

Accesso alla gestione per AireOS WLC tramite Server dei criteri di rete Microsoft

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazioni](#)

[Configurazione WLC](#)

[Configurazione Server dei criteri di rete Microsoft](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare l'accesso alla gestione per la GUI e la CLI del WLC di AireOS tramite il Server dei criteri di rete Microsoft.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza delle soluzioni per la sicurezza wireless
- Concetti su AAA e RADIUS
- Conoscenze base di Microsoft Server 2012
- Installazione di Server dei criteri di rete Microsoft e Active Directory (AD)

Componenti usati

Le informazioni fornite in questo documento si basano sui seguenti componenti software e hardware.

- Controller AireOS (5520) su 8.8.120.0
- Microsoft Server 2012

Nota: Questo documento ha lo scopo di fornire ai lettori un esempio della configurazione richiesta su un server Microsoft per l'accesso alla gestione WLC. La configurazione del server Microsoft Windows illustrata in questo documento è stata testata in laboratorio e ha funzionato come previsto. In caso di problemi con la configurazione, contattare Microsoft per assistenza. Il Cisco Technical Assistance Center (TAC) non supporta la configurazione del

server Microsoft Windows. Le guide all'installazione e alla configurazione di Microsoft Windows 2012 sono disponibili in Microsoft Tech Net.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Quando si accede alla CLI/GUI del WLC, all'utente viene richiesto di immettere le credenziali per eseguire correttamente l'accesso. È possibile verificare le credenziali rispetto a un database locale o a un server AAA esterno. In questo documento Microsoft Server dei criteri di rete viene utilizzato come server di autenticazione esterno.

Configurazioni

In questo esempio, due utenti sono configurati su AAA (NPS), ovvero **loginuser** e **adminuser**. **loginuser** dispone solo dell'accesso in sola lettura mentre **adminuser** dispone dell'accesso completo.

Configurazione WLC

Passaggio 1. Aggiungere il server RADIUS sul controller. Selezionare **Protezione > RADIUS > Autenticazione**. Fare clic su **Nuovo** per aggiungere il server. Verificare che l'opzione **management** sia abilitata in modo che il server possa essere utilizzato per l'accesso management, come mostrato nell'immagine.

The screenshot shows the Cisco ISE configuration interface for a RADIUS Authentication Server. The left sidebar contains a navigation menu with categories like AAA, Local EAP, Advanced EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, TrustSec, Local Policies, Umbrella, and Advanced. The main content area is titled 'RADIUS Authentication Servers > Edit' and displays various configuration parameters:

- Server Index: 2
- Server Address(Ipv4/Ipv6): 10.106.33.39
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- 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

Passo 2: passare a **Sicurezza > Ordine di priorità > Utente di gestione**. Verificare che RADIUS sia selezionato come uno dei tipi di autenticazione.

The screenshot shows the 'Priority Order > Management User' configuration page. Under the 'Authentication' section, there are two columns: 'Not Used' and 'Order Used for Authentication'. In the 'Not Used' column, 'TACACS+' is listed. In the 'Order Used for Authentication' column, 'RADIUS LOCAL' is listed and highlighted, indicating it is the current selection. There are 'Up' and 'Down' buttons next to the 'RADIUS LOCAL' entry to adjust its priority.

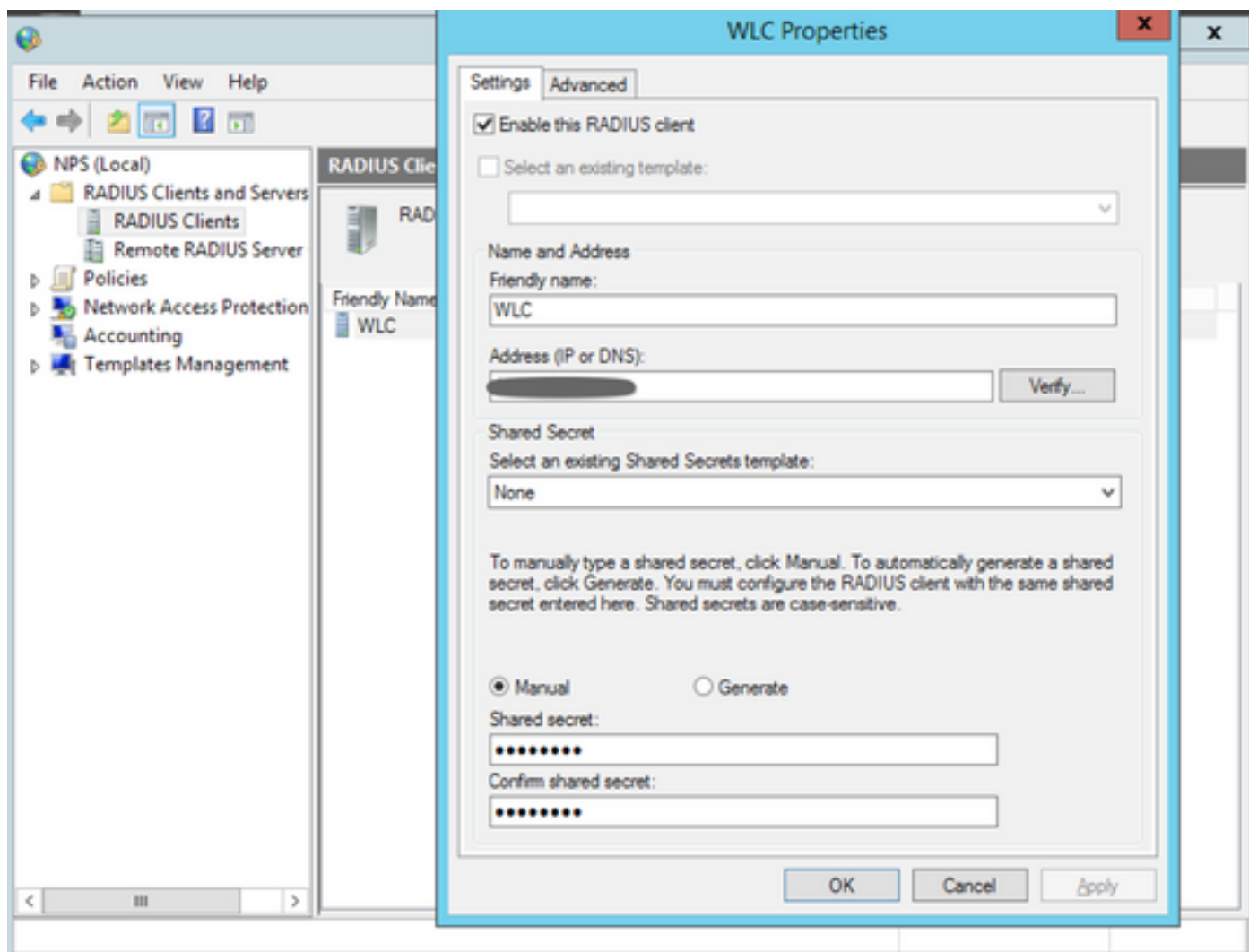
Nota: Se si seleziona RADIUS come prima priorità nell'ordine di autenticazione, le credenziali locali verranno utilizzate per l'autenticazione solo se il server RADIUS non è raggiungibile. Se si seleziona RADIUS come seconda priorità, le credenziali RADIUS verranno innanzitutto verificate rispetto al database locale e quindi verificate rispetto ai server RADIUS configurati.

