# 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.

cisco		<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Sa EEEDB
Security	RADIUS	Authenti	ication Server	rs > Edit					
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Auth Cached Users</li> <li>Fallback</li> <li>DNS</li> <li>Downloaded AVP</li> <li>TACACS+</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Password Policies</li> <li>Local EAP</li> <li>Advanced EAP</li> <li>Priority Order</li> <li>Certificate</li> <li>Access Control Lists</li> <li>Wireless Protection</li> <li>Policies</li> <li>Web Auth</li> <li>TrustSec</li> <li>Local Policies</li> <li>Umbrelia</li> </ul>	Server In Server Ad Shared S Shared S Confirm S Key Wrap Apply Cis Apply Cis Port Num Server St Support f Server Til Network I Managem Tunnel Provi PAC Provi IPSec Cisco ACA	dex ddress(Ipv4 ecret Forma ecret Shared Secr o co ISE Defa co ACA Def ber tatus for CoA meout User tent tent Retrans oxy a isioning A	at ret ault settings ault settings ault settings	2 10.106.33.3 ASCII ©  (Designed for 1812 Enabled © 5 second Canable Canable Enable Enable Enable	9 or FIPS custome ds ds	ers and requires a k	ey wrap complia	nt RADIU	S server;
h Advanced									

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

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

**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.

<b>@</b>	WLC Properties X	x
File Action View Help      NPS (Local)       RADIUS Clients and Servers        RADIUS Clients     RADIUS Clients    RADIUS Clients    RADIUS Clients    RADIUS Clients    RADIUS Clients     RADIUS Clients    RADIUS Clients     RADIUS Clients     RADIUS Clients     RADIUS Clients     RADIUS Clients     RADIUS Clients     RADIUS Clients     Radius Clients     Radius Clients     Radius Clients     Radius Clients     Radius Clients     Radius Clients     Radius Clients     Radius Clients     Remote RADIUS Server     Policies     Policies     Network Access Protection     Accounting     Priendly Name     WLC	Settings       Advanced         Image: Enable this RADIUS client       Image: Enable this RADIUS client         Image: Select an existing template:       Image: Enable this RADIUS client         Name and Address       Friendly name:         Image: WLC       Image: Enable this RADIUS         Address (IP or DNS):       Image: Enable this Shared Secret         Shared Secret       Image: Enable this Shared Secrets template:         None       Image: Image: Image: Enable this same shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret. Click Generate Shared secrets are case-sensitive.         Image:	

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.

0	Cisco WLC Properties	-
<ul> <li>File Action View Help</li> <li>File Action View Help</li> <li>Policies</li> <li>Policies</li> <li>Policies</li> <li>Network Policies</li> <li>Health Policies</li> <li>Network Access Protection</li> <li>System Health Validato</li> <li>Remediation Server Gro</li> <li>Accounting</li> <li>Templates Management</li> </ul>	Overview       Conditions       Settings         Policy name:       Settings         Policy state       Fenabled, 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 nether is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.         Image: Type of network access server:         Unspecified       v         Vendor specific:       10	
< III >	OK Cancel Appl	łv

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.

Cisco WLC Properties	x
Overview Conditions 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, ive 5 skips this policy and evaluates other policies, if additional policies are conligured.	
Condition Value	
See 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.	
Add Edit Bemove	
OK Cancel Apply	

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.

