

Acesso de gerenciamento para WLC AireOS por meio do Microsoft NPS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurações](#)

[Configuração de WLC](#)

[Configuração do Microsoft NPS](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve como configurar o acesso de gerenciamento para a GUI e CLI do AireOS WLC através do Microsoft Network Policy Server (NPS).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento das soluções de segurança sem fio
- Conceitos de AAA e RADIUS
- Conhecimento básico do Microsoft Server 2012
- Instalação do Microsoft NPS e Active Directory (AD)

Componentes Utilizados

As informações fornecidas neste documento são baseadas nos seguintes componentes de software e hardware.

- Controladora AireOS (5520) em 8.8.120.0
- Microsoft Server 2012

Note: Este documento destina-se a dar aos leitores um exemplo da configuração necessária em um servidor Microsoft para acesso de gerenciamento WLC. A configuração do servidor Microsoft Windows apresentada neste documento foi testada no laboratório e foi encontrada para funcionar como esperado. Se tiver problemas com a configuração, entre em contato com a Microsoft para obter ajuda. O Cisco Technical Assistance Center (TAC) não oferece

suporte à configuração do servidor Microsoft Windows. Os guias de instalação e configuração do Microsoft Windows 2012 podem ser encontrados no 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.

Informações de Apoio

Quando a CLI/GUI da WLC é acessada, o usuário é solicitado a inserir as credenciais para fazer login com êxito. As credenciais podem ser verificadas em um banco de dados local ou em um servidor AAA externo. Neste documento, o Microsoft NPS está sendo usado como o servidor de autenticação externa.

Configurações

Neste exemplo, dois usuários são configurados no AAA (NPS) viz. **loginuser** e **adminuser**. **loginuser** tem apenas o acesso somente leitura enquanto **adminuser** recebe acesso total.

Configuração de WLC

Etapa 1. Adicione o servidor RADIUS à controladora. Navegue até **Security > RADIUS > Authentication**. Clique em **Novo** para adicionar o servidor. Verifique se a opção **de gerenciamento** está habilitada para que esse servidor possa ser usado para acesso de gerenciamento, como mostrado nesta imagem.

Security

RADIUS Authentication Servers > Edit

- Server Index: 2
- Server Address(Ipv4/Ipv6): 10.106.33.39
- Shared Secret Format: ASCII
- Shared Secret: ***
- Confirm Shared Secret: ***
- Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Apply Cisco ISE Default settings:
- Apply Cisco ACA Default settings:
- Port Number: 1812
- Server Status: Enabled
- Support for CoA: Disabled
- Server Timeout: 5 seconds
- Network User: Enable
- Management: Enable
- Management Retransmit Timeout: 5 seconds
- Tunnel Proxy: Enable
- Realm List: [Realm List](#)
- PAC Provisioning: Enable
- IPSec: Enable
- Cisco ACA: Enable

Etapa 2. Navegue até **Segurança > Ordem de prioridade > Usuário de gerenciamento**. Verifique se RADIUS está selecionado como um dos tipos de autenticação.

Priority Order > Management User

Authentication

Not Used

- TACACS+

Order Used for Authentication

- RADIUS LOCAL

Up
Down

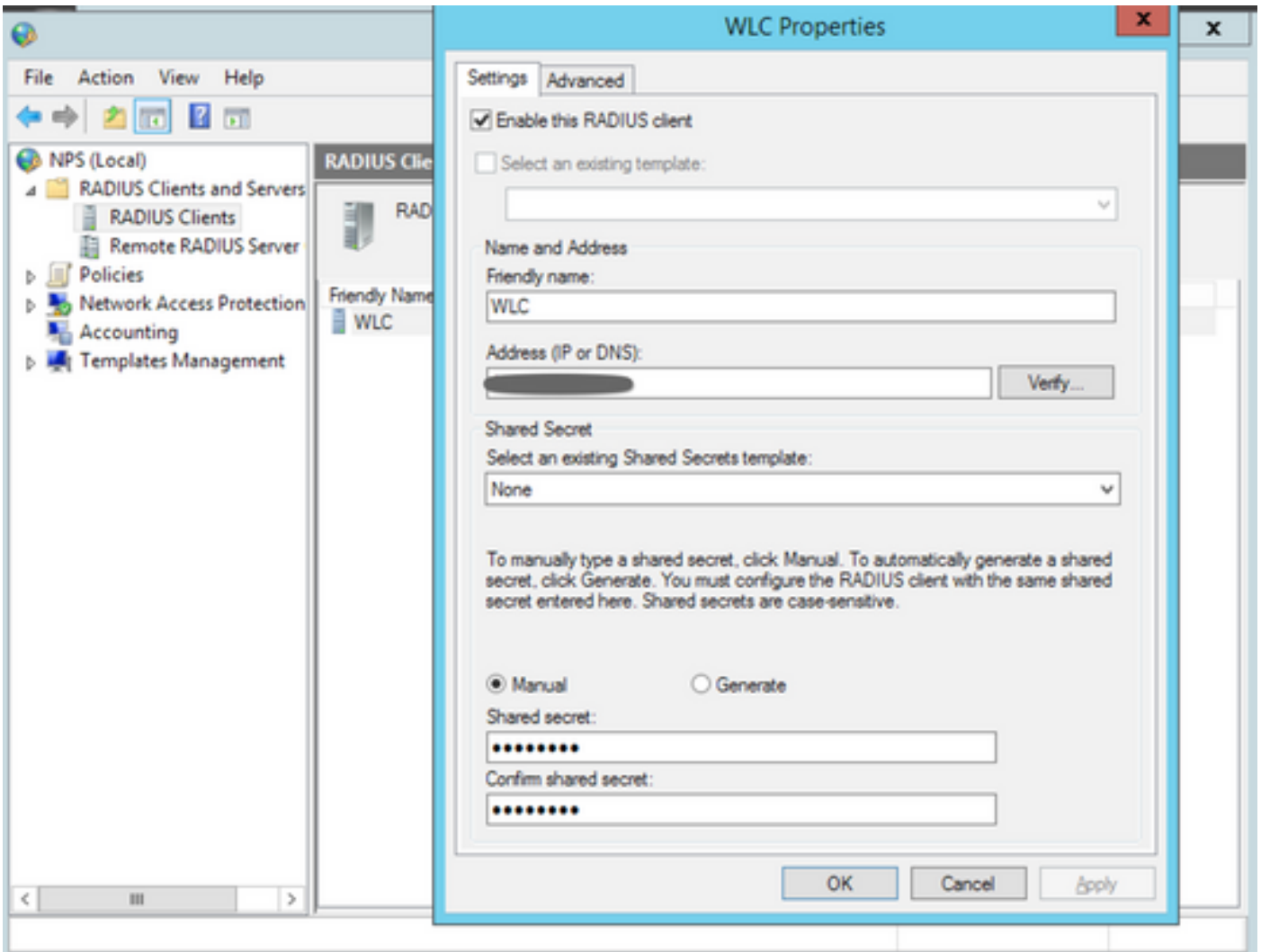
Note: Se RADIUS for selecionado como a primeira prioridade na ordem de autenticação, as credenciais locais serão usadas para autenticação somente se o servidor RADIUS estiver inacessível. Se RADIUS for selecionado como uma segunda prioridade, as credenciais RADIUS serão primeiro verificadas no banco de dados local e, em seguida, verificadas em relação aos servidores RADIUS configurados.

