

Accès à la gestion pour AireOS WLC via Microsoft NPS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configurations](#)

[Configuration WLC](#)

[Configuration NPS Microsoft](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer l'accès à la gestion pour l'interface utilisateur graphique et l'interface de ligne de commande du WLC AireOS via le serveur de stratégie réseau Microsoft (NPS).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance des solutions de sécurité sans fil
- Concepts AAA et RADIUS
- Connaissances de base de Microsoft Server 2012
- Installation de Microsoft NPS et Active Directory (AD)

Components Used

Les informations fournies dans ce document sont basées sur les composants logiciels et matériels suivants.

- Contrôleur AireOS (5520) sur 8.8.120.0
- Microsoft Server 2012

Note: Ce document est destiné à donner aux lecteurs un exemple de configuration requise sur un serveur Microsoft pour l'accès à la gestion WLC. La configuration du serveur Microsoft Windows présentée dans ce document a été testée dans les travaux pratiques et a fonctionné comme prévu. Si vous rencontrez des problèmes de configuration, contactez

Microsoft pour obtenir de l'aide. Le centre d'assistance technique Cisco (TAC) ne prend pas en charge la configuration du serveur Microsoft Windows. Les guides d'installation et de configuration de Microsoft Windows 2012 sont disponibles sur 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.

Informations générales

Lorsque l'interface CLI/GUI du WLC est accessible, l'utilisateur est invité à entrer les informations d'identification pour se connecter correctement. Les informations d'identification peuvent être vérifiées sur une base de données locale ou un serveur AAA externe. Dans ce document, Microsoft NPS est utilisé comme serveur d'authentification externe.

Configurations

Dans cet exemple, deux utilisateurs sont configurés sur AAA (NPS) viz. **loginuser** et **adminuser**. **loginuser** n'a qu'un accès en lecture seule tandis que **adminuser** bénéficie d'un accès complet.

Configuration WLC

Étape 1. Ajoutez le serveur RADIUS sur le contrôleur. Accédez à **Security > RADIUS > Authentication**. Cliquez sur **Nouveau** pour ajouter le serveur. Vérifiez que l'option **de gestion** est activée pour que ce serveur puisse être utilisé pour l'accès à la gestion, comme illustré dans cette image.

The screenshot shows the Cisco ISE Security configuration page for RADIUS Authentication Servers. The left sidebar contains a navigation menu with categories like AAA, Local EAP, and Advanced. The main content area is titled 'RADIUS Authentication Servers > Edit' and lists various configuration parameters for a specific server (Server Index 2). The parameters include Server Address (10.106.33.39), Shared Secret Format (ASCII), Shared Secret (masked with ***), Confirm Shared Secret (masked with ***), Key Wrap (disabled), Apply Cisco ISE Default settings (disabled), Apply Cisco ACA Default settings (disabled), Port Number (1812), Server Status (Enabled), Support for CoA (Disabled), Server Timeout (5 seconds), Network User (checked), Management (checked), Management Retransmit Timeout (5 seconds), Tunnel Proxy (disabled), Realm List (link), PAC Provisioning (disabled), IPSec (disabled), and Cisco ACA (disabled).

Étape 2. Accédez à **Sécurité > Ordre de priorité > Utilisateur de gestion**. Assurez-vous que RADIUS est sélectionné comme l'un des types d'authentification.

The screenshot shows the Cisco ISE Priority Order configuration page for the Management User. The page is titled 'Priority Order > Management User' and has a sub-section for 'Authentication'. Under 'Authentication', there are two boxes: 'Not Used' containing 'TACACS+' and 'Order Used for Authentication' containing 'RADIUS LOCAL'. Between the boxes are navigation buttons: '>' and '<' between the boxes, and 'Up' and 'Down' next to the 'RADIUS LOCAL' box.

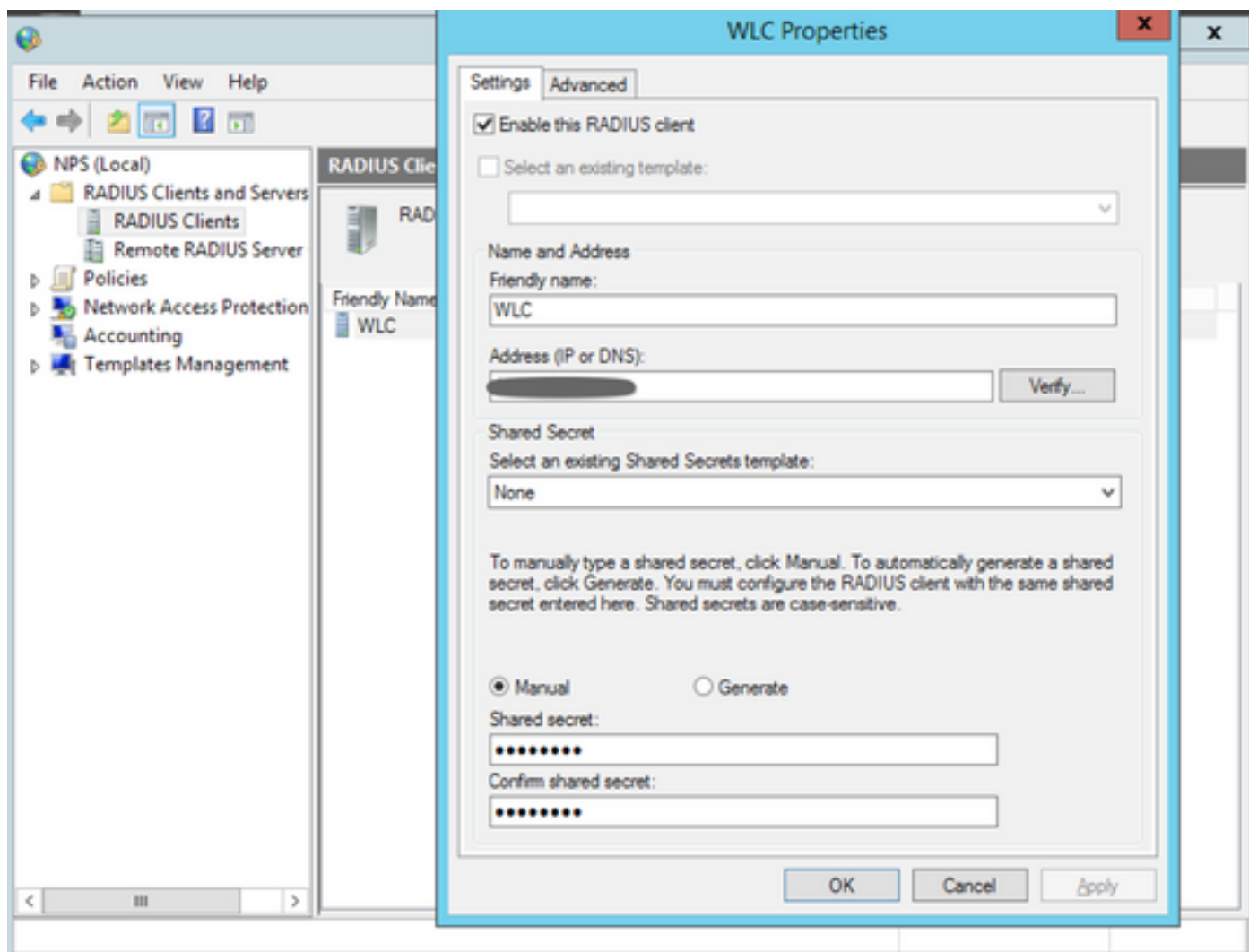
Note: Si RADIUS est sélectionné comme première priorité dans l'ordre d'authentification, les informations d'identification locales ne seront utilisées pour l'authentification que si le serveur RADIUS est inaccessible. Si RADIUS est sélectionné comme deuxième priorité, les informations d'identification RADIUS seront d'abord vérifiées par rapport à la base de données locale, puis vérifiées par rapport aux serveurs RADIUS configurés.

