Verwaltungszugriff für AireOS WLC über Microsoft NPS

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie der Verwaltungszugriff für die grafische Benutzeroberfläche und die Kommandozeile von AireOS WLC über den Microsoft Network Policy Server (NPS) konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnisse der Wireless-Sicherheitslösungen
- AAA- und RADIUS-Konzepte
- Grundkenntnisse von Microsoft Server 2012
- Installation von Microsoft NPS und Active Directory (AD)

Verwendete Komponenten

Die in diesem Dokument enthaltenen Informationen basieren auf den folgenden Software- und Hardwarekomponenten.

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

Hinweis: Dieses Dokument soll den Lesern ein Beispiel für die Konfiguration geben, die auf einem Microsoft-Server für den WLC-Verwaltungszugriff erforderlich ist. Die in diesem Dokument vorgestellte Microsoft Windows-Serverkonfiguration wurde in der Übung getestet und als normal befunden. Wenn Sie Probleme mit der Konfiguration haben, wenden Sie sich

an Microsoft, um Hilfe zu erhalten. Das Cisco Technical Assistance Center (TAC) unterstützt die Microsoft Windows-Serverkonfiguration nicht. Microsoft Windows 2012-Installations- und Konfigurationshandbücher finden Sie auf Microsoft Tech Net.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

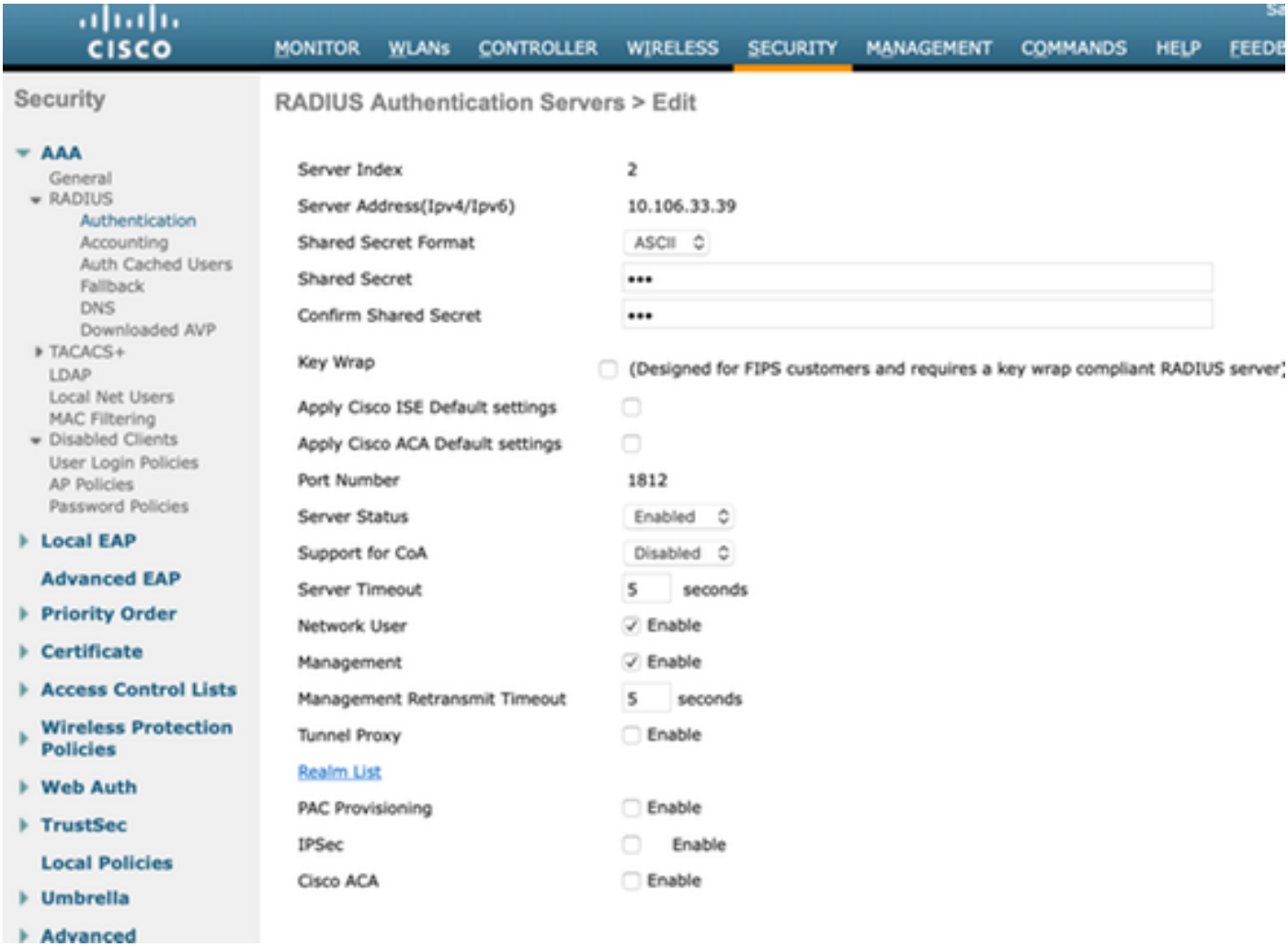
Beim Zugriff auf die WLC-CLI/GUI wird der Benutzer aufgefordert, die Anmeldeinformationen einzugeben, um sich erfolgreich anzumelden. Die Anmeldeinformationen können entweder anhand einer lokalen Datenbank oder eines externen AAA-Servers überprüft werden. In diesem Dokument wird Microsoft NPS als externer Authentifizierungsserver verwendet.

Konfigurationen

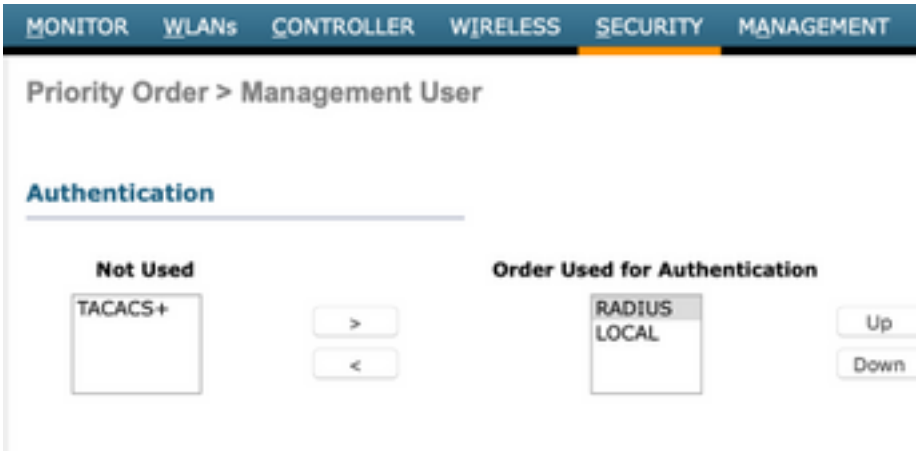
In diesem Beispiel werden zwei Benutzer für die AAA (NPS)-**VIZ** konfiguriert. **loginuser** und **adminuser**. **loginuser** hat nur Lesezugriff, während dem **Administrator** der volle Zugriff gewährt wird.

WLC-Konfiguration

Schritt 1: Fügen Sie den RADIUS-Server auf dem Controller hinzu. Navigieren Sie zu **Sicherheit > RADIUS > Authentication (Sicherheit > RADIUS > Authentifizierung)**. Klicken Sie auf **Neu**, um den Server hinzuzufügen. Stellen Sie sicher, dass die **Management**-Option aktiviert ist, damit dieser Server für den Verwaltungszugriff verwendet werden kann, wie in diesem Bild gezeigt.



Schritt 2: Navigieren Sie zu **Sicherheit > Priority Order > Management User**. Stellen Sie sicher, dass der RADIUS als einer der Authentifizierungstypen ausgewählt ist.