Configuração do Microsoft NPS

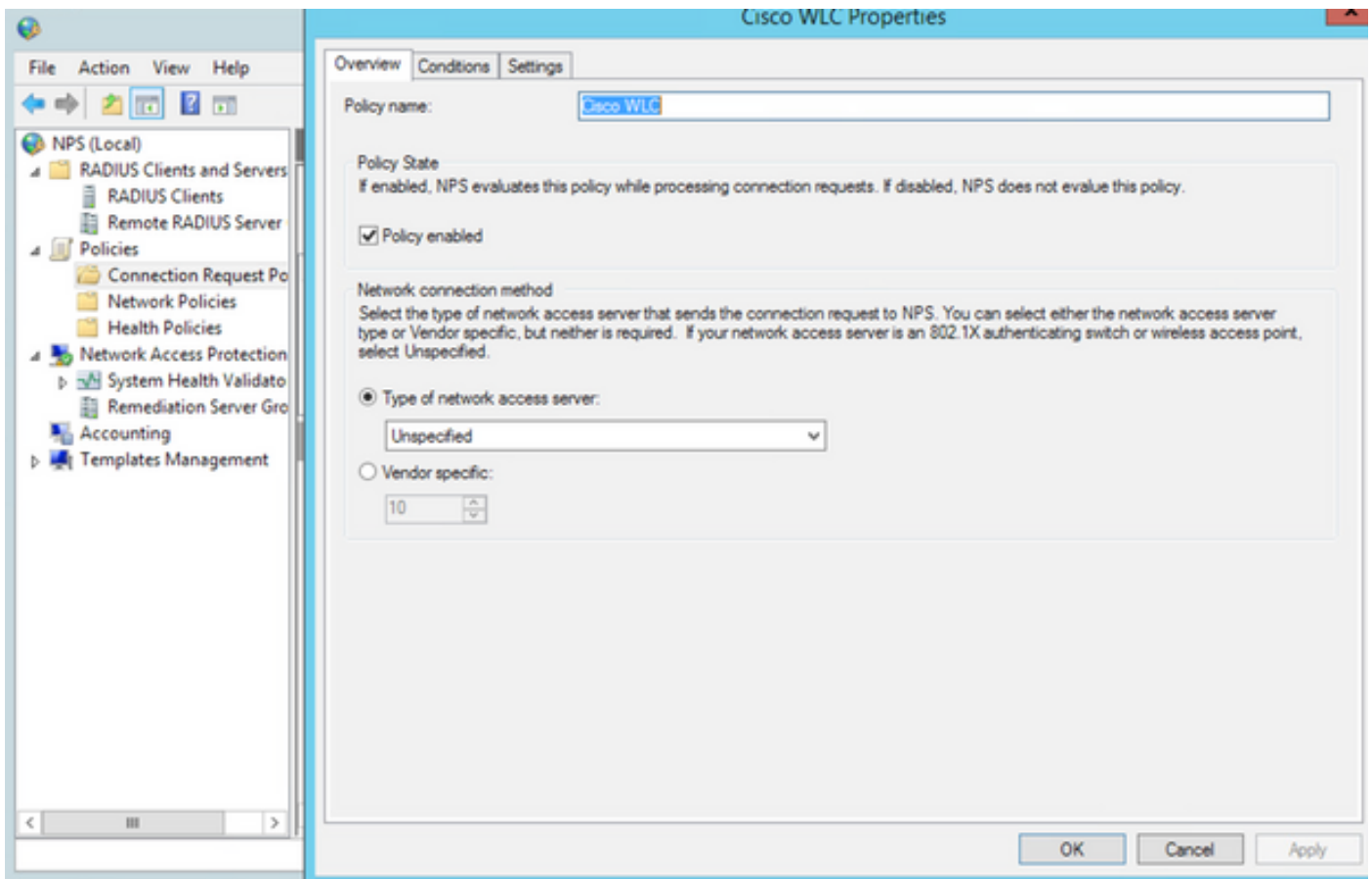
Etapa 1. Abra o servidor Microsoft NPS. Clique com o botão direito do mouse em **Clientes Radius**.

Clique em **New** para adicionar a WLC como o cliente RADIUS.

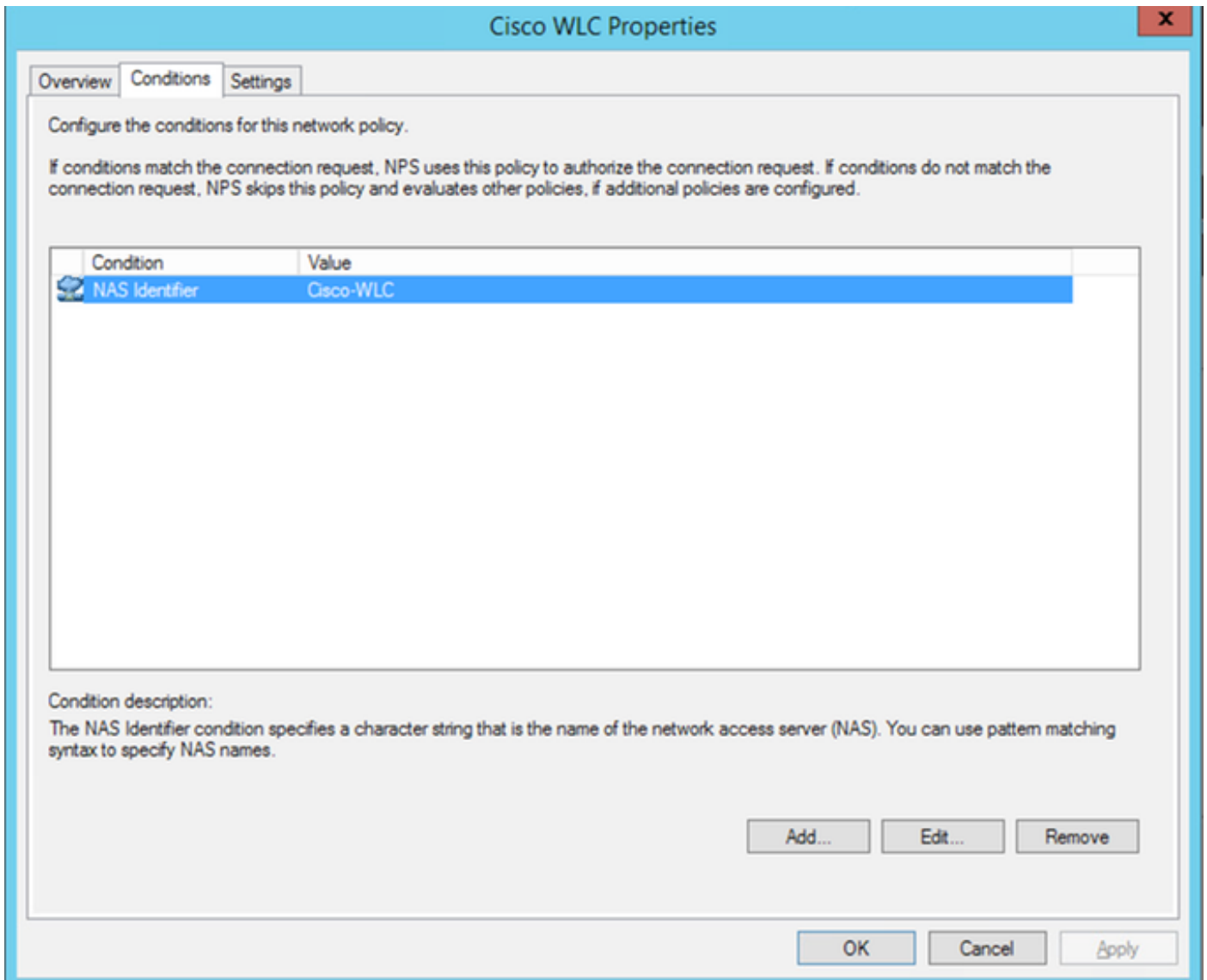
Insira os detalhes necessários. Certifique-se de que o segredo compartilhado seja o mesmo que o configurado na controladora enquanto o servidor RADIUS é adicionado.