Configuration NPS Microsoft

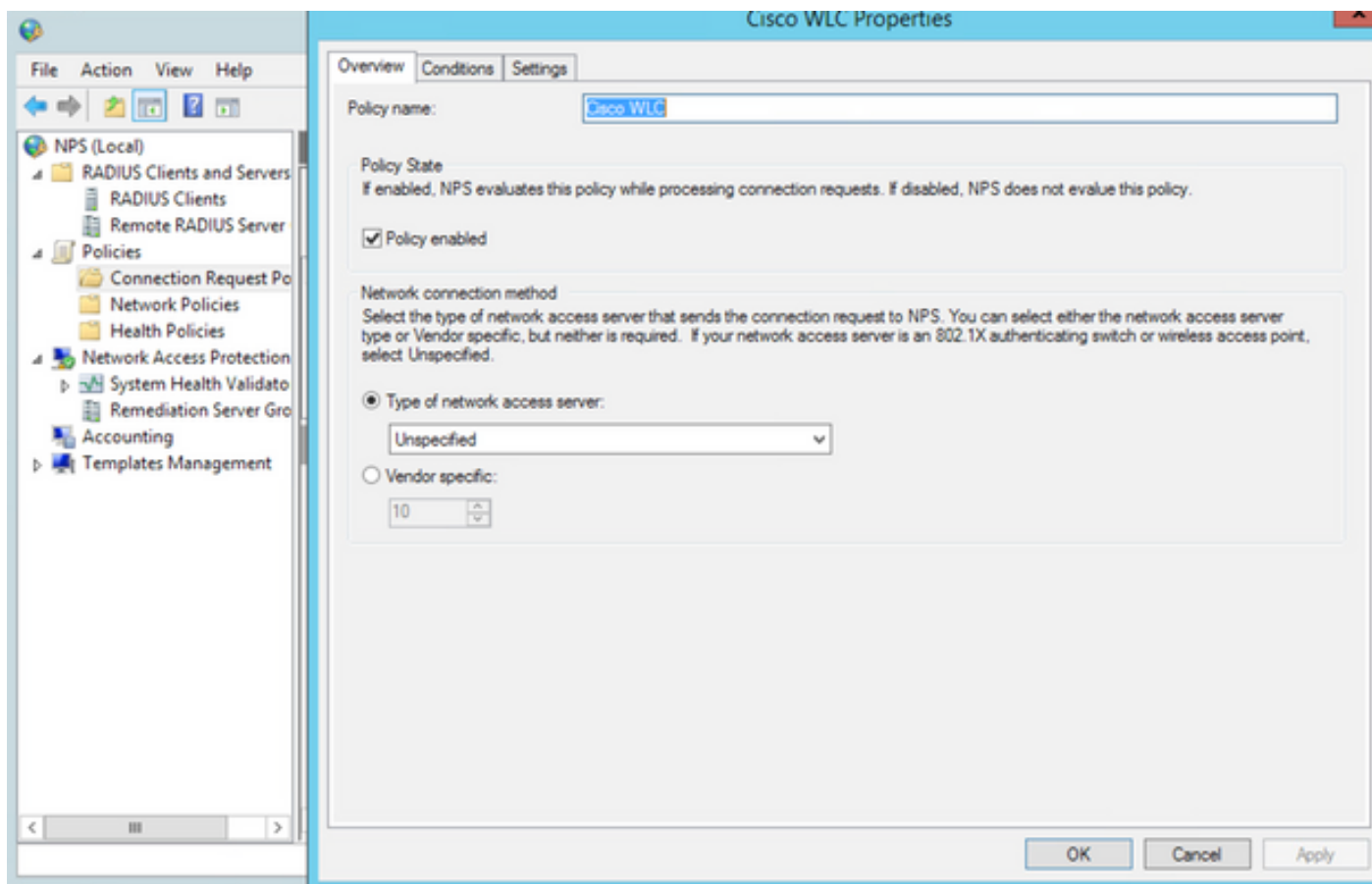
Étape 1. Ouvrez le serveur NPS Microsoft. Cliquez avec le bouton droit sur **Clients Radius**.

Cliquez sur **Nouveau** pour ajouter le WLC en tant que client RADIUS.

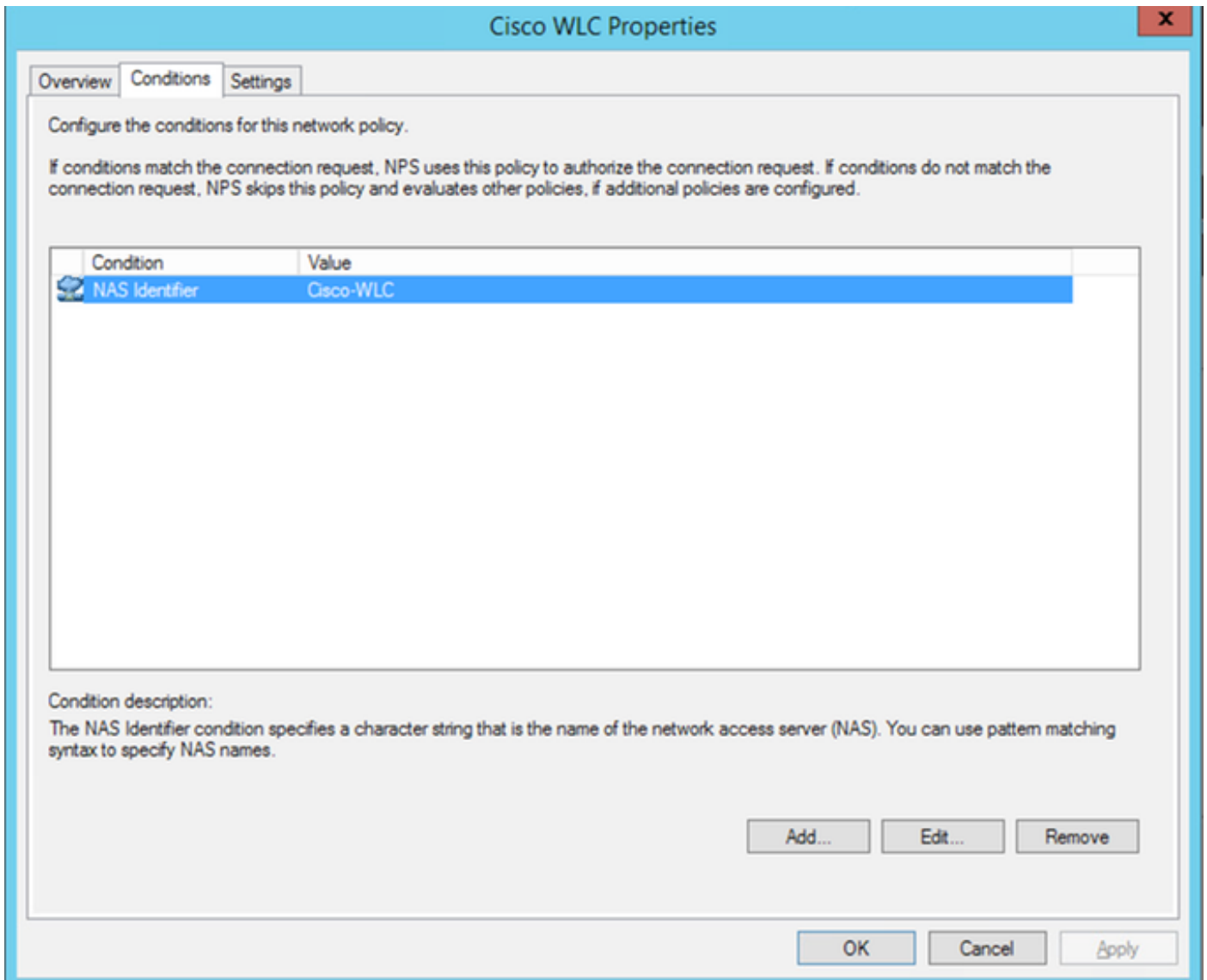
Saisissez les détails requis. Assurez-vous que le secret partagé est identique à celui configuré sur le contrôleur lors de l'ajout du serveur RADIUS.



