Acceso a la administración para AireOS WLC a través de Microsoft NPS

Contenido

Introducción

Este documento describe cómo configurar el acceso de administración para la GUI y CLI del WLC de AireOS a través de Microsoft Network Policy Server (NPS).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de las soluciones de seguridad inalámbrica
- Conceptos de AAA y RADIUS
- Conocimientos básicos de Microsoft Server 2012
- Instalación de Microsoft NPS y Active Directory (AD)

Componentes Utilizados

La información proporcionada en este documento se basa en los siguientes componentes de software y hardware.

- Controlador AireOS (5520) en 8.8.120.0
- Microsoft Server 2012

> **Nota:** Este documento tiene como objetivo dar a los lectores un ejemplo de la configuración requerida en un servidor Microsoft para el acceso de administración del WLC. La configuración del servidor de Microsoft Windows que se presenta en este documento se ha probado en el laboratorio y funciona según lo esperado. Si tiene problemas con la configuración, póngase en contacto con Microsoft para obtener ayuda. Cisco Technical

Assistance Center (TAC) no admite la configuración del servidor de Microsoft Windows. Las guías de instalación y configuración de Microsoft Windows 2012 se pueden encontrar en 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.

Antecedentes

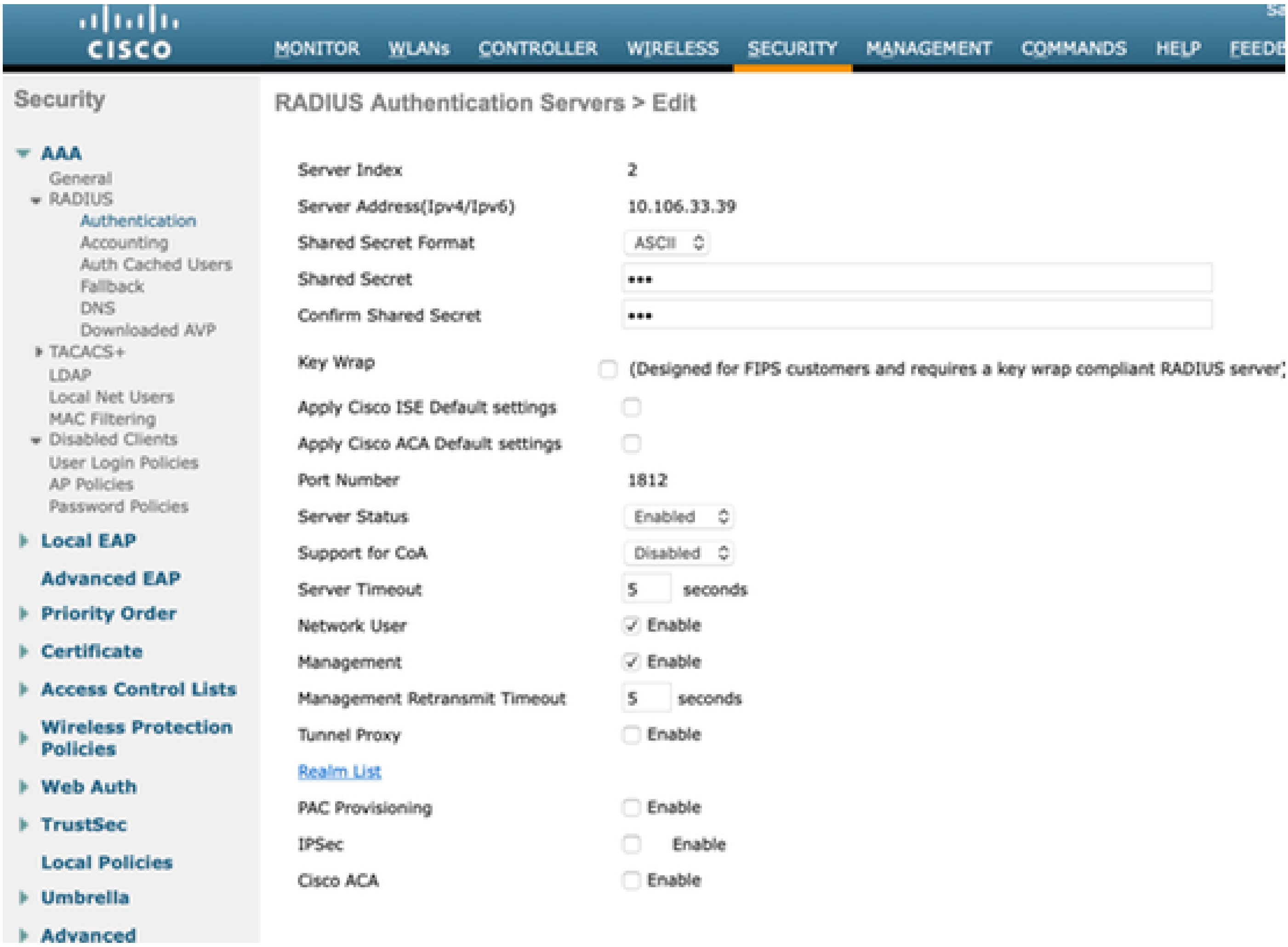
Cuando se accede a WLC CLI/GUI, se le pide al usuario que introduzca las credenciales para iniciar sesión correctamente. Las credenciales se pueden verificar con una base de datos local o con un servidor AAA externo. En este documento, Microsoft NPS se utiliza como servidor de autenticación externo.

Configuraciones

En este ejemplo, se configuran dos usuarios en el AAA (NPS) por ejemplo **loginuser** y **adminuser**. **loginuser** sólo tiene acceso de sólo lectura mientras que **adminuser** tiene acceso completo.

Configuración de WLC

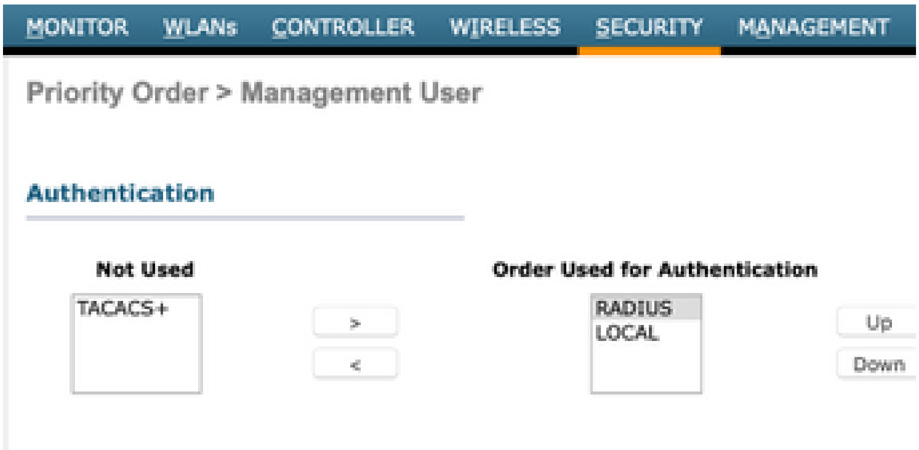
Paso 1. Agregue el servidor RADIUS en el controlador. Vaya a **Seguridad > RADIUS > Autenticación**. Haga clic en **Nuevo** para agregar el servidor. Asegúrese de que la opción **de administración** esté habilitada para que este servidor pueda utilizarse para el acceso de administración, como se muestra en esta imagen.



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	
PAC Provisioning	□ Enable
IPSec	□ Enable
Cisco ACA	□ Enable

Paso 2. Vaya a **Seguridad > Orden de prioridad > Usuario de administración**. Asegúrese de que RADIUS esté seleccionado como uno de los tipos de autenticación.