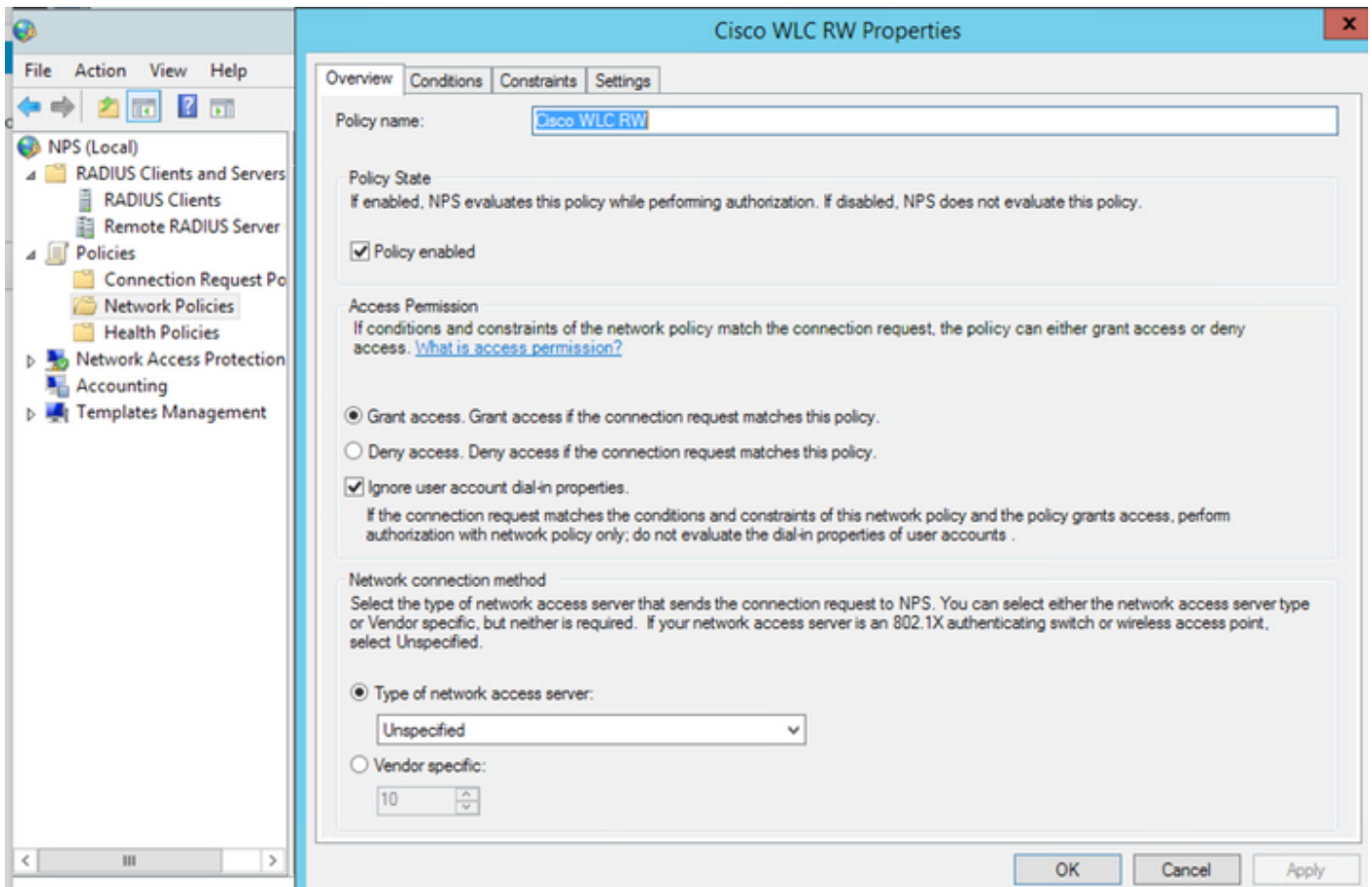
Etapa 2. Navegue para **Políticas > Políticas de solicitação de conexão**. Clique com o botão direito do mouse para adicionar uma nova política, como mostrado na imagem.



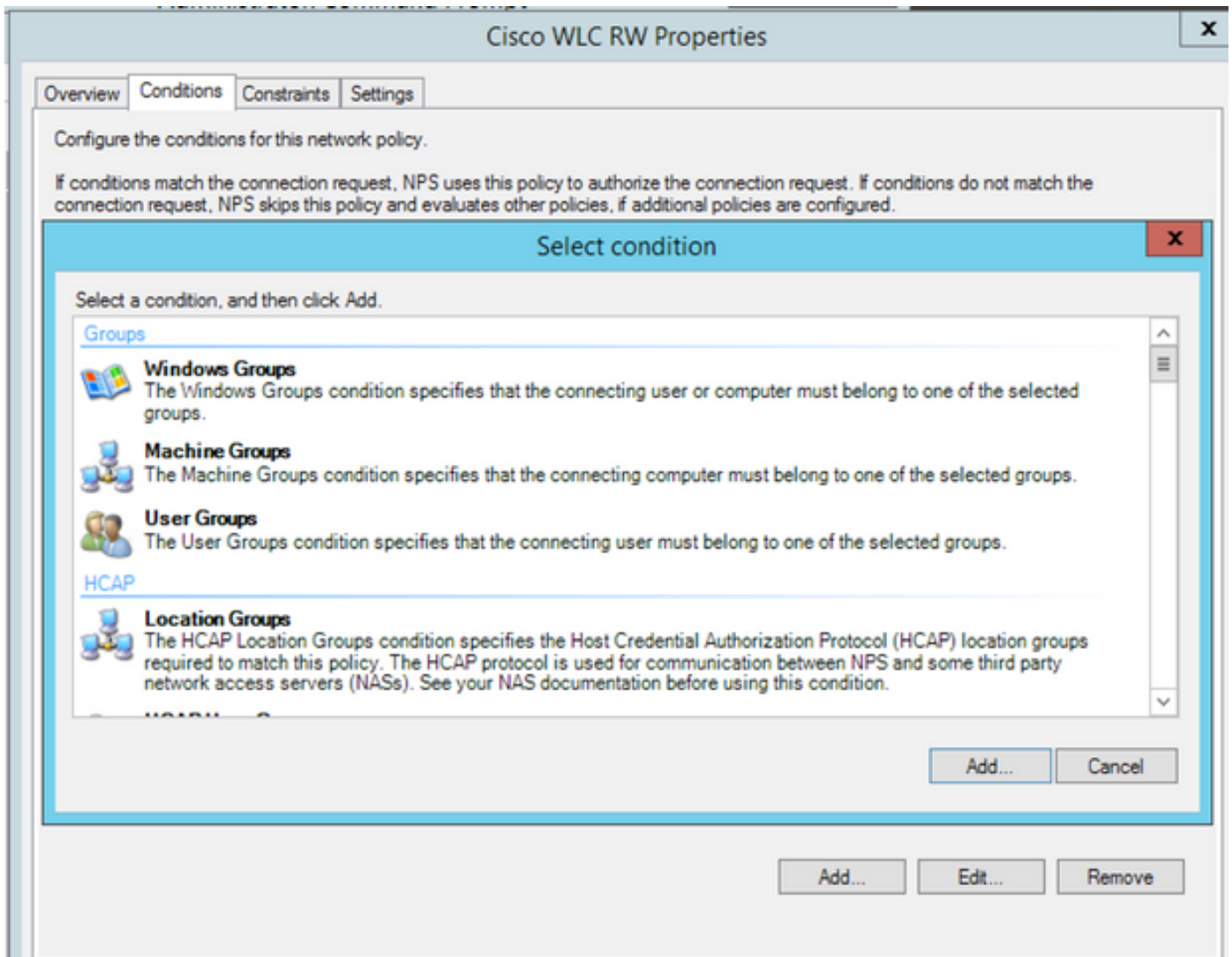
Etapa 3. Na guia **Condições**, selecione **Identificador NAS** como a nova condição. Quando solicitado, insira o nome do host do controlador como o valor, como mostrado na imagem.