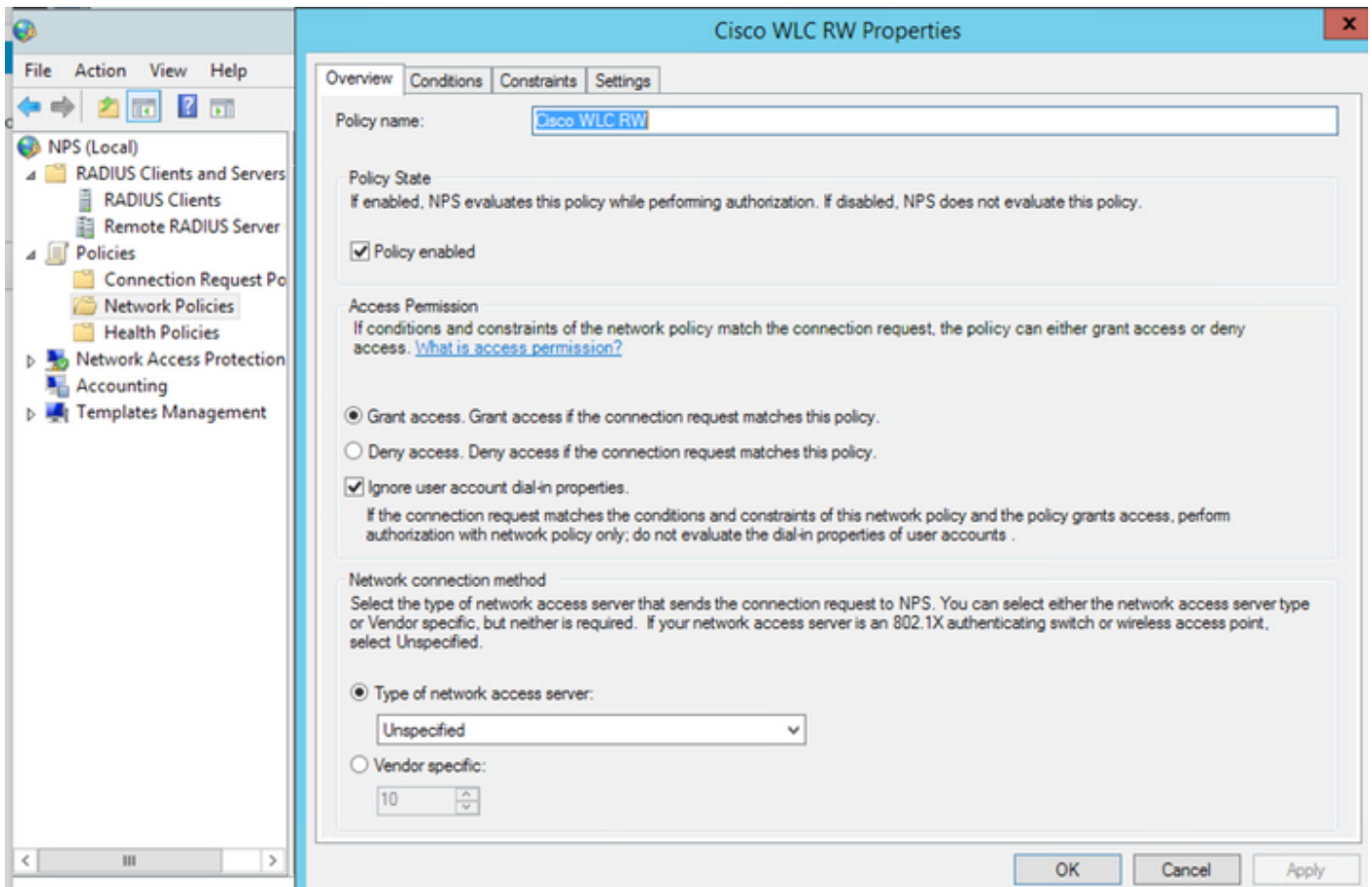
Étape 2. Accédez à **Stratégies > Stratégies de demande de connexion**. Cliquez avec le bouton droit de la souris pour ajouter une nouvelle stratégie, comme illustré dans l'image.



