# ىلع Cisco Airespace VSAs مداخ نيوكت لااتم Microsoft IAS RADIUS Server

## المحتويات

<u>المقدمة</u> المتطلبات الأساسية المكونات المستخدمة معلومات أساسية معلومات أساسية تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA على IAS تكوين نهج الوصول عن بعد على IAS مثال على التكوين مثال على التكوين معلومات ذات صلة معلومات ذات صلة

### <u>المقدمة</u>

يبدي هذا وثيقة أنت كيف أن يشكل Microsoft إنترنت صحة هوية خدمة (IAS) نادل أن يساند cisco Airespace بائع شعار خاص (VSAs). كود المورد ل Cisco Airespace VSAs **14179**.

## <u>المتطلبات الأساسية</u>

#### <u>المتطلبات</u>

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- معرفة كيفية تكوين خادم IAS
- معرفة تكوين نقاط الوصول في الوضع Lightweight (LAPs) ووحدات التحكم في الشبكة المحلية (LAN) اللاسلكية من Cisco (WLCs)
  - معرفة حلول الأمان اللاسلكية الموحدة من Cisco

#### <u>المكونات المستخدمة</u>

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- خادم Microsoft Windows 2000 مع IAS
- Cisco 4400 WLC أن يركض برمجية صيغة 4.0.206.0

- نقاط الوصول في الوضع Cisco 1000 Series LAPs
- مهايئ عميل لاسلكي a/b/g 802.11 مع برنامج ثابت 2.5
  - Aironet Desktop Utility (ADU)، الإصدار 2.5)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

**ملاحظة:** يهدف هذا المستند إلى إعطاء القارئ مثالا على التكوين المطلوب على خادم IAS لدعم Cisco Airespace VSAs. تم إختبار تكوين خادم IAS المقدم في هذا المستند في المعمل ويعمل كما هو متوقع. إذا واجهت مشكلة في تكوين خادم IAS، فاتصل ب Microsoft Windows للحصول على تعليمات. لا يدعم Cisco TAC تكوين Microsoft Windows Server.

يفترض هذا المستند أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تم تكوينه للعملية الأساسية وأن نقاط الوصول في الوضع Lightweight تم تسجيلها إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). إذا كنت مستخدما جديدا يحاول إعداد عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للعملية الأساسية باستخدام نقاط الوصول في الوضع Lightweight (LAP)، فارجع إلى <u>تسجيل نقطة الوصول في الوضع Lightweight (LaP) إلى</u> <u>وحدة تحكم شبكة LAN لاسلكية (WLC)</u>.

#### <u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

## <u>معلومات أساسية</u>

في معظم أنظمة الشبكة المحلية اللاسلكية (WLAN)، تحتوي كل شبكة محلية لاسلكية (WLAN) على سياسة ثابتة تنطبق على جميع العملاء المرتبطين بمعرف مجموعة الخدمة (SSID). وعلى الرغم من أنها فعالة، إلا أن هذه الطريقة لها قيود لأنها تتطلب من العملاء الاقتران ب SSIDs مختلفة لوراثة جودة الخدمة (QoS) ونهج الأمان المختلفة.

ومع ذلك، يدعم حل شبكة LAN اللاسلكية من Cisco شبكات الهوية، والتي تسمح للشبكة بالإعلان عن معرف خدمة (SSID) واحد ومستخدمين معينين لوراثة جودة الخدمة (QoS) المختلفة أو سياسات الأمان استنادا إلى ملفات تعريف المستخدمين الخاصة بهم. وتتضمن السياسات المحددة التي يمكنك التحكم فيها باستخدام شبكات الهوية ما يلي:

- **جودة الخدمة** عند وجودها في "قبول الوصول إلى RADIUS"، تتخطى قيمة مستوى جودة الخدمة قيمة جودة الخدمة المحددة في ملف تعريف WLAN.
- ACL—عندما تكون سمة قائمة التحكم في الوصول (ACL) موجودة في قبول الوصول إلى RADIUS، يقوم النظام بتطبيق اسم قائمة التحكم في الوصول (ACL) على محطة العميل بعد مصادقته. يتخطى هذا الإجراء أي قوائم تحكم في الوصول (ACL) يتم تعيينها إلى الواجهة.
  - VLAN عندما يكون اسم واجهة شبكة VLAN أو VLAN-Tag موجودا في "قبول الوصول إلى RADIUS"، يضع النظام العميل على واجهة معينة.
- معرف WLAN—عندما تكون سمة معرف الشبكة المحلية اللاسلكية (WLAN) موجودة في "قبول الوصول إلى WLAN"، يقوم النظام بتطبيق معرف الشبكة المحلية اللاسلكية (SSID) (WLAN"، يقوم النظام بتطبيق معرف الشبكة المحلية اللاسلكية (WLAN"، يقوم النظام بتطبيق معرف الشبكة المحلية اللاسلكية (WLAN") على محطة العميل بعد مصادقته. يتم إرسال معرف شبكة WLAN بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في مصادقته. يتم إرسال معرف شبكة WLAN بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في مصادقته. يتم إرسال معرف شبكة MLAN بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في جميع مثيلات المصادقة باستثناء IPSec. في حالة مصادقة الويب، إذا تلقت وحدة التحكم في الشبكة المحلية المحلية اللاسلكية (WLC) تعبي متيلات المصادقة باستثناء MLAN.
  - **قيمة DSCP** عندما تكون موجودة في قبول الوصول إلى RADIUS، تتجاوز قيمة DSCP قيمة DSCP المحددة في ملف تعريف WLAN.
- **802.1p-tag**—عندما تكون موجودة في "قبول الوصول إلى RADIUS"، تتجاوز قيمة 802.1p القيمة الافتراضية

المحددة في ملف تعريف WLAN.