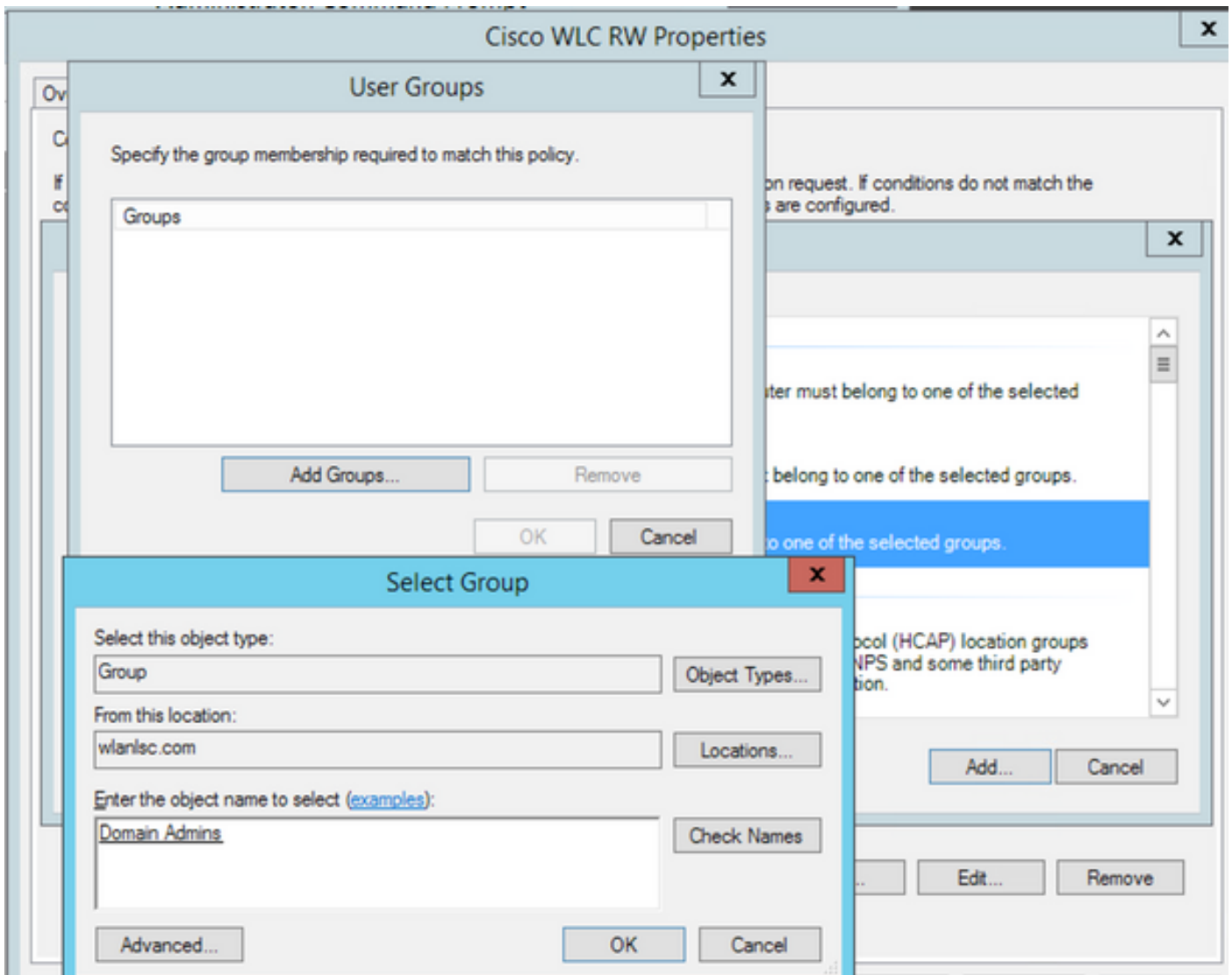
Etapa 4. Navegue até **Políticas > Políticas de rede**. Clique com o botão direito do mouse para adicionar uma nova política. Neste exemplo, a política é denominada **Cisco WLC RW**, o que implica que a política é usada para fornecer acesso completo (leitura/gravação). Verifique se a política está configurada conforme mostrado aqui.



