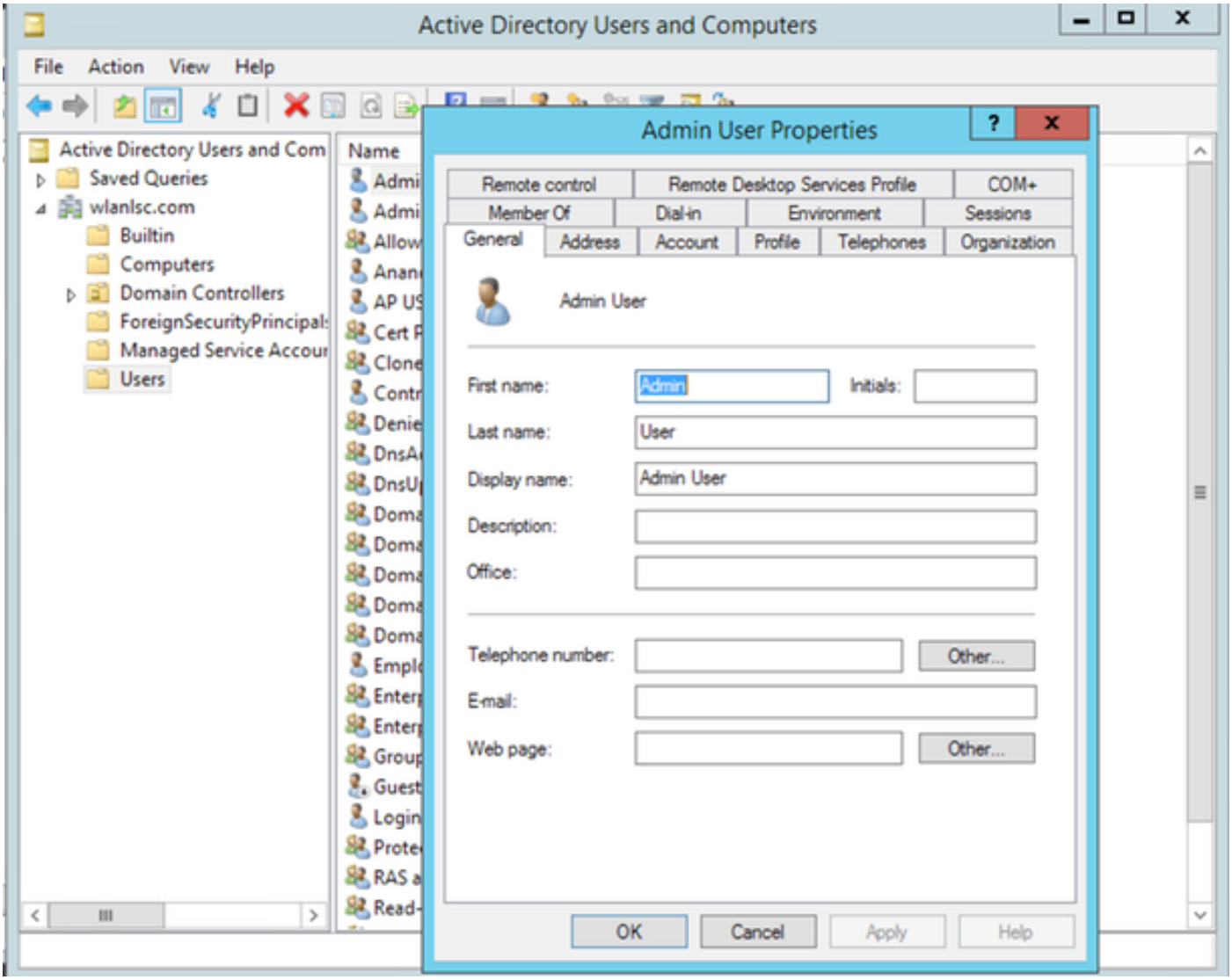
ステップ6：表示されたダイアロ**グボックス**の[Add Groups]をクリックします。表示される[グループ**の選**択]ウィンドウで、目的のオブジェク**トの種類と場所を**選択し、**図に示す**ように、必要なオブジェクト名を入力します。