**ملاحظة:** تدعم ميزة شبكة VLAN تصفية MAC، و 802.1X، و Wi-Fi Protected Access (WPA) فقط. لا تدعم ميزة شبكة VLAN مصادقة الويب أو IPSec. تم توسيع قاعدة بيانات عامل تصفية MAC المحلي لنظام التشغيل لتضمين اسم الواجهة. وهذا يسمح لعوامل تصفية MAC المحلية بتحديد الواجهة التي يجب تعيين العميل لها. كما يمكن إستخدام خادم RADIUS منفصل، ولكن يجب تعريف خادم RADIUS باستخدام قوائم الأمان.

راجع <u>تكوين شبكة الهوية</u> للحصول على مزيد من المعلومات حول شبكات الهوية.

## <u>شکلت ال IAS ل Airespace VSAs شکلت ال</u>

in order to شكلت ال IAS ل Airespace VSAs، أنت تحتاج أن يتم هذا steps:

1. <u>تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA على IAS</u>

2. <u>تكوين نهج الوصول عن بعد على IAS</u>

ملاحظة: يتم تكوين شبكات VSA بموجب نهج الوصول عن بعد.

<u>تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA على IAS</u>

أتمت هذا steps in order to شكلت ال WLC كعميل AAA على ال IAS:

1. انقر على **برامج > أدوات إدارية > خدمة مصادقة الإنترنت** لتشغيل IAS على خادم Microsoft

	.2000
Internet Authentication Service	
] <u>Accion</u> Mew  ] ← →	
Tree Internet Authentication Service (Local) Clents Remote Access Logging Remote Access Policies	Welcome to Internet Authentication Service Internet Authentication Service (IAS) performs centralized authentication, authorization, and accounting of users who connect to a network using virtual private network (VPN) and dial-up technology. IAS implements the IETF standard Remote Authentication Dial-in User Service (RADIUS) protocol. To enable the IAS server to read the remote access properties of user accounts in the Active Directory, on the Action menu, click Register Service in Active Directory.
	For more information about setting up IAS, see "Checklist: Configuring IAS for dial-up and VPN access" and "Checklist: Configuring IAS to outsource dial-up access" in online Help. For more information on IAS deployment scenarios, see topics "Dial-up corporate access", "Extranet access for business partners", "Internet Access", "Outsourced corporate access through service providers" in online Help.
	For troubleshooting information, see topic Troubleshooting in online Help.

- 2. انقر بزر الماوس الأيمن فوق المجلد **العملاء** واختر **عميل جديد** لإضافة عميل RADIUS جديد.
- 3. في نافذة "إضافة عميل"، أدخل اسم العميل واختر RADIUS كبروتوكول. ثم انقر فوق **التالي**.في هذا المثال،

اسم العميل هو *I-WLC.ملاحظة:* بشكل افتراضي، يتم تعيين البروتوكول على RADIUS.

Add Client		×
Name and Protocol Assign a name and protoco	ol for the client.	
Type a friendly name and p	protocol for the client.	
Eriendly name:	WLC-1	
Protocol:	RADIUS	•
	< <u>B</u> ack <u>N</u> ext >	Cancel

4. في نافذة Add RADIUS Client، أدخل **عنوان IP للعميل**، و**client-vendor**، و**السر المشترك**. بعد إدخال معلومات العميل، انقر فوق **إنهاء**.يبدي هذا مثال زبون يعين *1-WLC* مع عنوان *172.16.1.30*، الزبون-بائع ثبتت إلى cisco، والسر مشترك cisco123:

Client address (IP or DNS):	:
172.16.1.30	<u></u> ⊻erify
Client-Vendor:	
Cisco	
Client must always sen	d the signature attribute in the request
<u>S</u> hared secret:	*****
Confirm shared secret:	*****

مع هذه المعلومات، تتم إضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) المسمى ULC كعميل AAA لخادم IAS.

Action       year       Image: Control of the second of the secon					
Tree       Priordly Name       Address       Protocol       Client-Wendor         Image: Clients       Image: Clie	Action View   ⇔ → 💽 🖬 💼 🚱 😭				
Internet Authorbication Service (Local)   Image: Control   Image: Control  <	Tree	Friendly Name	Address	Protocol	Client-Vendor
	Internet Authentication Service (Local) Clients Remote Access Logging Remote Access Policies	DWLC-1	172.16.1.30	RADIUS	<u>Gisco</u>

تتمثل الخطوة التالية في إنشاء سياسة الوصول عن بعد وتكوين شبكات VSA.

<u>تكوين نهج الوصول عن بعد على IAS</u>

أكمل الخطوات التالية لتكوين نهج وصول عن بعد جديد على IAS:

- 1. إنقر بزر الماوس الأيمن فوق **نهج الوصول عن بعد** واختر **نهج AcceMS الجديد عن بعد**.يظهر إطار اسم النهج.
  - 2. أدخل اسم النهج وانقر فوق **التالي**.