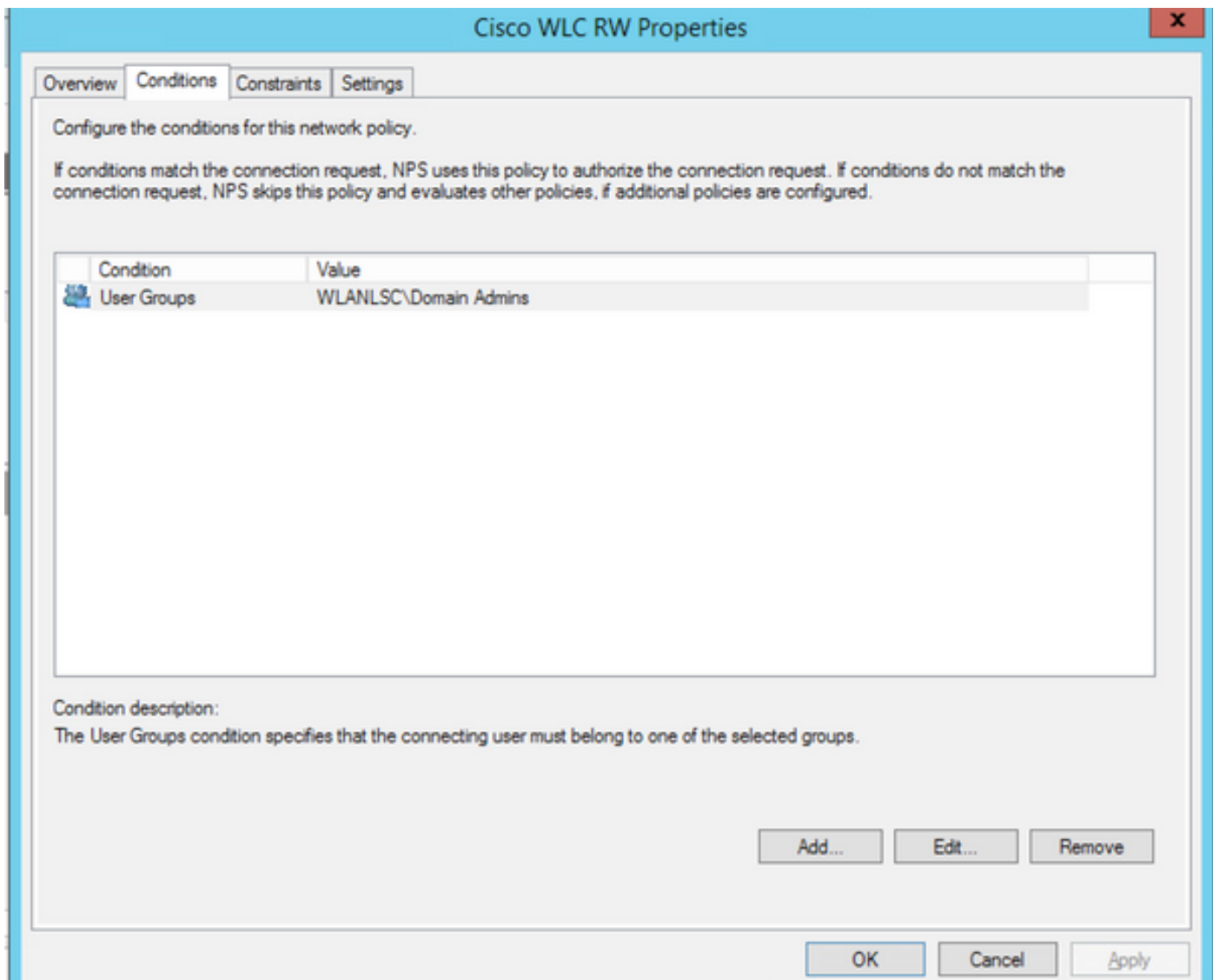
Etapa 5. Na guia **Condições**, clique em **Adicionar**. Selecione os **grupos de usuários** e clique em **Adicionar**, como mostrado na imagem.



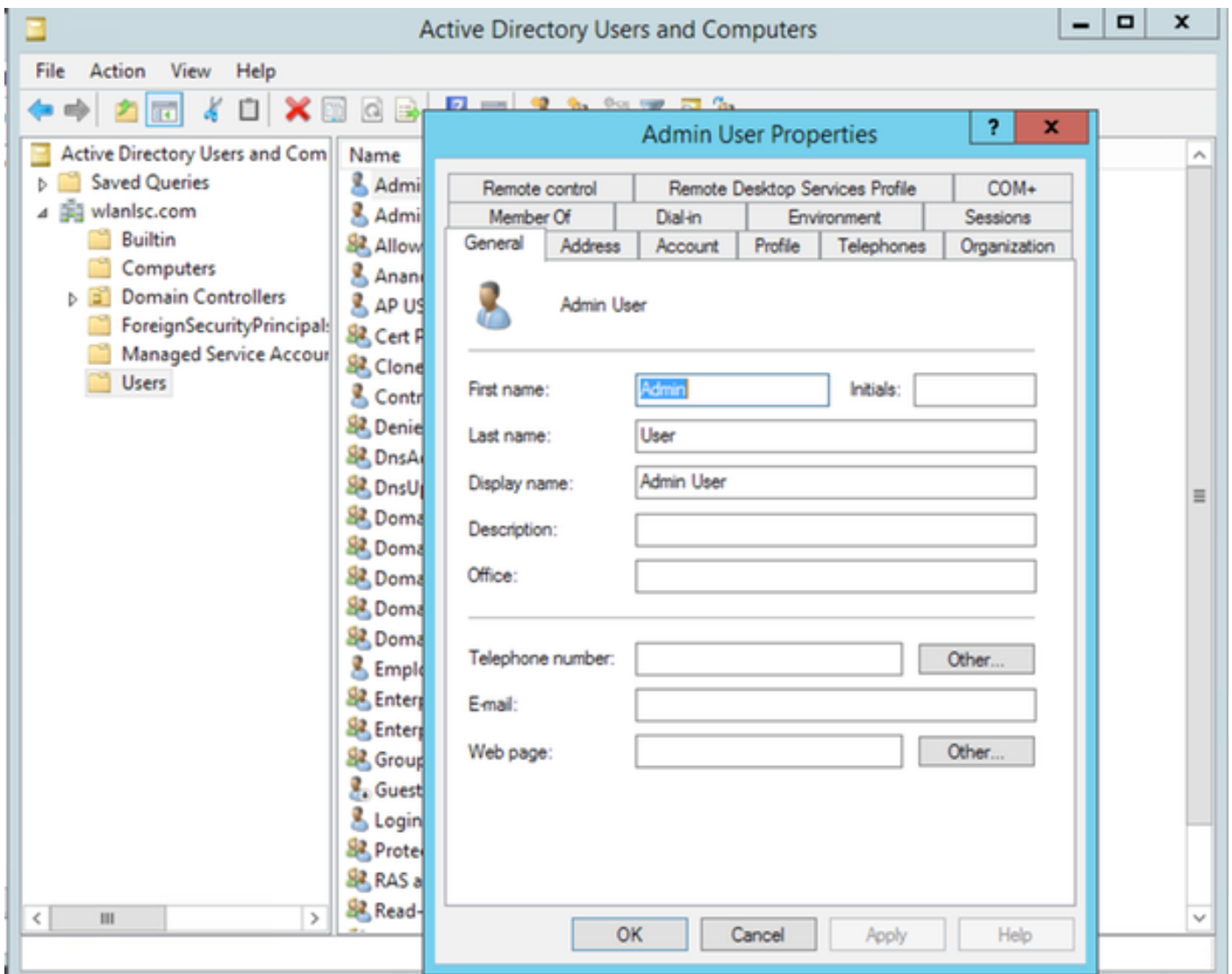
Etapa 6. Clique em **Adicionar grupos** na caixa de diálogo exibida. Na janela **Selecionar grupo** exibida, selecione o **tipo de objeto** e **local** desejados e insira o nome do objeto necessário, como mostrado na imagem.