Configurazione Server dei criteri di rete Microsoft

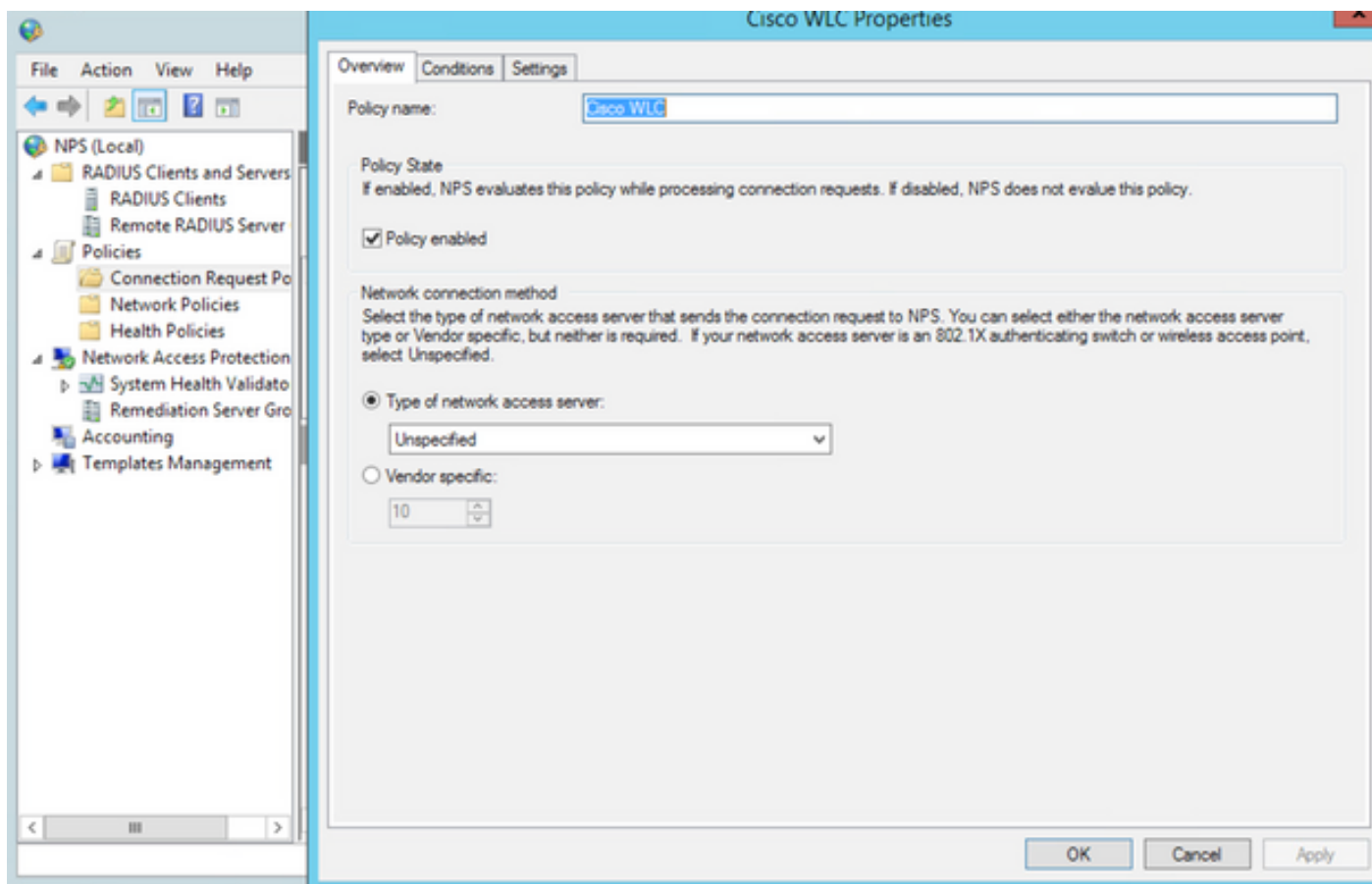
Passaggio 1. Aprire il Server dei criteri di rete Microsoft. Fare clic con il pulsante destro del mouse

su **Client Radius**. Fare clic su **New** (Nuovo) per aggiungere il WLC come client RADIUS.

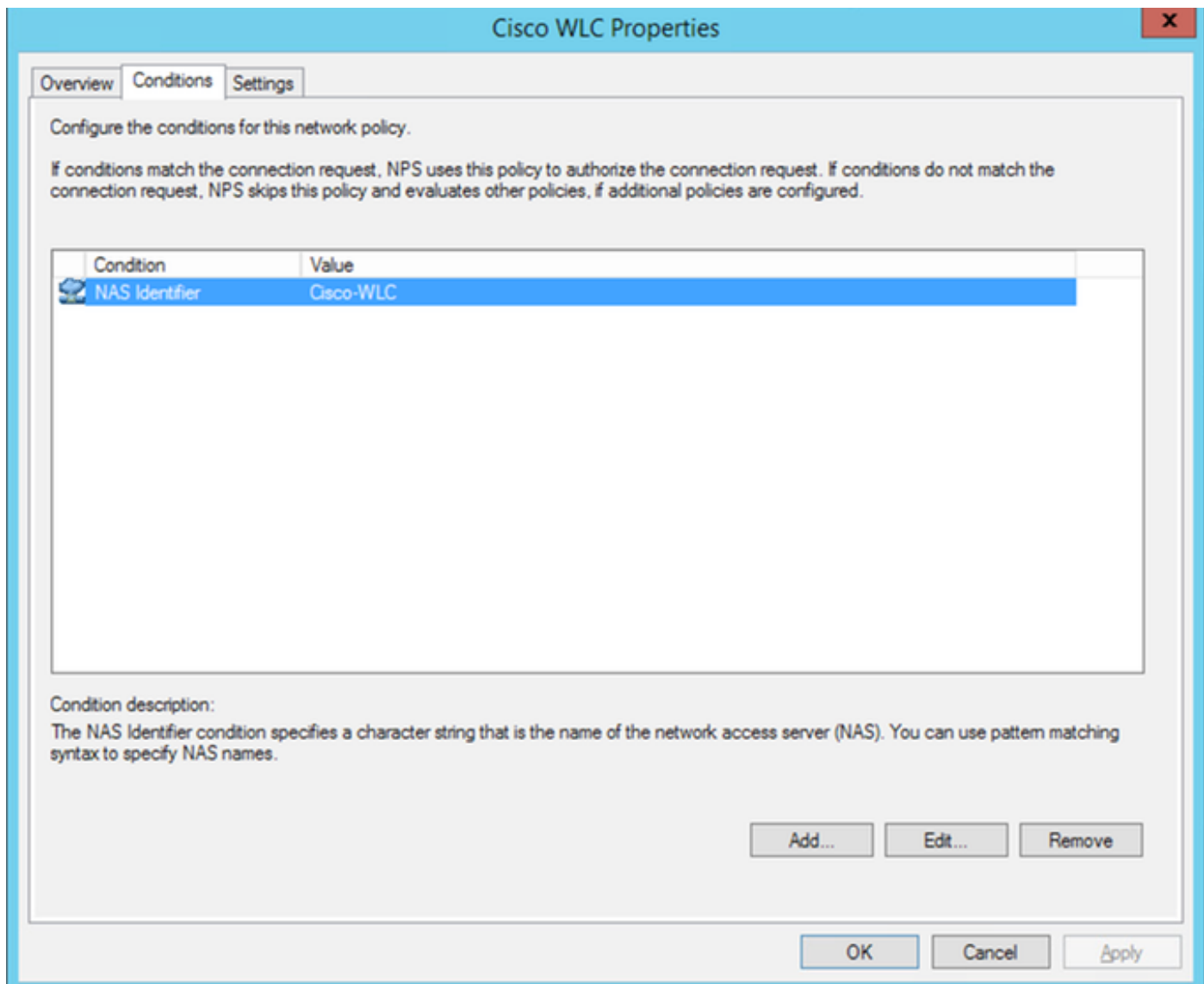
Immettere i dettagli richiesti. Verificare che il segreto condiviso sia uguale a quello configurato nel controller durante l'aggiunta del server RADIUS.