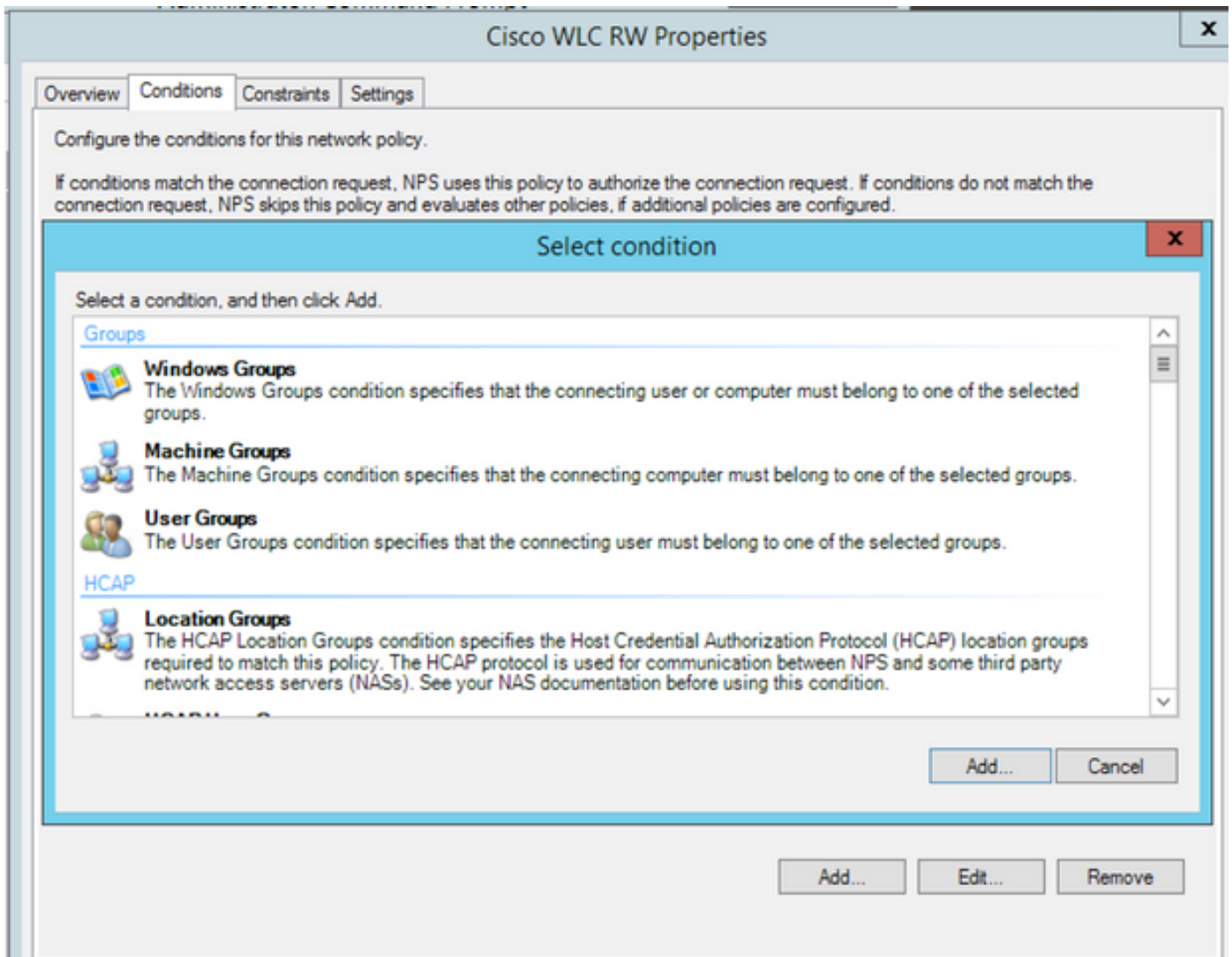
Étape 3. Sous l'onglet **Conditions**, sélectionnez **Identificateur NAS** comme nouvelle condition. Lorsque vous y êtes invité, entrez le nom d'hôte du contrôleur comme valeur, comme indiqué dans l'image.



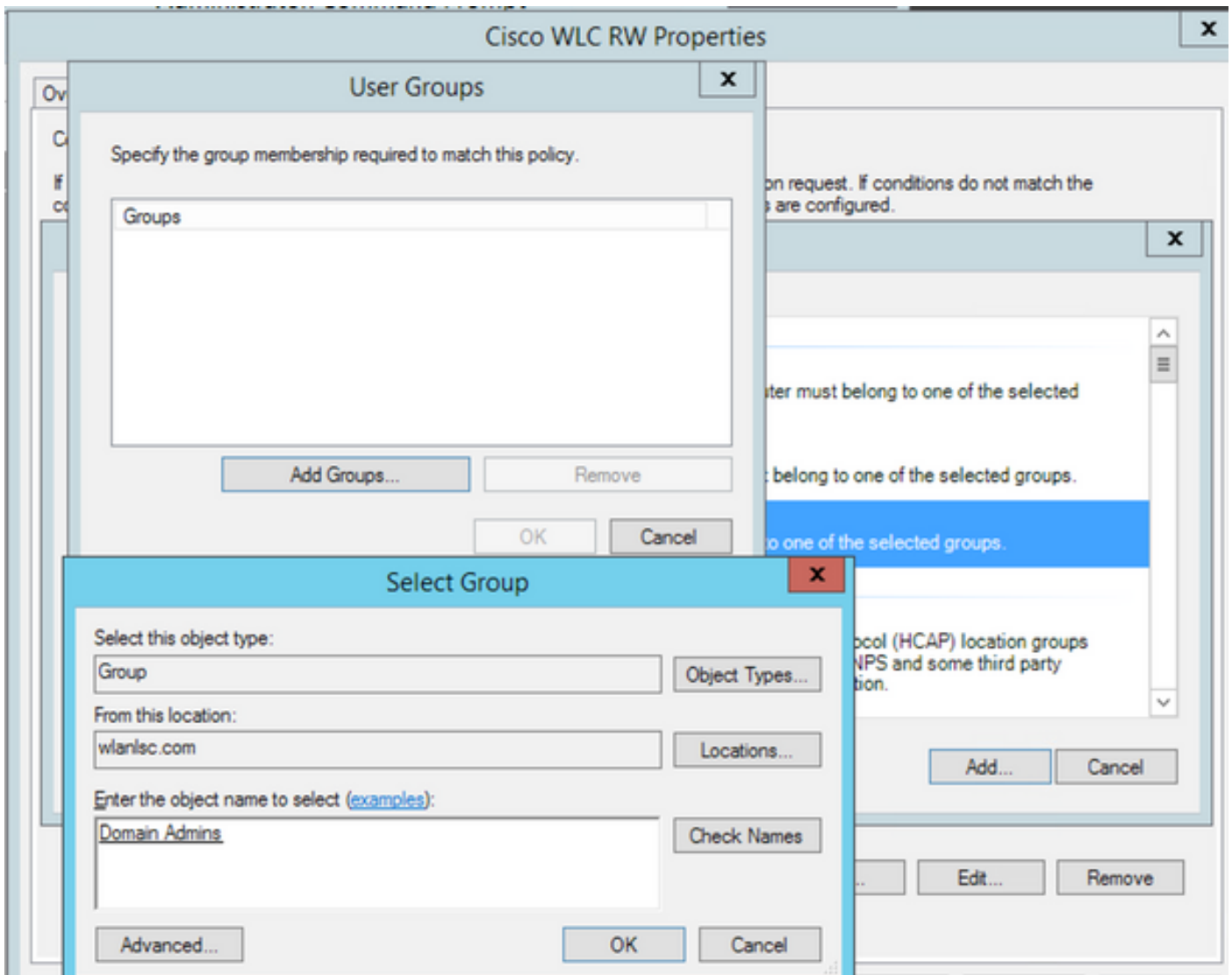
Étape 4. Accédez à **Politiques > Stratégies réseau**. Cliquez avec le bouton droit de la souris pour ajouter une nouvelle stratégie. Dans cet exemple, la stratégie est nommée **Cisco WLC RW**, ce qui implique que la stratégie est utilisée pour fournir un accès complet (lecture-écriture). Assurez-vous que la stratégie est configurée comme indiqué ici.