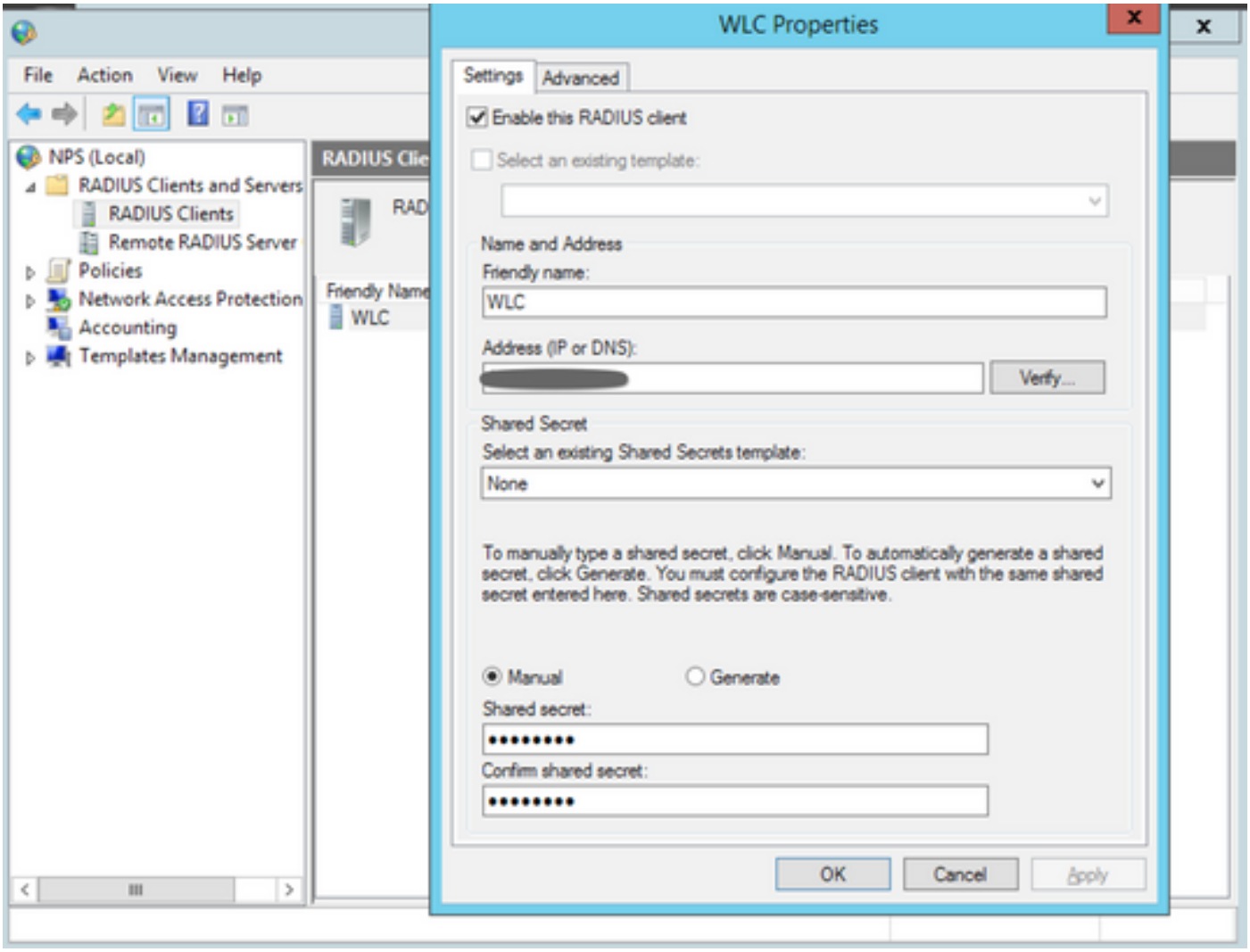
Hinweis: Wenn in der Authentifizierungsreihenfolge RADIUS als erste Priorität ausgewählt wird, werden lokale Anmeldeinformationen nur dann für die Authentifizierung verwendet, wenn der RADIUS-Server nicht erreichbar ist. Wenn RADIUS als zweite Priorität ausgewählt wird, werden die RADIUS-Anmeldeinformationen zuerst für die lokale Datenbank überprüft und anschließend für die konfigurierten RADIUS-Server überprüft.

Microsoft NPS-Konfiguration

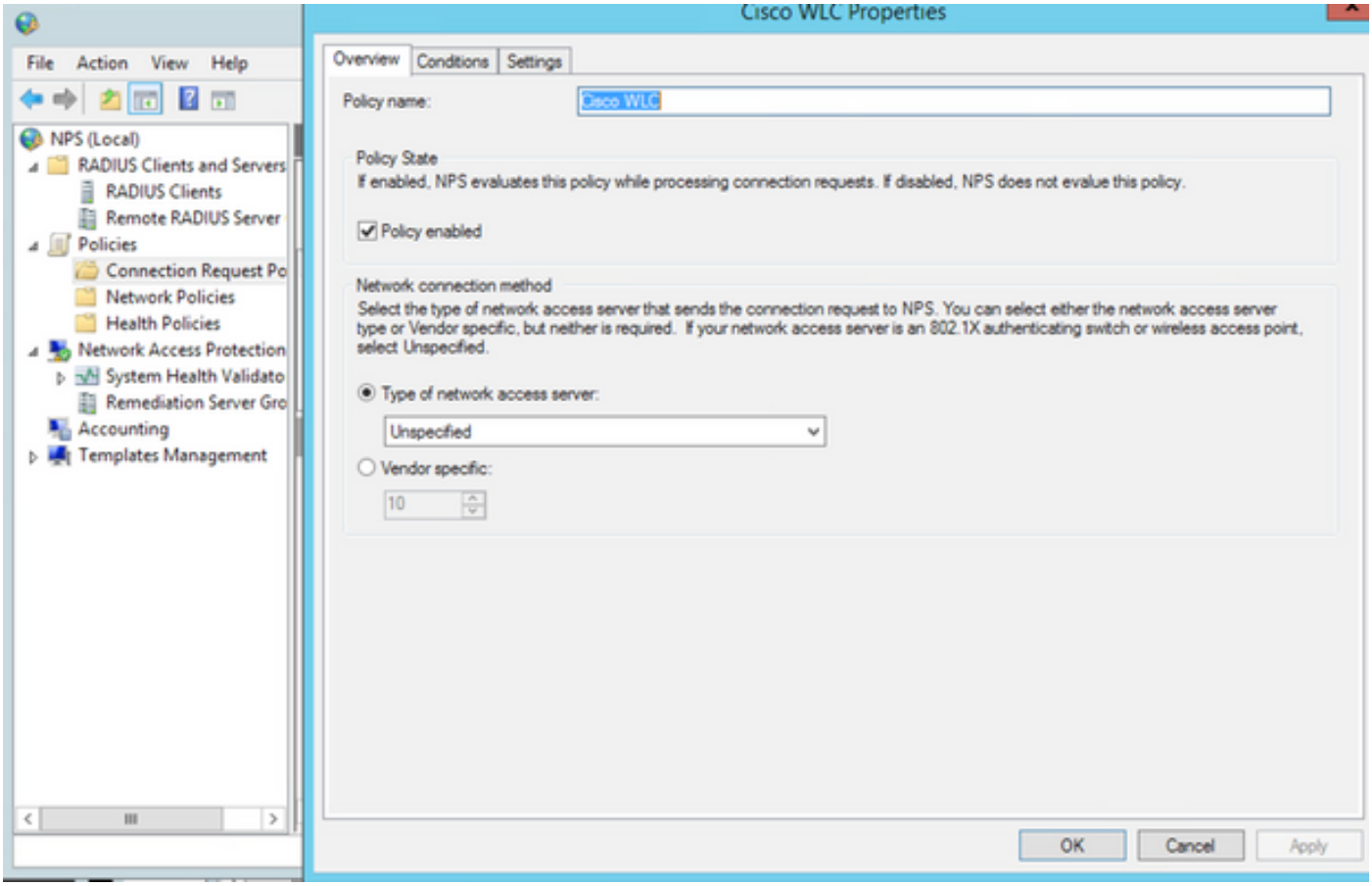
Schritt 1: Öffnen Sie den Microsoft NPS-Server. Klicken Sie mit der rechten Maustaste auf **Radius**

Clients. Klicken Sie auf **Neu**, um den WLC als RADIUS-Client hinzuzufügen.