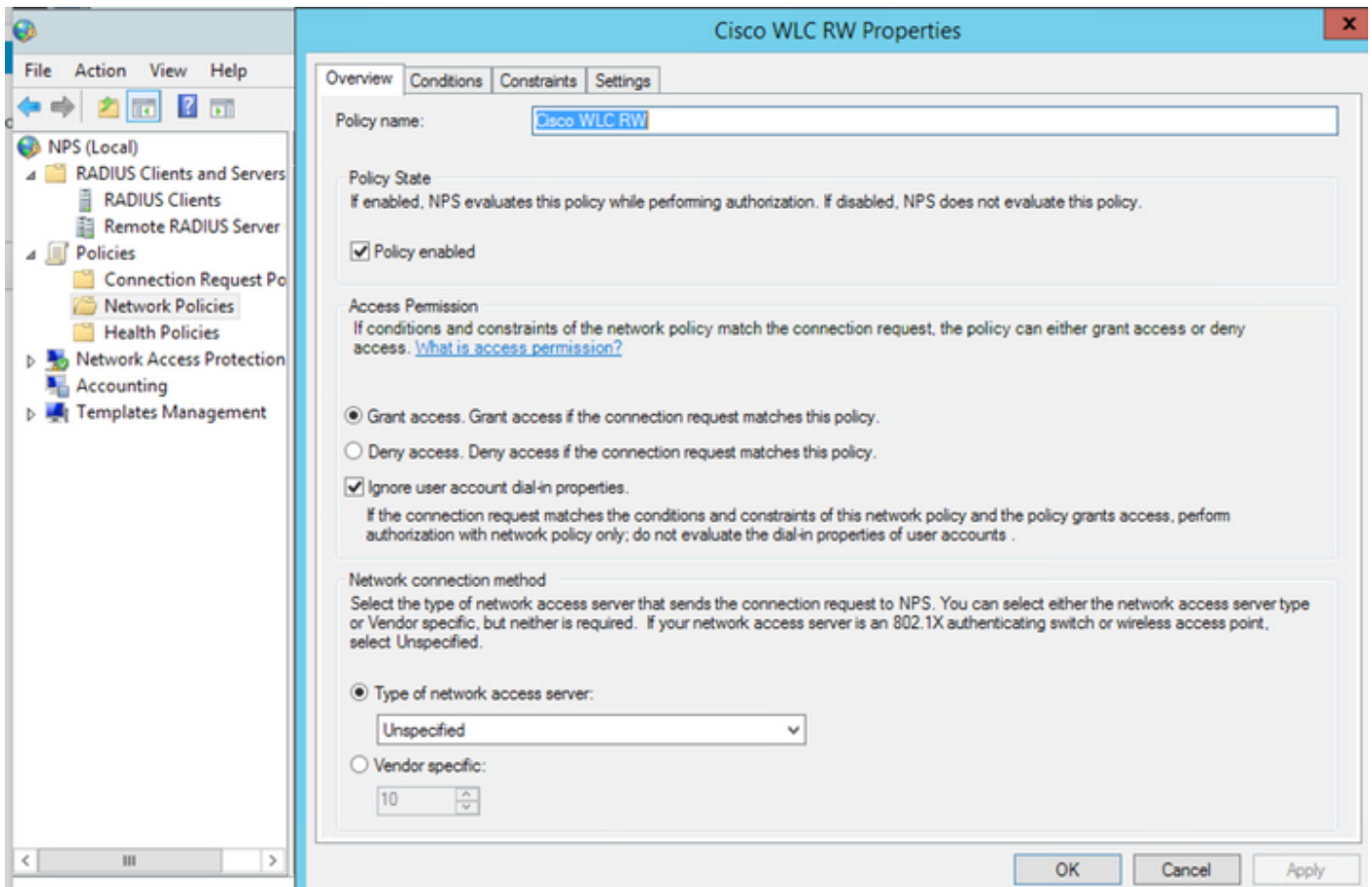
Passaggio 2. Passare a **Criteri > Criteri di richiesta di connessione**. Fare clic con il pulsante destro del mouse per aggiungere un nuovo criterio, come illustrato nell'immagine.



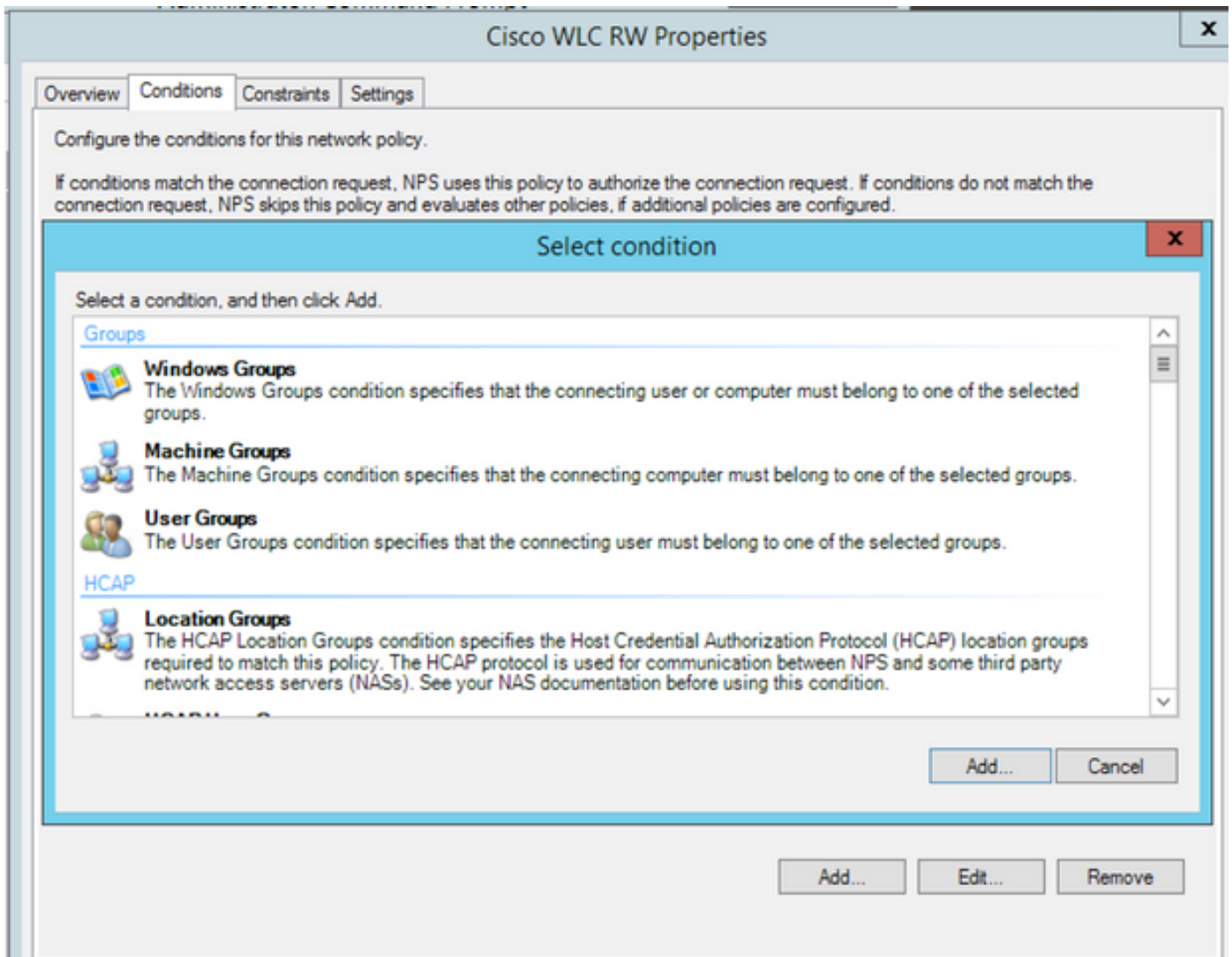
Passaggio 3. Nella scheda **Condizioni**, selezionare **Identificatore NAS** come nuova condizione. Quando richiesto, immettere il nome host del controller come valore, come mostrato nell'immagine.