Priority Order > Management User

Authentication

Not Used: TACACS+

Order Used for Authentication: RADIUS, LOCAL

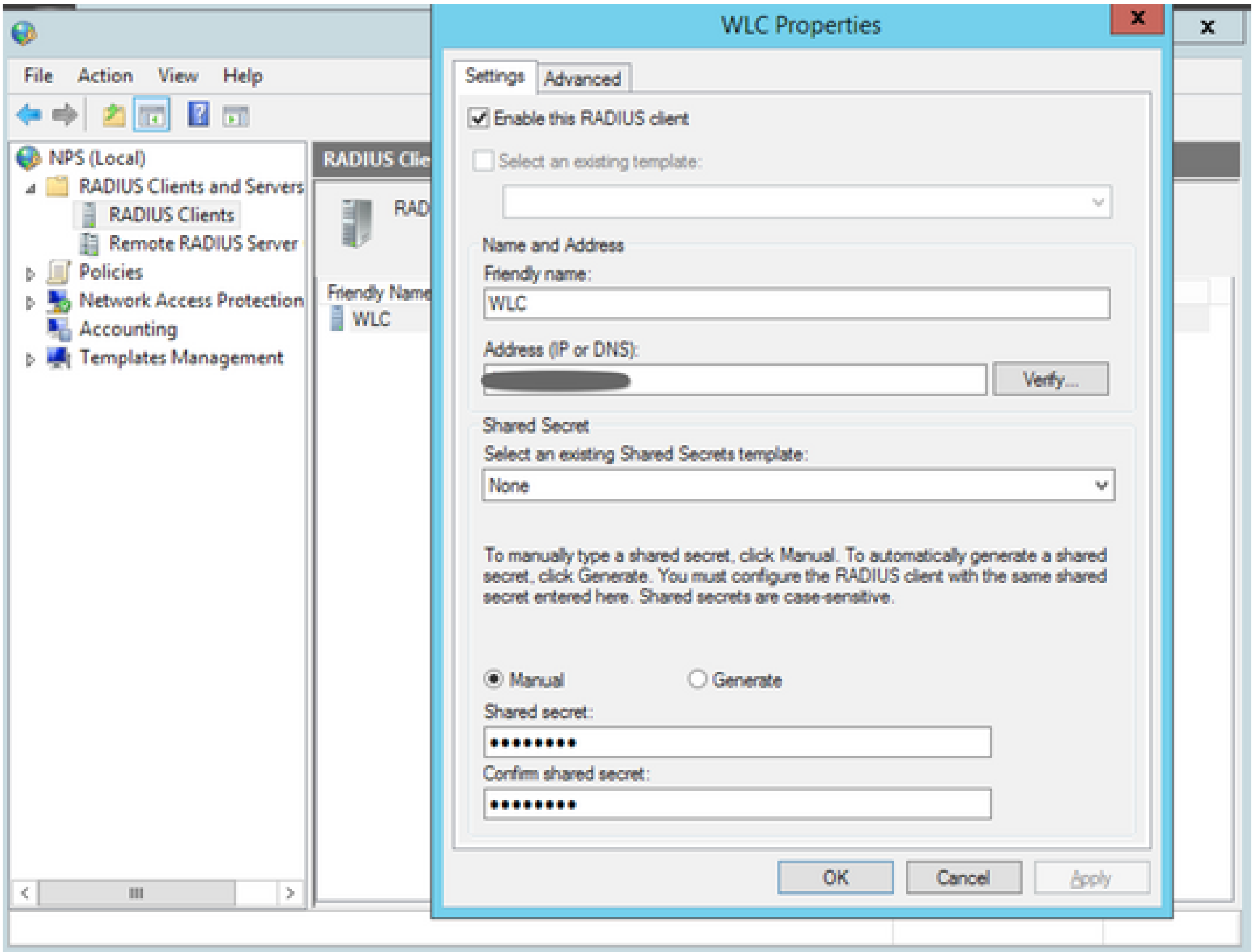
Nota: Si se selecciona RADIUS como la primera prioridad en el orden de autenticación, las credenciales locales se usarán para la autenticación sólo si el servidor RADIUS es inalcanzable. Si se selecciona RADIUS como segunda prioridad, primero se verificarán las credenciales RADIUS con respecto a la base de datos local y luego, se comprobarán con respecto a los servidores RADIUS configurados.

Configuración de NPS de Microsoft

Paso 1. Abra el servidor NPS de Microsoft. Haga clic con el botón derecho del ratón en **Clientes**

Radius. Haga clic en **New** para agregar el WLC como el cliente RADIUS.

Introduzca los detalles necesarios. Asegúrese de que el secreto compartido sea el mismo que el configurado en el controlador mientras se agrega el servidor RADIUS.



WLC Properties

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: WLC

Address (IP or DNS): [redacted]

Shared Secret

Select an existing Shared Secrets template: None

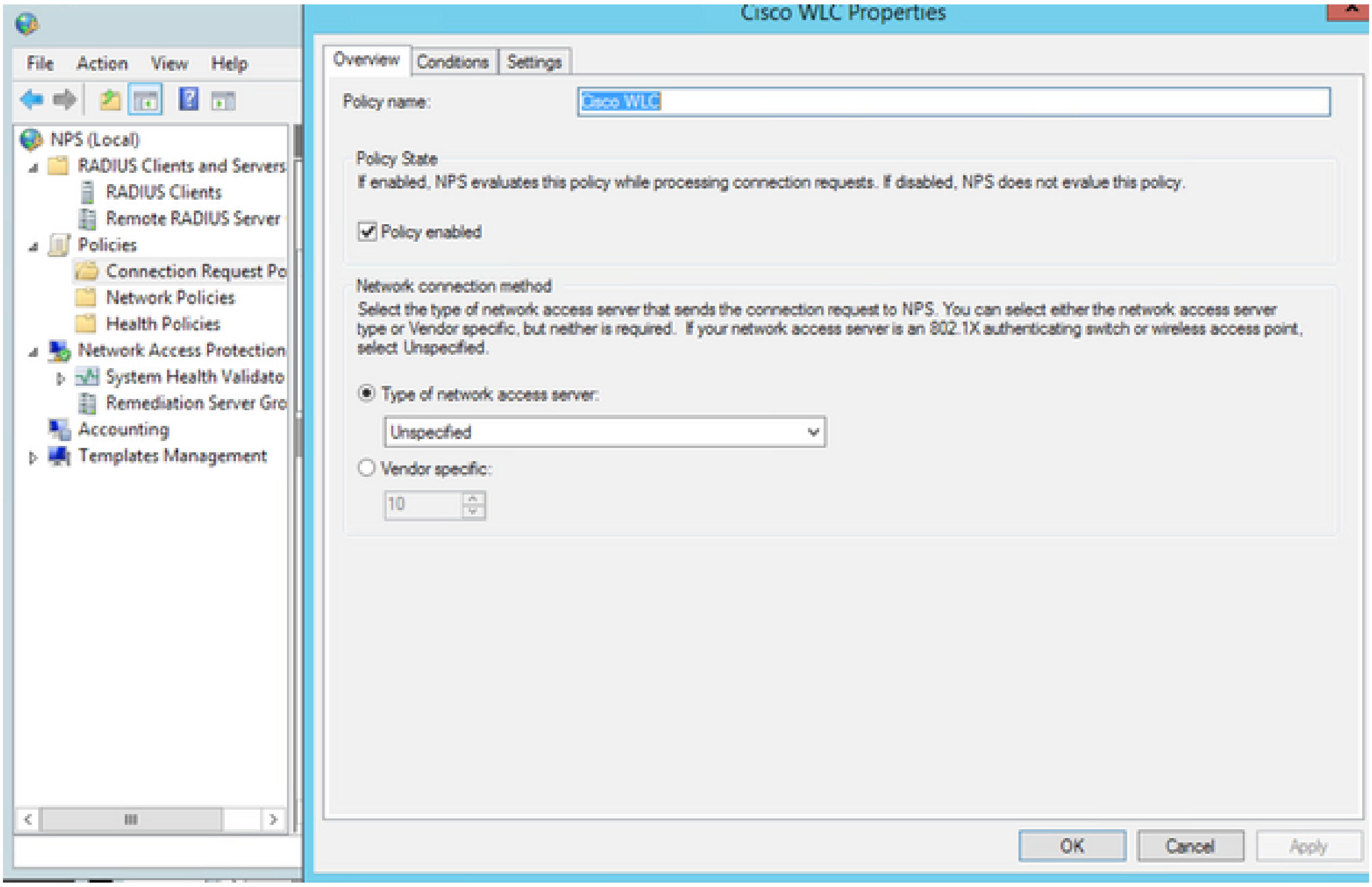
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: •••••••••

Confirm shared secret: •••••••••

Paso 2. Vaya a **Políticas > Políticas de Solicitud de Conexión**. Haga clic con el botón derecho del ratón para agregar una nueva directiva, como se muestra en la imagen.



Cisco WLC Properties

Policy name: Cisco WLC

Policy State

If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy.