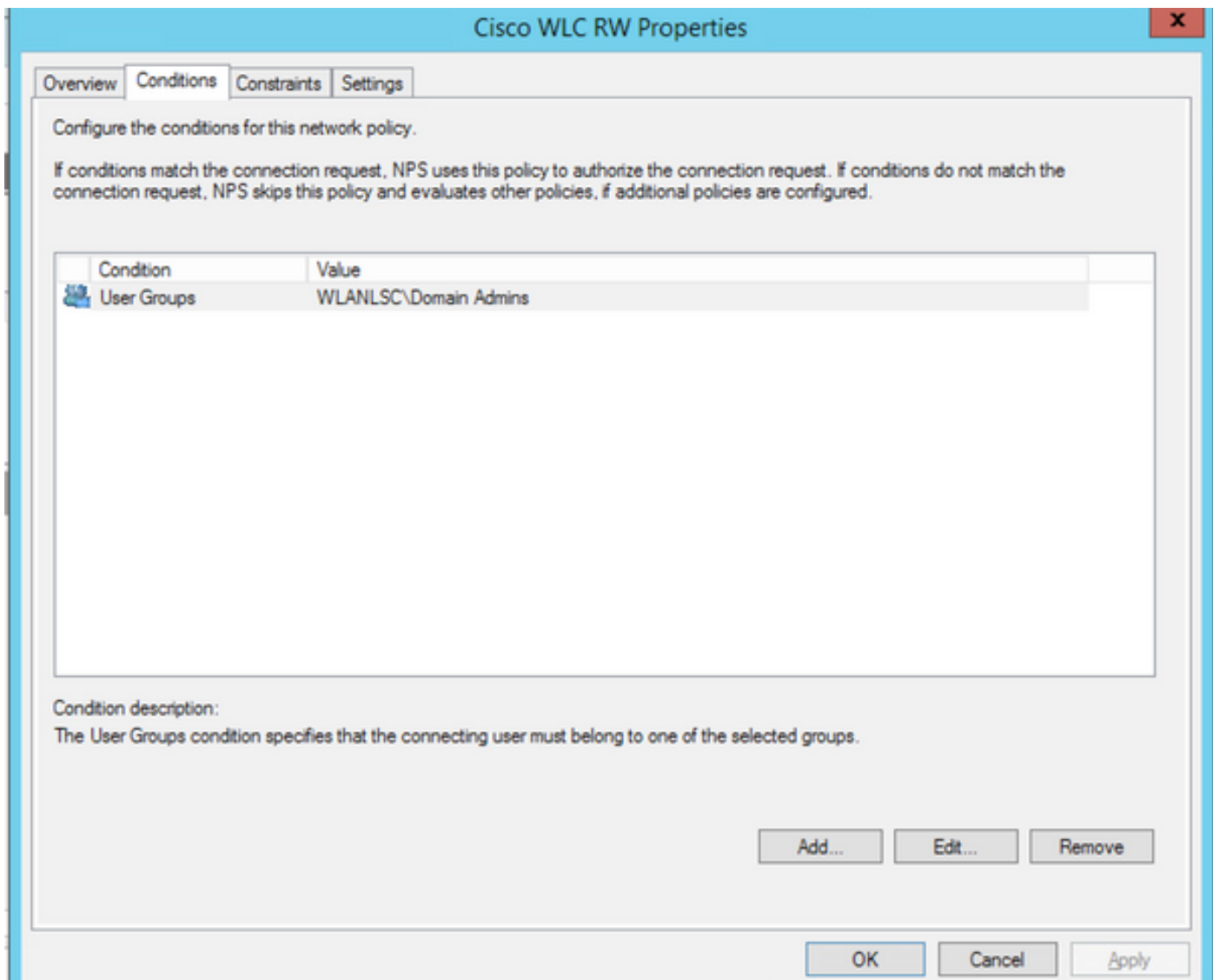
Étape 5. Sous l'onglet **Conditions**, cliquez sur **Ajouter**. Sélectionnez les **groupes d'utilisateurs** et cliquez sur **Ajouter**, comme illustré dans l'image.



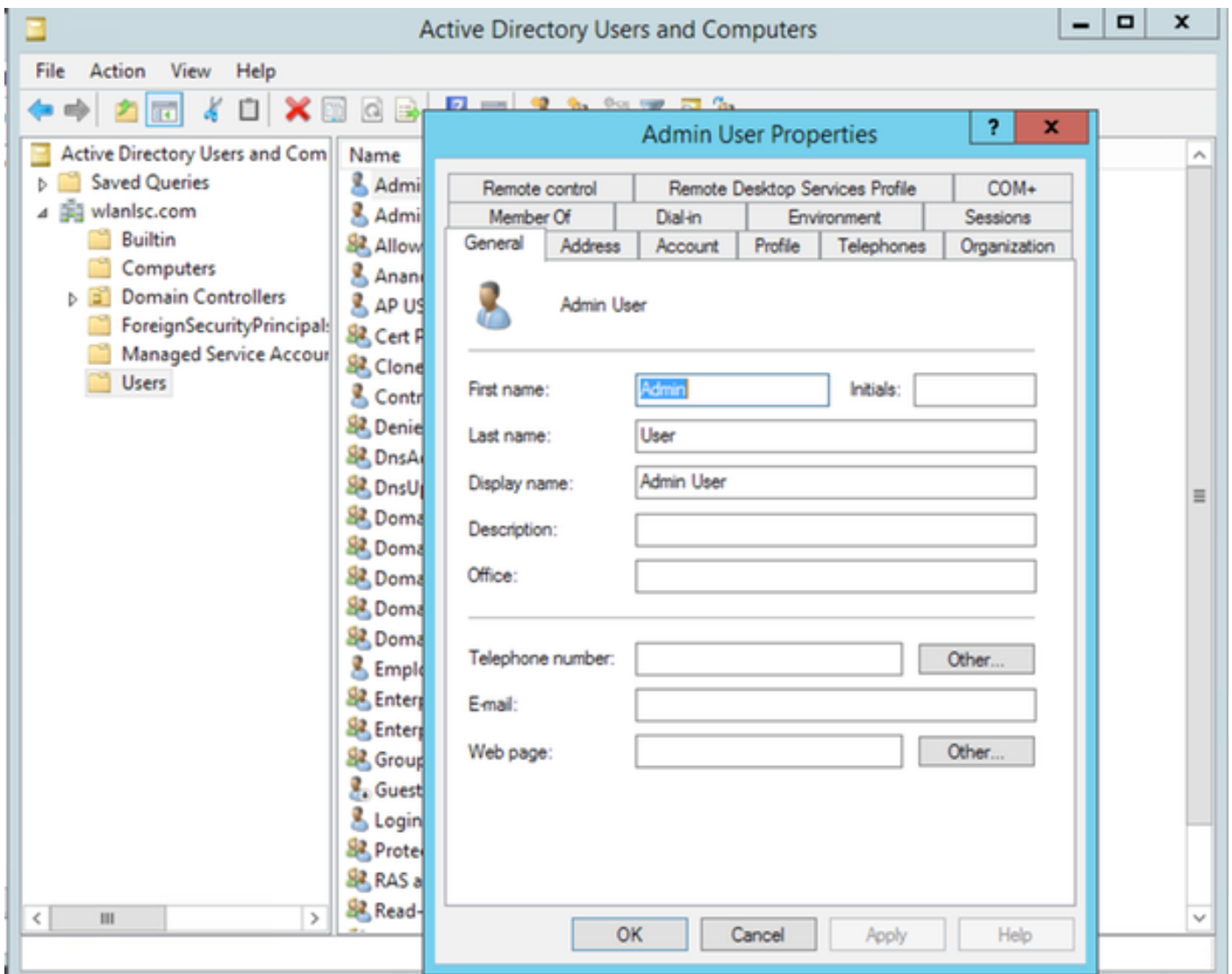
Étape 6. Cliquez sur **Ajouter des groupes** dans la boîte de dialogue qui s'affiche. Dans la fenêtre **Sélectionner un groupe** qui s'affiche, sélectionnez le **type d'objet** et **l'emplacement** et entrez le nom d'objet requis, comme indiqué dans l'image.