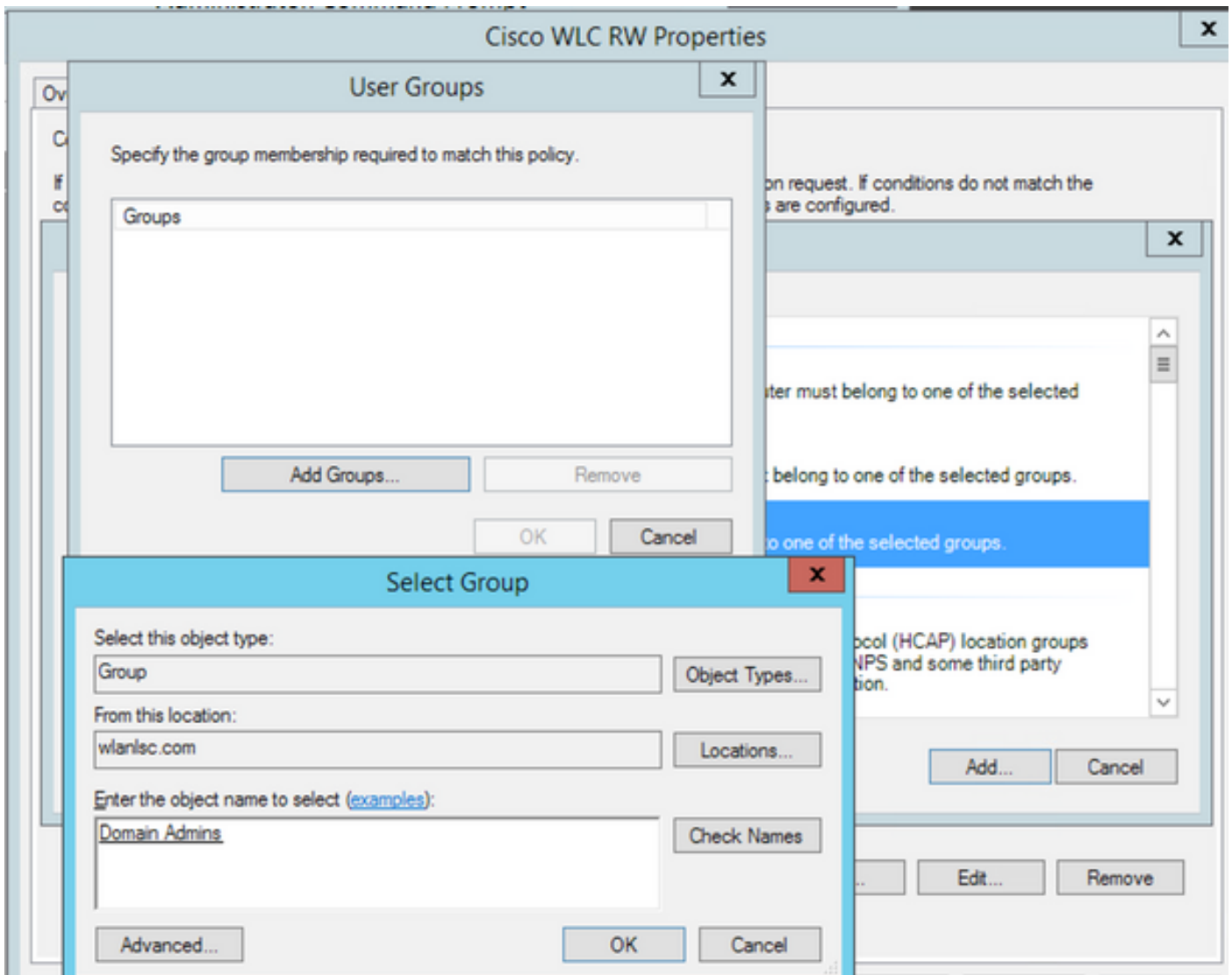
Passaggio 4. Passare a **Criteri > Criteri di rete**. Fare clic con il pulsante destro del mouse per aggiungere un nuovo criterio. In questo esempio, il criterio è denominato **Cisco WLC RW**, il che implica che il criterio venga utilizzato per fornire l'accesso completo (in lettura/scrittura). Verificare che il criterio sia configurato come illustrato di seguito.