☑ Policy enabled

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

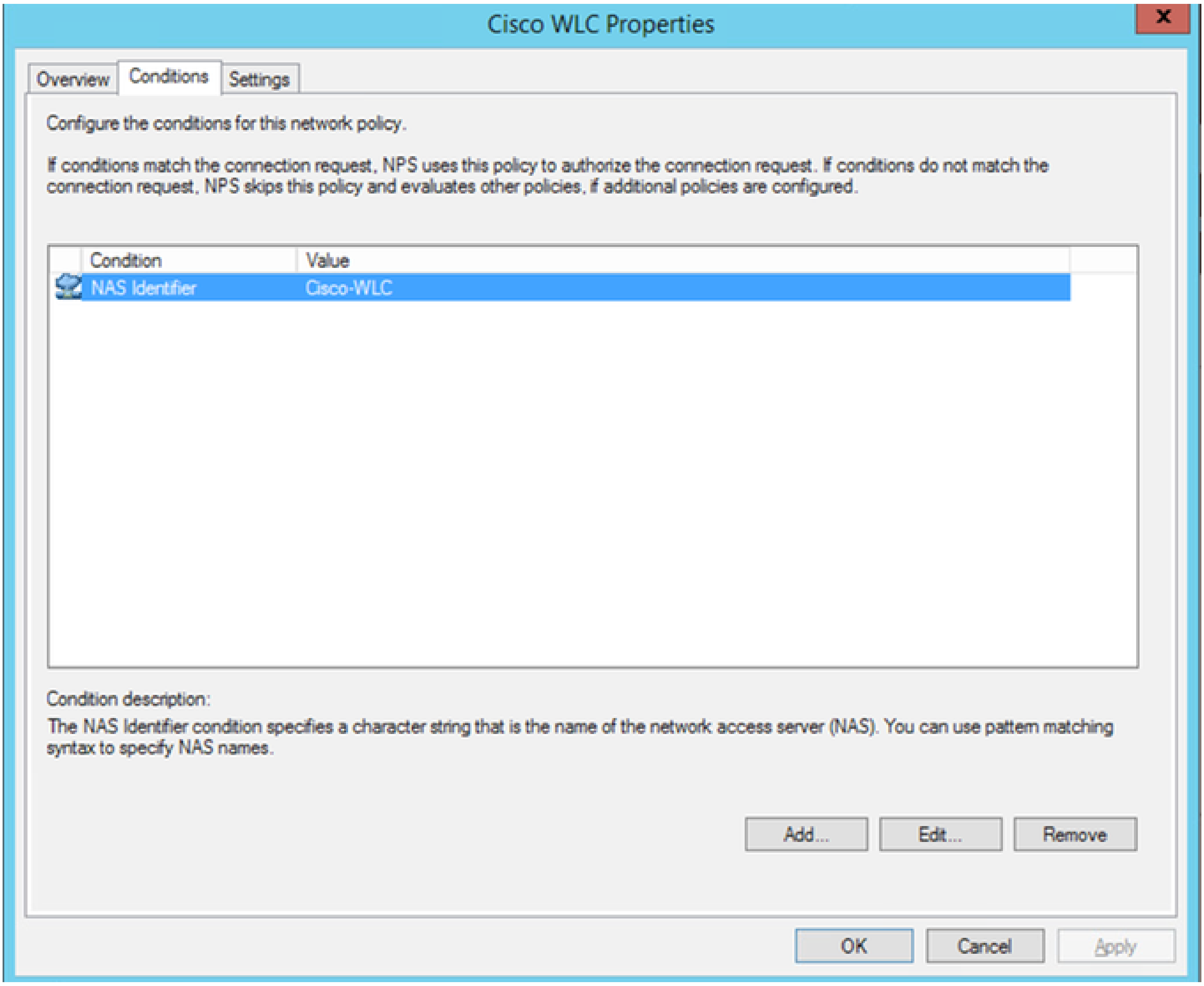
● Type of network access server:

Unspecified

○ Vendor specific:

10

Paso 3. En la pestaña **Condiciones**, seleccione **Identificador NAS** como la nueva condición. Cuando se le solicite, introduzca el nombre de host del controlador como valor, como se muestra en la imagen.



Cisco WLC Properties

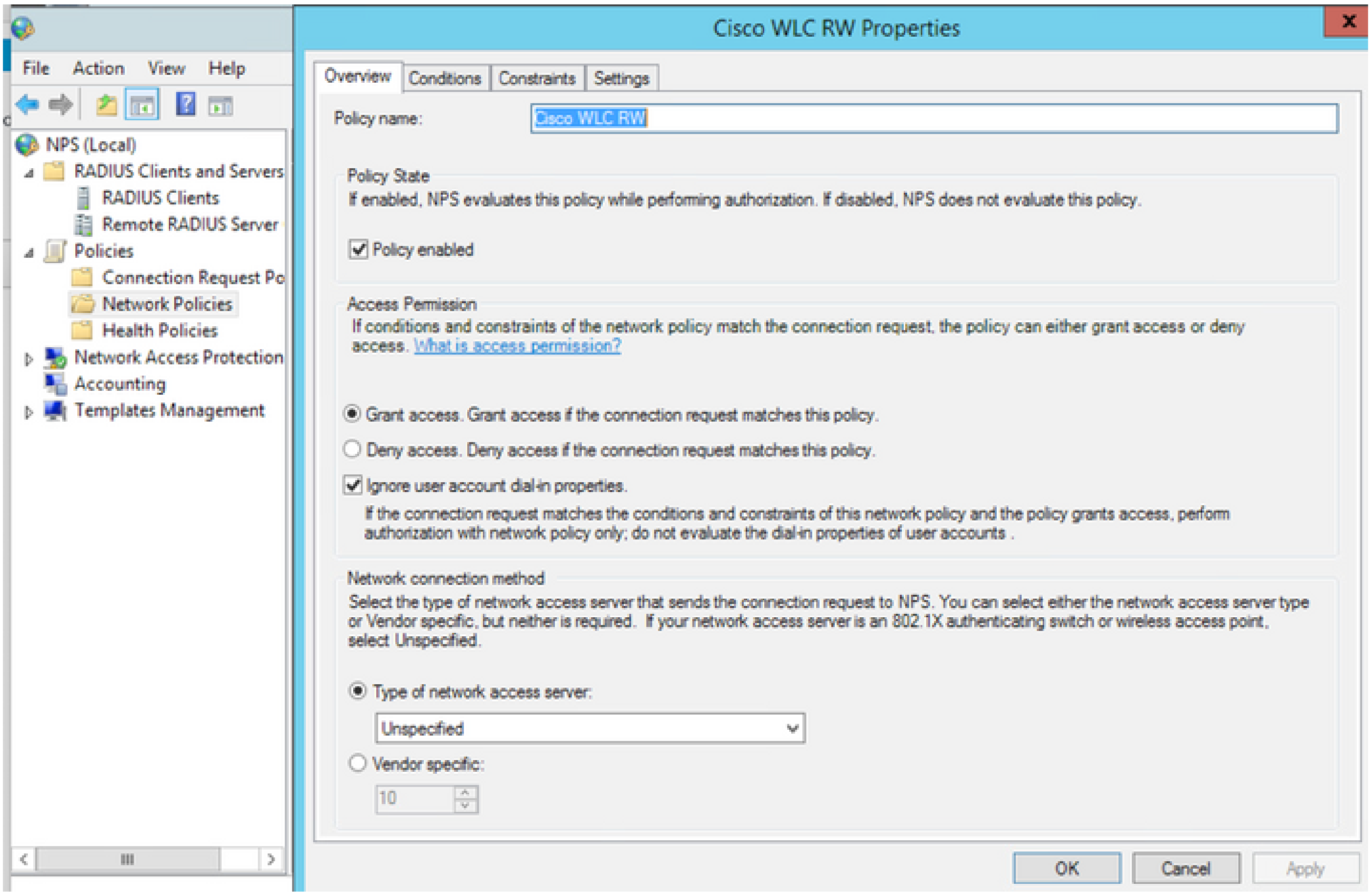
Configure the conditions for this network policy.

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
NAS Identifier	Cisco-WLC

Condition description:
The NAS Identifier condition specifies a character string that is the name of the network access server (NAS). You can use pattern matching syntax to specify NAS names.

Paso 4. Vaya a **Políticas > Políticas de red**. Haga clic con el botón derecho del ratón para agregar una nueva directiva. En este ejemplo, la política se denomina **WLC RW de Cisco**, lo que implica que la política se utiliza para proporcionar acceso completo (de lectura y escritura). Asegúrese de que la política está configurada como se muestra aquí.