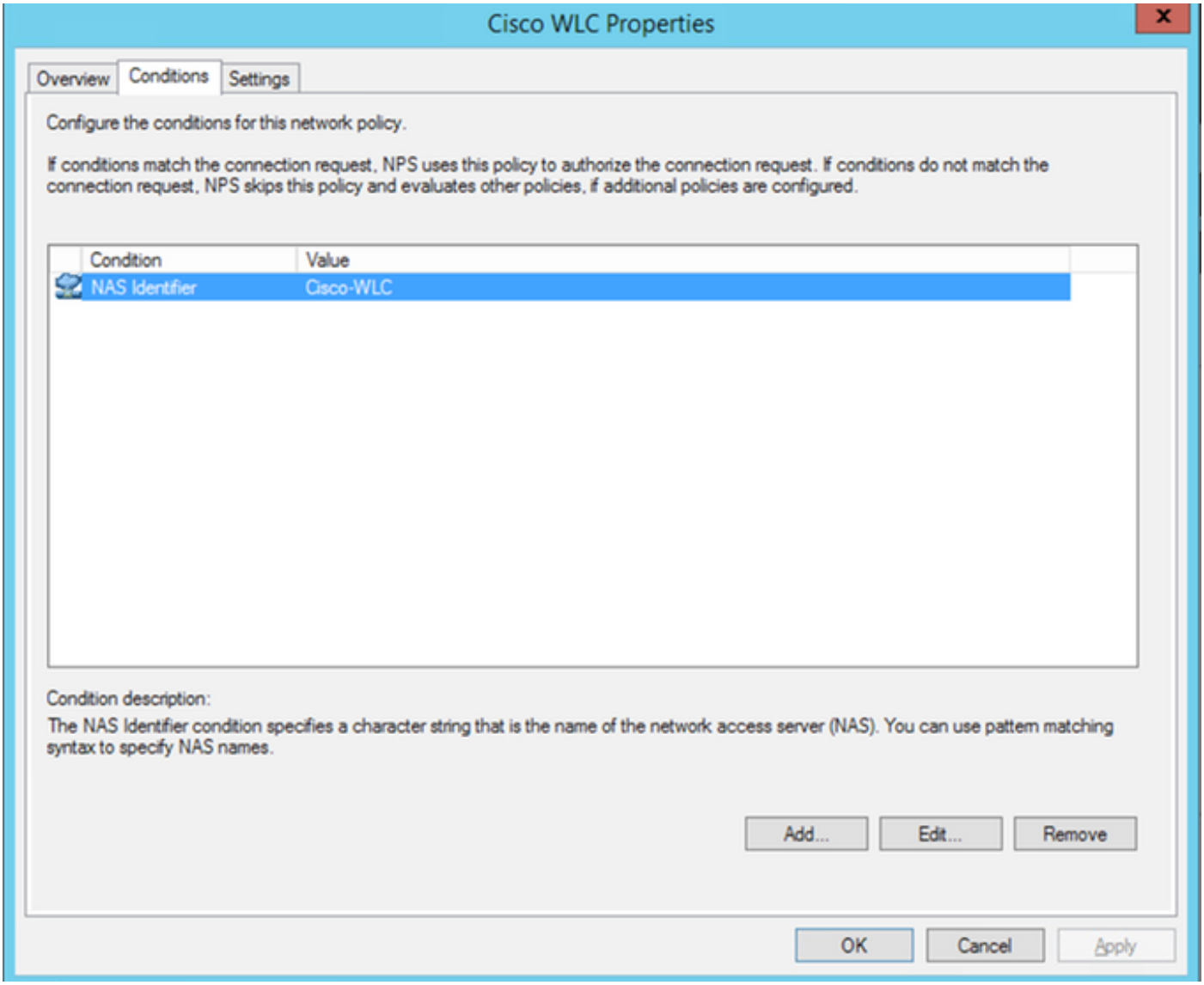
Geben Sie die erforderlichen Details ein. Stellen Sie sicher, dass der gemeinsam genutzte geheime Schlüssel mit dem auf dem Controller konfigurierten geheim ist, während der RADIUS-Server hinzugefügt wird.



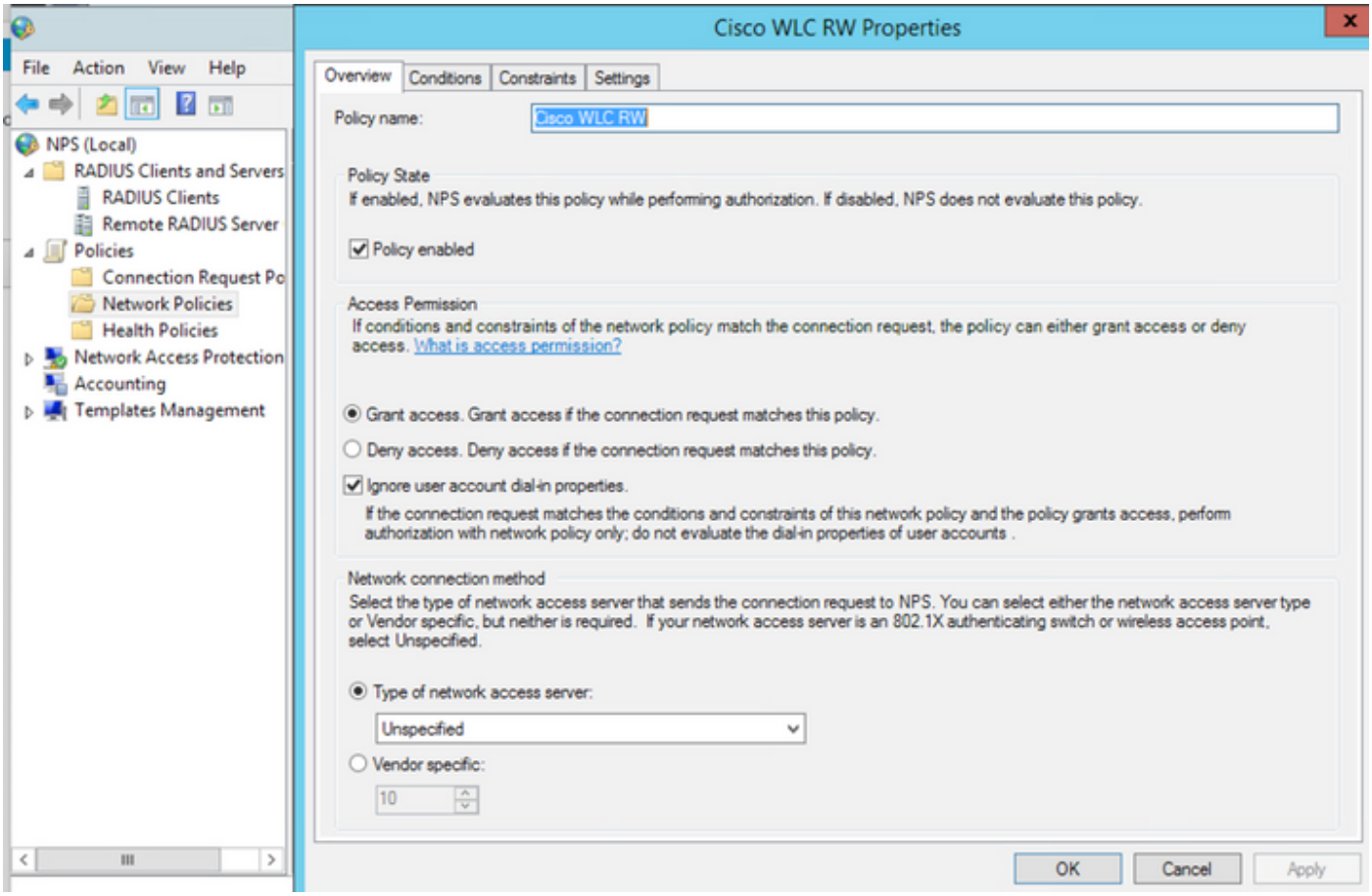
Schritt 2: Navigieren Sie zu **Richtlinien > Verbindungsanforderungsrichtlinien**. Klicken Sie mit der rechten Maustaste, um eine neue Richtlinie hinzuzufügen, wie im Bild gezeigt.