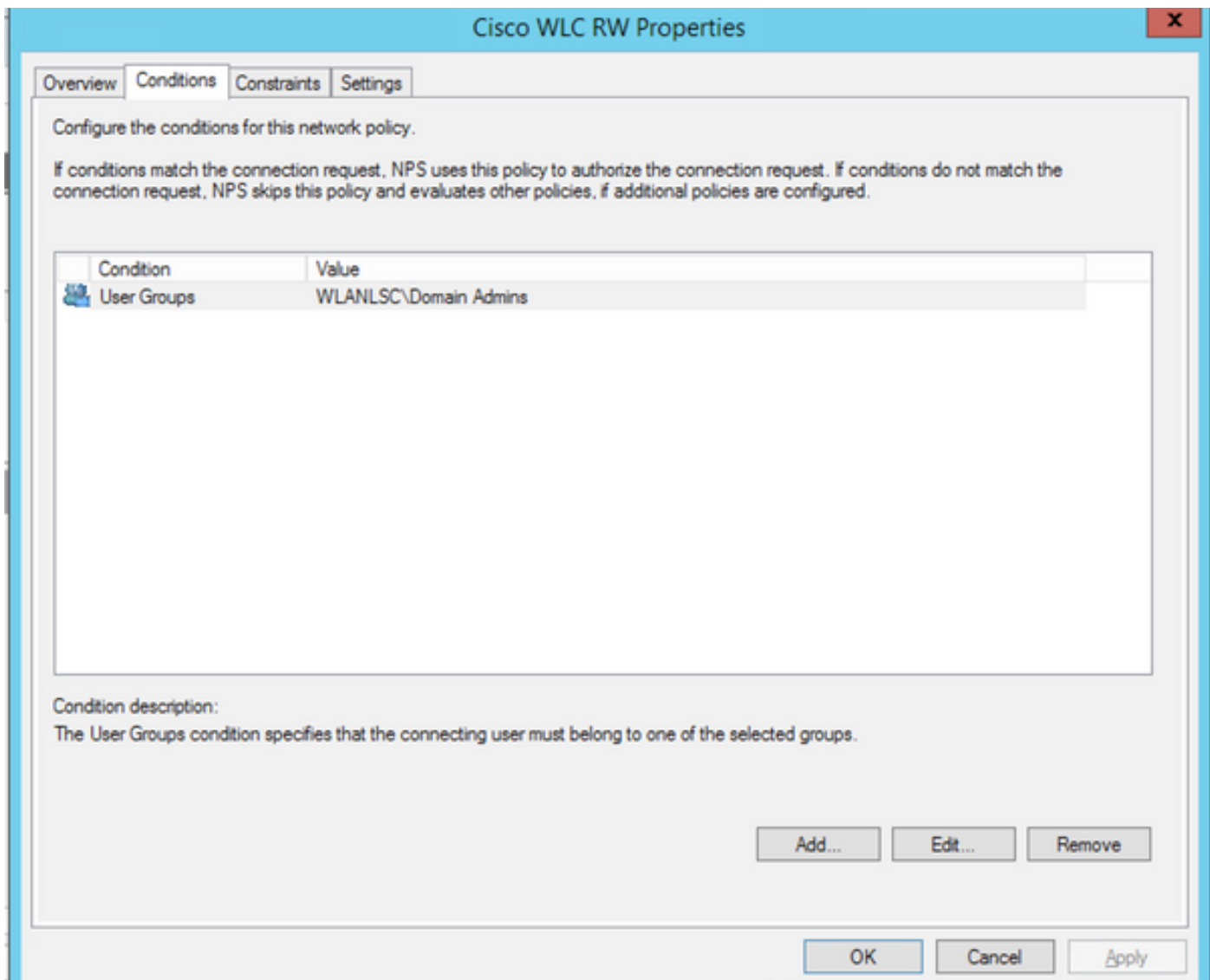
Passaggio 5. Nella scheda **Condizioni**, fare clic su **Aggiungi**. Selezionare i **gruppi di utenti** e fare clic su **Aggiungi**, come mostrato nell'immagine.



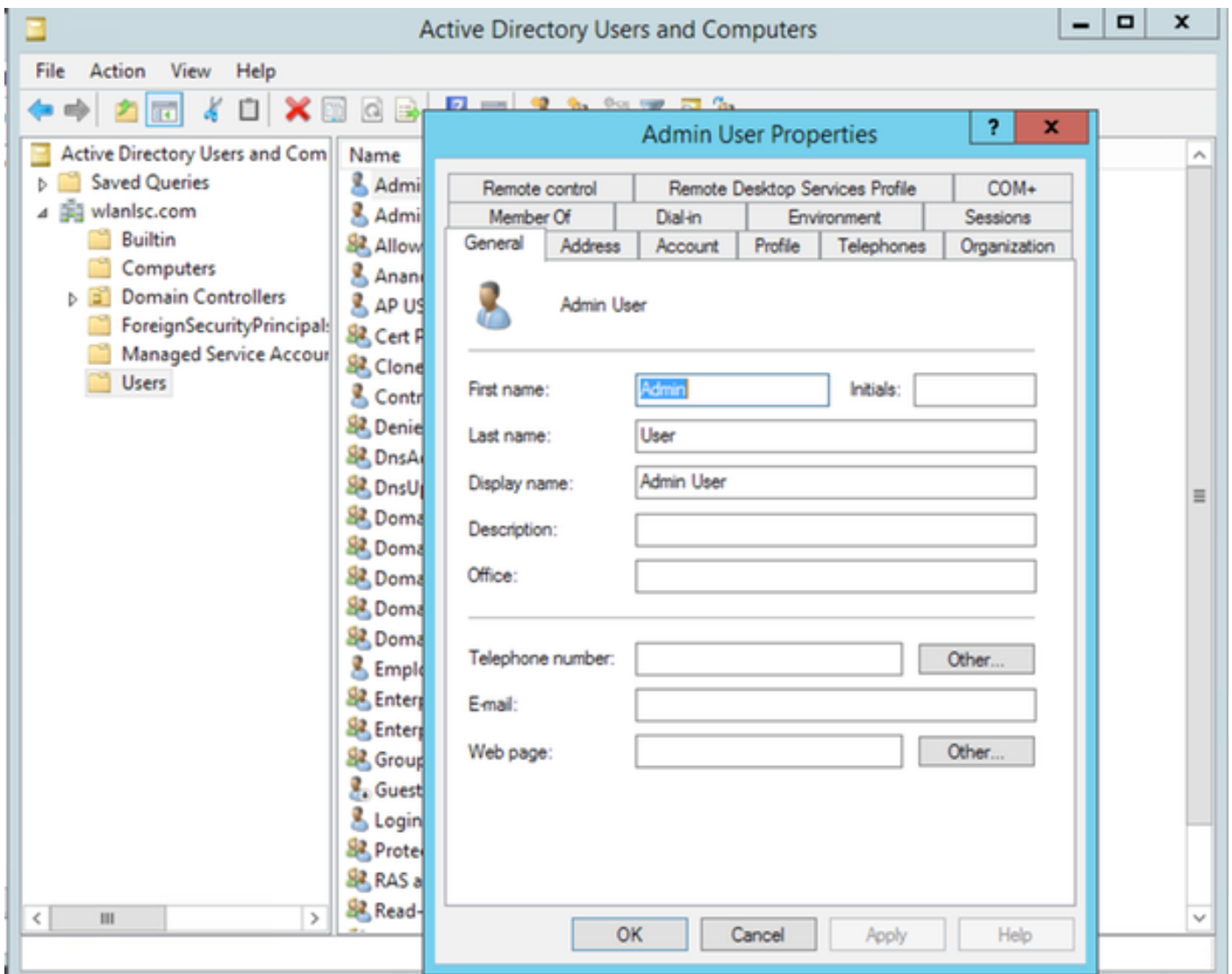
Passaggio 6. Fare clic su **Add Groups** nella finestra di dialogo visualizzata. Nella finestra **Selezione gruppo** visualizzata, selezionare il **tipo** e la **posizione** desiderati e immettere il nome dell'oggetto, come mostrato nell'immagine.