Re	mote Access Policy
oli	cy Name Specify a friendly name for the policy.
	A Remote Access Policy is a set of actions which can be applied to a group of users meeting certain conditions.
	Analogous to rules you can apply to incoming mail in an e-mail application, you can specify a set of conditions that must be matched for the Remote Access Policy to apply. You can then specify actions to be taken when the conditions are met.
	Policy friendly name:
	Airespace VSA
	< <u>B</u> ack. <u>N</u> ext > Cance

3. في الإطار التالي، حدد الشروط التي سيتم تطبيق نهج الوصول عن بعد عليها. طقطقة **يضيف** in order to حددت الشيط

	الشرط.
Add Remote Access Policy	Select Attribute
Conditions Determine the conditions to match.	Select the type of attribute to add, and then click the Add button. Attribute types:
Specify the conditions to match.	Name         Description           Called-Station-Id         Phone number dieled by user           Caling-Station-Id         Phone number from which call originated           Clemt-Friendy-Name         Friendy name for the RADIUS clemt. (IAS only)           Clemt-P-Address         IP address of RADIUS proxy or NAS. (IAS only)           Clemt-P-Address         IP address of RADIUS proxy or NAS. (IAS only)           Clemt-P-Address         Time periods and days of week during which use           FramedProtocol         The protocol to be used           NAS-Identitier         String identitying the NAS originating the request (IA           NAS-P-Address         IP address of the NAS originating the request (IA           NAS-Pont-Type         Type of physical port used by the NAS originatin           Service-Type         Type of service user has requested           Tunnel-Type         Tunneling protocols to be used           Windows-Groups         Windows groups that user belongs to
Add Hemove Edf	
< <u>B</u> ack <u>N</u> ext> Cancel	Add Cancel

4. من قائمة أنواع السمات ، حدد السمات التالية:**-client-ip-address**—أدخل عنوان IP الخاص بعميل AAA. في هذا مثال، ال WLCs عنوان دخلت لذلك السياسة يطبق إلى ربط من ال

	Client-IP-Address ?X	
	<u>Type a word or a wild card (for example, abc.*):</u>	
	172.16.1.30	
	OK Cancel	
محموعات		NLC
. فيما يلي	Wind—حدد مجموعة Windows (مجموعة المستخدمين) التي سيتم تطبيق النهج عليها	lows
	🕷 Groups ? 🗙	
	The following groups are currently in this condition.	
	<u>G</u> roups:	
	Name	
	CAT-TD-2K\Test-Clients	
	Add <u>B</u> emove	
	OK Cancel	
		مثال:

Conditions         Determine the conditions to match.         Specify the conditions to match.         Conditions:         Client-IP-Address matches "172.16.1.30" AND         Windows-Groups matches "CAT-TD-2K\Test-Clients"	d Remote Access Policy			×
Specify the conditions to match. <u>Conditions:</u> <u>Client-IP-Address matches "172.16.1.30" AND</u> Windows-Groups matches "CAT-TD-2K\Test-Clients"	Conditions Determine the conditions to match.			
<u>C</u> onditions: Client-IP-Address matches "172.16.1.30" AND Windows-Groups matches "CAT-TD-2K\Test-Clients"	Specify the conditions to match.			
Client-IP-Address matches "172.16.1.30" AND Windows-Groups matches "CAT-TD-2K\Test-Clients"	<u>C</u> onditions:			
Windows-Groups matches "CAT-TD-2KATest-Clients"	Client-IP-Address matches "172.16.1.30"	AND		
	Windows-Groups matches "CAT-TD-2K\T	l est-Ulients"		
Add Bemove Edit	Add Bemove Ed	ir I		
< <u>B</u> ack <u>N</u> ext > Cancel			<b>N N</b>	

يوضح هذا المثال شرطين فقط. إذا كان هناك المزيد من الشروط، فقم بإضافة هذه الشروط أيضا وانقر فوق **التالي**.يظهر إطار الأذون.

5. في الإطار أذون ، أختر **منح إذن الوصول عن بعد**.بعد إختيار هذا الخيار، يتم منح المستخدم حق الوصول، على أن يطابق المستخدم الشروط المحددة (من الخطوة 2).

d Rei	mote Access Policy
Perm	nissions
I	Determine whether to grant or deny remote access permission.
	You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users.
I	If a user matches the specified conditions:
	Grant remote access permission
	O Deny remote access permission
	Z Rack Neut > Cancel

- 6. انقر فوق **Next (التالي)**.
- 7. تتمثل الخطوة التالية في إعداد ملف تعريف المستخدم.على الرغم من أنه قد تكون قد حددت أنه يجب رفض المستخدمين أو منحهم حق الوصول بناء على الشروط، إلا أنه لا يزال من الممكن إستخدام ملف التعريف إذا تم تجاوز شروط هذا النهج على أساس كل مستخدم.

Add Remote Access Policy	×
User Profile	
Specify the user profile.	
You can now specify the profile for users who matched the conditions you have specified.	
Note: Even though you may have specified that users should be denied access, the profile can still be used if this policy's conditions are overridden on a per-user basis.	
Edit <u>P</u> rofile	
< <u>B</u> ack Finish Canc	el

طقطقة in order to شكلت المستعمل توصيف، **يحرر توصيف** على نافذة المستعمل التوصيف.تظهر نافذة "تحرير ملف تعريف الطلب

Edit Dial-in Profile			?	×
Authentication	Encryption	A	dvanced	1
Dial-in Constraints	IP	1	Multilink	Ì
Disconnect if idle for:		1	in.	
Restrict maximum sessio	n to:	1	📄 min.	
Restrict access to the fo	llowing days and tim	nes:		
	<u>E</u> dit			
Restrict <u>D</u> ial-in to this nu	imber only:			
🗖 🔲 <u>R</u> estrict Dial-in media: =				
FDDI			<u> </u>	
Token Ring				
Wireless - IEEE 802.11				
			-	
, 				
Г	04	Connect	/ lu	
	UN	Cancel	BPPPy	