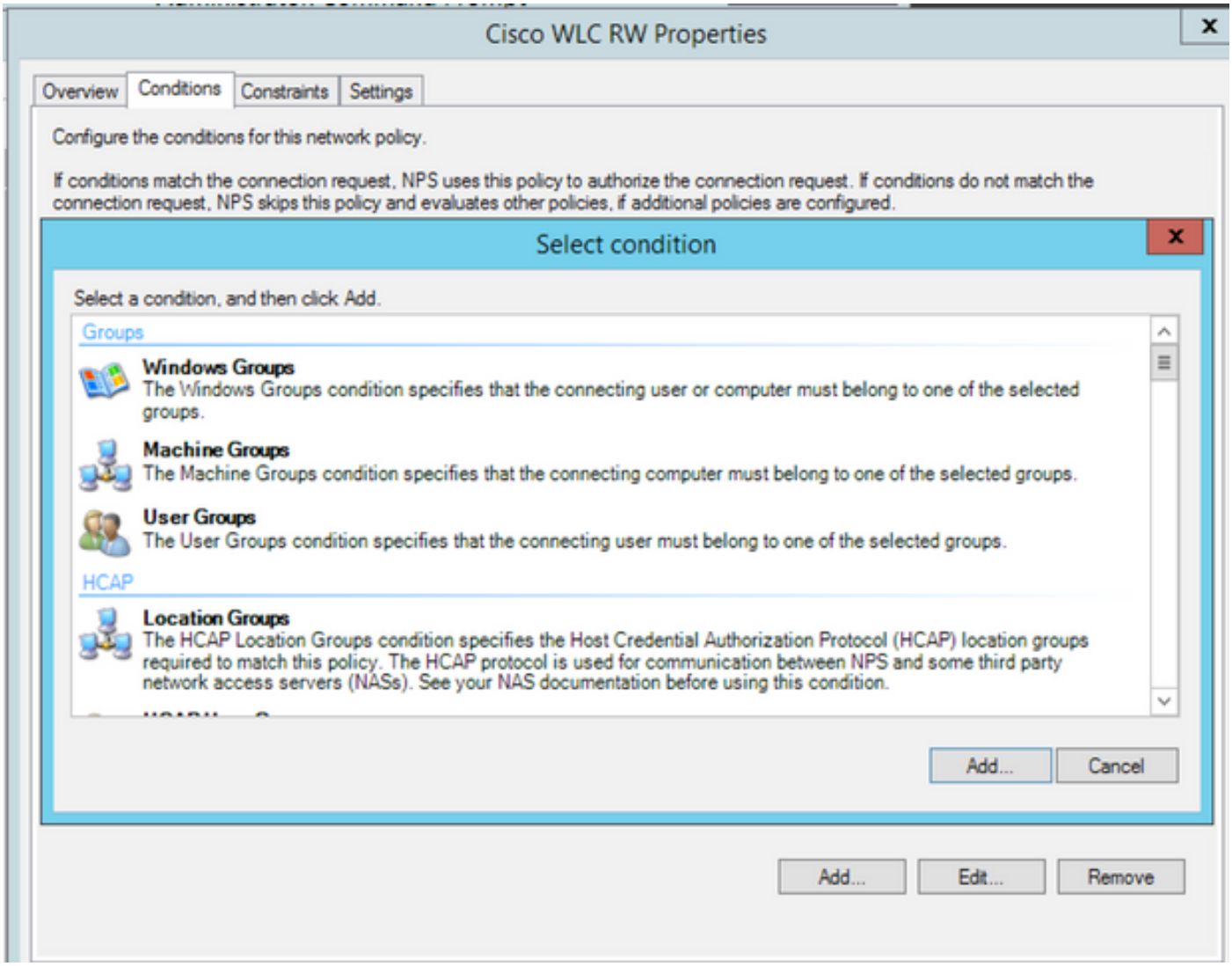
Schritt 3: Wählen Sie auf der Registerkarte **Bedingungen** die Option **NAS-ID** als neue Bedingung aus. Geben Sie bei Aufforderung den Hostnamen des Controllers als Wert ein, wie im Bild gezeigt.



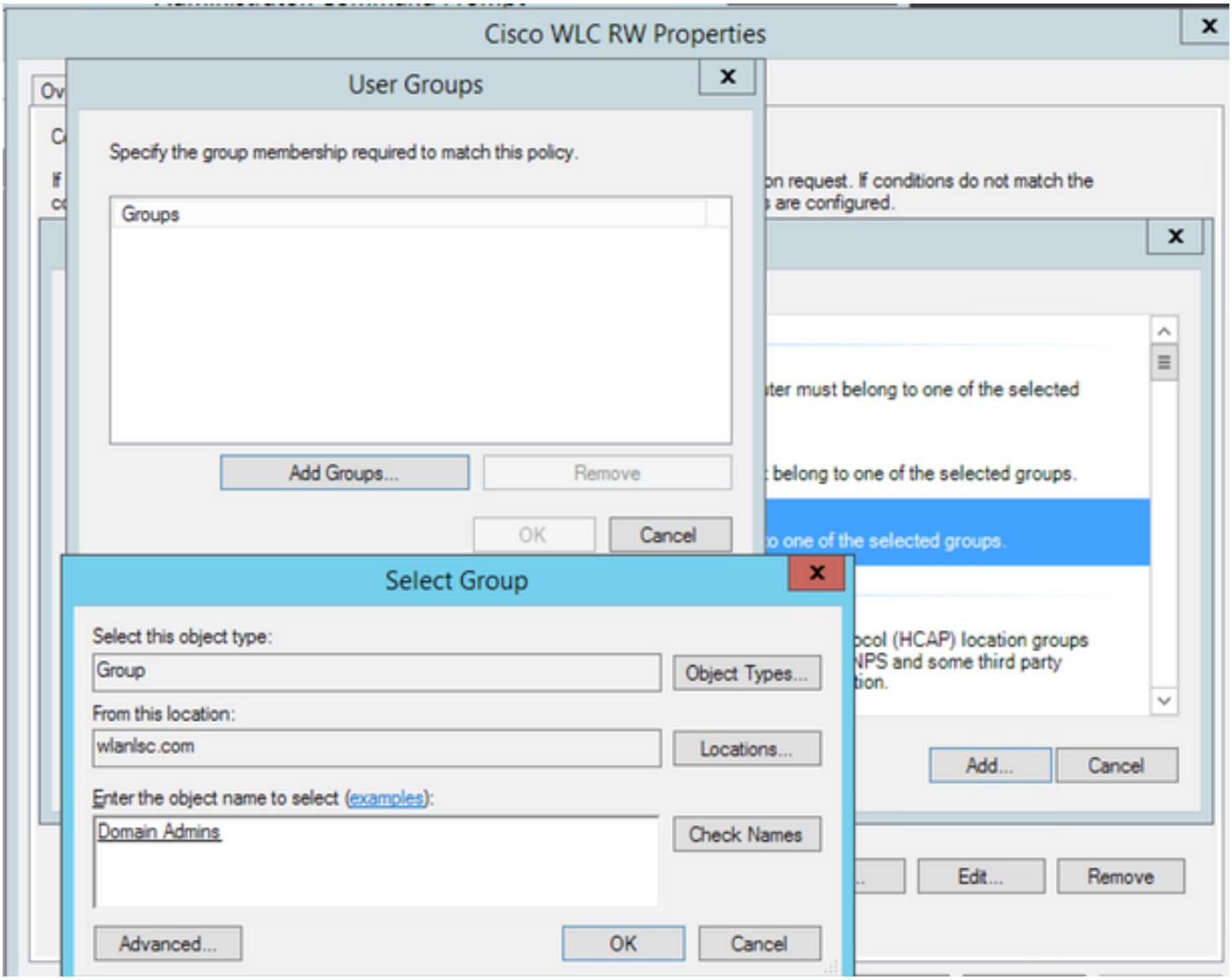
Schritt 4: Navigieren Sie zu **Richtlinien > Netzwerkrichtlinien**. Klicken Sie mit der rechten Maustaste, um eine neue Richtlinie hinzuzufügen. In diesem Beispiel wird die Richtlinie als **Cisco WLC RW** bezeichnet, was impliziert, dass die Richtlinie für den vollen (Lese- und Schreibzugriff) Zugriff verwendet wird. Stellen Sie sicher, dass die Richtlinie wie hier gezeigt konfiguriert ist.