0	Cisco WLC RW Properties	X
File Action View Help File Action Clients File Action Clien	Cisco WLC RW Properties         Overview       Conditions       Constraints       Settings         Policy name:       Image: Imag	
<ul> <li>Health Policies</li> <li>Metwork Access Protection</li> <li>Accounting</li> <li>Templates Management</li> </ul>	Grant access. Grant access if the connection request matches this policy.     O Beny access. Deny access if the connection request matches this policy.     O Deny access. Deny access if the connection request matches this policy.     O Ignore user account dial-in properties.     If the connection request matches the 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	
< III >	OK Cancel Apply	

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

Configure t	he condition	s for this net	vork policy											
f condition	ns match the n request, N	connection r PS skips this	equest, NF policy and	S uses this evaluates o	policy to other polici	authorize es, if add	the conn ditional po	licies ar	equest. If e configure	conditio ed.	ns do not	match the	•	
					Selec	ct con	dition							×
Select a	condition, a	and then click	Add.											
Group	s	-											- i	4
<b>1</b>	Windows The Windo groups. Machine ( The Machi	Groups ws Groups o Groups ne Groups o	ondition sp andition sp	ecifies that	at the conn	necting ( ecting c	user or co omputer r	mputer must be	must belo	ong to o e of the	ne of the s	groups.		
HCAP	Location (	ips Groups condi Groups	tion specif	ies that the	e connecti	ng user	must belo	ong to o	ne of the s	selecte	d groups.			
	required to network ac	match this p cess servers	olicy. The (NASs).	HCAP pro See your N	tocol is us IAS docum	sed for c nentation	ommunica before u	ation be sing thi	on Protoc tween NP s conditio	ol (HC) S and s n.	some third	i party		~
											Add		Cancel	

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.

	Cisco WLC RW Properties	
v	User Groups X	
Ci F	Specify the group membership required to match this policy. on request. If conditions do not match the	,
ľ	Groups are configured.	x
		^
	iter must belong to one of the selected	≡
	Add Groups Remove belong to one of the selected groups.	
	OK Cancel o one of the selected groups.	
-	Select Group	
	Select this object type: Group Object Types Docol (HCAP) location groups NPS and some third party	
	From this location:	V
	wlanlsc.com Locations Add	Cancel
	Enter the object name to select (examples): Domain Admins Check Names	
		Remove
	Advanced OK Cancel	

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

			Cisco WLC RW	/ Properties			
verview	Conditions	Constraints	ettings				
Configure If conditio	the condition ons match the on request, N	ns for this netw e connection r IPS skips this (	k policy. uest, NPS uses this policy to author icy and evaluates other policies, if a	ize the connection dditional policies a	n request. If condi are configured.	tions do not matc	h the
Cor	ndition	V	e				
🚜 Use	er Groups	W	NLSC\Domain Admins				
Condition	description:						
Condition The User	description: Groups cond	dition specifies	at the connecting user must belong	to one of the sele	ected groups.		
Condition The User	description: Groups cond	dition specifies	at the connecting user must belong	to one of the sele	ected groups. Add	Edt	Remove

**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.

	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 Ar US AC ert P AC Contr C	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 >	St Doma Doma Doma Emple Enter; Coup Login RAS a Read-	Office: Telephone number: E-mail: Web page:	K C	ancel	Apply	Other Other		<ul> <li></li> </ul>

			Active [	Directory	Users ar	nd Compute	ers	
File Act	ion View Hel	lp		Admin Us	ser Prop	erties	?	×
→ Ctive → Sav → ₩ wia → ₩ → ₩ → ₩ → ₩ → ₩ → ₩	Directory Users ar red Queries anlsc.com Builtin Computers Domain Controlle ForeignSecurityP Managed Service Users	nd Remote co General A Member of: Name Domain Ad	ntrol Address X	Remote Dial-in	Desktop Se Profile Env ory Domain Users	rvices Profile Telephones ironment	COM+ Organizat Sessions	ion ir ac rou rou rou rou rou s G re p istra
		Add Primary grou Set Prima	p: Do ny Group	emove main Admins There is n you have application	o need to Macintosh ns. Cancel	change Primary clients or POSI	group unless X-compliant	istra rou rou rou rou rou

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

	Cisco WLC RW Properties
Overview Conditions Constraints Setting Configure the constraints for this network pol If all constraints are not matched by the conr Constraints: Constraints Authentication Methods	s icy. rection request, network access is denied. Allow access only to those clients that authenticate with the specified methods.
<ul> <li>Idle Timeout</li> <li>Session Timeout</li> <li>Called Station ID</li> <li>Day and time restrictions</li> <li>NAS Port Type</li> </ul>	EAP types are negotiated between NPS and the client in the order in which they are Isted. EAP Types:   Move Up Move Down  Add Edit Remove 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) Vuencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method Perform machine health check only
	OK Cancel Apply

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.