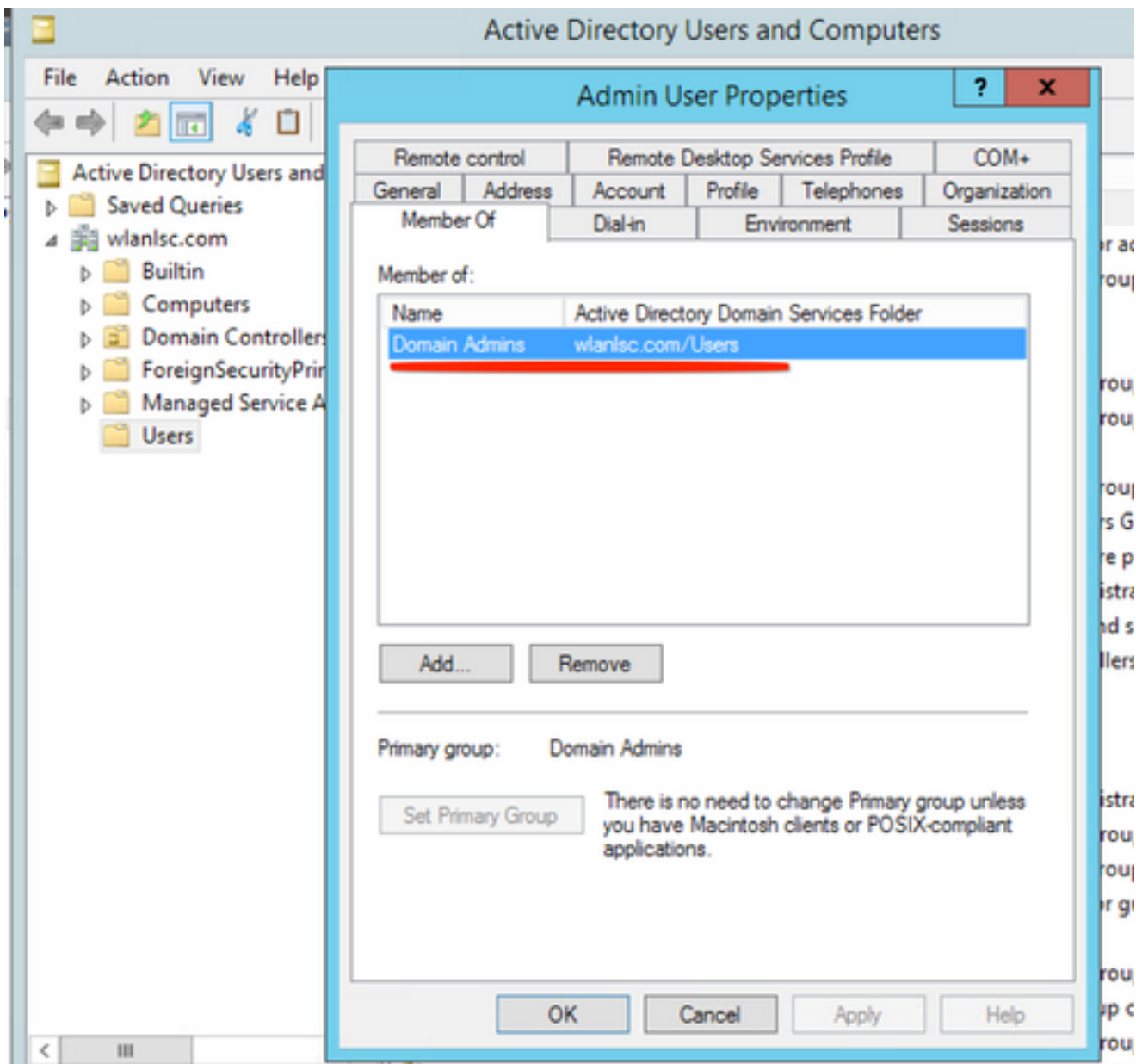


La condition, si elle est ajoutée correctement, doit être affichée ici.

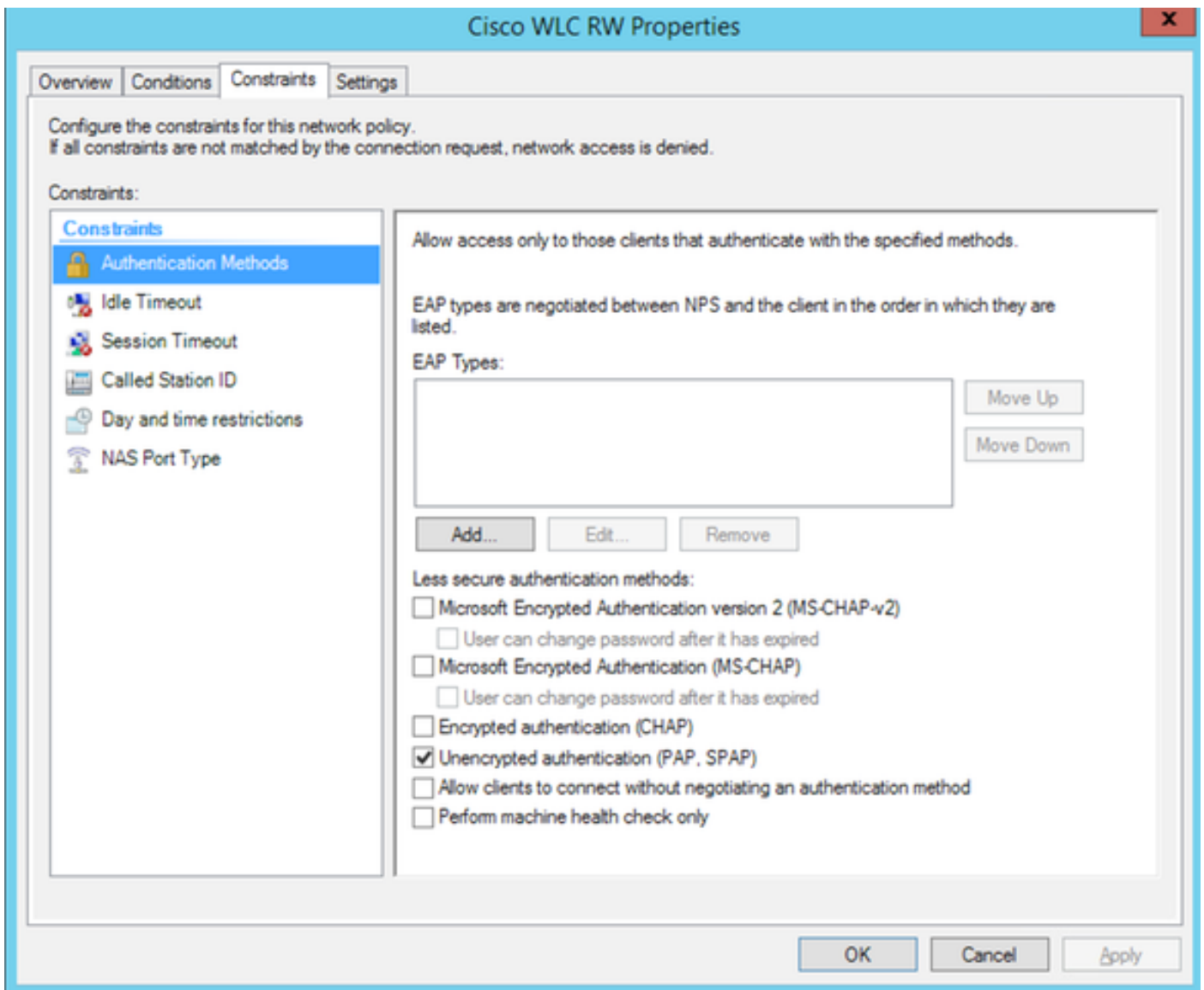


Note: Pour connaître les détails de l'emplacement et du nom de l'objet, ouvrez le répertoire actif et recherchez le nom d'utilisateur souhaité. Dans cet exemple, **les administrateurs de domaine** se composent d'utilisateurs auxquels un accès complet est accordé. **adminuser** fait partie de ce nom d'objet.