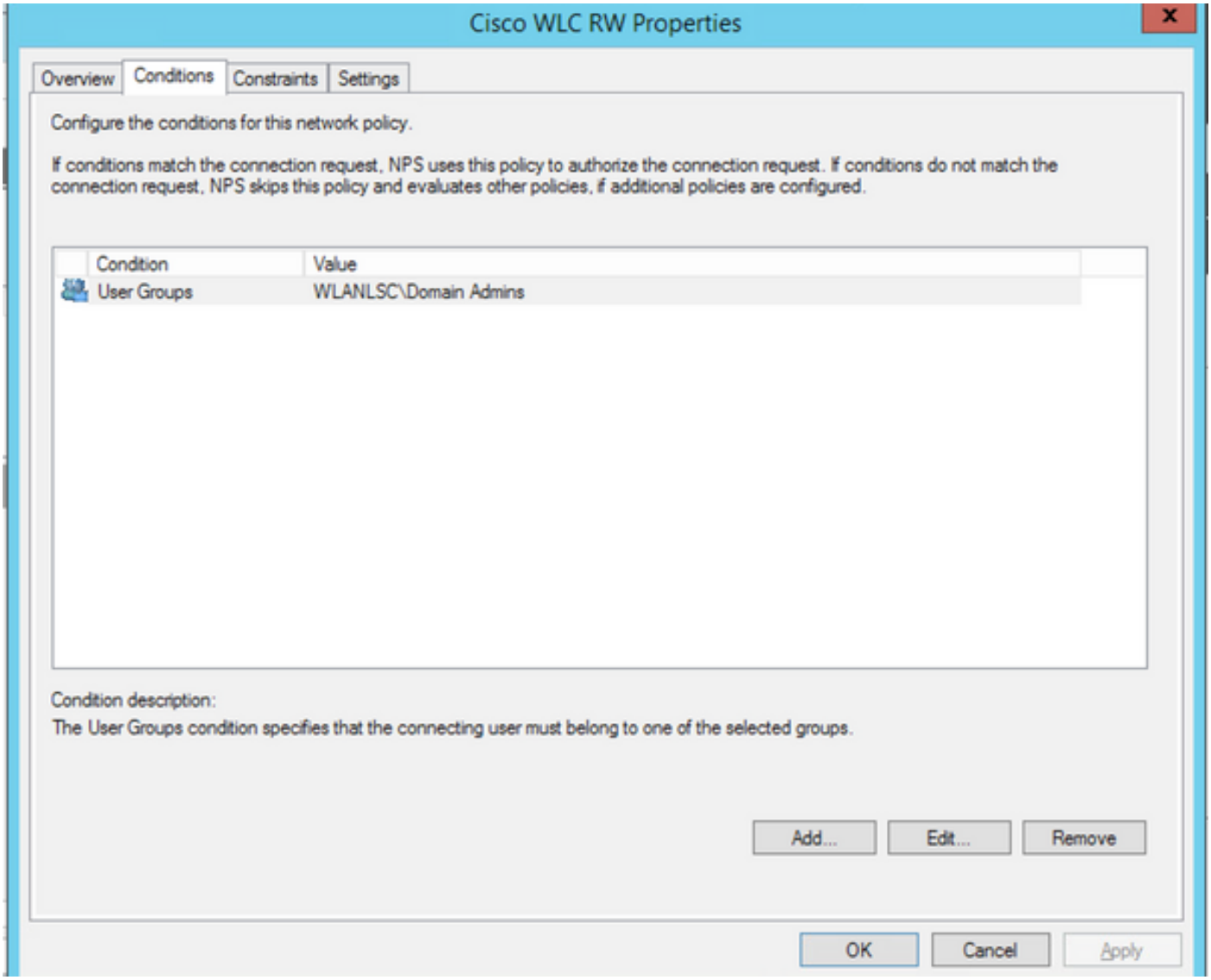
Schritt 5: Klicken Sie auf der Registerkarte **Bedingungen** auf **Hinzufügen**. Wählen Sie die **Benutzergruppen aus** und klicken Sie auf **Hinzufügen**, wie im Bild gezeigt.



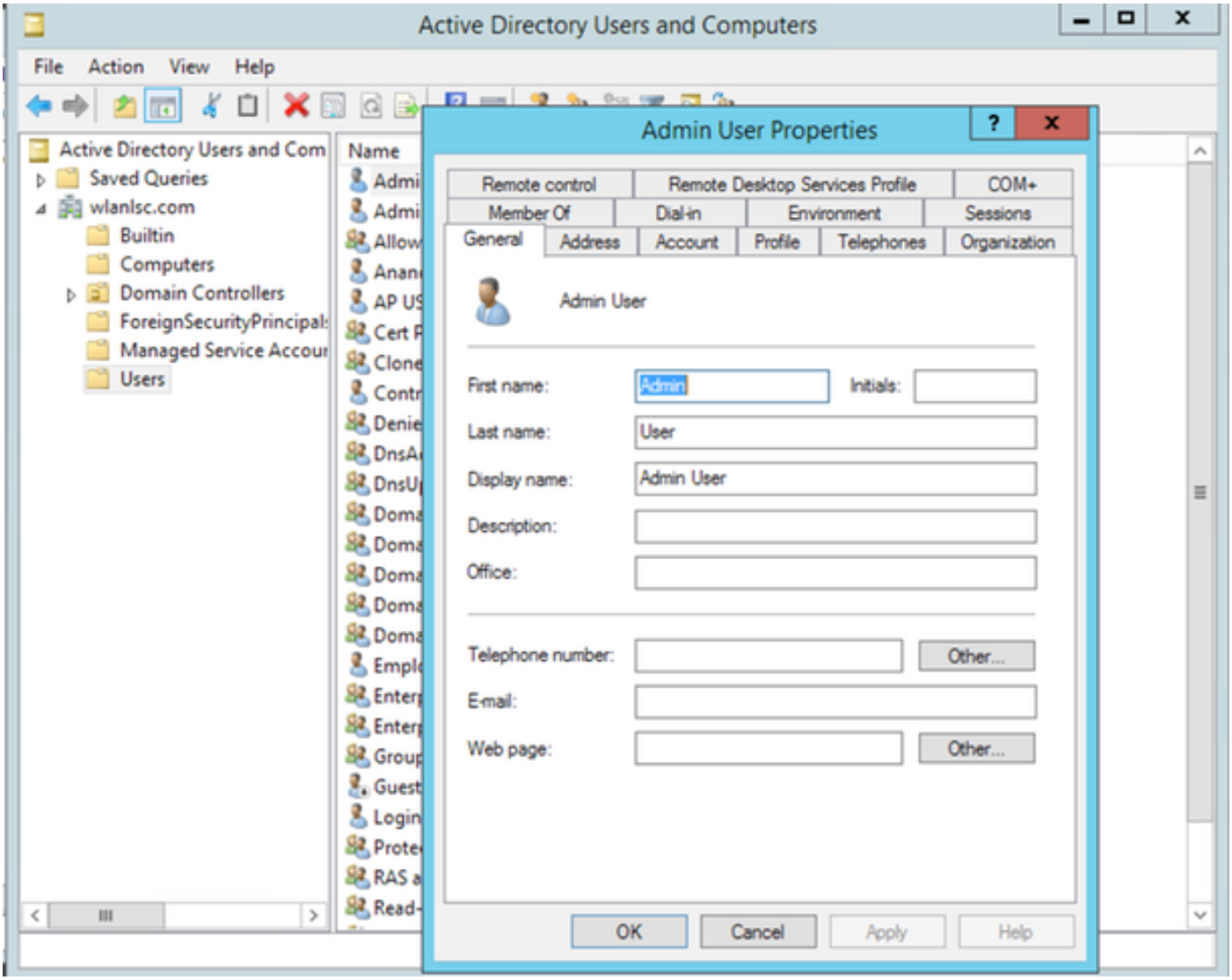
Schritt 6: Klicken Sie im angezeigten Dialogfeld auf **Gruppen hinzufügen**. Wählen Sie im sich öffnenden Fenster **Gruppe auswählen** den gewünschten **Objekttyp** und **Speicherort** aus, und geben Sie den gewünschten Objektnamen ein, wie im Bild gezeigt.