علامة التبويب **المصادقة**، ثم أختر طريقة المصادقة المستخدمة في الشبكة المحلية اللاسلكية (WLAN).يستخدم هذا المثال مصادقة غير مشفرة (،PAP

dit Dial-in Profile		? ×
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
Check the authentication r	methods which are allowe	d for this connection.
Extensible Authentica	ation Protocol	
Select the EAP type whic	ch is acceptable for this p	olicy.
Protected EAP (PEAP)	<u> </u>	Configure
Microsoft Encrypted /	Authentication version <u>2</u> (I	MS-CHAP v2)
Microsoft Encrypted A	Authentication (MS-CHAP	ງ
Encrypted Authentica	ation (CHAP)	
Unencrypted Authent	tication (PAP, SPAP)	
Unauthenticated Access		
Allow remote PPP clie any authentication m	ents to connect without n ethod.	egotiating

علامة التبويب **خيارات متقدمة**. قم بإزالة كافة المعلمات الافتراضية وانقر فوق

Dial-in Constraints	, IP	Multilink
Authentication	Encryption	Advanced
Specify additional connect Access Server.	tion attributes to be retur	ned to the Remote
Parameters:		
Name	Vendor	Value
Add     Berror	ove <u>E</u> dit	
Add Remo	ove <u>E</u> dit	Cancel Apply
Add Bema	ove Edit OK	د Cancel <u>Apply</u>

RADIUS attributes:			Enumerable Attribute Information
Name	Vendor	Description 🔺	
Reply-Message	RADIUS Standard	Message to be displayed to user when authenticati	Attribute name:
Service-Type	RADIUS Standard	Type of service user has requested	Service-Type
Tunnel-Assignment-ID	RADIUS Standard	Tunnel to which a session is to be assigned	
Tunnel-Client-Auth-ID	RADIUS Standard	Name used by the tunnel initiator during the authen	Attribute number:
Tunnel-Client-Endpt	RADIUS Standard	IP address of the initiator end of the tunnel	
Tunnel-Medium-Type	RADIUS Standard	Transport medium to use when creating a tunnel to	þ
Tunnel-Password	RADIUS Standard	Password for authenticating to a remote server	
Tunnel-Preference	RADIUS Standard	Relative preference assigned to each tunnel when	Attribute format:
Tunnel-Pvt-Group-ID	RADIUS Standard	Group ID for a particular tunneled session	Enumerator
Tunnel-Server-Auth-ID	RADIUS Standard	Name used by the tunnel terminator during the auth	
Tunnel-Server-Endpt	RADIUS Standard	IP address of the server end of the tunnel	Allihuta value
Tunnel-Type	RADIUS Standard	Tunneling protocols to be used	Building Agne.
Vendor-Specific	RADIUS Standard	Used to support proprietary NAS features	Login
Cisco-AV-Pair	Cisco	Cisco AV Pair VSA	
Ignore-User-Dialin-Properties	Microsoft	Ignore the user's dial-in properties	
USR-ACCM-Type	U.S. Robotics, I	Description not available	
USR-AT-Call-Input-Filter	U.S. Robotics, I	Description not available	OK Cancel
USR-AT-Call-Output-Filter	U.S. Robotics, I	Description not available	
USR-AT-Input-Filter	U.S. Robotics, I	Description not available	
USR-AT-Output-Filter	U.S. Robotics, I	Description not available	
4		•	
		Add Close	

بعد ذلك، يلزمك تحديد السمة **الخاصة بالمورد** من قائمة سمات

#### .RADIUS

Add Attributes	<u>?</u> ×	ľ	Multivalued Attribute Information
To add an attribute to the Profile, select the attribut $\label{eq:RADIUS} RADIUS attributes;$	e and click Add		Attribute name: Vendor-Specific
Name         Vendor           Reply-Message         FADIUS Standard           Service-Type         FADIUS Standard           Turnel-Assignmant-ID         FADIUS Standard           Turnel-Assignmant-ID         FADIUS Standard           Turnel-Clerk-Endpt         FADIUS Standard           Turnel-Medium-Type         FADIUS Standard           Turnel-Pastword         FADIUS Standard           Turnel-Server-Auth-ID         FADIUS Standard           Turnel-Server-Endpt         FADIUS Standard           Turnel-Server-Endpt         FADIUS Standard           Turnel-Server-Endpt         RADIUS Standard           Turnel-Server-Endpt         RADIUS Standard           Turnel-Server-Endpt         RADIUS Standard           Turnel-Server-Endpt         RADIUS Standard           Usra-At-Cal-Input-Fiter         U.S. Robotics, L           USR-At-Cal-Input-Fiter         U.S. Robotics, L           USR-At-Cal-Input-Fiter         U.S. Robotics, L           USR-At-Cal-Uu	Description     Message to be displayed to user when authenticab     Type of service user has requested     Turnel to which a session is to be assigned     Name used by the tunnel initiator during the authen     IP address of the initiator end of the turnel     Transport medium to use when creating a tunnel fo     Password for authenticating to a remote server     Relative preference assigned to each turnel when     Group ID for a particular turneled session     Name used by the tunnel terminator during the auth     IP address of the server end of the tunnel     Turneling protocols to be used     Used to support proprietary NAS features     Cisco AV Pair VSA     Ignore the usef's dial-in properties     Description not available     Description not available     Description not available     Description not available     Description not available		Attribute number: 26 Attribute format: OctetString Attribute values: Vendor Value Move_Down Move_Down Ennove Ent.
	Add Close		0% Cancel