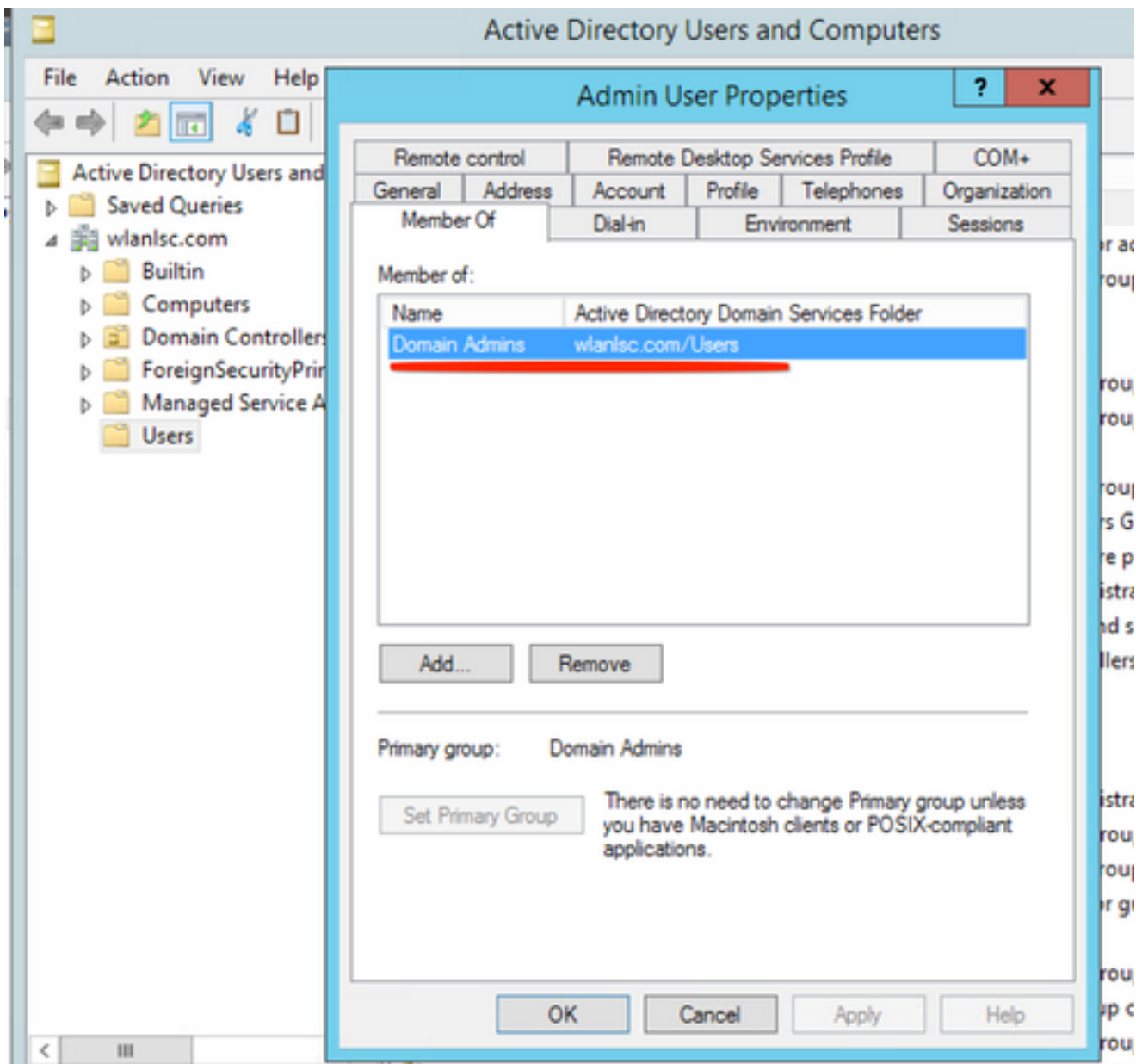


La condizione, se aggiunta correttamente, dovrebbe essere simile a quella illustrata di seguito.

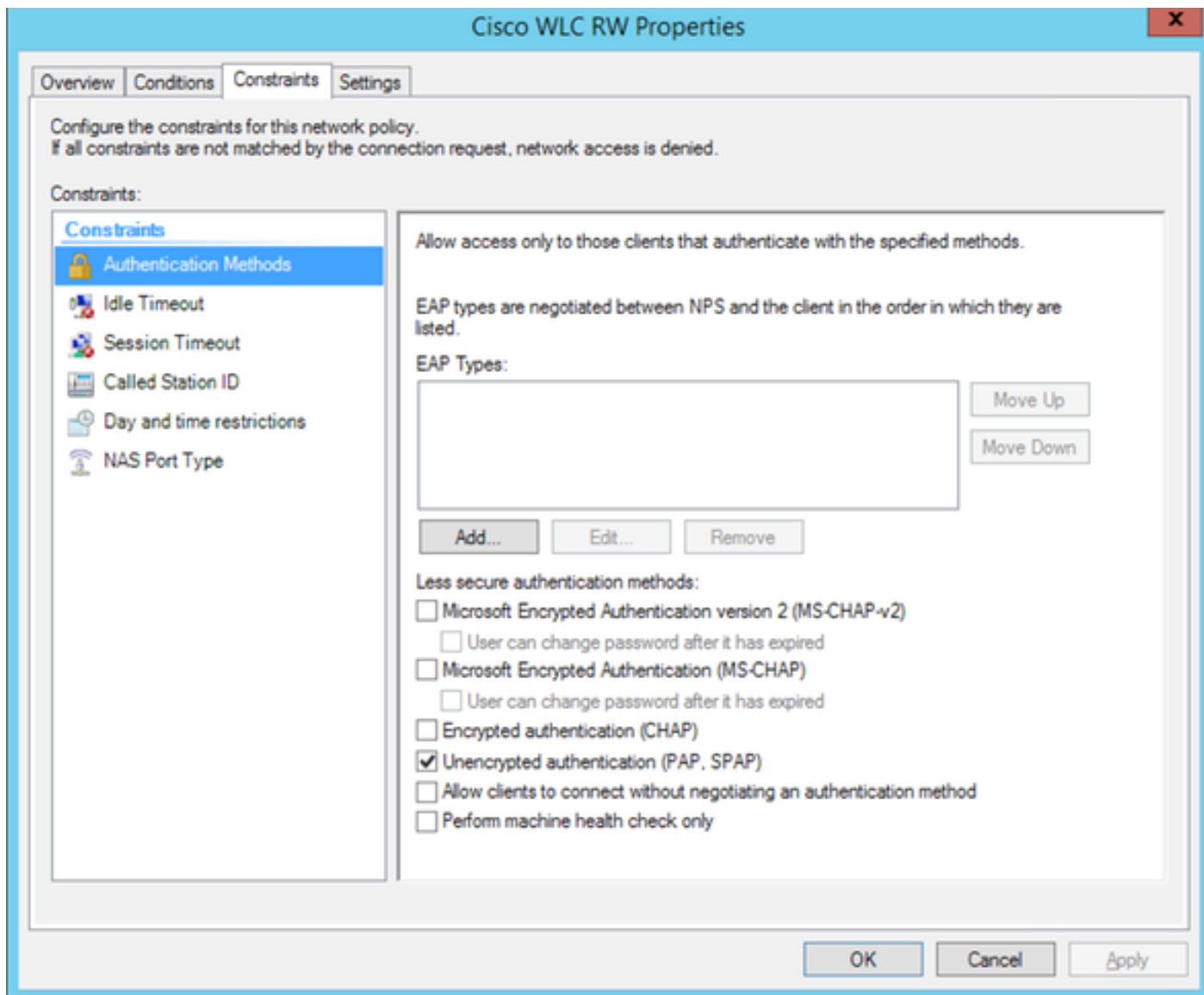


Nota: Per conoscere i dettagli relativi al percorso e al nome dell'oggetto, aprire Active Directory e cercare il nome utente desiderato. Nell'esempio, **Domain Admins** è costituito da utenti a cui è concesso l'accesso completo. **adminuser** fa parte del nome dell'oggetto.