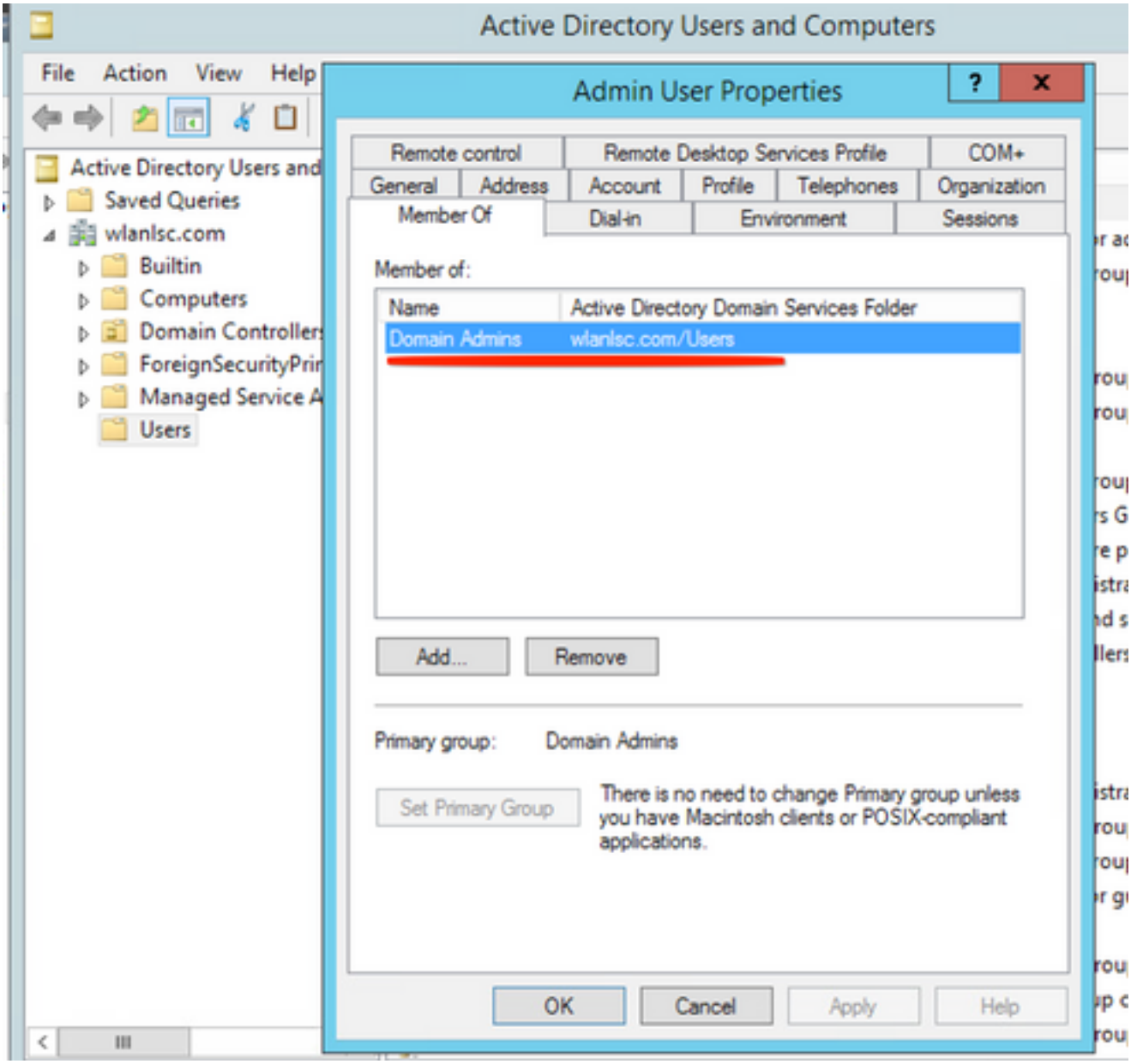


Wenn die Bedingung korrekt hinzugefügt wird, sollte sie wie hier gezeigt aussehen.

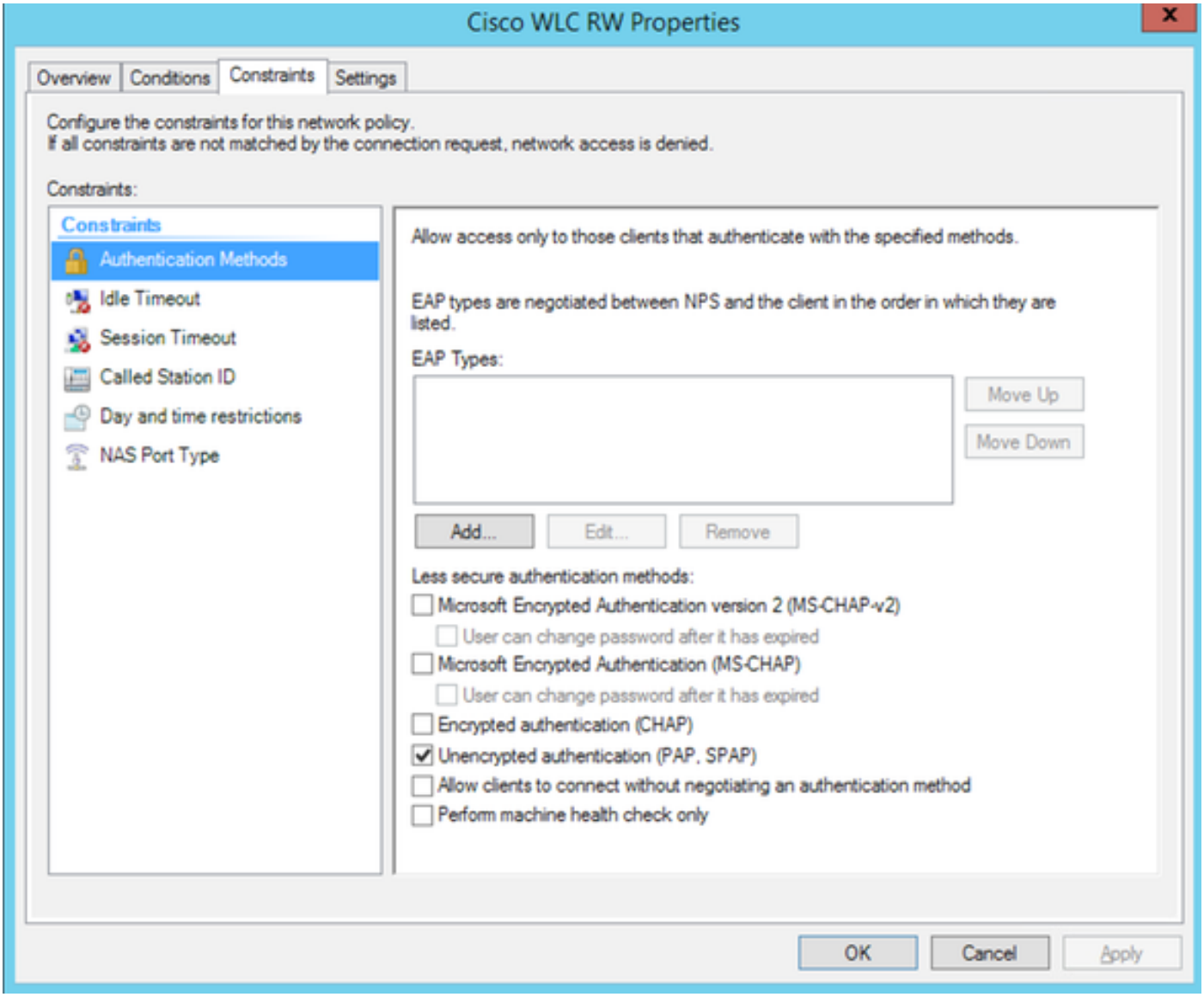


Hinweis: Um Details zu Speicherort und Objektnamen zu erfahren, öffnen Sie das aktive Verzeichnis, und suchen Sie nach dem gewünschten Benutzernamen. In diesem Beispiel besteht **Domänen-Administratoren** aus Benutzern, die vollständigen Zugriff erhalten. **adminuser** ist Teil dieses Objektnamens.