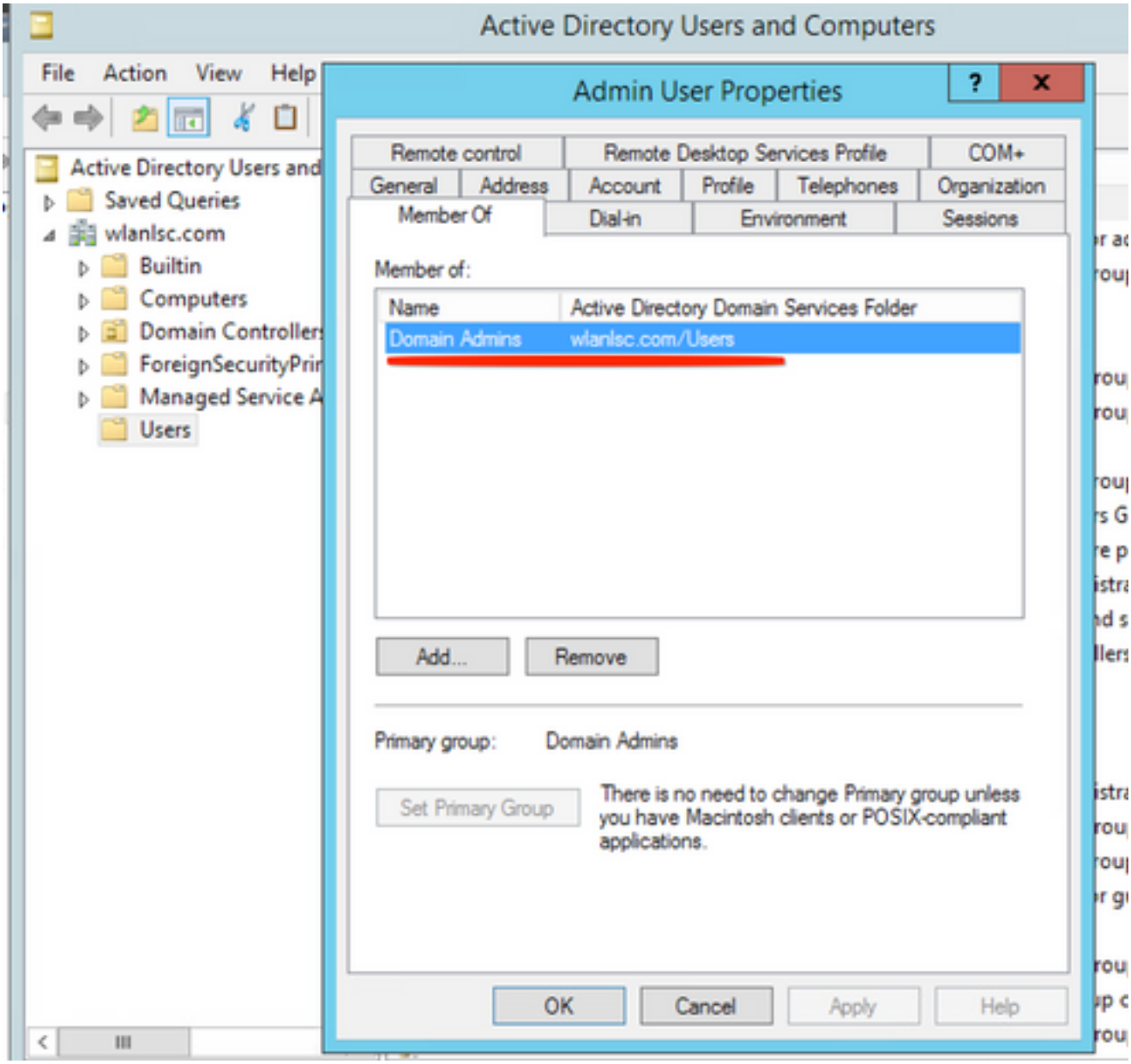


条件が正しく追加されると、次のようになります。

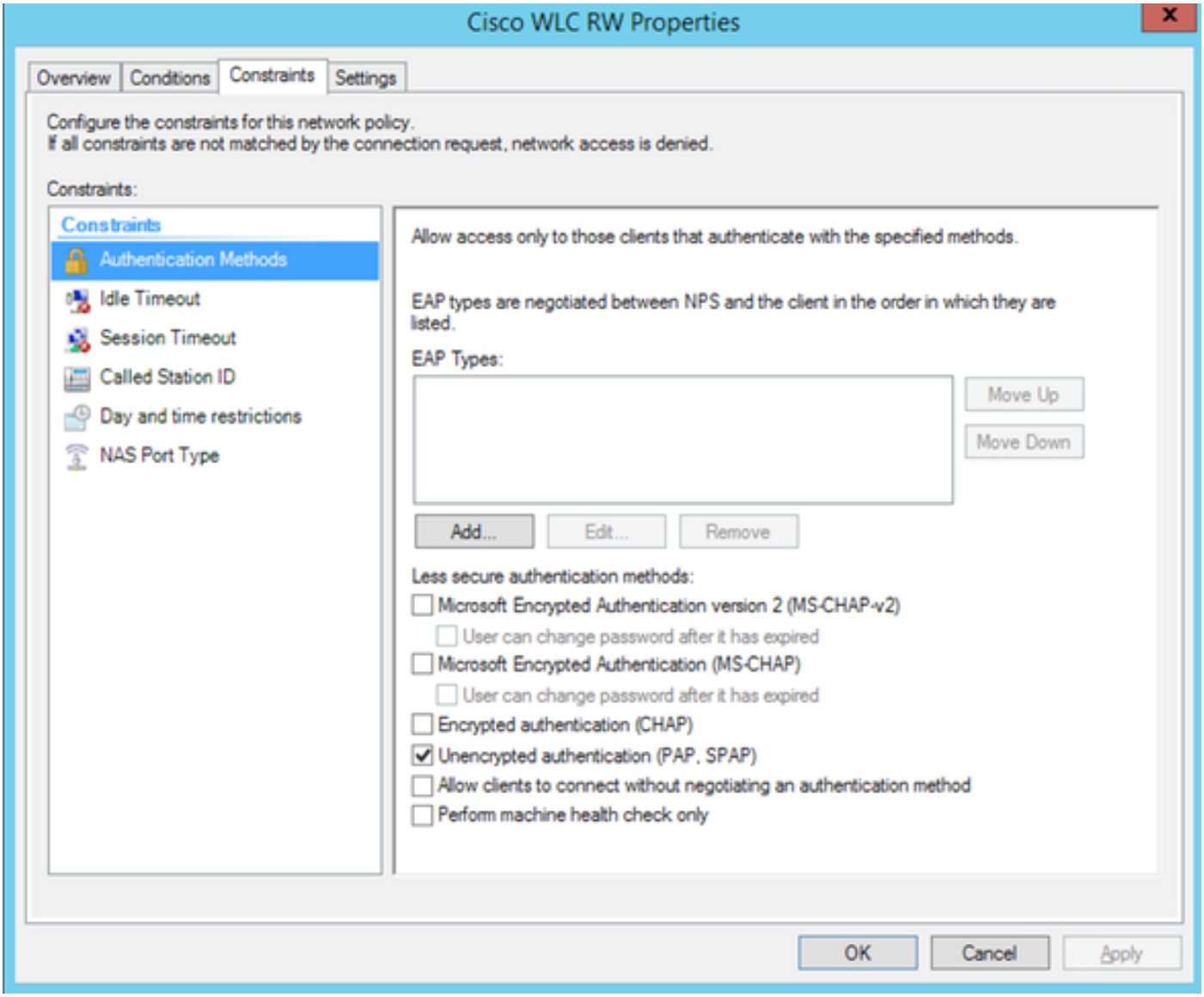


注：場所とオブジェクト名の詳細を確認するには、active directoryを開き、目的のユーザ名を探します。この例では、**Domain Admins**はフルアクセス権を付与されたユーザーで構成されています。**adminuser**はこのオブジェクト名の一部です。