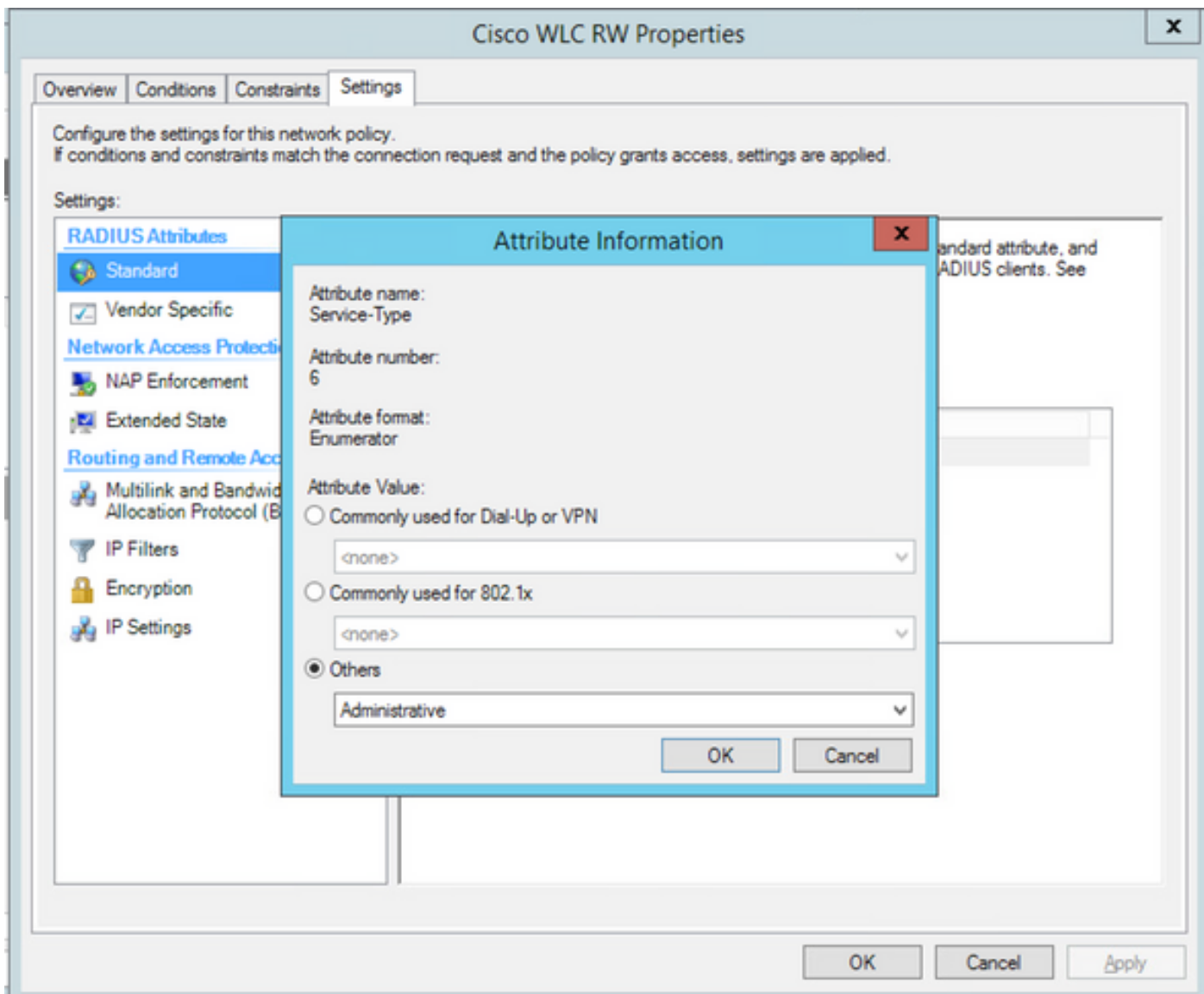




Passaggio 7. Nella scheda **Vincoli**, passare a **Metodi di autenticazione** e accertarsi che sia selezionata solo l'**autenticazione non crittografata**.



Passaggio 8. Nella scheda **Impostazioni**, selezionare **Attributi RADIUS > Standard**. Fare clic su **Add** per aggiungere un nuovo attributo, **Service-Type**. Dal menu a discesa, selezionare **Amministrativo** per fornire l'accesso completo agli utenti mappati a questo criterio. Fare clic su **Applica** per salvare le modifiche, come mostrato nell'immagine.




Nota: Se si desidera concedere l'accesso in sola lettura a utenti specifici, selezionare NAS-Prompt dall'elenco a discesa. In questo esempio, viene creato un altro criterio denominato **Cisco WLC RO** per fornire l'accesso in sola lettura agli utenti sotto il nome oggetto **Domain Users**.

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...

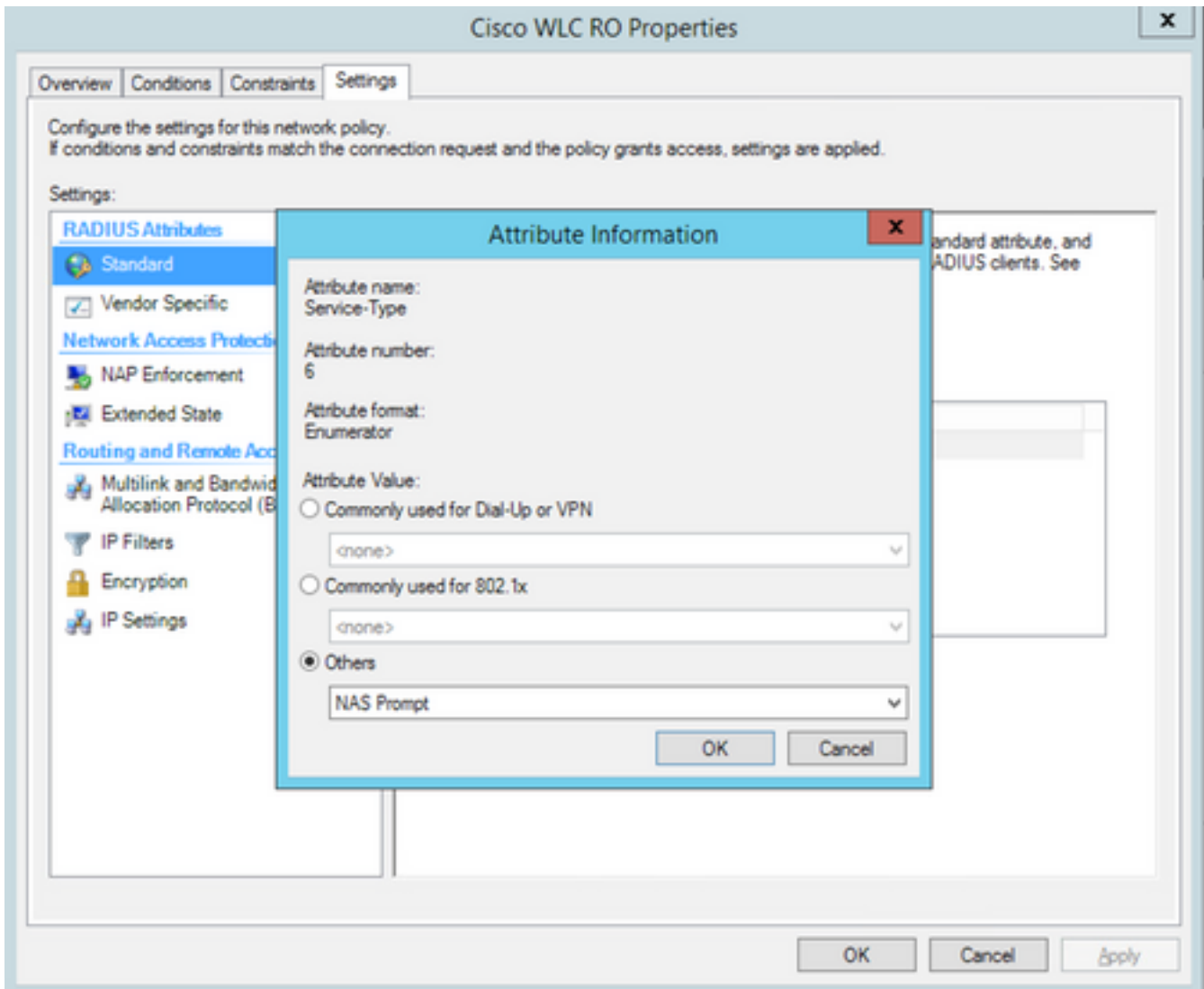
Edit...