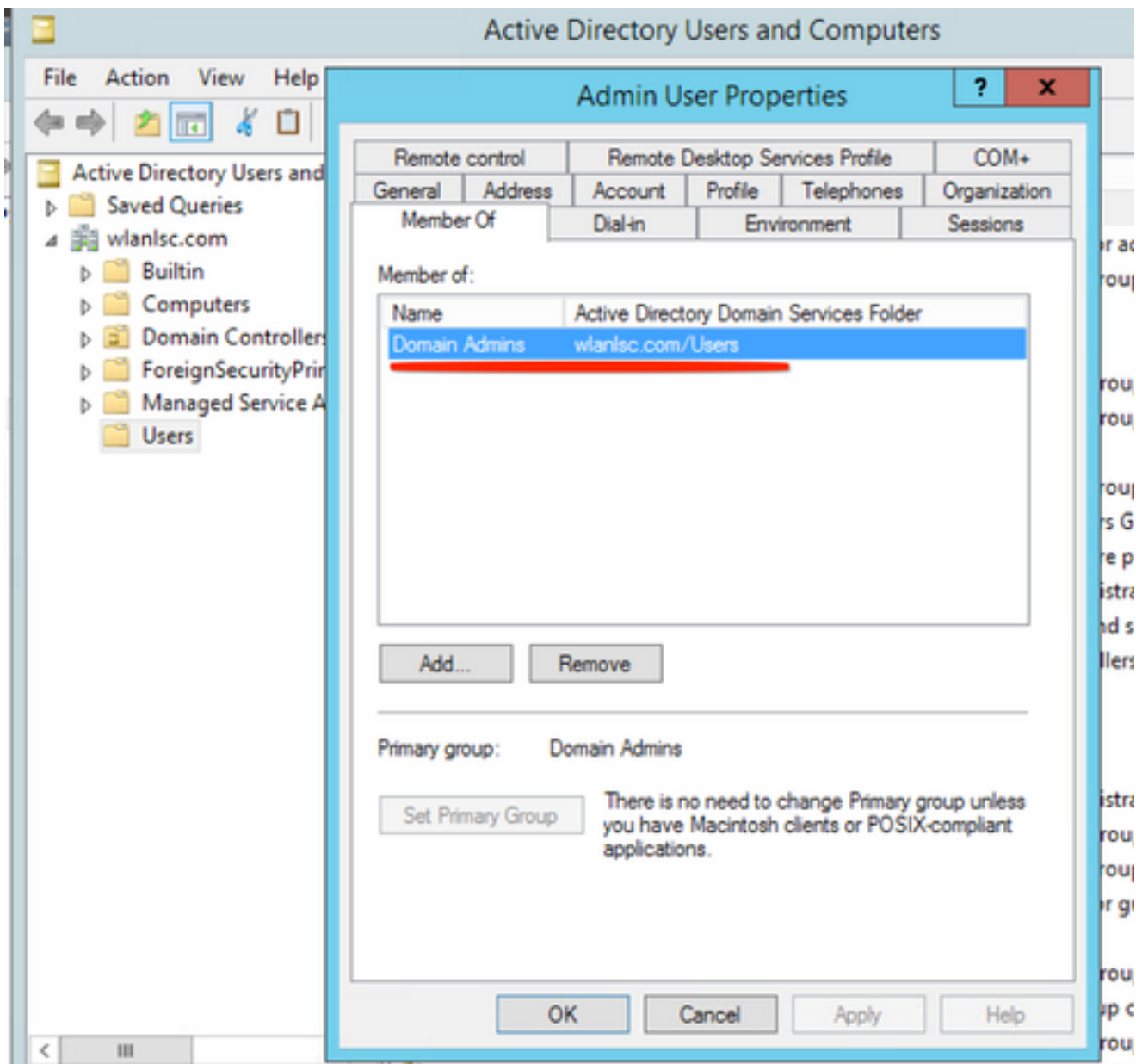


A condição, se adicionada corretamente, deve ser exibida como mostrado aqui.

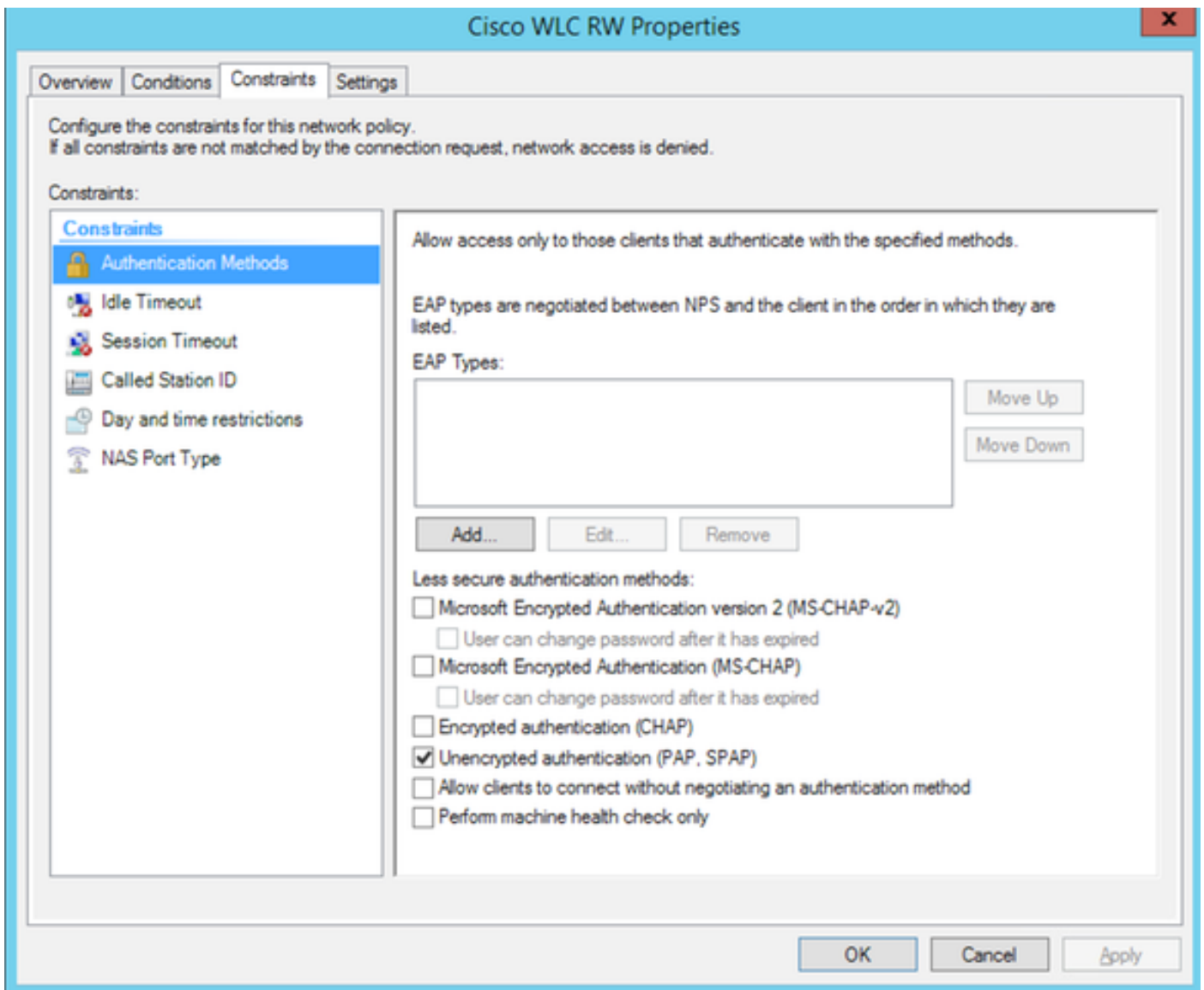


Note: Para descobrir a localização e os detalhes do nome do objeto, abra o active directory e procure o nome de usuário desejado. Neste exemplo, os **Domain Admins** consistem em usuários que recebem acesso total. **adminuser** faz parte deste nome de objeto.