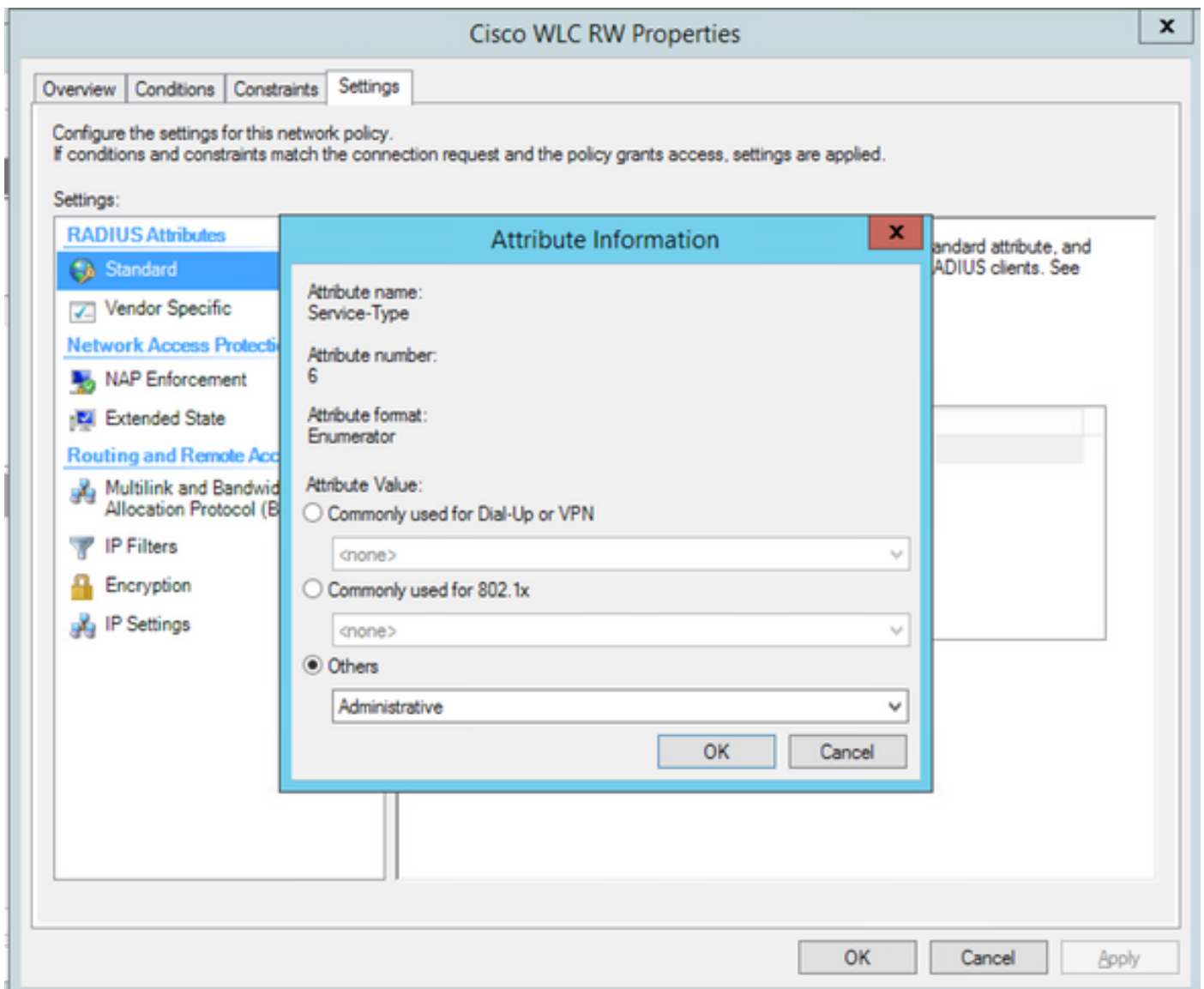




Étape 7. Sous l'onglet **Contraintes**, accédez à **Méthodes d'authentification** et assurez-vous que seule l'**authentification non chiffrée** est cochée.



Étape 8. Sous l'onglet **Paramètres**, accédez à **Attributs RADIUS > Standard**. Cliquez sur **Ajouter** pour ajouter un nouvel attribut, **Service-Type**. Dans le menu déroulant, sélectionnez **Administrative** pour fournir un accès complet aux utilisateurs mappés à cette stratégie. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications, comme le montre l'image.



Note: Si vous souhaitez accorder un accès en lecture seule à des utilisateurs spécifiques, sélectionnez Invite NAS dans la liste déroulante. Dans cet exemple, une autre stratégie nommée **Cisco WLC RO** est créée pour fournir un accès en lecture seule aux utilisateurs sous le nom d'objet **Utilisateurs du domaine**.


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...

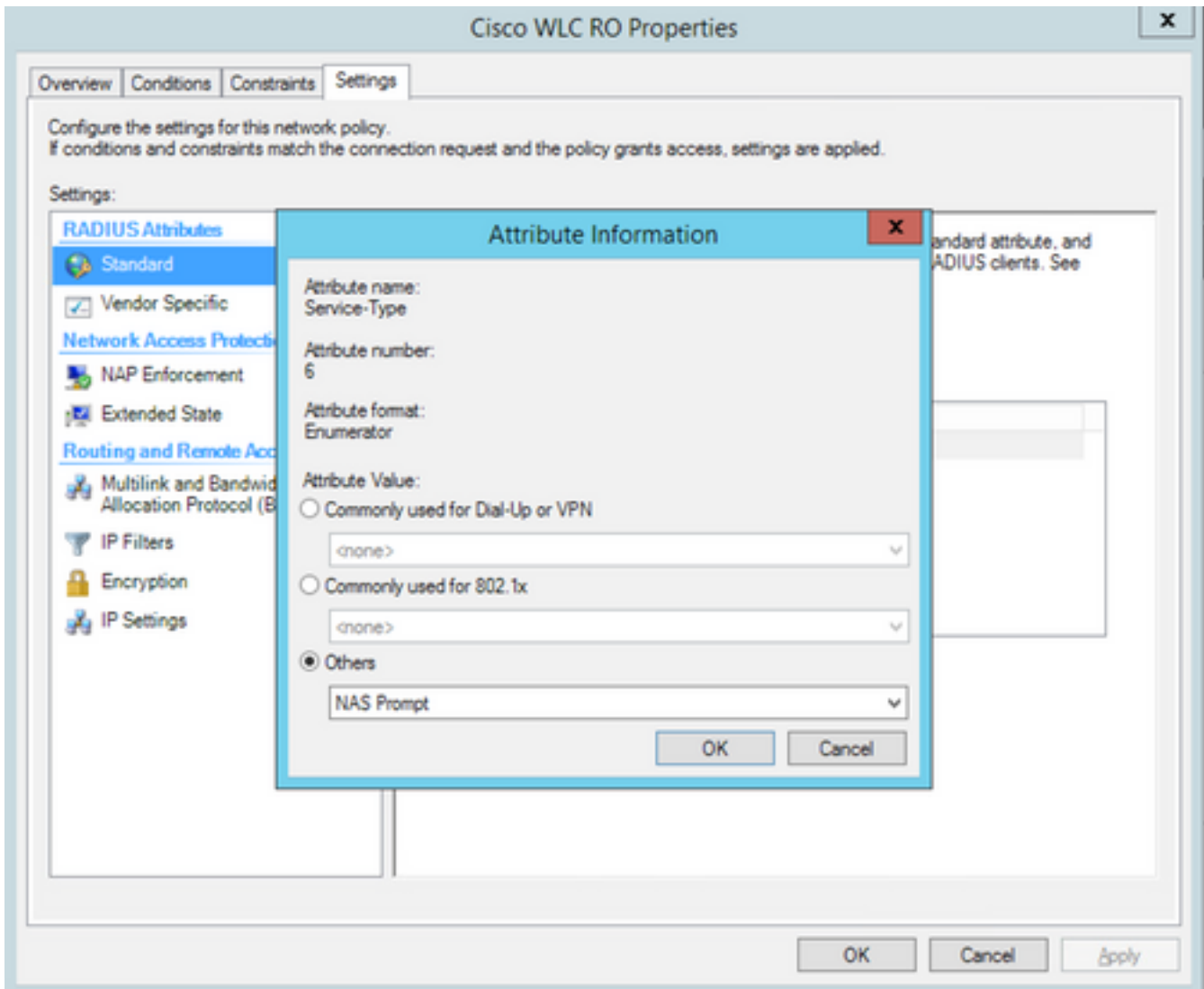
Edit...