ADILIS Attributes	Attribute lefermation X	
Charderd	Attribute information	andard attribute, and
Standard	Attribute name:	ADIOS CIEILS, See
Vendor Specific	Service-Type	
Network Access Protecti	Attribute number:	
NAP Enforcement	6	
Extended State	Attribute format: Enumerator	
Routing and Remote Acc		
Multilink and Bandwid Allocation Protocol (B	Attribute Value: Commonly used for Dial-Up or VPN	
IP Filters	<pre></pre>	
Encryption	O Commonly used for 802.1x	
No IP Settings	<none></none>	
	Others	
	Administrative	
	OK Crock	
	UK Calicei	

**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 Constr	aints 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				
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				

Overview       Conditions       Constraints       Settings         Corfigure the settings for this network policy.       if conditions and constraints match the connection request and the policy grants access, settings are applied.         Settings:       RADIUS Attributes       Attribute Information       andard attribute, and ADIUS clerts. See         Vendor Specific       Attribute name:       Service-Type       Attribute number:       6         NAP Enforcement       Attribute format:       Attribute format:       Image: Commonly used for Dial-Up or VPN       Image: Commonly used for B02.1x         IP Filters       Commonly used for 802.1x       Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         IP Settings       NAS Prompt       V         IVAS Prompt       OK       Cancel	x	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: RADIUS Attributes RADIUS Attributes Attribute Information Attribute Informati		aints Settings	Overview Conditions Constra
RADIUS Attributes       Attribute Information       x       andard attribute, and ADIUS clients. See         Image: Standard       Attribute name: Service-Type       andard attribute, and ADIUS clients. See         Image: NAP Enforcement       Attribute number: 6       attribute number: 7       attribute number: 7<		retwork policy. atch the connection request and the policy grants access, settings are applied.	Configure the settings for this n if conditions and constraints ma Settings:
Standard       Attribute name: Service-Type       Attribute name: Service-Type       Attribute name: Service-Type         Mathematic Access Protection Souting and Remote Access Attribute format: Enumerator       Attribute name: Service-Type       Attribute name: Service-Type       Attribute name: Service-Type         Multilink and Bandwid Allocation Protocol (6 Service)       Attribute format: Enumerator       Attribute format: Enumerator       Image: Service-Type         IP Filters       Commonly used for Dial-Up or VPN       Image: Service-Type       Image: Service-Type         IP Settings       Commonly used for 802.1x       Image: Service-Type       Image: Service-Type         IP Settings       Others       Image: Service-Type       Image: Service-Type	hose as white backness	Attribute Information	RADIUS Attributes
Network Access Protecti       Attribute number:         Image: Extended State       Attribute format:         Routing and Remote Acce       Attribute format:         Image: Routing and Remote Acce       Attribute format:         Image: Routing and Remote Acce       Attribute format:         Image: Routing and Remote Acce       Attribute Value:         Image: Routing and Remote Acce       Attribute Value:         Image: Routing and Remote Acce       Attribute Value:         Image: Routing and Remote Acce       Commonly used for Dial-Up or VPN         Image: Routing and Remote Acce       Image: Routing and Remote