في الإطار التالي، طقطقت **يضيف** in order to حددت VSA جديد.يظهر نافذة معلومات السمة الخاصة بالمورد.تحت تحديد مورد خادم الوصول إلى الشبكة، أختر **إدخال رمز المورد**.دخلت البائع رمز ل Airespace VSAs. كود المورد ل Cisco Airespace VSAs **14179**.لأن هذه السمة تتفق مع مواصفات RADIUS RFC ل VSAs، أختر **نعم. إنها** 

Vendor-Specific	
Specify network access services and the service of	ver vendor.
Select from list:	RADIUS Standard
Enter Vendor Code:	14179
vendor specific attributes.	
<ul> <li>vendor specific attributes.</li> <li>Yes. It conforms.</li> <li>No. It does not conform.</li> </ul>	

**السمة**.دخلت في ال configure VSA (متوافق مع RFC) نافذة، البائع يعين سمة رقم، السمة شكل والسمة قيمة، أي يعتمد على ال VSA أن أنت تريد أن يستعمل.لإعداد معرف WLAN على أساس كل مستخدم:**اسم السمة**—Airespace-WLAN-id**رقم السمة المعين من قبل المورد**—1**تنسيق السمة**—عدد صحيح/عشريhian-id**وساله 1** 

	Configure VSA (RFC compliant)	? ×
	Vendor-assigned attribute number:	
	<u> </u>	
	Attribute format:	
	Decimal	<b></b>
	Attri <u>b</u> ute value:	
	2	
	,	
الإعداد ملف تعريف جودة المعرب ميرقيا	Airespace-OoS-level — i.e.ul	الخرمة على أساس كل مستخدما
المعين من قبل	اسمه — evel – العادة المرقع الممه الم	الحدمة على النباس بل مستحدم.ا <b>سم ا</b>
3 - برونز <b>مثال 2</b>	عشري <b>القيمة</b> —0 - فضة؛ 1 - ذهب؛ 2 - بلاتينيوم؛	ا <b>لمورد</b> —2 <b>تنسيق السمة</b> —عدد صحيح/
3 - برونز <b>مثال 2</b>	عشري <b>القيمة</b> —0 - فضة؛ 1 - ذهب؛ 2 - بلاتينيوم؛ <b>Configure ¥SA (RFC compliant)</b>	المورد—2تنسيق السمة—عدد صحيح∕: ▼ <b>؟</b>
3 - برونز <b>مثال 2</b>	عشري <b>القيمة</b> —0 - فضة؛ 1 - ذهب؛ 2 - بلاتينيوم؛ Configure VSA (RFC compliant) Vendor-assigned attribute number:	المورد—2تنسيق السمة—عدد صحيح/: الله المورد ا المورد المورد
3 - برونز <b>مثال 2</b>	عشري <b>القيمة</b> —0 - فضة؛ 1 - ذهب؛ 2 - بلاتينيوم؛ Configure VSA (RFC compliant) ⊻endor-assigned attribute number: 2	المورد—2تنسيق السمة—عدد صحيح/: الا ع: ?
3 - برونز <b>مثال 2</b>	عشري <b>القيمة</b> —0 - فضة؛ 1 - ذهب؛ 2 - بلاتينيوم؛ Configure VSA (RFC compliant) Vendor-assigned attribute number: 2	المورد—2تنسيق السمة—عدد صحيح/: الله الله المورد الم
3 - برونز <b>مثال 2</b>	عشري <b>القيمة</b> —0 - فضة؛ 1 - ذهب؛ 2 - بلاتينيوم؛ Configure VSA (RFC compliant) Vendor-assigned attribute number: 2 <u>Attribute format:</u>	المورد—2تنسيق السمة—عدد صحيح/: ▼ ؟
3 - بَرونزَمثالَ 2	عشري <b>القيمة</b> —0 - فضة؛ 1 - ذهب؛ 2 - بلاتينيوم؛ Configure VSA (RFC compliant) Vendor-assigned attribute number: 2 <u>A</u> ttribute format: Decimal	المورد—2تنسيق السمة—عدد صحيح/: ▼ ؟
3 - بَرونزَمثالَ 2	عشري <b>القيمة</b>	المورد—2تنسيق السمة—عدد صحيح/: ♥♥ ♥
3 - بَرونزَمثالَ 2	عشري <b>القيمة</b>	المورد—2تنسيق السمة—عدد صحيح/: ♥♥ ?
3 - بَرونزَمثالَ 2	عشري <b>القيمة</b> 0 - فضة؛ 1 - ذهب؛ 2 - بلاتينيوم؛ Configure VSA (RFC compliant) Vendor-assigned attribute number: 2 <u>Attribute format:</u> Decimal Attri <u>b</u> ute value: 3	المورد—2تنسيق السمة—عدد صحيح/: ▼ ? ▼
3 - بَرونزَمثالَ 2	عشري <b>القيمة</b>	المورد—2تنسيق السمة—عدد صحيح/: ▼ ?
3 - بَرونزَمثالَ 2	عشري <b>القيمة</b> 0 - فضة؛ 1 - ذهب؛ 2 - بلاتينيوم؛ Configure VSA (RFC compliant) Vendor-assigned attribute number: 2 <u>Attribute format:</u> Decimal Attri <u>b</u> ute value: 3	المورد—2تنسيق السمة—عدد صحيح/:
3 - بَرُونزَمْثَالَ 2	عشري <b>القيمة</b> 0-فضة؛ 1 - ذهب؛ 2 - بلاتينيوم؛ Configure VSA (RFC compliant) ⊻endor-assigned attribute number: 2 <u>A</u> ttribute format: Decimal Attri <u>b</u> ute value: 3	المورد—2تنسيق السمة—عدد صحيح/:

أساس كل مستخدم:**اسم السمة —** Airespace-DSCP**ترقيم السمة المعين من قبل المورد—3تنسيق السمة**—عدد صحيح/عشري**القيمة**—قيمة DSCP**مثال 3** 

	Configure VSA (RFC compliant)	? ×
	Vendor-assigned attribute number:	
	3	
	Attribute format:	
	Decimal	▼
	Attri <u>b</u> ute value:	
	46	
		OK Cancel
ــلإعداد علامة 802		
, من قبل	Airespace-802.1p-tagرقم السمة المعين	على أساس كل مستخدم: <b>اسم السمة</b> — السمية 10 من عن المقدم عنه من عن
	سریالعیمہ—علامہ OU2. 1Pمیں 4 Configure VSA (RFC compliant)	المورد—4تنسيق السمه—عدد صحيح/عنا × ?
	Vendor-assigned attribute number:	
	4	
	Attribute format:	
	Uecimai	
	Attri <u>b</u> ute value:	
	5	
		OK Cancel
لإعداد الواجهة (AN		······································
		2

على اساس كل مستخدم:**اسم السمة**—irespace-interface-name **المورد**—5**تنسيق السمة**—السلسلة**القيمة**—interface-name**مثال 5** 

? ×
<b>_</b>
_
OK Cancel
۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔
المورد—6تنسيق السمة—السله ♦♦♦♦
▼

- 8. ما إن يشكل أنت ال VSAs، طقطقت **ok** إلى أن أنت ترى المستعمل مرجع نافذة.
- 9. بعد ذلك، انقر فوق **إنهاء** لإكمال التكوين.يمكنك مشاهدة النهج الجديد ضمن نهج الوصول عن بعد.

🐤 Internet Authentication Service		
Action View 🛛 🗢 🔶 🛐 😼 😭		
Tree	Name	Order
Internet Authentication Service (Local) Clients Remote Access Logging Remote Access Policies	Arespace VSA	1

#### <u>مثال على التكوين</u>

في هذا المثال، يتم تكوين شبكة WLAN لمصادقة الويب. تتم مصادقة المستخدمين بواسطة خادم IAS RADIUS، ويتم تكوين خادم RADIUS لتخصيص نهج جودة الخدمة (QoS) على أساس كل مستخدم.

11.11			Save Co	infiguration Ping Logout P
	MONITOR WLANS CO	NTROLLER WIRELESS SECURITY MAN	AGEMENT COMMANDS	HELP
s	WLANs > Edit			< Back Apply
	WLAN ID	1		
s oups VLAN	WLAN SSID	SSID-WLC2		
	General Policies		Security Policies	
	Radio Policy	All	Laura 2 Canada	Mana
	Admin Status	C Enabled	Layer 2 Security	MAC Eitering
	Session Timeout (secs)	0		- Hare Hitering
	Quality of Service (QoS)	Silver (best effort)	Layer 3 Security	None 💌
	WMM Policy	Disabled 🗸		🕑 Web Policy *
	7920 Phone Support	🔝 Client CAC Limit 📋 AP CAC Limit		Authentication O Passthree
	Broadcast SSID	Enabled	Preauthenticatio	none 🛩
	Aironet IE	Enabled		-
	Allow AAA Override	🗹 Enabled	* Web Policy cannot and L2TP.	be used in combination with IP
	Client Exclusion	Enabled ** 60	** When client excl	usion is enabled, a timeout value
	DHCP Server	Timeout Value (secs)	to reset excluded cl *** CKIP is not sup	will require administrative overr ients) corted by 10xx APs
	DHCP Addr. Assignment	Required		
	Interface Name	internal 💌		
	MFP Version Required	1		
	MFP Signature Generation	(Global MFP Disabled)		
	H-REAP Local Switching			
	* H-REAP Local Switching and FORTRESS authentic	not supported with IPSEC, L2TP, PPTP, CRANITE ations.	E	
	Radius Servers			
		Authentication Servers Accounting Serve	0	
	Sarvar 1	IP:172.16.1.1. Port:1812 V none V		

كما يمكنك أن ترى من هذا الإطار، يتم تمكين مصادقة الويب، وخادم المصادقة هو 172.16.1.1، كما يتم تمكين تجاوز AAA على شبكة WLAN. تم تعيين إعداد جودة الخدمة الافتراضي لشبكة WLAN هذه إلى Silver.

على خادم IAS RADIUS، يتم تكوين سياسة وصول عن بعد تقوم بإرجاع السمة البرونزية لجودة الخدمة في طلب قبول RADIUS. ويتم القيام بذلك عند تكوين معرف فئة المورد (VSA) الخاص بسمة جودة الخدمة.

Configure ¥SA (RFC compliant)	? ×
⊻endor-assigned attribute number:	
2	
<u>A</u> ttribute format:	
Decimal	•
Attri <u>b</u> ute value:	
3	
OK	Cancel

راجع قسم <u>تكوين نهج الوصول عن بعد على IAS</u> في هذا المستند للحصول على معلومات تفصيلية حول كيفية تكوين نهج الوصول عن بعد على خادم IAS.

بمجرد تكوين خادم IAS و WLC و LAP لهذا الإعداد، يمكن للعملاء اللاسلكيين إستخدام مصادقة الويب للاتصال.