Remove

OK

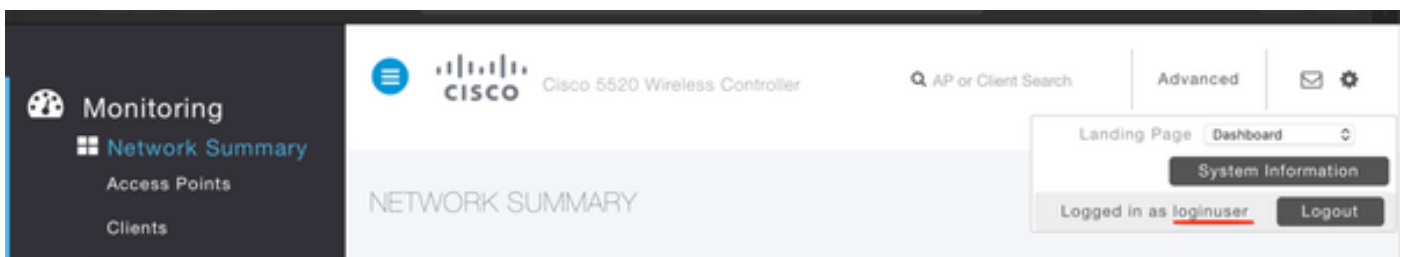
Cancel

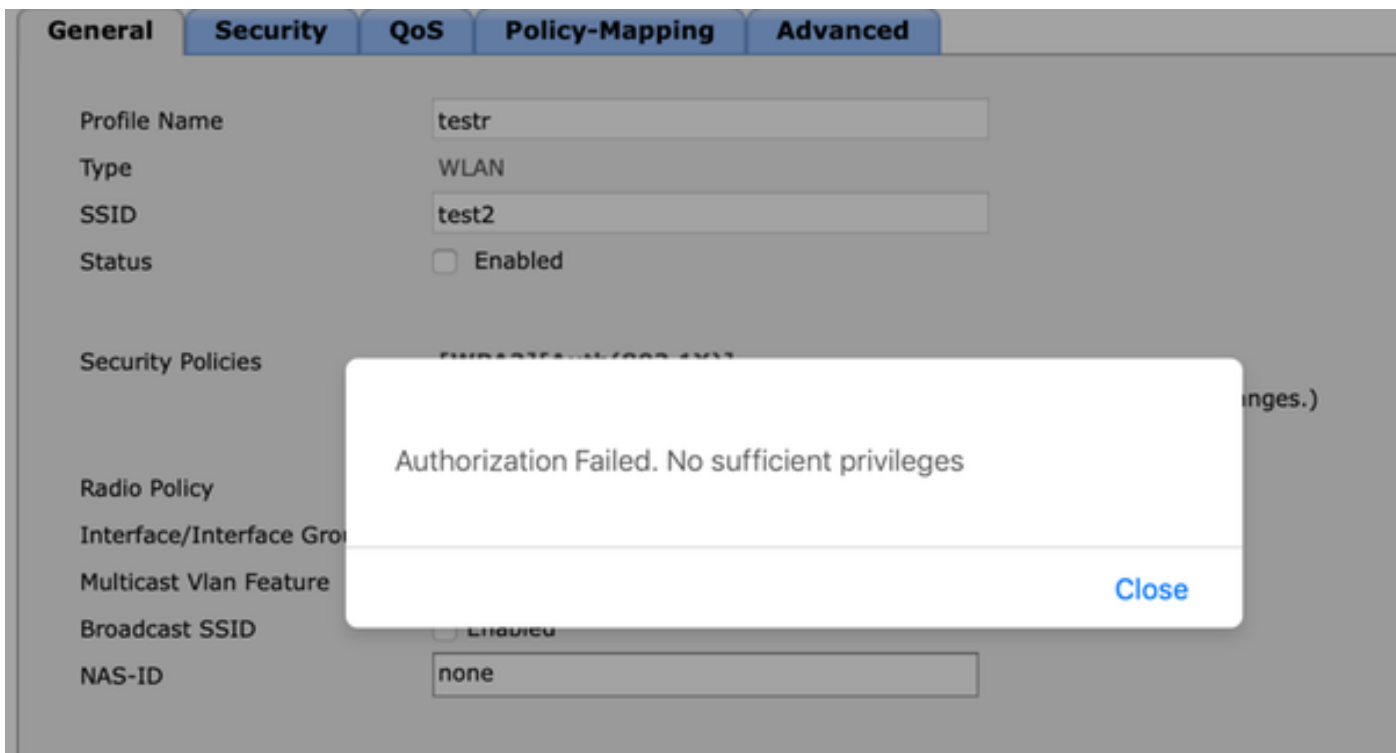
Apply



Vérification

1. Lorsque les informations d'identification **de l'utilisateur de connexion** sont utilisées, l'utilisateur n'est pas autorisé à configurer des modifications sur le contrôleur.





À partir de **debug aaa all enable**, vous pouvez voir que la valeur de l'attribut service-type dans la réponse d'autorisation est 7, ce qui correspond à l'invite 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. Lorsque les informations d'identification **adminuser** sont utilisées, l'utilisateur doit disposer d'un accès complet avec la valeur **6 de type de service**, qui correspond à **administratif**.

```
*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)
```

Dépannage

Afin de dépanner l'accès de gestion au WLC via NPS, exécutez la commande **debug aaa all enable**.

1. Les journaux lorsque des informations d'identification incorrectes sont utilisées sont affichés ici.

```
*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. Les journaux lorsque service-type est utilisé avec une valeur autre que Administrative (value=6) ou NAS-prompt (value=7) sont affichés comme suit. Dans ce cas, la connexion échoue même si l'authentification réussit.

```
*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-Identifiser.....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
```