Verwaltungszugriff für AireOS WLC über Microsoft NPS

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurationen WLC-Konfiguration Microsoft NPS-Konfiguration Überprüfen Fehlerbehebung

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.

cisco		<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Sa EEEDB
Security	RADIUS	Authenti	ication Server	rs > Edit					
 AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrelia 	Server In Server Ad Shared Se Confirm S Key Wrap Apply Cise Apply Cise Apply Cise Port Num Server St Support f Server Til Network I Managem Tunnel Pro Realm Lis PAC Provi IPSec Cisco ACA	dex ddress(Ipv4 ecret Forma ecret Shared Secr o co ISE Defa co ACA Def ber atus for CoA meout User tent tent Retrans oxy a isioning	(/Ipv6) at ret ault settings ault settings	2 10.106.33.3 ASCII O (Designed for 1812 Enabled O Disabled O S secon C Enable Enable Enable Enable	9 r FIPS customo ds ds	ers and requires a k	ey wrap complia	nt RADIU	S server;
h Advanced									

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

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Priority O	rder > N	lanagement l	Jser		
Authentic	ation				
Not L	lsed		Order U	sed for Authe	ntication
TACACS	i+	>		RADIUS	Up
		<			Down

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.

•	WLC Properties	×	x
File Action View Help Image: Second Sec	WLC Properties Settings Advanced Image: Select an existing template: Image: Name and Address Friendly name: WLC Address (IP or DNS): Image: Select an existing Shared Secret stemplate: None To manually type a shared secret, click Manual. To automatically gen secret, click Generate. You must configure the RADIUS client with the secret entered here. Shared secrets are case-sensitive. Image: Manual Generate Shared secret: Shared secret:	Verfy	x
	Shared secret:		
< III >	OK Cancel	Apply	

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

0	Cisco WLC Properties	-
File Action View Help File Action View Help Provide the second	Overview Conditions Settings Policy name: Oteco WLC Provide the settings Policy state # enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy. Image: Policy enabled Policy enabled	
Connection Request Po Connection Request Po Network Policies Health Policies System Health Validato Remediation Server Gro Accounting Templates Management	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 nether 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	
< III >	OK Cancel App	ły

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.

	Cisco WLC Properties	x
Overview Conditions Settings	s	
Configure the conditions for this If conditions match the connect connection request, NPS skips	s network policy. tion request, NPS uses this policy to authorize the connection request. If conditions do not match the this policy and evaluates other policies, if additional policies are configured.	
Condition	Value	
NAS Identifier	Cisco-WLC	
Condition description: The NAS Identifier condition sp syntax to specify NAS names.	ecifies a character string that is the name of the network access server (NAS). You can use pattern matching	
	Add Edit Remove	
	OK Cancel App	pły

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.

0	Cisco WLC RW Properties	X
File Action View Help	Overview Conditions Constraints Settings Policy name: Disco WLC RW Policy State]
 RADIUS Clients Remote RADIUS Server Policies Connection Request Po 	If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. Policy enabled	
 Network Policies Health Policies Network Access Protection Accounting 	Access Pemission 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?	
þ 🛒 Femplates Management	 ● 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.	
	Unspecified V O Vendor specific: 10 🔷	
< III >	OK Cancel Apply	

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

Overview	Conditions	Constraints	Settings									
Configure	the condition	ns for this net	vork policy									
If condition connection	ns match the n request, N	Connection r PS skips this	equest, NP policy and (S uses this period	policy to au her policies	thorize the	connectional policies	n request. If c are configure	ondition d.	s do not ma	stch the	
					Select	conditi	on					×
Select a	a condition, a	and then click	Add.									
Group	S											^
10	Windows The Windo groups.	Groups ws Groups c	ondition sp	pecifies that	the conne	cting user	or compu	ter must belor	ng to on	e of the sel	ected	Ξ
	The Machi User Gro The User (ne Groups co ups Groups condi	ondition sp tion specif	ecifies that ies that the	the connecting	ting comp	uter must t belong t	belong to one o one of the s	e of the s	selected gr groups.	oups.	
	Location The HCAP required to network ac	Groups Location Gro match this p ccess servers	oups condi olicy. The s (NASs). S	tion specific HCAP proto See your NA	es the Hos locol is use S docume	t Credentia d for comm ntation bef	I Authoriz nunication ore using	ation Protoco between NPS this condition	I (HCAF S and so	²) location ome third p	groups arty	~
										Add	Canc	el
								Add		Edit	Remo	ove

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.

		Cisco WLC RW P	roperties	s		3
v	User Groups		x			
C Specify the group memb	ership required to match	h this policy.		on reques are confi	t. If conditions do not match the igured.	
Groups						x
						~
				iter must	belong to one of the selected	Ξ
A	dd Groups	Remove		: belong to	o one of the selected groups.	
	Select Gr	OK Car	ncel	to one of t	he selected groups.	
Select this object type:		-			pcol (HCAP) location groups	
Group			Object Ty	pes	NPS and some third party pon.	_
From this location:						~
wlanlsc.com			Locatio	ns	Add Cancel	
Enter the object name to s	elect (<u>examples</u>):		(C			
Doman Admins			Check N	ames	Edit Remove	•
Advanced		ОК	Car	ncel		

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

			Cisco WLC RW Properties
verview	Conditions	Constraints	Settings
Configure If condition	the condition ons match the on request, N	ns for this network of the second sec	work policy. equest, NPS uses this policy to authorize the connection request. If conditions do not match the policy and evaluates other policies, if additional policies are configured.
Cor	ndition	V	alue
🏭 Use	er Groups	W	/LANLSC\Domain Admins
	4		
condition	description:		
Condition The User	Groups cond	lition specifies	that the connecting user must belong to one of the selected groups.
Condition The User	Groups cond	ition specifies	a that the connecting user must belong to one of the selected groups. Add Edit Remove

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.

	Ac	tive Directory Use	rs and Con	nputers			-	x
File Action View Help Active Directory Users and Com Active Directory Users and Com Saved Queries Wanlsc.com Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accour Users	Admi Name Admi Admi Admi Admi Allow Anan AP US AR US AP US AC Contr AC Contr AC Contr AC Contr AC Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma	Remote control Member Of General Address Admin Use First name: Last name: Display name: Description: Office:	rs and Con Admin Us Remote D Dial-in Account er User Admin User	er Prope Desktop Sen Envir Profile	erties vices Profile onment Telephones	COM+ Sessions Organization		×
< III >	B Doma Doma Doma Emple Enter; Group Coup Login RAS a RAS a Read-	Office: Telephone number: E-mail: Web page:	K C	ancel	Apply	Other Other		

File Action View Help Active Directory Users and Saved Queries Saved Queries	Remote control General Address Member Of Member of: Name Domain Admins	Admin Use Remote De Account Dial-in Active Director wanisc.com/U	er Properties esktop Services Profile Profile Telephones Environment y Domain Services Fok	COM+ COM+ Sessions	
Active Directory Users and Saved Queries Saved Qu	Remote control General Address Member Of Member of: Name Domain Admins	Remote De Account Dial-in Active Director wlanlsc.com/U	esktop Services Profile Profile Telephones Environment y Domain Services Fold	COM+ s Organizatio Sessions der	
Active Directory Users and Saved Queries Saved Qu					
	Add Primary group:	Remove Domain Admins There is no you have M applications	need to change Primar lacintosh clients or POS s.	ry group unless SIX-compliant Help	is p n n n

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

	Cisco WLC RW Properties
Overview Conditions Constraints Setting Configure the constraints for this network po If all constraints are not matched by the con Constraints:	Icy. nection request, network access is denied.
Authentication Methods	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: Move Up
Pay and time restrictions	Add Edt Remove
	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 OK Cancel Apply

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.

f conditions and constraints m Settings:	atch the connection request and the policy grants access, settings are applied.	
RADIUS Attributes	Attribute Information X andard attribute, a	nd
Standard Vendor Specific	Attribute name: Service-Type	5
NAP Enforcement	Attribute number: 6	
Extended State Routing and Remote Acc	Attribute format: Enumerator	H
Multilink and Bandwid Allocation Protocol (B	Attribute Value: Commonly used for Dial-Up or VPN	
IP Filters	<none></none>	
Encryption	O Commonly used for 802.1x	
🚜 IP Settings	<none></none>	
	Others	
	Administrative V	
	OK Cancel	

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 Constr	aints Settings
Configure the conditions for thi If conditions match the connec connection request, NPS skips	s network policy. tion request, NPS uses this policy to authorize the connection request. If conditions do not match the this policy and evaluates other policies, if additional policies are configured.
Condition	Value
all User Groups	WLANLSC\Domain Users
Condition description: The User Groups condition spe	ecifies that the connecting user must belong to one of the selected groups.
	OK Cancel Apply

	Cisco WLC RO Properties	X
Overview Conditions Constr	aints Settings	
Configure the settings for this r if conditions and constraints m Settings:	network policy. atch the connection request and the policy grants access, settings are applied.	
RADIUS Attributes	Attribute Information X and and attribute and	_
Standard	Attribute name: Service-Type	
NAP Enforcement	Attribute number: 6	
Extended State	Attribute format: Enumerator	
Multilink and Bandwid Allocation Protocol (B	Attribute Value: O Commonly used for Dial-Up or VPN	
P Filters	(none> V	
Encryption	O Commonly used for 802.1x	
R IP Settings	<pre></pre>	
	Others	
	NAS Prompt V	
	OK Cancel	
	OK Cancel &	ply

Überprüfen

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



eneral	Security	QoS	Policy-Mapping	Advanced		
Profile Na	ame	tes	tr			
Туре		WL	AN			
SSID		tes	t2			
Status			Enabled			
Security	Policies	Autho	rization Failed. No su	fficient privileges		inges.)
Radio Pol	licy					
Interface	/Interface Gro					
Multinget	Vian Feature				Close	
Multicast						
Broadcas	t SSID	0	Induicu			

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 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 (gid: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:
protocolUsed.....0x0000001
*radiusTransportThread: Dec 07 22:20:14.668:
*radiusTransportThread: Dec 07 22:20:14.668: Packet contains 2 AVPs:
*radiusTransportThread: Dec 07 22:20:14.668: AVP[01] Service-
*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:
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-
*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 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:
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 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 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:

protocolUsed.....0xfffffff

*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:
*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[03] Service-
Type.....0x00000007 (7) (4 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[04] Nas-Ip-
*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: resultCode.....0
*radiusTransportThread: Dec 07 22:46:31.853:
protocolUsed.....0x0000001
*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
```