Cisco WLC RW Properties

Policy name: Cisco WLC RW

Policy State

If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☑ Policy enabled

Access Permission

If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?

● Grant access. Grant access if the connection request matches this policy.

○ Deny access. Deny access if the connection request matches this policy.

☑ Ignore user account dial-in properties.

If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

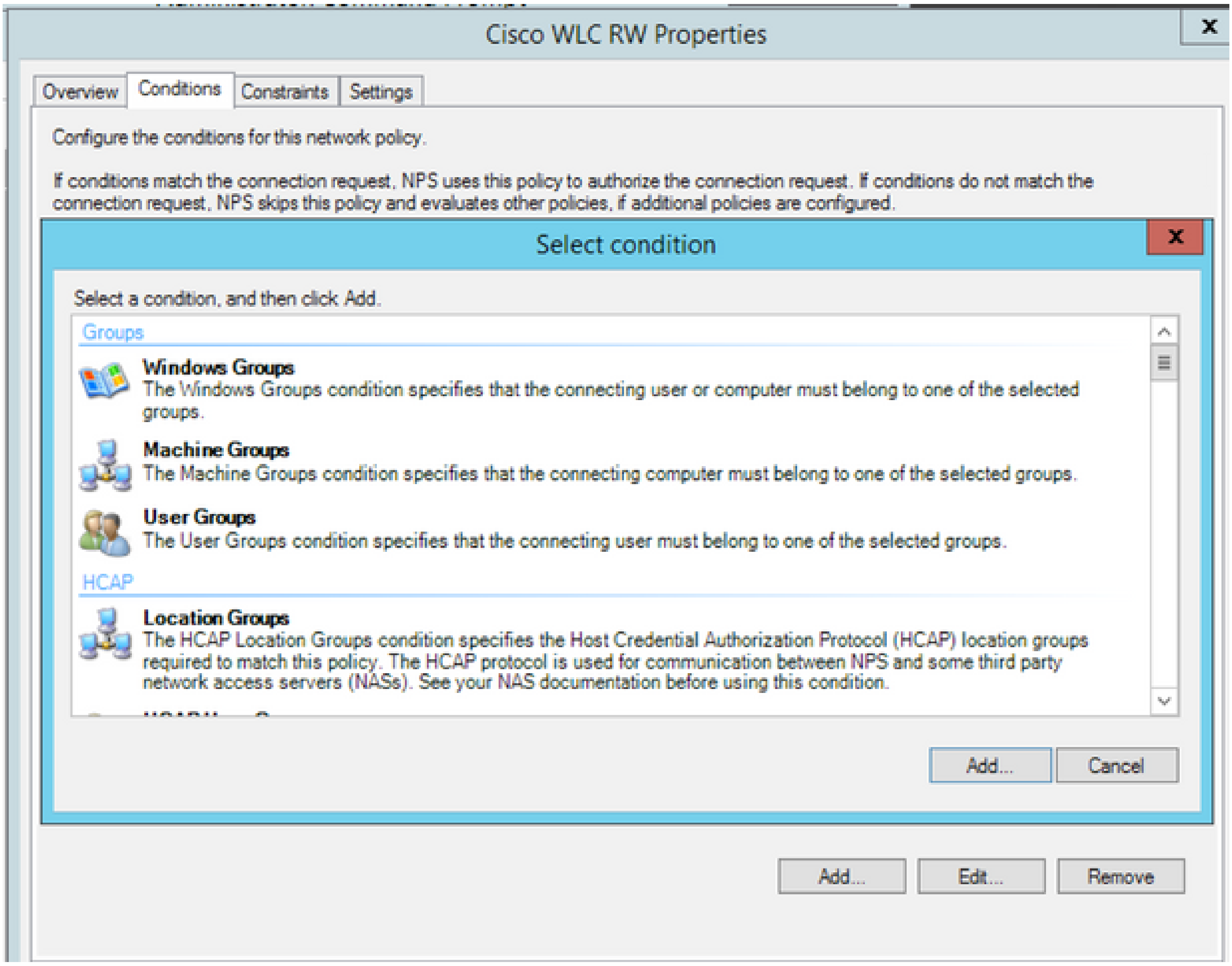
● Type of network access server:

Unspecified

○ Vendor specific:

10

Paso 5. En la ficha **Condiciones**, haga clic en **Agregar**. Seleccione los **grupos de usuarios** y haga clic en **Agregar**, como se muestra en la imagen.



Cisco WLC RW Properties

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.

Select condition

Select a condition, and then click Add.

Groups

Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

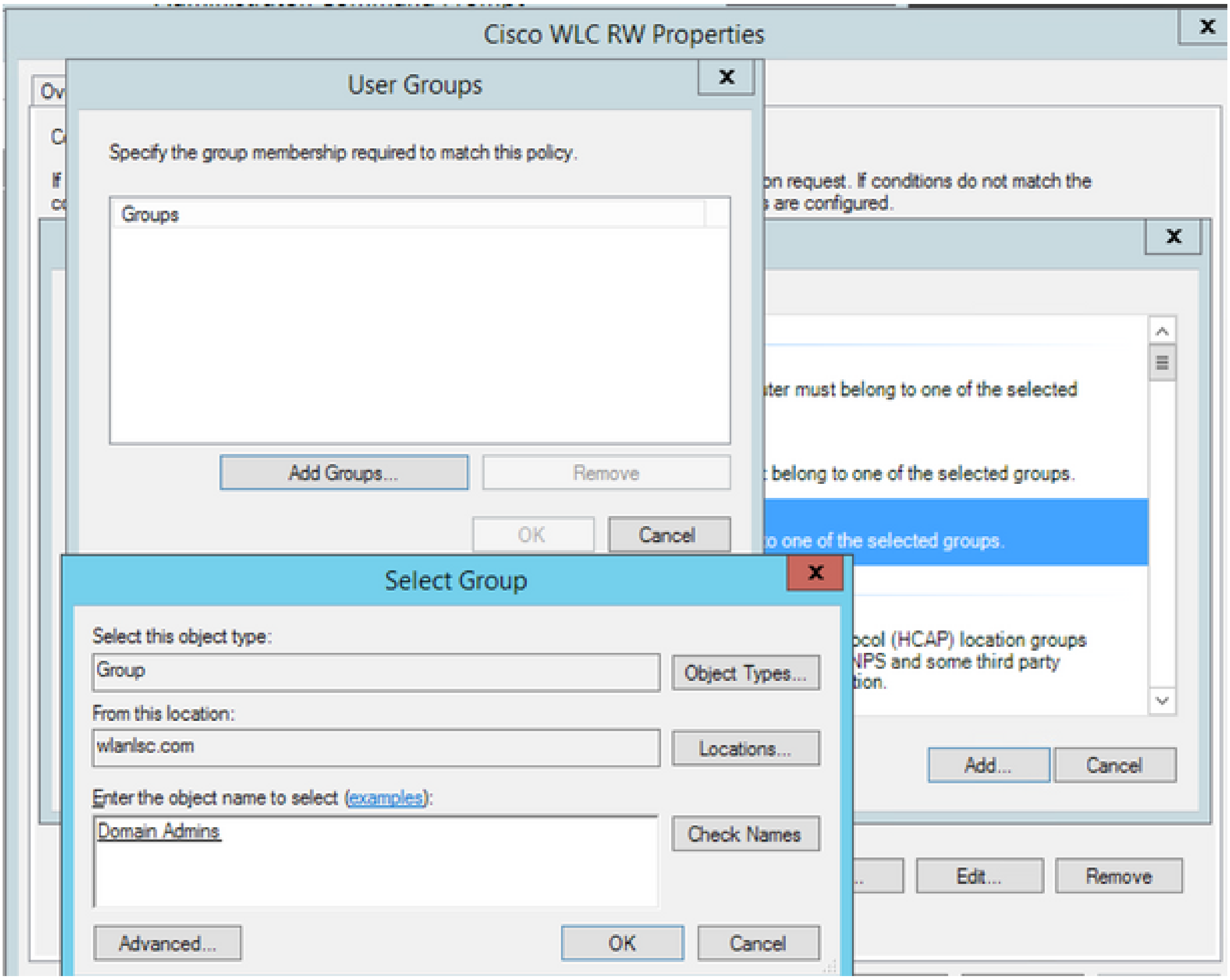
Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

HCAP

Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

Paso 6. Haga clic en **Agregar grupos** en el cuadro de diálogo que aparece. En la ventana **Select Group** que aparece, seleccione el **tipo de objeto** y la **ubicación** que desee e introduzca el nombre de objeto necesario, como se muestra en la imagen.