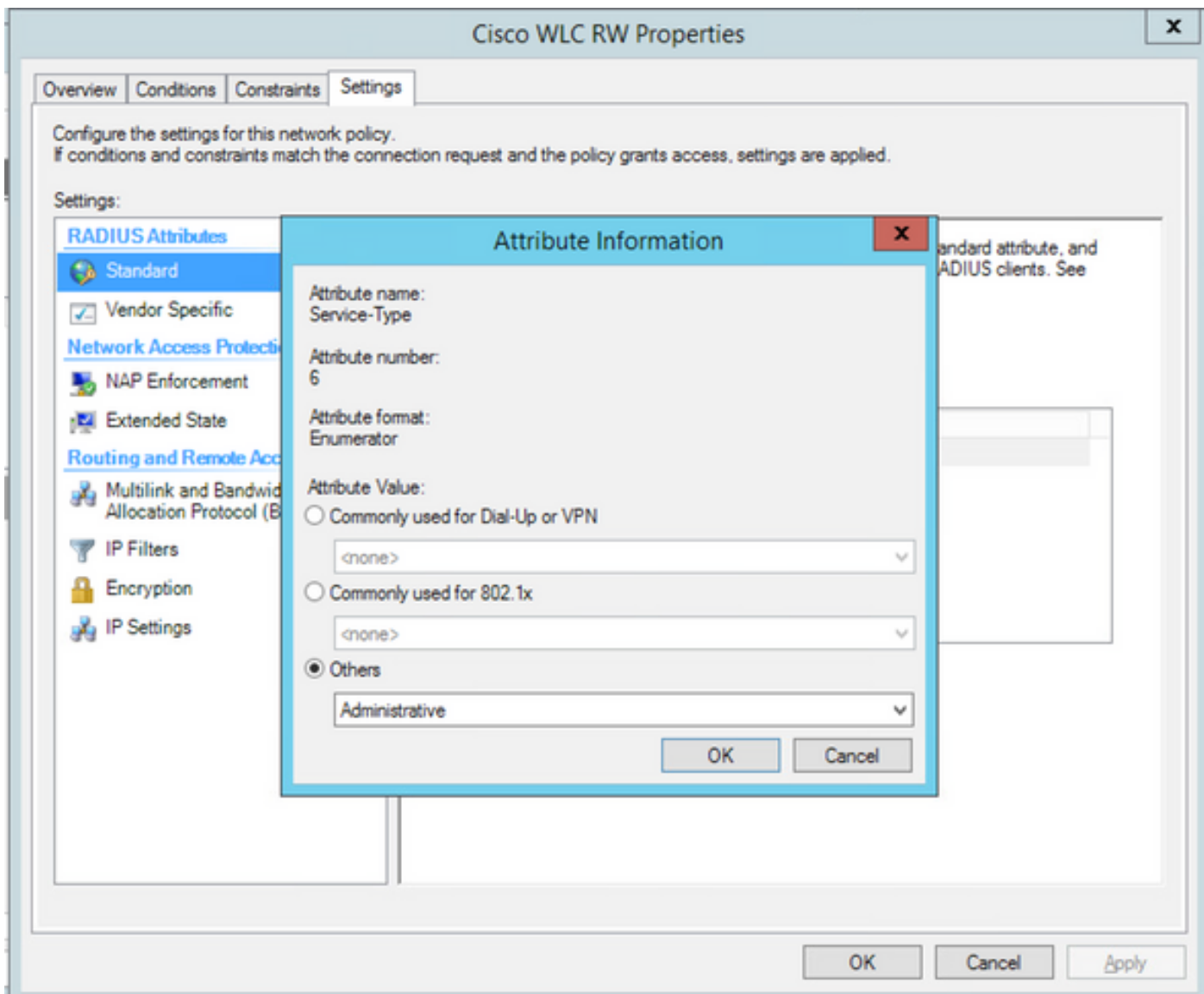




Passo 7. Na guia **Restrições**, navegue para **Métodos de autenticação** e verifique se somente a **autenticação não criptografada** está marcada.



Etapa 8. Na guia **Settings**, navegue para **RADIUS Attributes > Standard**. Clique em **Add** para adicionar um novo atributo, **Service-Type**. No menu suspenso, selecione **Administrative** para fornecer acesso total aos usuários mapeados para essa política. Clique em **Aplicar** para salvar as alterações, conforme mostrado na imagem.




Note: Se desejar fornecer acesso somente leitura a usuários específicos, selecione NAS-Prompt na lista suspensa. Neste exemplo, outra política chamada **Cisco WLC RO** é criada para fornecer acesso somente leitura aos usuários sob o nome do objeto **Usuários de domínio**.

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...

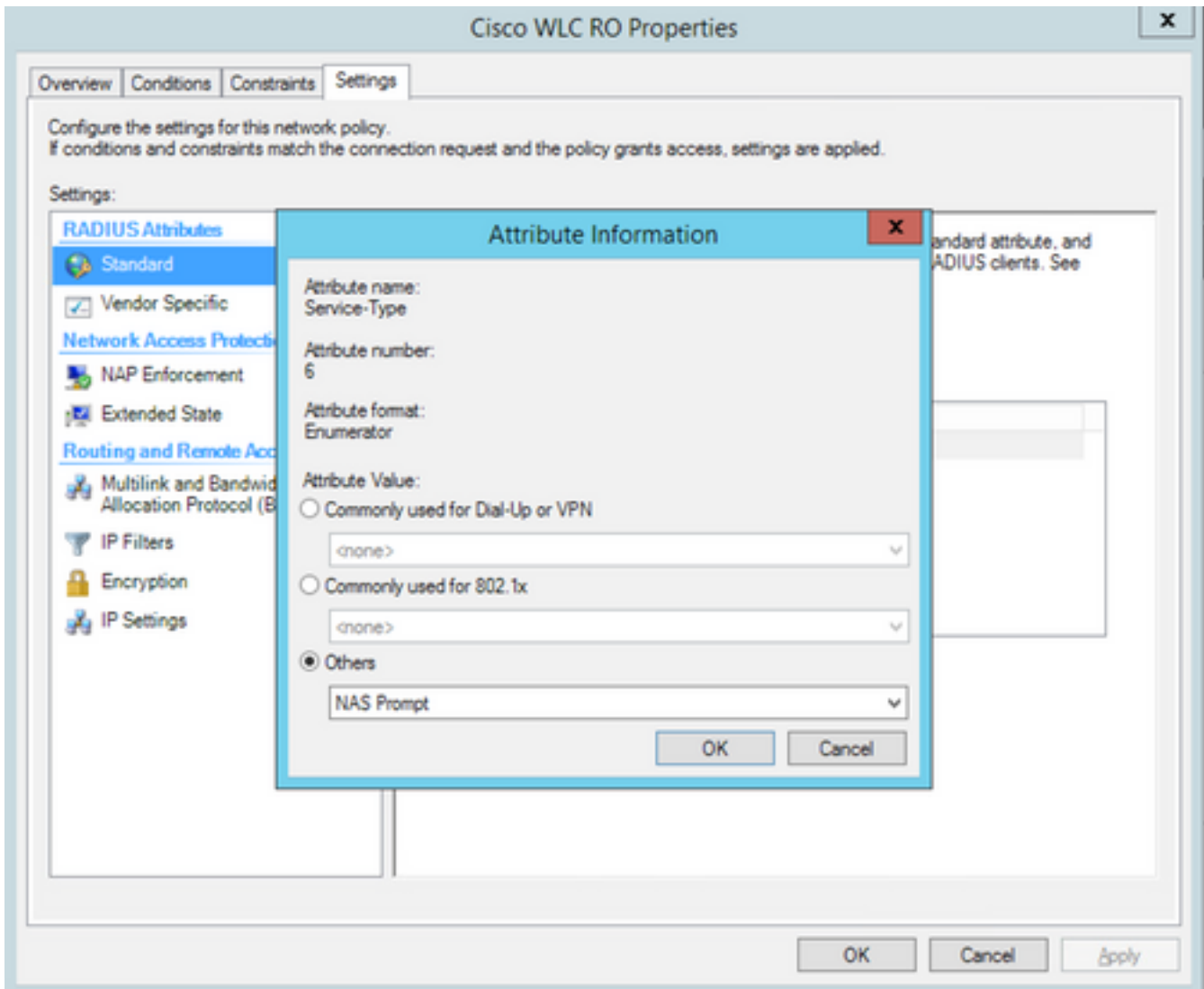
Edit...