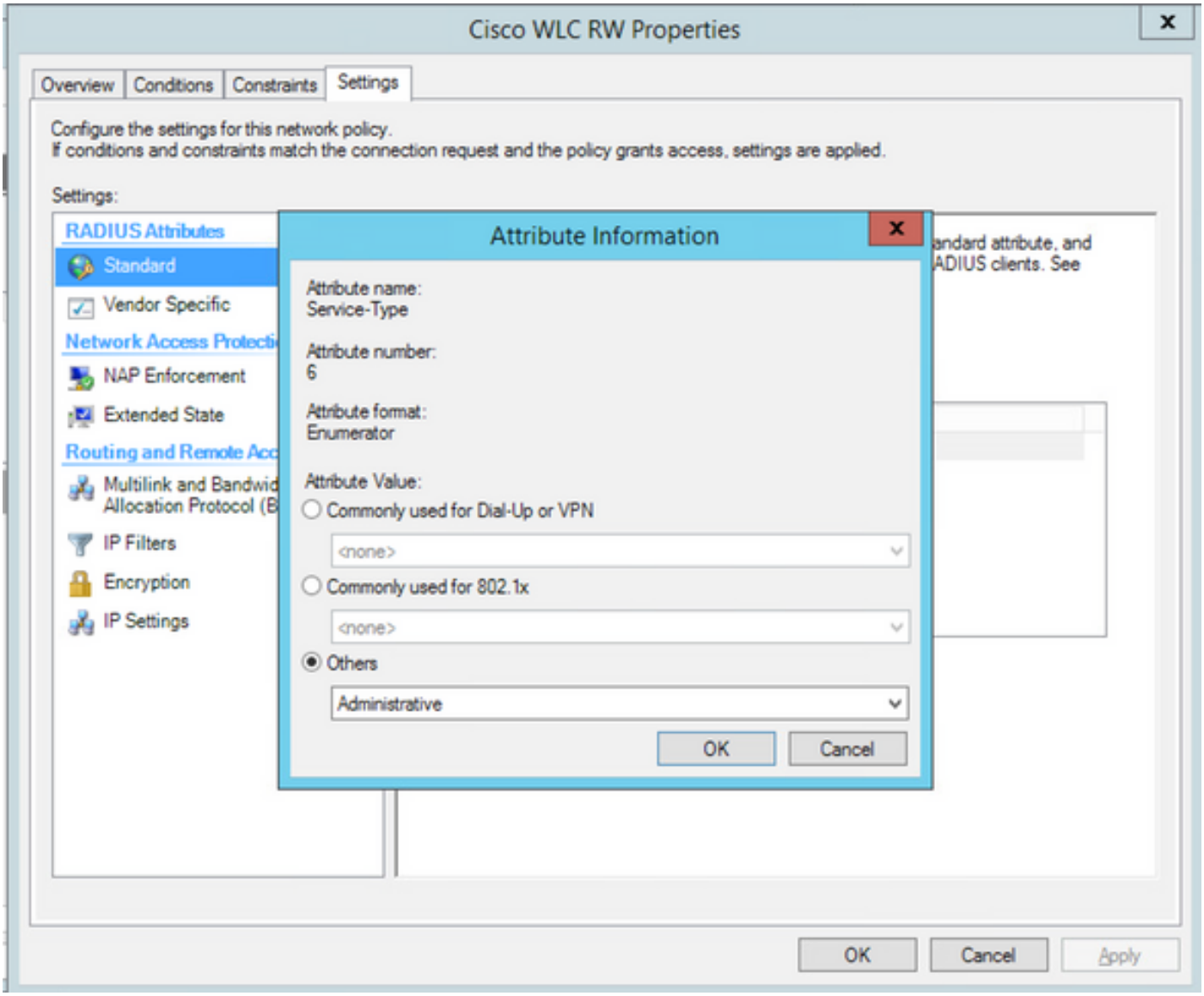

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
wlanlsc.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name
Admin User Properties
Remote control
Remote Desktop Services Profile
COM+
Member Of
Dial-in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