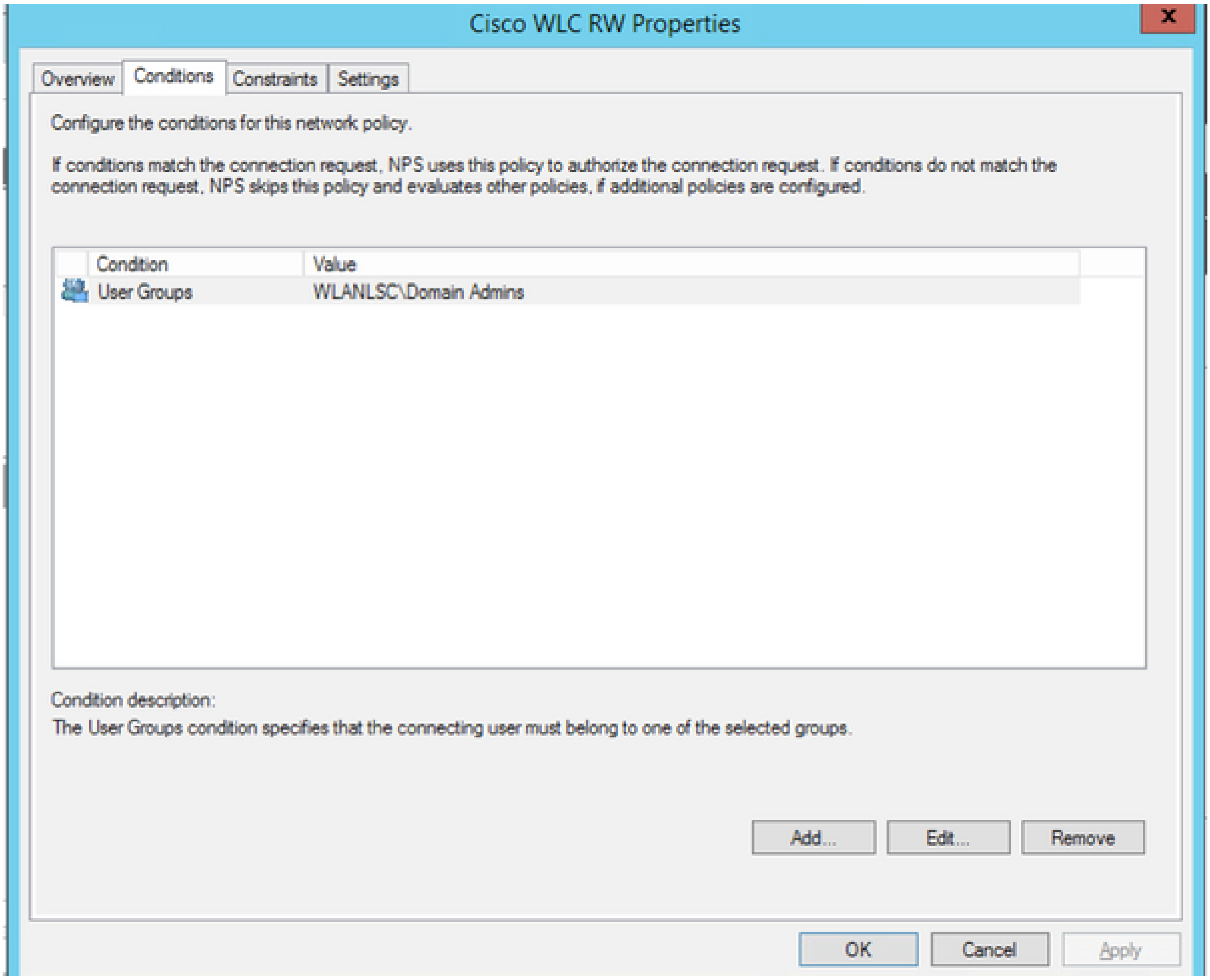
Cisco WLC RW Properties
User Groups
Specify the group membership required to match this policy.
Groups
Add Groups...
Remove
OK
Cancel
on request. If conditions do not match the
are configured.
ter must belong to one of the selected
belong to one of the selected groups.
o one of the selected groups.
ocol (HCAP) location groups
NPS and some third party
tion.
Add...
Cancel
Edit...
Remove
Select Group
Object Types...
Locations...
Check Names
Advanced...
OK
Cancel

Select this object type:
Group

From this location:
wlanlsc.com

Enter the object name to select (examples):
Domain Admins

La condición, si se agrega correctamente, debe verse como se muestra aquí.



Cisco WLC RW Properties

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 Admins

Condition description:
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

Nota: Para averiguar la ubicación y los detalles del nombre del objeto, abra el directorio activo y busque el nombre de usuario deseado. En este ejemplo, **Domain Admins** consta de usuarios a los que se les da acceso completo. **adminuser** forma parte de este nombre de objeto.

Admin User Properties

Admin User

First name: Admin

Initials:

Last name: User

Display name: Admin User

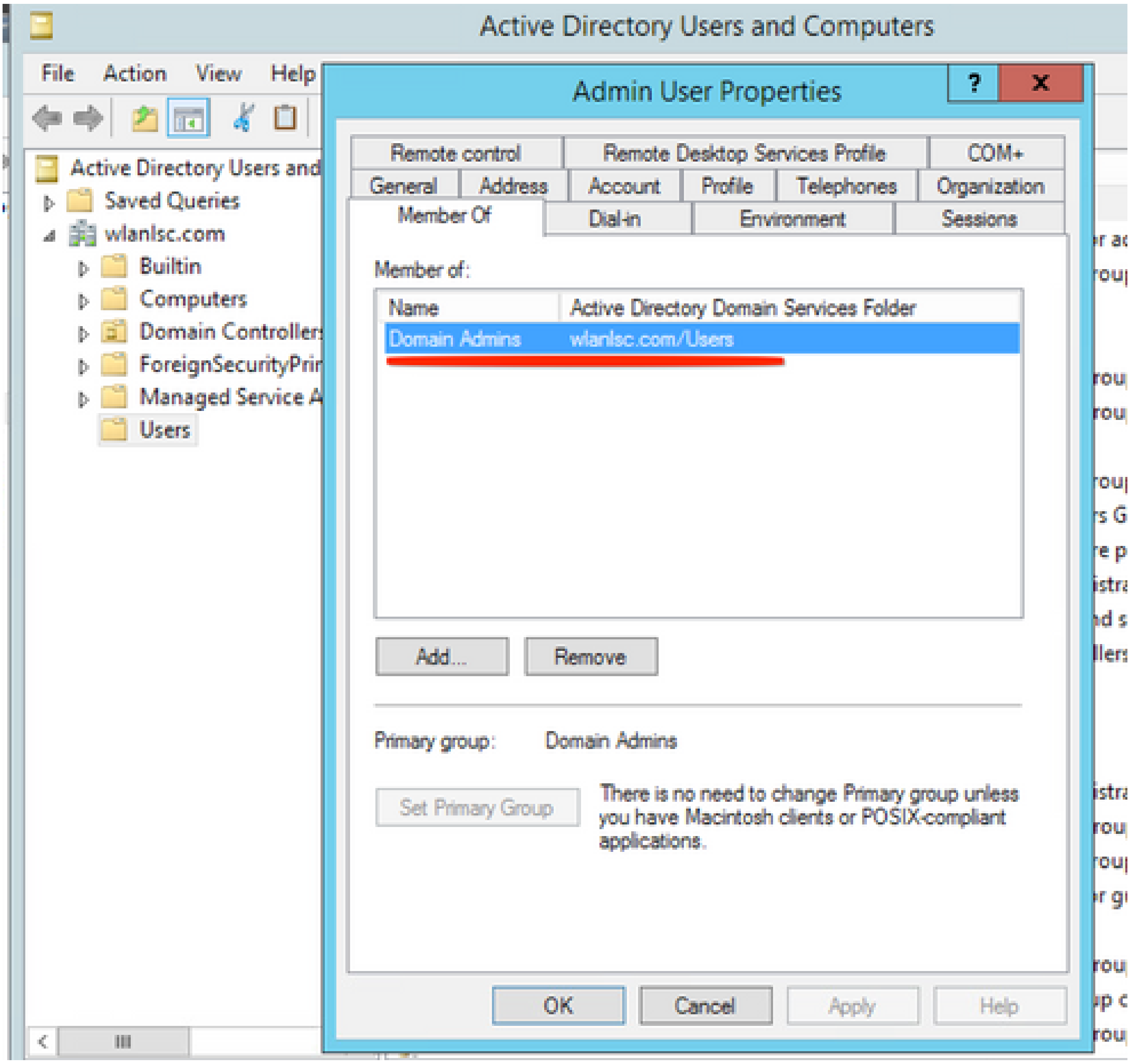
Description:

Office:

Telephone number:

E-mail:

Web page:



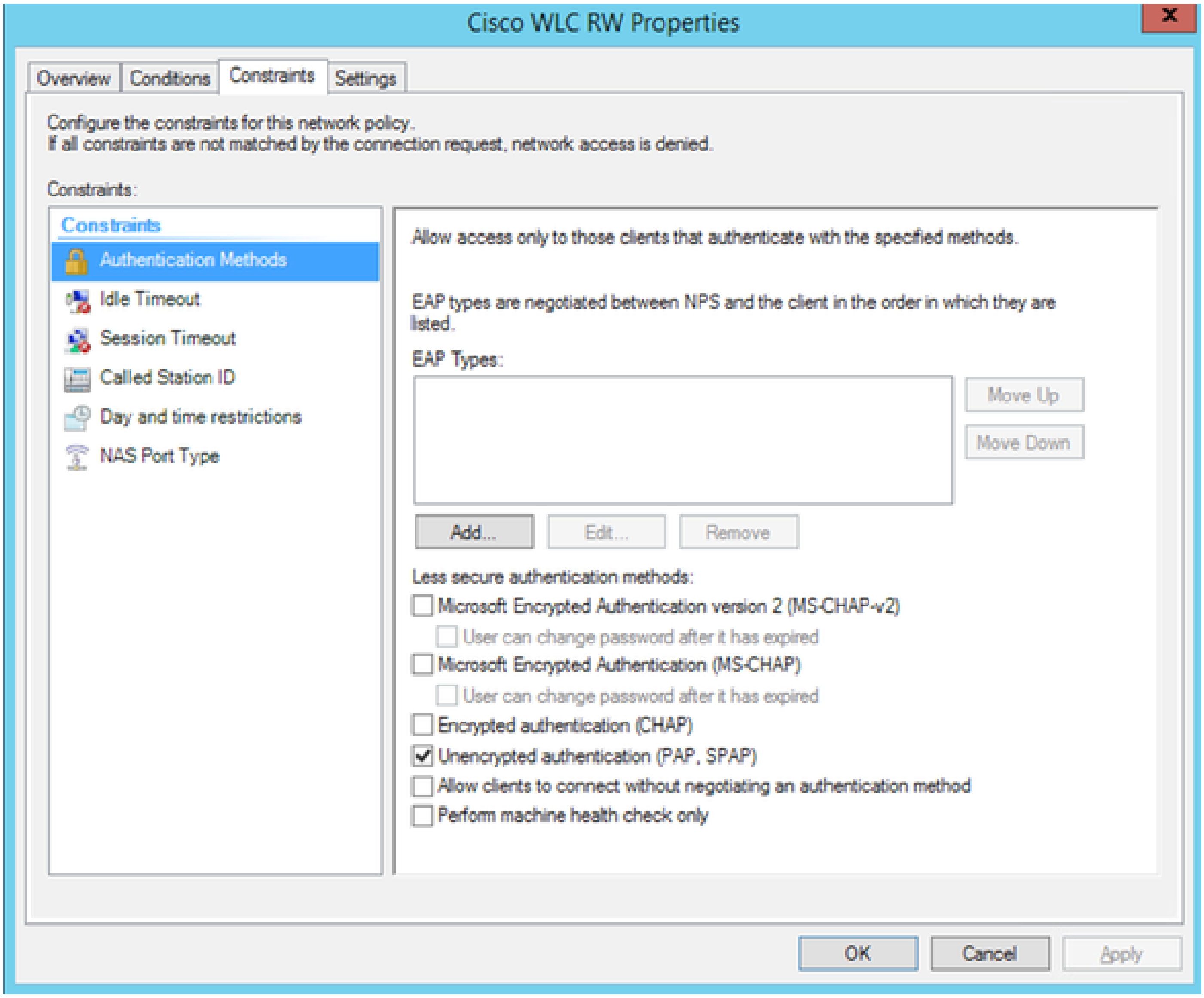
Member of:

Name	Active Directory Domain Services Folder
Domain Admins	wlanlsc.com/Users

Primary group: Domain Admins

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Paso 7. En la pestaña **Restricciones**, navegue hasta **Métodos de Autenticación** y asegúrese de que sólo se verifique la **autenticación no cifrada**.



Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Allow access only to those clients that authenticate with the specified methods.

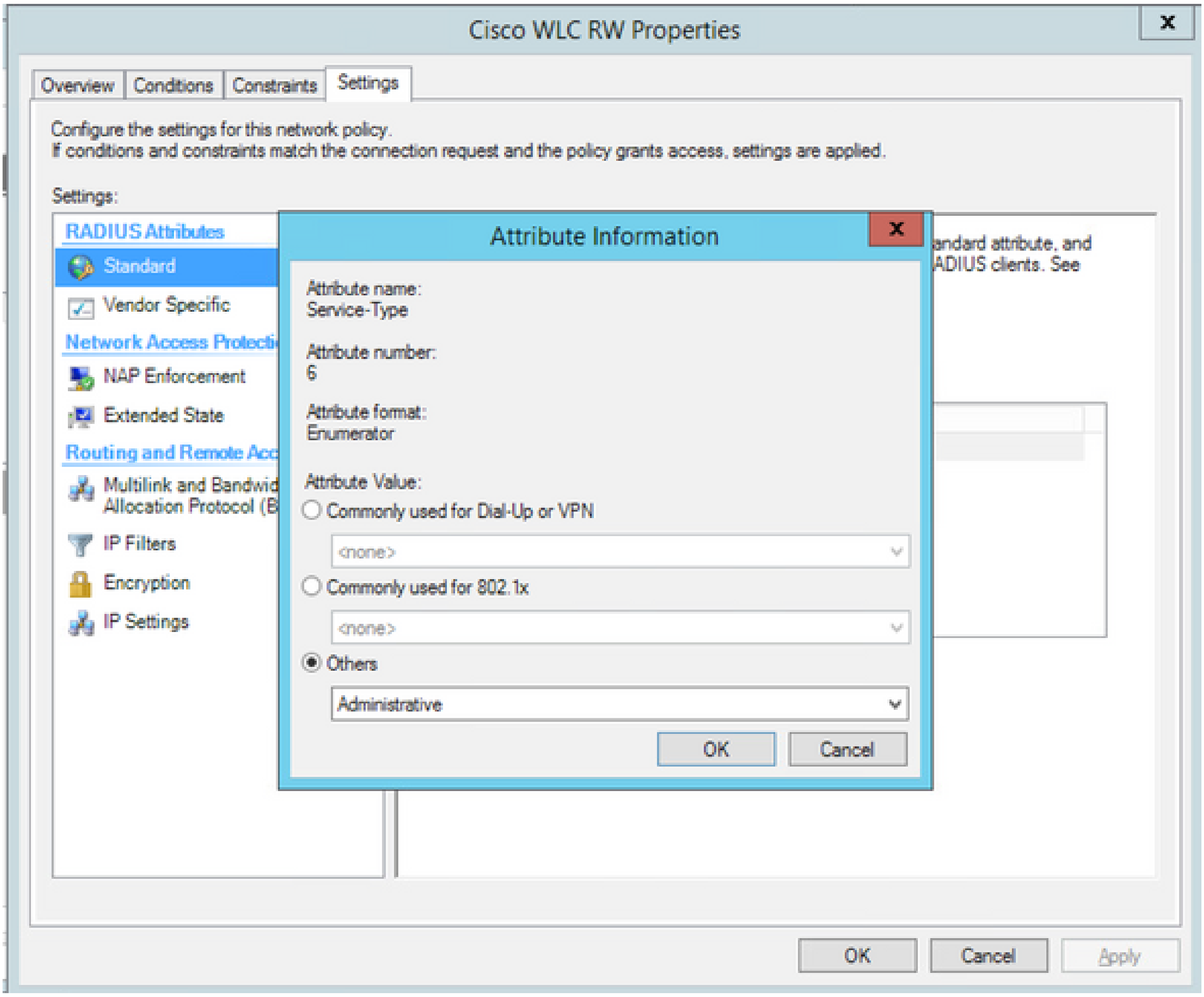
EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

□ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
□ User can change password after it has expired
□ Microsoft Encrypted Authentication (MS-CHAP)
□ User can change password after it has expired
□ Encrypted authentication (CHAP)
☑ Unencrypted authentication (PAP, SPAP)
□ Allow clients to connect without negotiating an authentication method
□ Perform machine health check only

Paso 8. Bajo la pestaña **Settings**, navegue hasta **RADIUS Attributes > Standard**. Haga clic en **Agregar** para agregar un nuevo atributo, **Tipo de servicio**. En el menú desplegable, seleccione **Administrative** para proporcionar acceso completo a los usuarios asignados a esta política. Haga clic en Aplicar para guardar los cambios, como se muestra en la imagen.