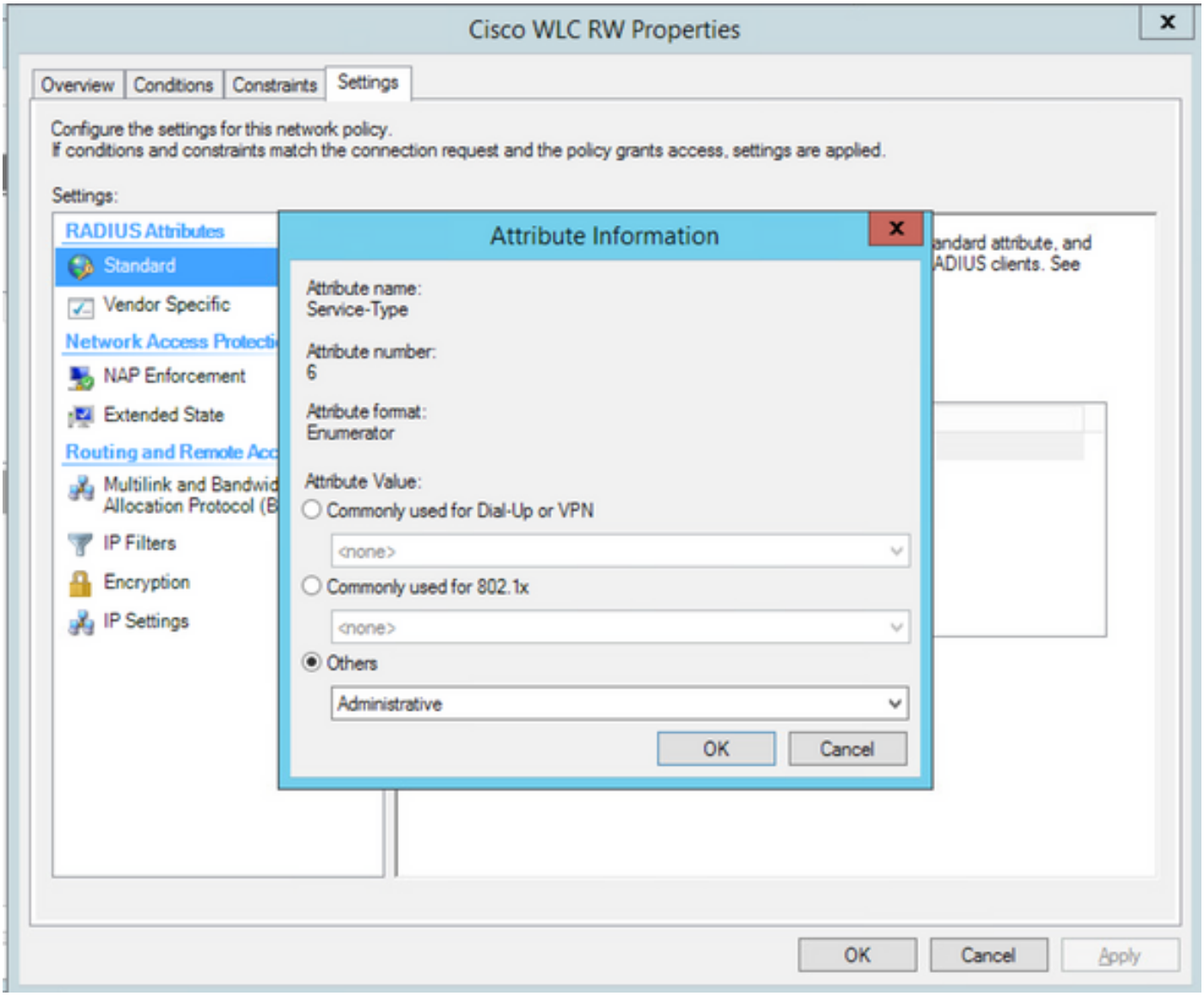

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
wlanlsc.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name
Admin User Properties
Remote control
Remote Desktop Services Profile
COM+
Member Of
Dial-in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



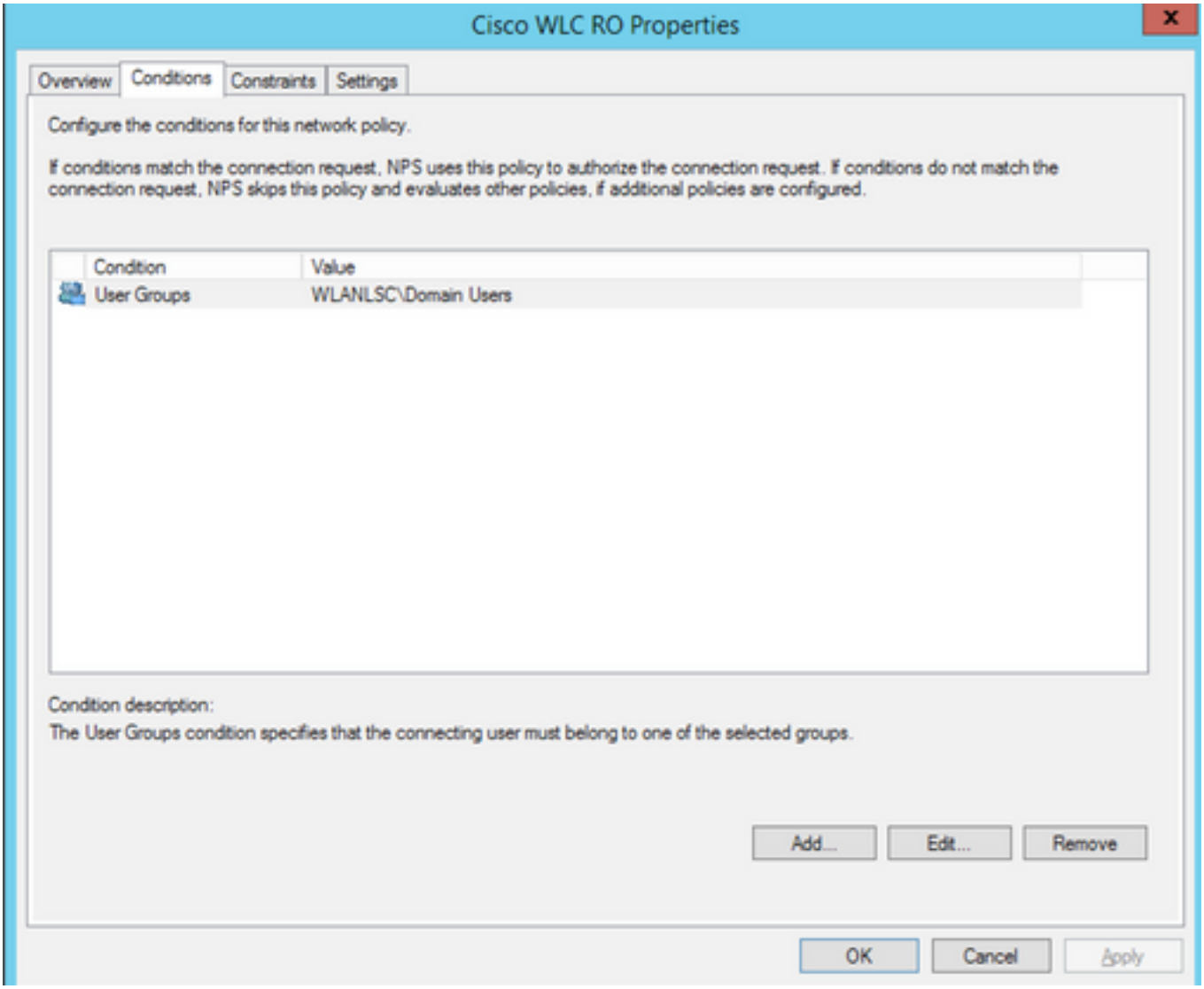
Schritt 7: Navigieren Sie auf der Registerkarte **Einschränkungen** zu **Authentifizierungsmethoden**, und stellen Sie sicher, dass nur **unverschlüsselte Authentifizierung** aktiviert ist.

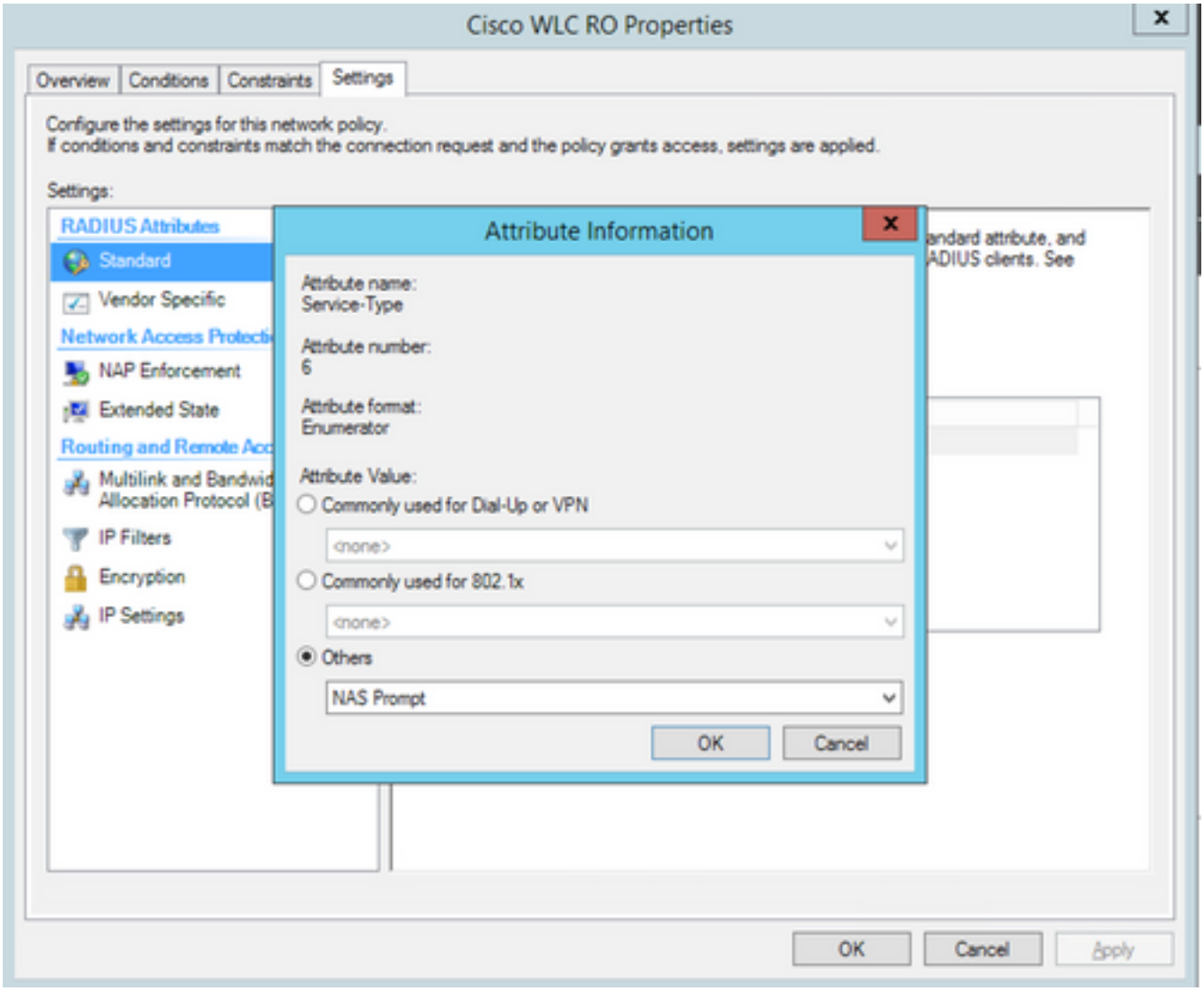


Schritt 8: Navigieren Sie auf der Registerkarte **Einstellungen** zu **RADIUS Attributes > Standard**. Klicken Sie auf **Hinzufügen**, um ein neues Attribut, **Servicetyp, hinzuzufügen**. Wählen Sie im Dropdown-Menü **Verwaltung** aus, um den Benutzern, die dieser Richtlinie zugeordnet sind, vollständigen Zugriff zu gewähren. Klicken Sie auf Apply, um die Änderungen zu speichern, wie im Bild gezeigt.