Remove

OK

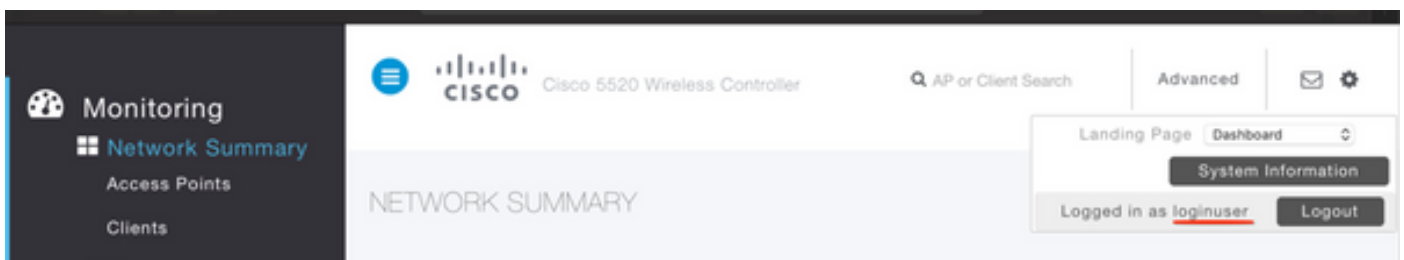
Cancel

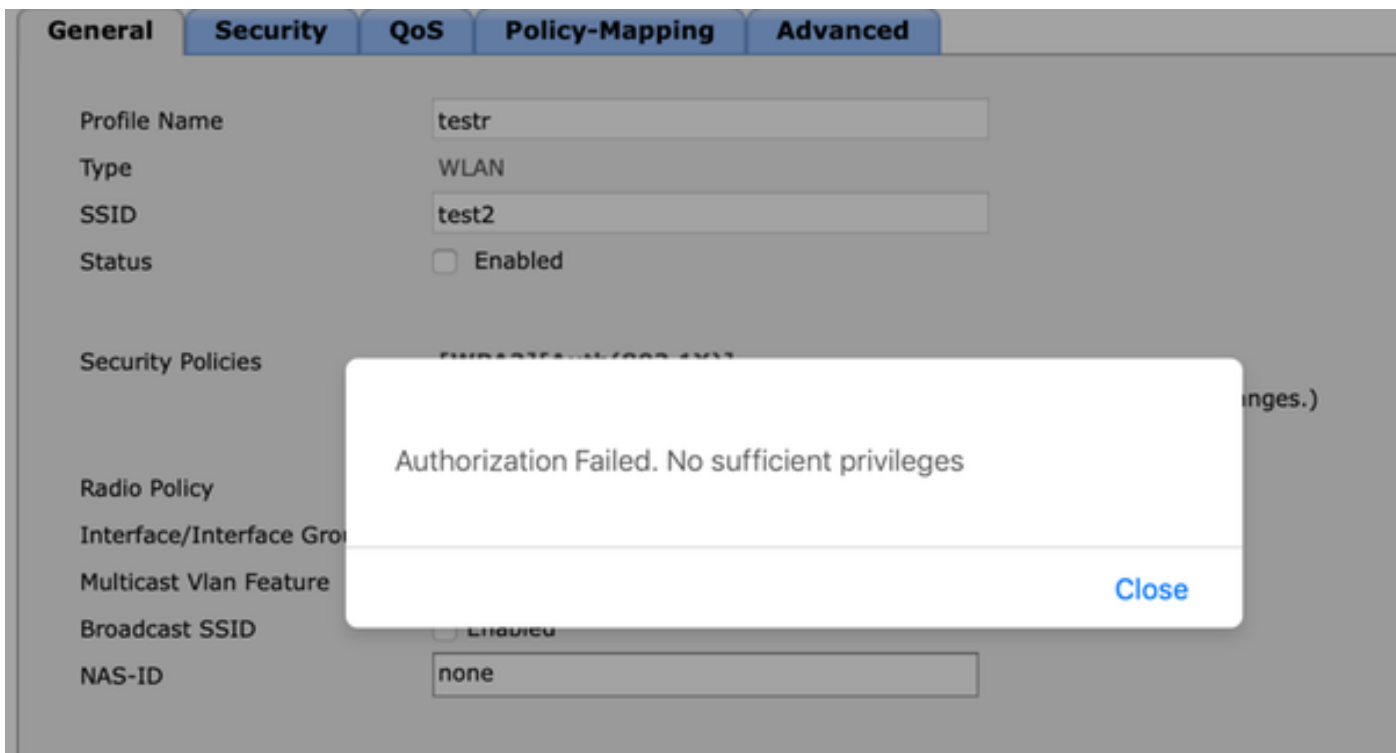
Apply



Verificar

1. Quando as credenciais **loginuser** são usadas, o usuário não tem permissão para configurar nenhuma alteração no controlador.





No **debug aaa all enable**, você pode ver que o valor do atributo **service-type** na resposta de autorização é 7, o que corresponde ao prompt do NAS.

```
*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. Quando as credenciais de **administrador** são usadas, o usuário deve ter acesso total com o valor 6 do tipo de serviço, que corresponde ao administrativo.

```
*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
*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-Identifer.....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

Para solucionar problemas de acesso de gerenciamento à WLC através do NPS, execute o comando **debug aaa all enable**.

1. Os registros quando credenciais incorretas são usadas são mostrados aqui.

```
*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. Os registros quando service-type é usado com um valor diferente de Administrative (value=6) ou NAS-prompt (value=7) são mostrados da seguinte maneira. Nesse caso, o login falha mesmo se a autenticação for bem-sucedida.

```
*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-Identififer.....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
```