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

Attribute Information

Attribute name:
Service-Type

Attribute number:
6

Attribute format:
Enumerator

Attribute Value:

○ Commonly used for Dial-Up or VPN

<none>

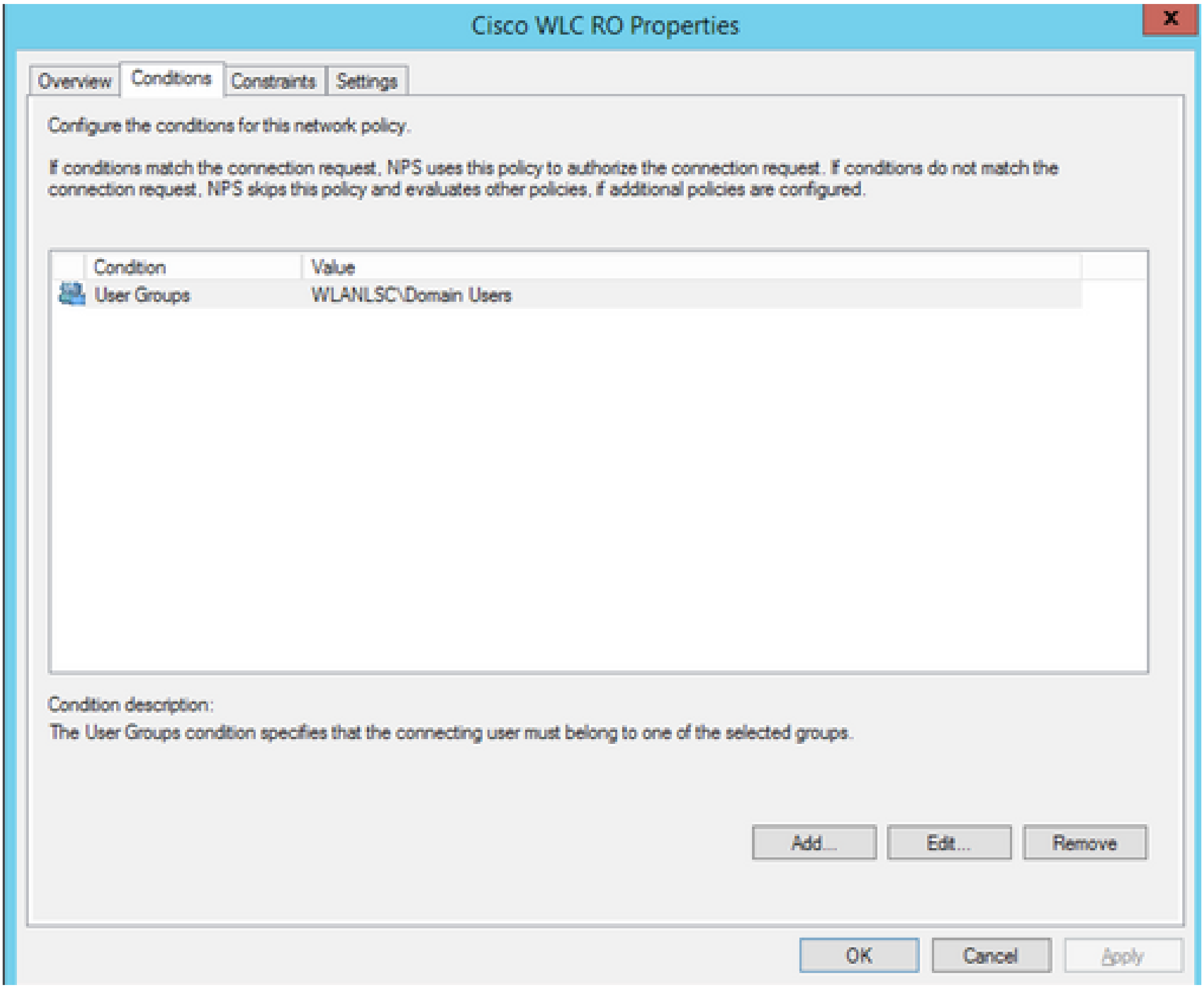
○ Commonly used for 802.1x

<none>

● Others

Administrative

Nota: Si desea otorgar acceso de sólo lectura a usuarios específicos, seleccione NAS-Prompt en la lista desplegable. En este ejemplo, otra política llamada **Cisco WLC RO** se crea para proporcionar acceso de sólo lectura a los usuarios bajo el **nombre de objeto** de **Usuarios de Dominio**.



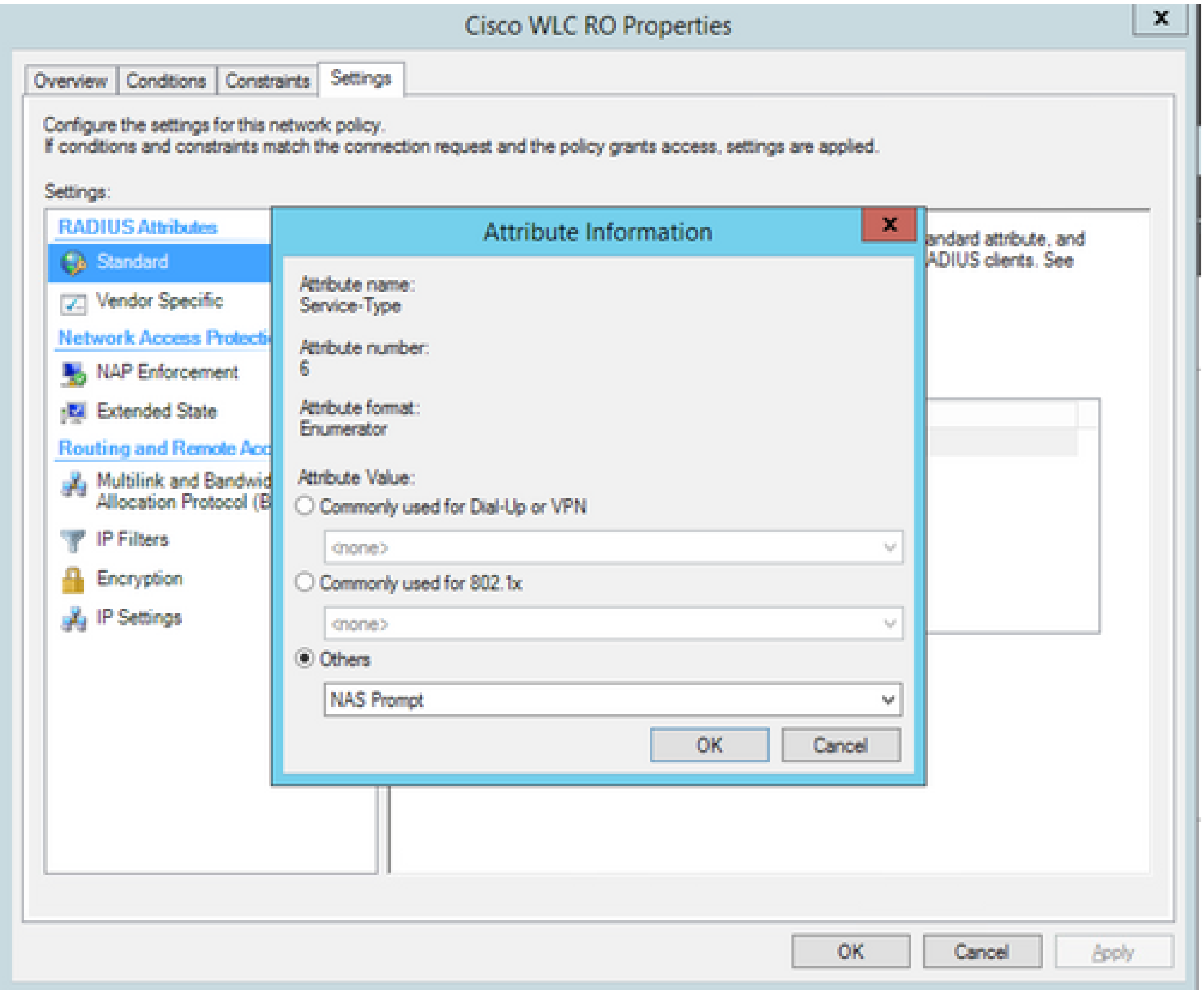
Configure the conditions for this network policy.