#### <u>التحقق من الصحة</u>

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

عندما يتصل المستخدم بشبكة WLAN بمعرف مستخدم وكلمة مرور، يقوم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بتمرير بيانات الاعتماد إلى خادم IAS RADIUS الذي يصادق المستخدم في مقابل الشروط وملف تعريف المستخدم الذي تم تكوينه في نهج الوصول عن بعد. إذا نجحت مصادقة المستخدم، يرجع خادم RADIUS طلب قبول RADIUS الذي يحتوي أيضا على قيم تجاوز AAA. في هذه الحالة، يتم إرجاع سياسة جودة الخدمة الخاصة بالمستخدم.

يمكنك إصدار الأمر debug aaa all enable لعرض تسلسل الأحداث التي تحدث أثناء المصادقة. هنا نموذج للمخرجات:

Cisco Controller) > debug aaa all enable) Wed Apr 18 18:14:24 2007: User admin authenticated Wed Apr 18 18:14:24 2007: 28:1f:00:00:00:00 Returning AAA Error 'Success' (0) for mobile 28:1f:00:00:00:00 Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c structureSize.....70 Wed Apr 18 18:14:24 2007: Wed Apr 18 18:14:24 2007: resultCode.....0 Wed Apr 18 18:14:24 2007: protocolUsed.....0x0000008 proxvState 28:1F:00:00:00:00-00:00 :Wed Apr 18 18:14:24 2007: Packet contains 2 AVPs .....Wed Apr 18 18:14:24 2007: AVP[01] Service-Type (0x0000006 (6) (4 bytes .....Wed Apr 18 18:14:24 2007: AVP[02] Airespace / WLAN-Identifier (0x00000000 (0) (4 bytes Wed Apr 18 18:14:24 2007: User admin authenticated Wed Apr 18 18:14:24 2007: 29:1f:00:00:00:00 Returning AAA Error 'Success' (0) for mobile 29:1f:00:00:00:00 Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c Wed Apr 18 18:14:24 2007: structureSize.....70 Wed Apr 18 18:14:24 2007: resultCode.....0 Wed Apr 18 18:14:24 2007: protocolUsed.....0x00000008 proxyState 29:1F:00:00:00:00-00:00 :Wed Apr 18 18:14:24 2007: Packet contains 2 AVPs .....Wed Apr 18 18:14:24 2007: AVP[01] Service-Type (0x0000006 (6) (4 bytes AVP[02] Airespace / WLAN-Identifier .....Wed Apr 18 18:14:24 2007: (0x00000000 (0) (4 bytes Wed Apr 18 18:15:08 2007: Unable to find requested user entry for User-VLAN10 Wed Apr 18 18:15:08 2007: AuthenticationRequest: 0xa64c8bc Wed Apr 18 18:15:08 2007: Callback.....0x8250c40 protocolType.....0x0000001 Wed Apr 18 18:15:08 2007: proxyState AC:E6:57-00:00:00:40:96 (Wed Apr 18 18:15:08 2007: Packet contains 8 AVPs (not shown Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Successful transmission of Authentication Packet id 26) to 172.16.1.1:1812, proxy state 00:40:96:ac:e6:57-96:ac) ....h...

Wed Apr 18 18:15:08 2007: 00000010: 00 00 00 00 01 0d 55 73 65 72 2d 56 4c 41 4e 31 User-VLAN1..... Wed Apr 18 18:15:08 2007: 00000020: 30 02 12 fa 32 57 ba 2a ba 57 38 11 bc 9a 5d 59 2W.\*.W8...]Y...0 Wed Apr 18 18:15:08 2007: 00000030: ed ca 23 06 06 00 00 00 01 04 06 ac 10 01 1e 20 Wed Apr 18 18:15:08 2007: 00000040: 06 57 4c 43 32 1a 0c 00 00 37 63 01 06 00 00 00 ....WLC2....7c. Wed Apr 18 18:15:08 2007: 00000050: 01 1f 0a 32 30 2e 30 2e 30 2e 31 1e 0d 31 37 32 172..20.0.0.1... Wed Apr 18 18:15:08 2007: 00000060: 2e 31 36 2e 31 2e 33 30 .16.1.30 Wed Apr 18 18:15:08 2007: 00000000: 02 la 00 46 3f cf lb cc e4 ea 41 3e 28 7e cc bc ..~)<F?....A... Wed Apr 18 18:15:08 2007: 00000010: 00 e1 61 ae 1a 0c 00 00 37 63 02 06 00 00 03 .....a....7c.. Wed Apr 18 18:15:08 2007: 00000020: 06 06 00 00 00 01 19 20 37 d0 03 e6 00 00 01 37 7.....7..... Wed Apr 18 18:15:08 2007: 00000030: 00 01 ac 10 01 01 01 c7 7a 8b 35 20 31 80 00 00 ...z.5.1..... Wed Apr 18 18:15:08 2007: 00000040: 00 00 00 00 1b Wed Apr 18 18:15:08 2007: \*\*\*\*Enter processIncomingMessages: response code=2 Wed Apr 18 18:15:08 2007: \*\*\*\*Enter processRadiusResponse: response code=2 Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Access-Accept received from RADIUS server for mobile 00:40:96:ac:e6:57 receiveId = 0 172.16.1.1 Wed Apr 18 18:15:08 2007: AuthorizationResponse: 0x9802520 Wed Apr 18 18:15:08 2007: structureSize.....114 Wed Apr 18 18:15:08 2007: resultCode.....0 Wed Apr 18 18:15:08 2007: protocolUsed.....0x00000001 proxyState AC:E6:57-00:00:00:40:96 :Wed Apr 18 18:15:08 2007: Packet contains 3 AVPs ......Wed Apr 18 18:15:08 2007: AVP[01] Airespace / QOS-Level (0x0000003 (3) (4 bytes AVP[02] Service-Type (0x0000001 (1) (4 bytes .....Wed Apr 18 18:15:08 2007: AVP[03] Class (DATA (30 bytes Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Applying new AAA override for station ac:e6:57:00:40:96 Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57 source: 48, valid bits: 0x3 qosLevel: 3, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 ' :vlanIfName: '', aclName Wed Apr 18 18:15:12 2007: AccountingMessage Accounting Start: 0xa64c8bc :Wed Apr 18 18:15:12 2007: Packet contains 13 AVPs .....Wed Apr 18 18:15:12 2007: AVP[01] User-Name (User-VLAN10 (11 bytes .....Wed Apr 18 18:15:12 2007: AVP[02] Nas-Port (0x0000001 (1) (4 bytes (0xac10011e (-1408237282) (4 bytes AVP[04] NAS-Identifier .....Wed Apr 18 18:15:12 2007: (0x574c4332 (1464615730) (4 bytes .....Wed Apr 18 18:15:12 2007: AVP[05] Airespace / WLAN-Identifier (0x0000001 (1) (4 bytes AVP[06] Acct-Session-Id .....Wed Apr 18 18:15:12 2007: (4626602c/00:40:96:ac:e6:57/16 (29 bytes .....Wed Apr 18 18:15:12 2007: AVP[07] Acct-Authentic (0x0000001 (1) (4 bytes ......Wed Apr 18 18:15:12 2007: AVP[08] Tunnel-Type (0x000000d (13) (4 bytes .....Wed Apr 18 18:15:12 2007: AVP[09] Tunnel-Medium-Type (0x0000006 (6) (4 bytes