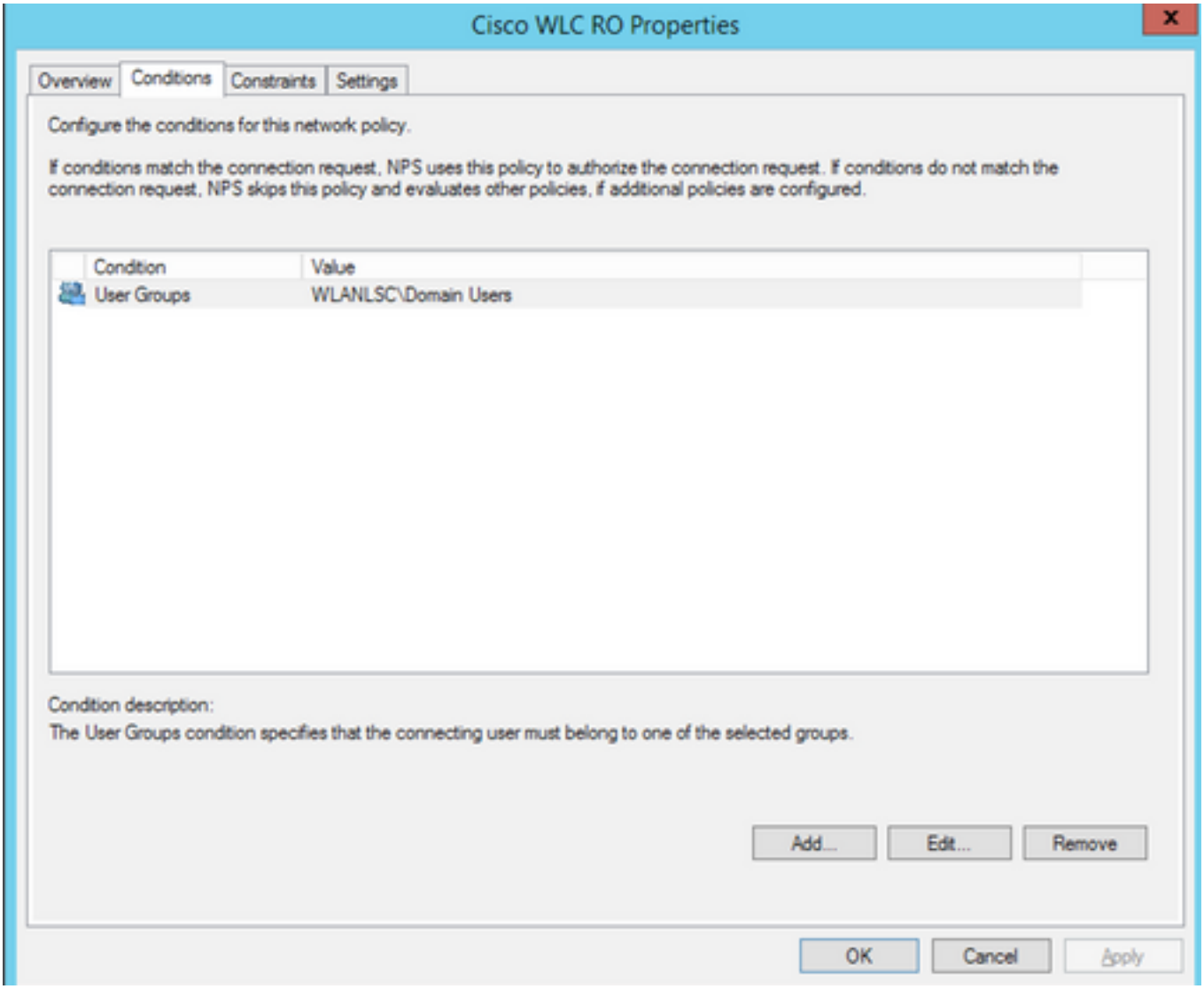
ステップ7:[Constraints]タブの下で、[Authentication Methods]に移動し、[unencrypted authentication]だけがオンになっていることを確認します。

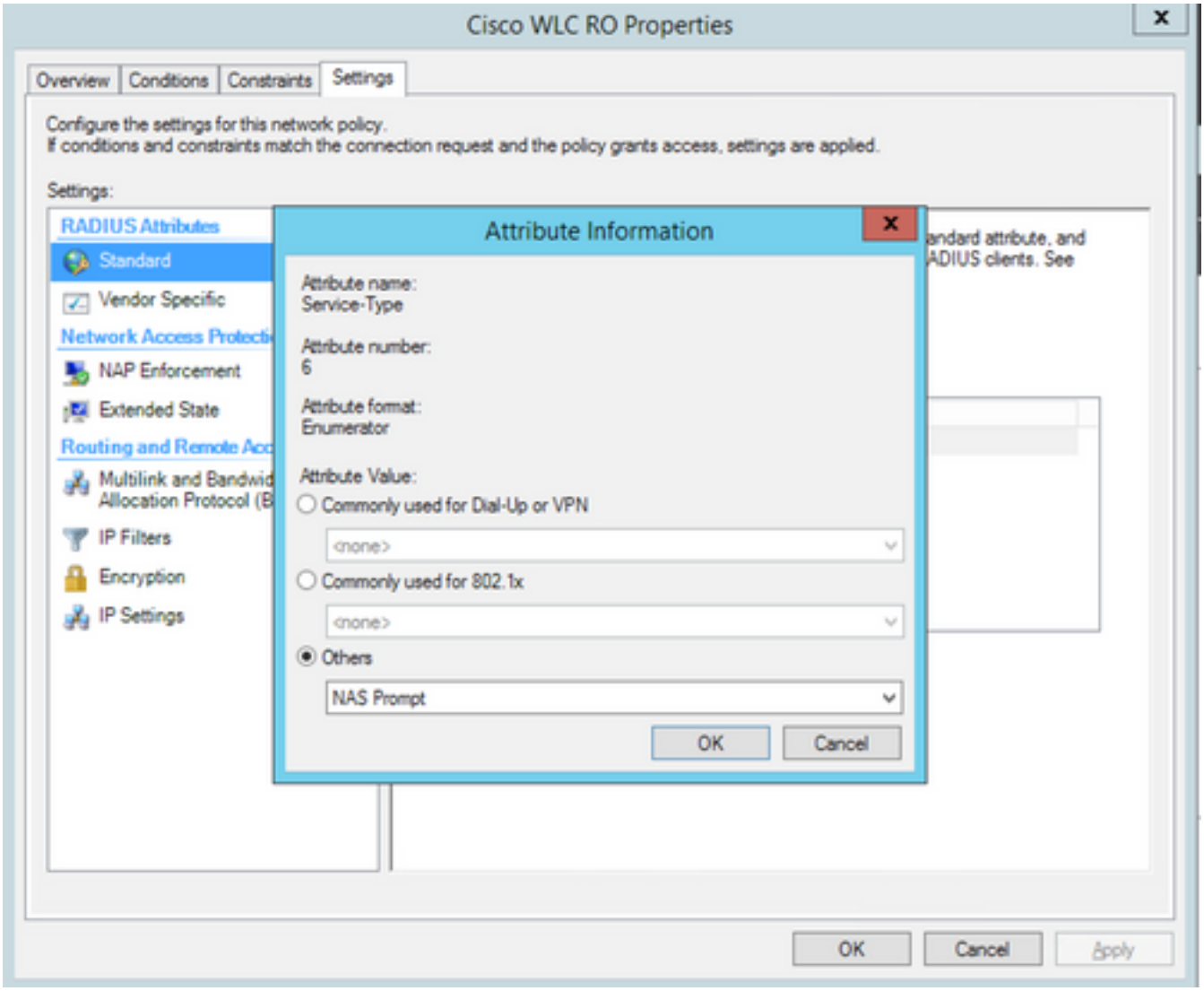


ステップ8:[Settings]タブで、[RADIUS Attributes] > [Standard]に移動します。[追加]をクリックして、新しい属性Service-Typeを追加します。このポリシーにマップされているユーザーへの完全なアクセスを提供するには、ドロップダウンメニューから[管理]を選択します。図に示すように、[Apply]をクリックして変更を保存します。



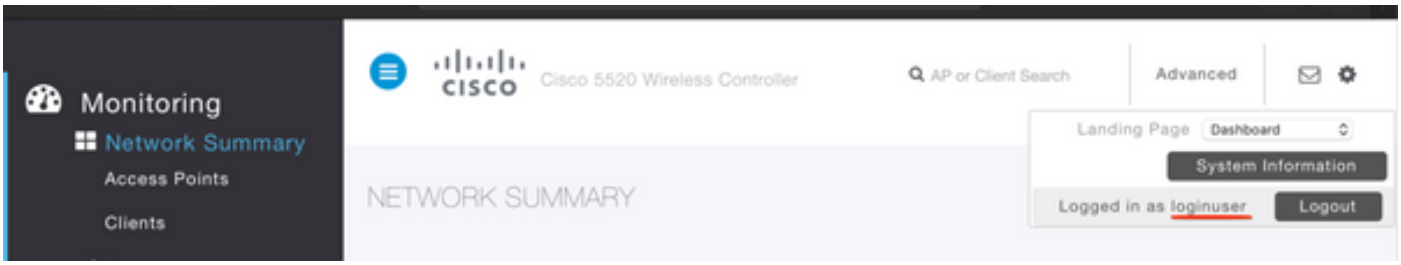
注：特定のユーザに対して読み取り専用アクセスを許可する場合は、ドロップダウンから[NAS-Prompt]を選択します。この例では、[Domain Users]オブジェクト名の下のユーザに読み取り専用アクセスを提供するために、**Cisco WLC RO**という名前の別のポリシーが作成されます。

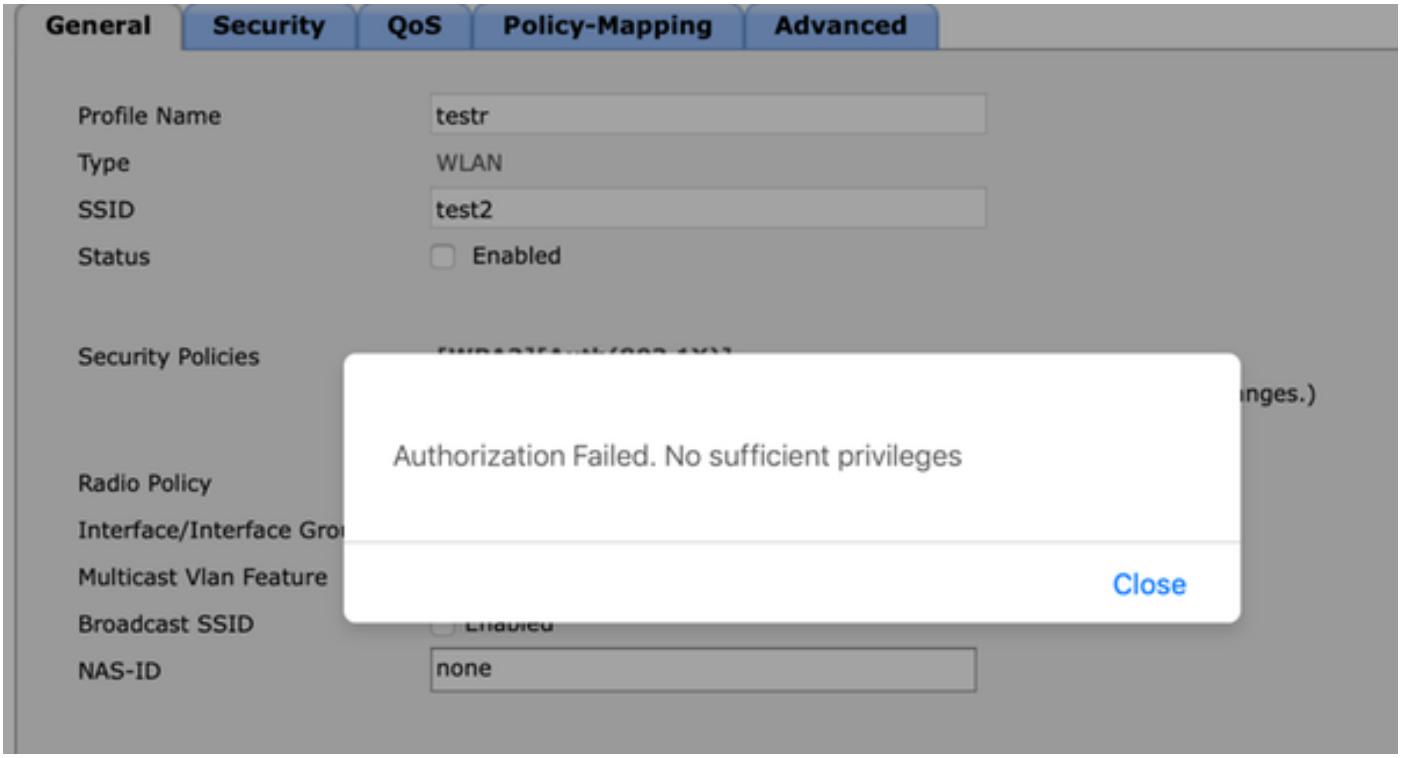

Cisco WLC RO Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates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



確認

1.ログインユーザー資格情報を使用する場合、ユーザーはコントローラーに変更を構成できません。

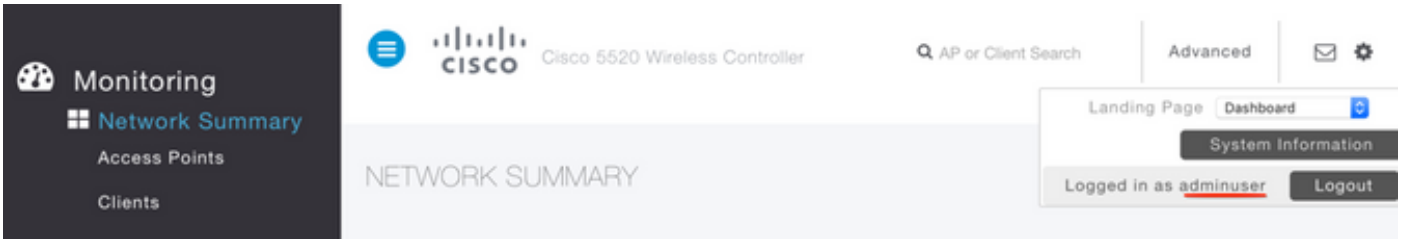




debug aaa all enableから、許可応答のservice-type属性の値が7（NASプロンプトに対応）であることがわかります。

```
*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.管理者ユーザーの資格情報を使用する場合、ユーザーは管理に対応するservice-type値6を使用して完全にアクセスする必要があります。




```
*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)
```

トラブルシュート

NPSを介したWLCへの管理アクセスをトラブルシューティングするには、**debug aaa all enable**コマンドを実行します。

1.誤ったクレデンシャルが使用された場合のログを次に示します。

```
*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. service-typeがAdministrative (value=6)またはNAS-prompt (value=7)以外の値で使用される場合のログを次に示します。この場合、認証が成功しても口グインは失敗します。

```
*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
```