Acce         Image: Routing and Remote Acce       Attribute Value:         Image: Routing and Remote Acce       Commonly used for Dial-Up or VPN         Image: Routing and Remote Acce       Image: Routing and Remote Acce         Image: Routing and Remote Acce       Image: Routing and Remote Acce         Image: Routing and Remote Acce       Image: Routing and Remote Acce         Image: Routing and Remote Acce       Image: Routing and Remote Acce         Image: Routing and Remote Acce       Image: Routing and Remote Acce         Image: Routing and Remote Acce       Image: Routing and Remote Acce         Image: Routing and Remote Acce       Image: Routing and Remote Acce         Image: Routing and Remote Acce <td< td=""><td>ADIUS clients. See</td><td>Attribute name: Service-Type</td><td>Standard Vendor Specific</td></td<>	ADIUS clients. See	Attribute name: Service-Type	Standard Vendor Specific
Image: Extended State Attribute format: Enumerator   Routing and Remote Acc   Image: Multilink and Bandwid Allocation Protocol (8)   Image: Pilters   Image: Pilt		Attribute number: 6	Network Access Protection
Multilink and Bandwic Allocation Protocol (B   IP Filters   IP Settings     Commonly used for Dial-Up or VPN     IP Settings     Others     NAS Prompt     OK		Attribute format: Enumerator	Extended State Routing and Remote Acc
<sup>™</sup> IP Filters <sup>Qnone&gt;</sup> <sup>∨</sup> <sup>△</sup> Encryption <sup>Qnone&gt;</sup> <sup>∨</sup> <sup>№</sup> IP Settings <sup>Qnone&gt;</sup> <sup>∨</sup> <sup>Qnone&gt;</sup> <sup>Qnone&gt;</sup> <sup>∨</sup> <sup>Qnone&gt;</sup> <sup>Qnone&gt;</sup> <sup>∨</sup> <sup>Qnone&gt;</sup> <sup>Qnone&gt;</sup> <sup>∨</sup> <sup>Mnone&gt;</sup> <sup>Qnone&gt;</sup> <sup>∨</sup> <sup>Mnone&gt;</sup> <sup>Qnone&gt;</sup> <sup>∨</sup> <sup>Mnone&gt;</sup> <sup>Qnone&gt;</sup> <sup>∨</sup> <sup>Mnone&gt;</sup> <sup>Mnone&gt;</sup> <sup>∨</sup> <sup>Mnone&gt;</sup> <sup>Mnone&gt;</sup> <sup>∨</sup> <sup>Mnone&gt;</sup> <sup>Mnone&gt;</sup> <sup>∨</sup> <sup>Mnone&gt;</sup> <sup>Mnone&gt;</sup> <sup>Mnone&gt;</sup> <sup>Mnone&gt;</sup> <sup>Mnone&gt;</sup> <sup>N</sup> <sup>Mnone&gt;</sup> <sup>Mnone&gt;</sup> <sup>Mnone&gt;</sup>		Attribute Value: Commonly used for Dial-Up or VPN	Multilink and Bandwid Allocation Protocol (B
IP Settings       ○ Commonly used for 802.1x         IP Settings       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for 802.1x       Image: Commonly used for 802.1x         Image: Commonly used for		(none> V	P Filters
IP Settings		<ul> <li>Commonly used for 802.1x</li> </ul>	Encryption
Others      NAS Prompt      OK      Cancel		(none> V	R IP Settings
NAS Prompt V OK Cancel		Others	
OK Cancel		NAS Prompt V	
		OK Cancel	
	-		
OK Crocel Arch	Carral	OK	

### 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.



General	ecurity	QoS	Policy-Mapping	Advanced	
Profile Name		tes	tr		
Туре					
SSID		test2			
Status		Enabled			
Security Polic	ies			inges.)	
Radio Policy		Author	rization Failed. No su	ufficient privileges	
Interface/Inte	erface Gro				
Multicast Vlar	Feature			Close	
Broadcast SS	ID	<b>.</b>	Induicu		
NAS-ID		nor	ne		

Àpartir 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 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:
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. 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:
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)
```

# 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 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

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:
*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
```