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.



Cisco WLC RO Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

Attribute Information

Attribute name:
Service-Type

Attribute number:
6

Attribute format:
Enumerator

Attribute Value:

○ Commonly used for Dial-Up or VPN

<none>

○ Commonly used for 802.1x

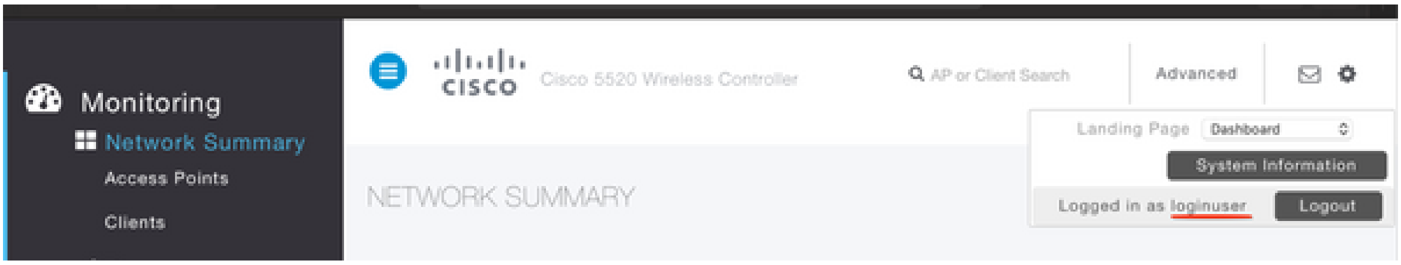
<none>

● Others

NAS Prompt

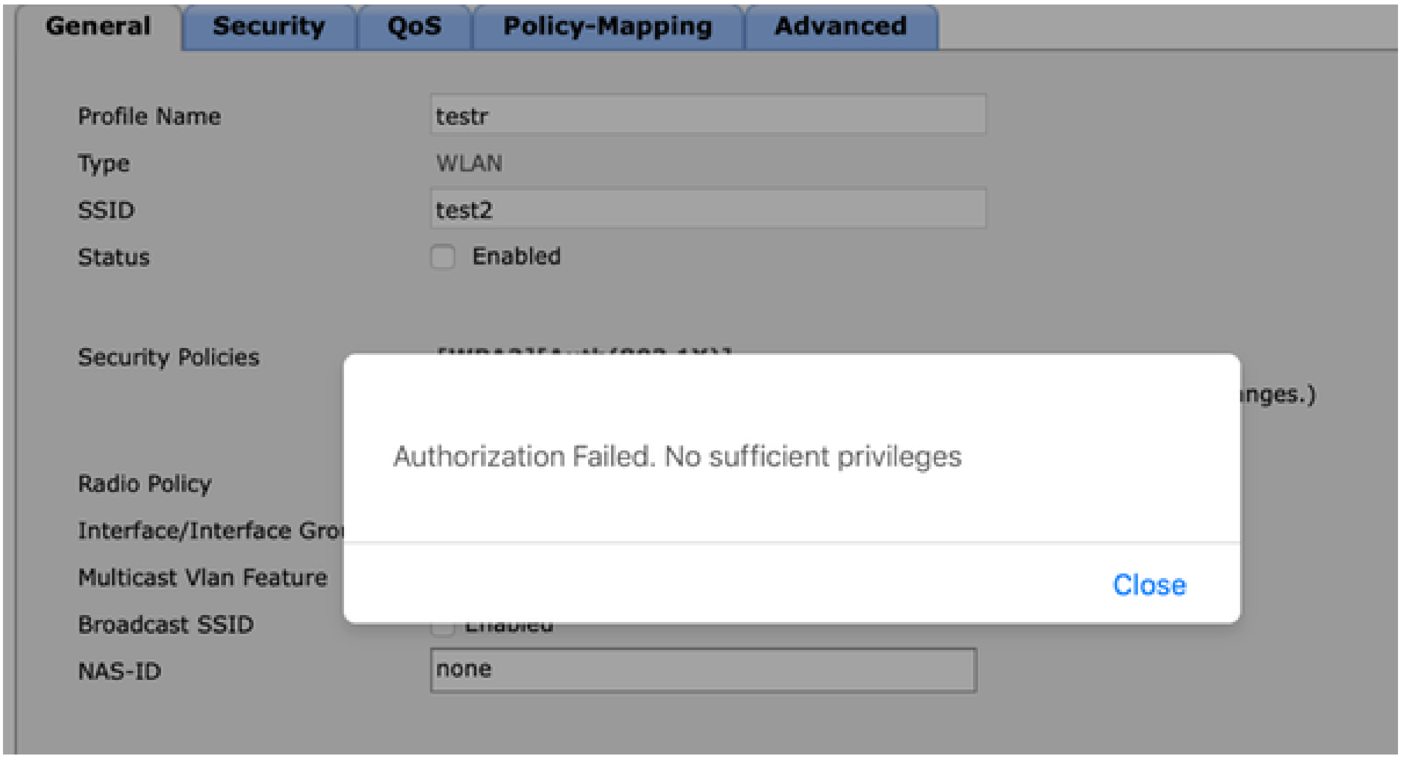
Verificación

1. Cuando se utilizan las credenciales **loginuser**, el usuario no puede configurar ningún cambio en el controlador.



NETWORK SUMMARY

Logged in as loginuser



Profile Name testr

Type WLAN

SSID test2

Status □ Enabled

Security Policies

Radio Policy

Interface/Interface Gro

Multicast Vlan Feature

Broadcast SSID

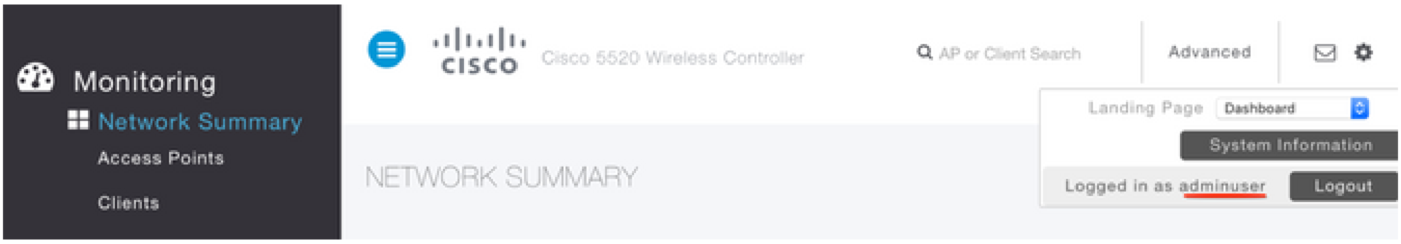
NAS-ID none

Authorization Failed. No sufficient privileges

Desde **debug aaa all enable**, puede ver que el valor del atributo service-type en la respuesta de autorización es 7, que corresponde a 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. Cuando se utilizan **las** credenciales **del administrador**, el usuario debe tener acceso completo con el **valor de tipo de servicio** 6, que corresponde a **administrativo**.



Landing Page Dashboard

Logged in as adminuser

```
*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

Para resolver problemas de acceso de administración al WLC a través de NPS, ejecute el comando **debug aaa all enable**.

1. Aquí se muestran los registros cuando se utilizan credenciales incorrectas.

```
*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. Los registros cuando se utiliza service-type con un valor distinto de **Administrative (value=6)** o **NAS-prompt (value=7)** se muestran de la siguiente manera. En tal caso, el login falla incluso si la autenticación se realiza correctamente.

```
*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
```