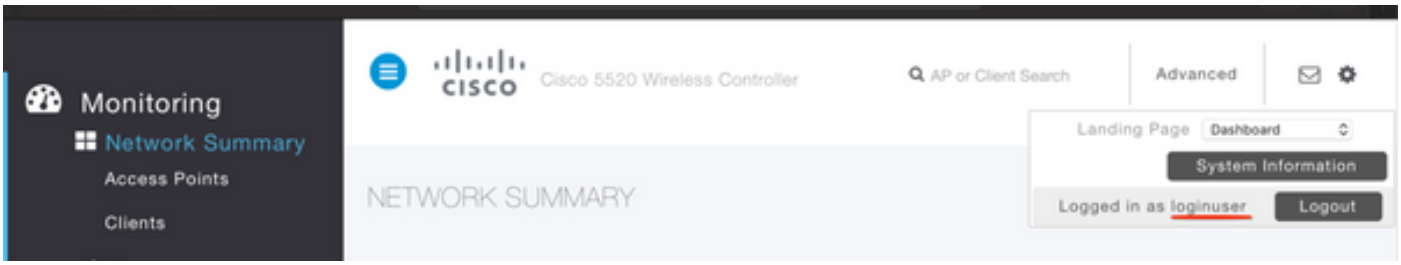
Hinweis: Wenn Sie bestimmten Benutzern schreibgeschützten Zugriff gewähren möchten, wählen Sie im Dropdown-Menü die Option NAS-Prompt aus. In diesem Beispiel wird eine weitere Richtlinie mit dem Namen **Cisco WLC RO** erstellt, um Benutzern unter dem Objektnamen **Domain Users** schreibgeschützten Zugriff bereitzustellen.

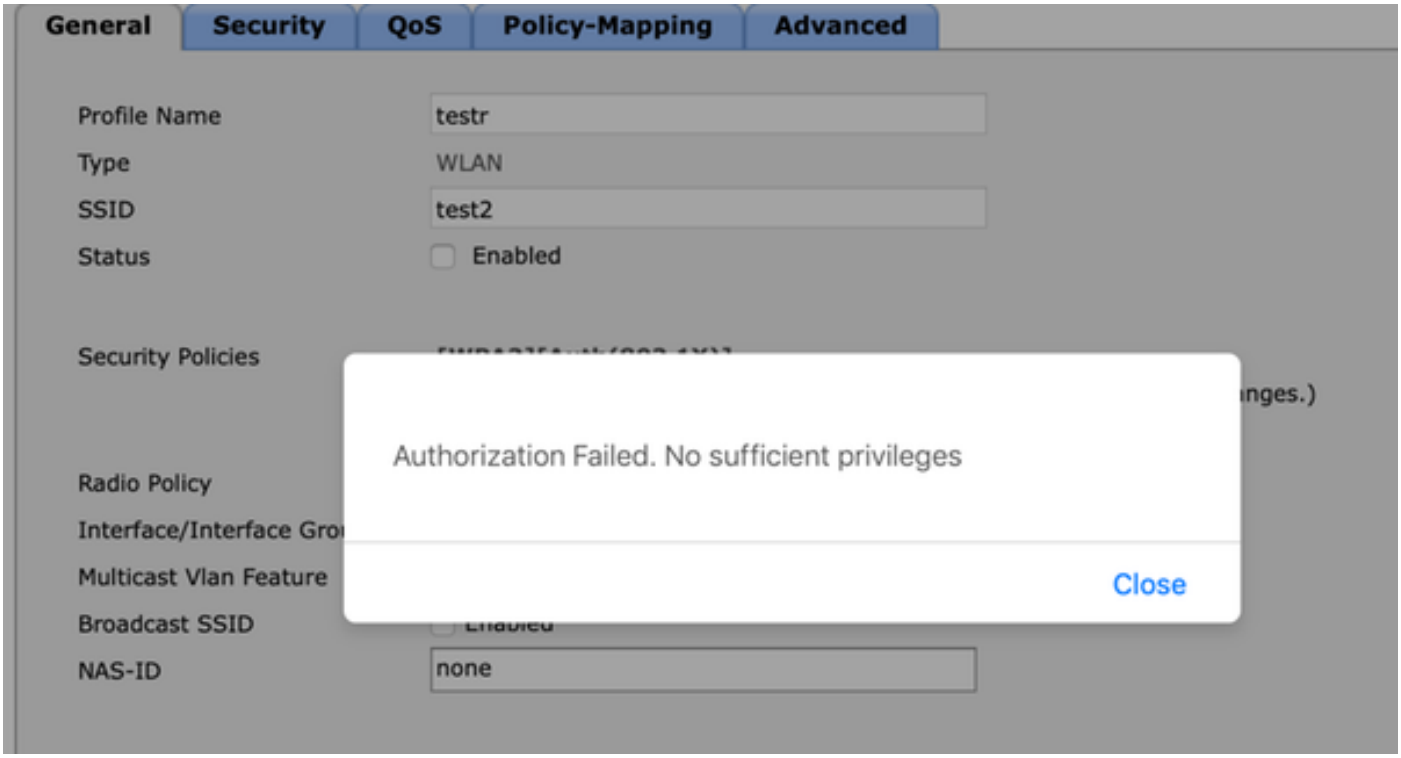

Cisco WLC RO Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates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



Überprüfen

1. Wenn **Anmeldeinformationen** verwendet werden, kann der Benutzer keine Änderungen am Controller konfigurieren.

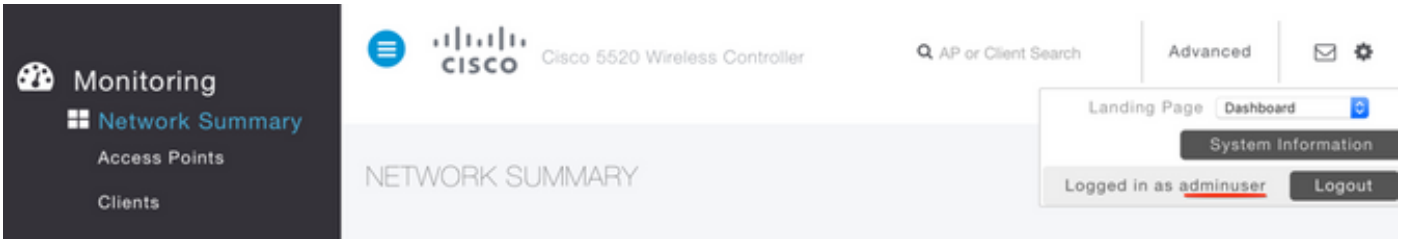




Aus **debug aaaa all enable** können Sie sehen, dass der Wert des Diensttypattributs in der Autorisierungsantwort 7 ist, der NAS-Prompt entspricht.

```
*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. Wenn **Administratorberechtigungen** verwendet werden, sollte der Benutzer vollen Zugriff mit dem **Diensttyp** Wert 6 haben, der der **Administrator** entspricht.




```
*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)
```

Fehlerbehebung

Führen Sie den Befehl **debug aa all enable** aus, um die Fehlerbehebung für den Verwaltungszugriff auf WLC über NPS durchzuführen.

1. Hier werden Protokolle angezeigt, wenn falsche Anmeldeinformationen verwendet werden.

```
*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. Die Protokolle, in denen der Diensttyp mit einem anderen Wert als Administrative (value=6) oder NAS-Prompt (value=7) verwendet wird, werden wie folgt angezeigt. In diesem Fall schlägt die Anmeldung selbst dann fehl, wenn die Authentifizierung erfolgreich ist.

```
*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
```