Remove

OK

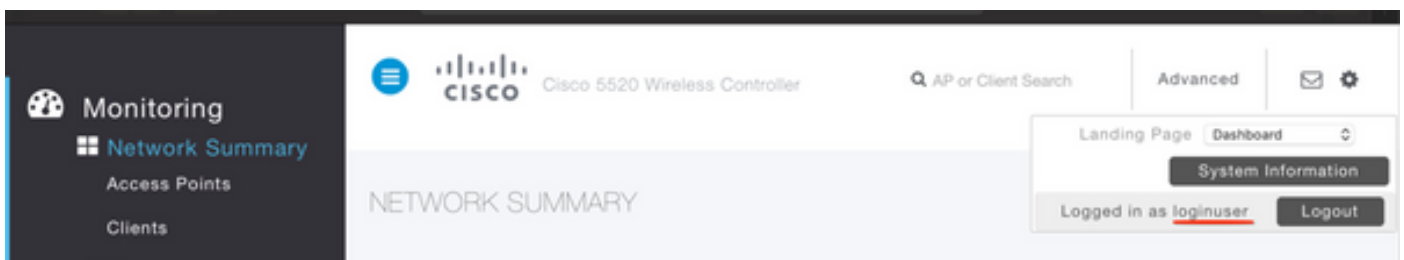
Cancel

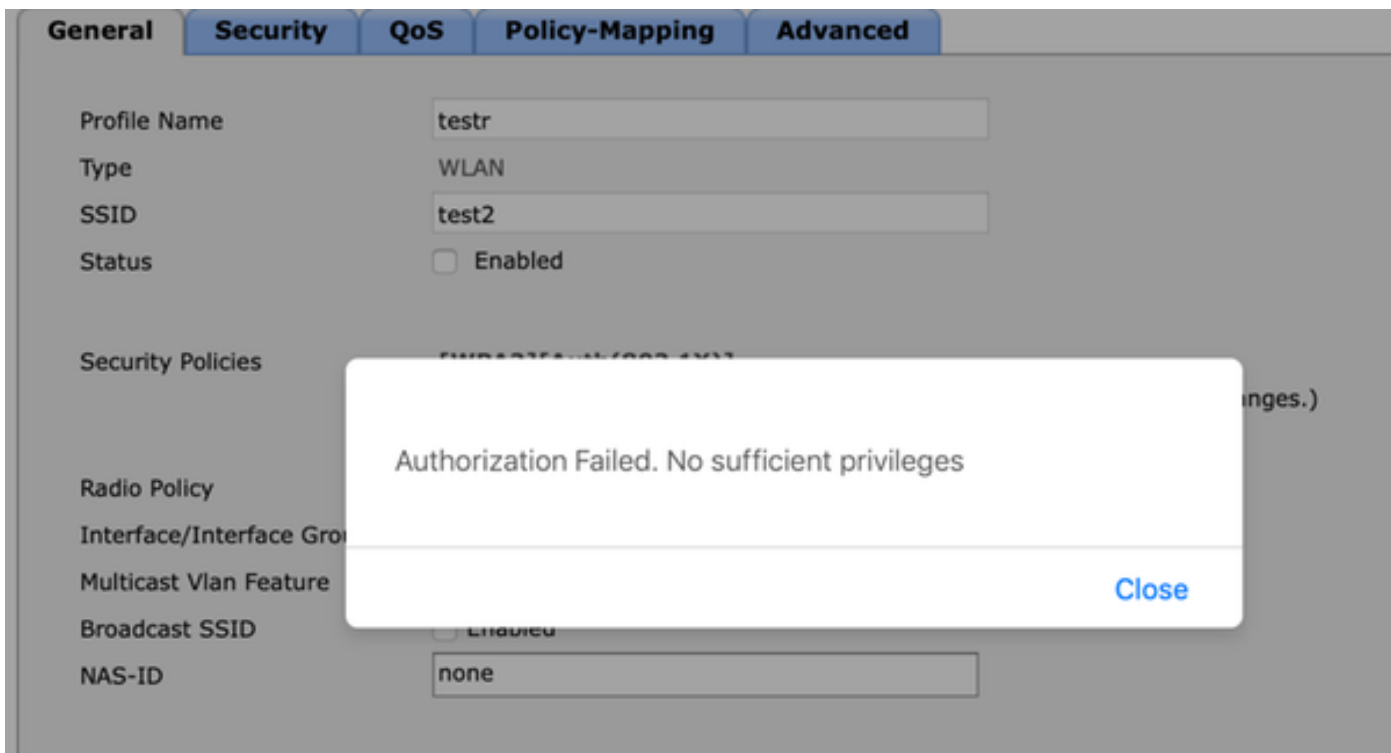
Apply



Verifica

1. Quando vengono utilizzate le credenziali **loginuser**, all'utente non è consentito configurare alcuna modifica sul controller.





Da **debug aaa all enable** è possibile verificare che il valore dell'attributo **service-type** nella risposta all'autorizzazione è **7**, che corrisponde al prompt **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 vengono utilizzate le credenziali **adminuser**, l'utente deve disporre dell'accesso completo con il valore del **tipo di servizio 6**, che corrisponde a **amministrativo**.

```
*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)
```

Risoluzione dei problemi

Per risolvere i problemi di accesso alla gestione di WLC tramite Server dei criteri di rete, eseguire il comando **debug aaa all enable**.

1. Di seguito sono riportati i log in caso di utilizzo di credenziali errate.

```
*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. I registri quando service-type viene utilizzato con un valore diverso da Administrative (valore=6) o NAS-prompt (valore=7) vengono visualizzati come segue. In questo caso, l'accesso non riesce anche se l'autenticazione ha esito positivo.

```
*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-Identifiler.....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
```