AVP[10] Tunnel-Group-Id	Wed Apr 18 18:15:12 2007:
	(0x3230 (12848) (2 bytes
AVP[11] Acct-Status-Type	
	(0x0000001 (1) (4 bytes
AVP[12] Calling-Station-Id	
	(bytes 8) 20.0.0.1
AVP[13] Called-Station-Id	
	(bytes 11) 172,16,1,30

كما يمكنك أن ترى من المخرجات، فإن المستخدم تتم مصادقته. ثم، يتم إرجاع قيم تجاوز AAA باستخدام رسالة قبول RADIUS. وفي هذه الحالة، يتم إعطاء المستخدم سياسة جودة الخدمة (QoS) البرونزية.

يمكنك التحقق من ذلك على واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) كذلك. فيما يلي مثال:

	MONITOR WLANS CONTR	OLLER WIRELESS SECU	RITY MANAGEMENT COMM	Save Configuration Ping Logout P IANDS HELP
nitor	Clients > Detail			< Back Link Test Remov
imary	Client Properties		AP Properties	
listics Introller	MAC Address	00:40:96:ac:e6:57	AP Address	00:0b:85:5b:fb:d0
rts	IP Address	20.0.0.1	AP Name	ap:5b:fb:d0
eless one APs	User Name	User-VLAN10	AP Type	802.11a
own Rogue APs	Port Number	1	WLAN SSID	SSID-WLC2
gue Clients hoc Rogues	Interface	internal	Status	Associated
2.11a Radios 2.11b/g Radios	VLAN ID	20	Association ID	1
ents	CCX Version	CCXv3	802.11 Authentication	Open System
DIUS Servers	E2E Version	Not Supported	Reason Code	0
	Mobility Role	Local	Status Code	0
	Mobility Peer IP Address	N/A	CF Pollable	Not Implemented
	Policy Manager State	RUN	CF Poll Request	Not Implemented
	Security Information		Short Preamble	Not Implemented
	Security Policy Completed	Yes	PBCC	Not Implemented
	Policy Type	N/A	Channel Agility	Not Implemented
	Encryption Cipher	None	Timeout	0
	EAP Type	N/A	WEP State	WEP Disable
	Quality of Service Propert	ies		
	WMM State	Disabled		
	QoS Level	Bronze		
	Diff Serv Code Point (DSCP)	disabled		
	802.1p Tag	disabled		

**ملاحظة:** ملف تعريف جودة الخدمة الافتراضي ل SSID هذا هو Silver. ومع ذلك، نظرا لتحديد تجاوز المصادقة والتفويض والمحاسبة (AAA) وتكوين المستخدم باستخدام ملف تعريف جودة الخدمة (QoS) البرونزي على خادم IAS، يتم تجاوز ملف تعريف جودة الخدمة الافتراضي.

## استكشاف الأخطاء وإصلاحها

أنت يستطيع استعملت ال **debug aaa all enable** أمر على ال WLC أن يتحرى التشكيل. يتم عرض مثال على إخراج تصحيح الأخطاء هذا في شبكة عمل في قسم <u>التحقق</u> من هذا المستند.

**ملاحظة:** ارجع إلى <u>معلومات مهمة حول أوامر التصحيح</u> قبل إستخدام أوامر debug.

#### معلومات ذات صلة

- <u>دليل تكوين وحدة تحكم شبكة LAN اللاسلكية، الإصدار 4.0 من Cisco</u>
- <u>تقييد الوصول إلى شبكة WLAN استنادا إلى SSID باستخدام WLC ومثال تكوين ACS الآمن من Cisco</u>
  - <u>دعم المنتج اللاسلكي</u>
  - الدعم التقني والمستندات Cisco Systems

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما