# Cisco Aironet VSA's op Microsoft IAS Radius Server Configuratievoorbeeld

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Achtergrondinformatie De IAS voor Airespace VSA's configureren De WLC configureren als een AAA-client in de IAS Het externe toegangsbeleid op de IAS configureren Configuratievoorbeeld Verifiëren Problemen oplossen Gerelateerde informatie

# **Inleiding**

Dit document toont hoe u een Microsoft Internet Verification Service (IAS)-server kunt configureren ter ondersteuning van Cisco Aironet Vendor Specific Attributes (VSA's). De leveranciercode voor Cisco Airesponders is **14179**.

# Voorwaarden

### Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Kennis van de wijze waarop u een IAS-server moet configureren
- Kennis van de configuratie van Lichtgewicht Access Point (LAP's) en Cisco draadloze LANcontrollers (WLC's)
- Kennis van Cisco Unified Wireless Security-oplossingen

#### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

Microsoft Windows 2000-server met IAS

- Cisco 4400 WLC-software versie 4.0.206.0
- Cisco 1000 Series LAP's
- 802.11 a/b/g draadloze clientadapter met firmware 2.5
- Aironet Desktop Utility (ADU) versie 2.5

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

**Opmerking:** Dit document is bedoeld om de lezer een voorbeeld te geven over de configuratie die op de IAS-server vereist is ter ondersteuning van VSA's van Cisco Airespo. De DIA-serverconfiguratie die in dit document wordt gepresenteerd, is in het laboratorium getest en werkt zoals verwacht. Als u de IAS-server niet kunt configureren, neemt u contact op met Microsoft voor ondersteuning. Cisco TAC ondersteunt Microsoft Windows-serverconfiguratie niet.

Dit document gaat ervan uit dat de WLC is ingesteld voor een eenvoudige bediening en dat de LAP's zijn geregistreerd op de WLC. Als u een nieuwe gebruiker bent die probeert om de WLC in te stellen voor basisbediening met LAN's, raadpleegt u Lichtgewicht AP (LAP)-registratie naar een draadloze LAN-controller (WLC).

#### **Conventies**

Raadpleeg <u>Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor</u> meer informatie over documentconventies.

# **Achtergrondinformatie**

In de meeste draadloze LAN-systemen (WLAN) heeft elk WLAN een statisch beleid dat van toepassing is op alle klanten die bij een serviceset ID (SSID) zijn gekoppeld. Hoewel krachtig, heeft deze methode beperkingen omdat het van cliënten vereist om met verschillende SSIDs te associëren om verschillend QoS en veiligheidsbeleid te erven.

Maar de Cisco draadloze LAN-oplossing ondersteunt identiteitsnetwerken, waardoor het netwerk kan adverteren met één SSID en bepaalde gebruikers om verschillende QoS- of beveiligingsbeleid te erven op basis van hun gebruikersprofielen. Het specifieke beleid dat u kunt controleren met behulp van identiteitsnetwerken is onder meer:

- Quality-of-Service—Wanneer deze in een RADIUS-toegangsaccepteren wordt aangeboden, heeft de QoS-Level-waarde te boven de QoS-waarde die in het WLAN-profiel is gespecificeerd.
- ACL-wanneer de eigenschap Toegangscontrolelijst (ACL) aanwezig is in de RADIUStoegangscontrole Accept, past het systeem de ACL-naam op het clientstation toe nadat dit voor authentiek is verklaard. Dit heeft betrekking op ACL's die aan de interface zijn toegewezen.
- VLAN-Wanneer een VLAN-interface-naam of VLAN-tag in een RADIUS-toegangscontrole aanwezig is, plaatst het systeem de client op een specifieke interface.
- WLAN-id Wanneer de WLAN-ID eigenschap in de RADIUS-toegangscontrole aanwezig is, past het systeem de WLAN-ID (SSID) op het clientstation toe nadat deze voor authentiek is verklaard. De WLAN-id wordt door de WLC verzonden in alle gevallen van verificatie behalve

IPSec. In het geval van web authenticatie, als de WLC een WLAN-ID eigenschap in de authenticatiereactie van de AAA-server ontvangt en deze niet overeenkomt met de ID van de WLAN, wordt verificatie verworpen. Andere beveiligingsmethoden doen dat niet.

- **DSCP-waarde** Wanneer deze in een RADIUS-toegangsbestand aanwezig is, heeft de DSCP-waarde voorrang op de DSCP-waarde die in het WLAN-profiel is gespecificeerd.
- **802.1p-Tag** Wanneer u een RADIUS-toegangsaccepteren hebt, heeft de 802.1p waarde te veel waarde dan gespecificeerd in het WLAN-profiel.

**Opmerking:** de functie VLAN ondersteunt alleen MAC-filtering, 802.1X en Wi-Fi Protected Access (WAP). De VLAN-functie ondersteunt geen webverificatie of IPSec. De lokale MAC Filter database van het besturingssysteem is uitgebreid om de interfacenaam op te nemen. Hiermee kunnen lokale MAC-filters specificeren welke interface de client moet worden toegewezen. Er kan ook een afzonderlijke RADIUS-server worden gebruikt, maar de RADIUS-server moet worden gedefinieerd met behulp van de Security menu's.

Raadpleeg Identiteitsnetwerken configureren voor meer informatie over identiteitsnetwerken.

# De IAS voor Airespace VSA's configureren

Om de IAS voor VSA's te kunnen configureren moet u deze stappen voltooien:

- 1. De WLC configureren als een AAA-client in de IAS
- 2. <u>Het externe toegangsbeleid op de IAS configureren</u>

**Opmerking:** de VSA's zijn ingesteld onder het beleid voor externe toegang.

#### De WLC configureren als een AAA-client in de IAS

Voltooi deze stappen om de WLC te configureren als een AAA-cliënt in de IAS:

 Klik op Programma's > Administratieve Gereedschappen > Internet Verificatieservice om IAS te starten op de Microsoft 2000server.



- 2. Klik met de rechtermuisknop op de map **Clients** en kies **Nieuwe client** om een nieuwe RADIUS-client toe te voegen.
- Voer in het venster Add Client de naam van de client in en kies RADIUS als protocol. Klik vervolgens op Volgende. In dit voorbeeld is de naam van de client WLC-1. Opmerking: standaard is het protocol ingesteld op RADIUS.

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

4. Voer in het venster RADIUS-client toe het IP-adres van de client, de client-verkoper en het gedeelde geheim in. Klik op Voltooien nadat u de clientinformatie hebt ingevoerd.Dit voorbeeld toont een client met de naam WLC-1 met een IP-adres van 172.16.1.30. De client-verkoper wordt op Cisco ingesteld en het gedeelde geheim is cisco123:

Add RADIUS Client	×
Client Information Specify information regarding the client.	
Client address (IP or DNS):	
172.16.1.30	⊻erify
Client-Vendor:	
Cisco	▼
Client must always send the signature attribute in the reques	st
Shared secret:	
Confirm shared secret:	
< <u>B</u> ack	Finish Cancel

Met deze informatie wordt de WLC genaamd WLC-1 toegevoegd als AAA-client van de IASserver.

🏸 Internet Authentication Service	
Tree Friendly Name Address Protocol Client-Vendor	
Treenet Authentication Service (Loca)  Remote Access Logging  Remote Access Policies	

De volgende stap is een beleid voor toegang op afstand te maken en de VSA's te configureren.

#### Het externe toegangsbeleid op de IAS configureren

Voltooi deze stappen om een nieuw beleid voor externe toegang op de IAS te vormen:

- 1. Klik met de rechtermuisknop op **beleid voor toegang op afstand** en kies **Nieuw Remote AccessMS-beleid**.Het venster Policy Name verschijnt.
- 2. Voer de naam van het beleid in en klik op **Volgende**.

e	mote Access Policy
olio	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
i	Policy mendly name:
ļ	Allespace VSA
	<ul> <li>K Back Next &gt; Cano</li> </ul>

3. Selecteer in het volgende venster de voorwaarden waarvoor het beleid voor externe toegang van toepassing zal zijn. Klik op **Add** om de voorwaarden te selecteren.

Add Remote Access Policy Conditions Determine the conditions to match.	×	Select Attribute Select the type of attribute Attribute types:	e to add, and then click the Add button.
Specify the conditions to match.		Name           Called-Station-Id           Caling-Station-Id           Client-Friendly-Name           Client-Praddress           Client-Vendor           Day-And-Time-Restric           Framed-Protocol           NAS-Identitier           NAS-Identitier           NAS-Identitier           Service-Type           Service-Type           Tunnel-Type           Windows-Groups	Description Phone number dialed by user Phone number from which call originated Friendly name for the RADIUS client. (IAS only) IP address of RADIUS client. (IAS only) Manufacturer of RADIUS proxy or NAS. (IAS only) Time periods and days of week during which use The protocol to be used String identifying the NAS originating the request IP address of the task originating Type of service user has requested Tunneling protocols to be used Windows groups that user belongs to
Add Bernove Edt	<u>B</u> ack <u>N</u> ext> Cancel	<u>.</u>	Add Cancel

4. Selecteer in het menu Eigenschappen de volgende eigenschappen: **Client-IP-Adres**-Voer het IP-adres van de AAA-client in. In dit voorbeeld, wordt het IP van de WLCs adres ingevoerd zodat het beleid op pakketten van de WLC van toepassing

Client-IP-Address		? ×
Type a word or a wild card	(for example, abc.*):	
172.16.1.30		
	ОК	Cancel
is		Windows

**Groepen**-Selecteer de Windows-groep (de gebruikersgroep) waarvoor het beleid van toepassing is. Hierna volgt een

201	B Groups	? ×
	The following groups are currently in this condition.	
	<u>G</u> roups:	
	Name	
	CAT-TD-2K\Test-Clients	
voorboold:	Add <u>R</u> emove	Cancel

Add Remote Access Policy	×
Conditions Determine the conditions to match.	
Specify the conditions to match.	
Conditions:	1
Windows-Groups matches "CAT-TD-2K\Test-Clients"	
A <u>d</u> d <u>R</u> emove <u>E</u> dit	
< <u>B</u> ack <u>N</u> ext > Cano	cel

Dit voorbeeld laat slechts twee voorwaarden zien. Als er meer voorwaarden zijn, kunt u deze voorwaarden ook toevoegen en op **Volgende** klikken.Het venster Access verschijnt.

 Kies in het venster Toegang op afstand verlenen.Nadat u deze optie hebt geselecteerd, krijgt de gebruiker toegang, mits de gebruiker de gespecificeerde voorwaarden aanpast (uit stap 2).

dd Remo	ote Access Policy
Permis	sions
De	termine whether to grant or deny remote access permission.
Yo	u can use a Remote Access Policy either to grant certain access privileges to a out of users, or to act as a filter and deny access privileges to a group of users
gr. If :	where matches the specified conditions:
	Contractes the specified conditions.
0	Deny remote access permission
	< <u>B</u> ack <u>N</u> ext> Cancel

- 6. Klik op Volgende.
- 7. De volgende stap is het instellen van het gebruikersprofiel.Ook al zou u hebben opgegeven dat gebruikers op basis van de voorwaarden toegang geweigerd of verleend zouden moeten worden, het profiel kan nog steeds worden gebruikt als de voorwaarden van dit beleid op een per-gebruiker-basis worden overschreven.

×
-

Klik om het gebruikersprofiel te configureren op **Profiel bewerken** in het venster Gebruikersprofiel.Het venster Profiel bewerken

dit Dial-in Profile			Ľ	? ×
Authentication	Encryption	1	Advanced	[
Dial-in Constraints	IP		Multilink	-i I
Disconnect if idle for		1	≓ min.	
🔲 Restrict <u>m</u> aximum sess	ion to:	1	⊥ min.	
Restrict access to the	following days and tin	nes: —		- 11
	<u>E</u> dit			
Restrict <u>D</u> ial-in to this r	number only:			-
Restrict Dial-in media:				
			<b></b>	
Token Ring				
Wireless - IEEE 802.1	1			
Wireless - Other				
Cable			<b>_</b>	
				┘┃╠
	OF	Canaal	1 America	
		Cancel		

verschijnt.

op het tabblad **Verificatie** en kies vervolgens de verificatiemethode die in WLAN wordt gebruikt.Dit voorbeeld gebruikt Unencryptie Verificatie (PAP,

Edit Dial-in Profile		? ×
Dial-in Constraints Authentication	IP Encryption	Multilink     Advanced
Check the authentication r	methods which are allowe	ed for this connection.
Select the EAP type which	ch is acceptable for this p	policy.
Microsoft Encrypted	Authentication version <u>2</u>	MS-CHAP v2)
Microsoft Encrypted /	Authentication (MS-CHAF	- -)
Encrypted Authentica     Unencrypted Authentica	ation (CHAP) tication (PAP, SPAP)	
Unauthenticated Access	8	
Allow remote <u>P</u> PP clive any authentication m	ents to connect without r ethod.	negotiating
	OK C.	ancel <u>A</u> pply

het tabblad Geavanceerd. Verwijder alle standaardparameters en klik op

Dial-in Constraints	Í IP	Multilink
Authentication	Encryption	Advanced
Specify additional connect Access Server. Parameters:	tion attributes to be retu	rned to the Remote
Name	Vendor	Value

cteer in het venster Add Attributes de optie Service-Type en kies vervolgens de Loginwaarde uit het volgende

#### venster.

A	ld Attributes		<u> </u>	
	To add an attribute to the Prof	ile, select the attribute	e and click Add.	
1	RADIUS attributes:			Enumerable Attribute Information
	Name	Vendor	Description 🔺	
	Name Reply-Message Service:Type Tunnel-Assignment-ID Tunnel-Dient-Endpt Tunnel-Dient-Endpt Tunnel-Paseword Tunnel-Preference Tunnel-Preference Tunnel-Preference Tunnel-Preference Tunnel-Server-Auth-ID Tunnel-Server-Auth-ID Tunnel-Server-Endpt Tunnel-Type Vendor-Specific Cisco-AV-Pair Ignore-User-Dialin-Properties USR-ADCM-Type USR-AT-Cal-Input-Filter USR-AT-Cal-Input-Filter USR-AT-Cal-Output-Filter USR-AT-Output-Filter	Vendor RADIUS Standard RADIUS Standard U.S. Robotics, I U.S. Robotics, I U.S. Robotics, I U.S. Robotics, I	Description Message to be displayed to user when authenticati Type of service user has requested Tunnel 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 tunnel Transport medium to use when creating a tunnel to Password for authenticating to a remote server Relative preference assigned to each tunnel when Group ID for a particular tunneled ression Name used by the tunnel tunnel do each tunnel when Group ID for a particular tunneled ression Name used by the tunnel tunnel do each tunnel Used to support proprietary NAS features Circo AV Pair VSA Ignore the user's dialin properties Description not available	Attribute name: Service-Type Attribute number: 6 Attribute format: Enumerator Attribute value: Login
			Add Close	

# Vervolgens moet u de **leverancierspecifieke** eigenschap van de RADIUS-lijst selecteren.

Ad	ld Attributes		<u>? ×</u>	ŀ	Multivalued Attribute Information	? ×
F	To add an attribute to the Prof RADIU <u>S</u> attributes:	ile, select the attribute	e and blick Add		Attribute name: Vendor-Specific	
	Name	Vendor	Description	L		
Reply-Message RADIUS Standard Message to be displayed to user when authentication Attr		Attribute number:				
	Service-Type	RADIUS Standard	Type of service user has requested	L	26	
	Tunnel-Assignment-ID	RADIUS Standard	Tunnel to which a session is to be assigned	L		
	Tunnel-Client-Auth-ID	RADIUS Standard	Name used by the tunnel initiator during the authen	L	Attribute format:	
	Tunnel-Client-Endpt	RADIUS Standard	IP address of the initiator end of the tunnel	L	OctelString	
	Tunnel-Medium-Type	RADIUS Standard	Transport medium to use when creating a tunnel fo	L	locassid	
	Tunnel-Pastword	RADIUS Standard	Password for authenticating to a remote server	L	Attribute wakter:	
	Turnel-Preference	DADILIC Standard	Fielative preference assigned to each tunnel when Group ID for a particular travailed persion	L		
	Turnel-Server-Auth-ID	RADIUS Standard	Name used by the transitionator during the auth	L	Vendor Value	Move Up
	Turnel-Server-Endpt	BADIUS Standard	IP address of the server end of the tunnel	L		
	Tunnel-Tyne	BADILIS Standard	Tunneling protocols to be used	L		Move <u>D</u> own
	Vendor-Specific	RADIUS Standard	Used to support proprietary NAS features	L		·····
	Cisco-AV-Pair	Cisco	Cisco AV Pair VSA	L		<u>: 800 ;</u>
	Ignore-User-Dialin-Properties	Microsoft	Ignore the user's dial-in properties	L		
	USR-ACCM-Type	U.S. Robolics, I	Description not available	L		Femane
	USR-AT-Call-Input-Filter	U.S. Robolics, I	Description not available	L		2.0
	USR-AT-Call-Output-Filter	U.S. Robolics, I	Description not available	L		<u>E</u> 60
	USB-AT-Input-Filter	U.S. Robolics, I	Description not available	L		
	USR-AT-Output-Filter	U.S. Robolics, I	Description not available	L		
	4		E E	L		
			Add Close		0K	Cancel

Klik in het volgende venster op **Add** om een nieuwe VSA te selecteren.Het venster Informatie over leverancierspecifieke kenmerken verschijnt.Selecteer onder Verkenner van netwerktoegangsserver de optie **Verkopers code invoeren**.Voer de leveranciercode in voor VSA's. De leveranciercode voor Cisco Airesponders is **14179**.Omdat deze eigenschap met de RADIUS RFC specificatie voor VSAs in overeenstemming is, kies **Ja. Het is in** 

Vendor-Specific	
1.0.000.000000	
Specify network access	server vendor.
C Select from list:	RADIUS Standard
Enter Vendor Code:	14179
Specify whether the attri vendor specific attribute	ibute conforms to the RADIUS RFC specification s.
Specify whether the attri vendor specific attribute Yes. It conforms.	ibute conforms to the RADIUS RFC specification s.
Specify whether the attri vendor specific attribute Yes. It conforms. No. It does not confo	ibute conforms to the RADIUS RFC specification s. orm.
Specify whether the attrivendor specific attribute Yes. It conforms No. It does not conform Configure Attribute	ibute conforms to the RADIUS RFC specification s. orm.
Specify whether the attrivendor specific attribute Yes. It conforms. No. It does not conformation of the configure Attribute	ibute conforms to the RADIUS RFC specification s. orm.

#### overeenstemming.

Klik op **Eigenschappen configureren**.Typ in het venster Configure VSA (RFC compatibel) het leveranciernummer, de notatie en de waarde van Kenmerken, die afhankelijk zijn van de

VSA die u wilt gebruiken.Voor het instellen van de WLAN-ID op een gebruikersbasis:**Naam**: **ABBYY**-WLAN-id**Toewijzingsnummer van de verkoper** - 1**Opmaak van kenmerken**: geïntegreerd/decimaal**Waarde**—WLAN-id**Voorbeeld 1** 

Configure VSA (RFC compliant)		? ×
Vendor-assigned attribute number:		
1		
<u>A</u> ttribute format:		
Decimal		•
Attri <u>b</u> ute value:		
2		
	OK	Cancel

Voor het instellen

van het QoS-profiel per gebruiker:**Naam**: ABBYY-ABBYY QoS-niveau**Aan de verkoper toegewezen attributennummer — 20pmaak van kenmerken**:

	? ×
	<b>•</b>
ОК С	ancel
	OK C

Voor het instellen van de DSCP-waarde per gebruiker:**Naam** van **kenmerk**—Airespace-DSCP**Toewijzing van verkoper**:3**Opmaak van kenmerken**: geïntegreerd/decimaal**Waarde**—DSCP-

waardeVoorbeeld 3

	Configure VSA (RFC compliant)	
	Vendor-assigned attribute number:	
	3	
	Attribute format:	
	Decimal	
	Attri <u>b</u> ute value:	
	46	
	OK Cancel	
ļ		Voor het instellen

van de 802.1p-tag per gebruiker: Naam van kenmerk: Airespace-802.1p-Tag**Toewijzingsnummer van de verkoper**—4**Opmaak van kenmerken**: geïntegreerd/decimaal**Waarde**: 802.1p-label**Voorbeeld 4** 

Configure VSA (RFC compliant)	? ×
⊻endor-assigned attribute number:	
4	
Attribute format:	
Decimal	▼
Attri <u>b</u> ute value:	
5	
	OK Cancel
	Vo

Voor het instellen

van de interface (VLAN) per gebruiker:**Naam**:interface-interface-naam van **kenmerkEigendomsnummer van de verkoper**—5**Opmaak**-string van **kenmerkenWaarde**—interface-naam**Voorbeeld 5** 

Configure VSA (RFC compliant)		? ×
Vendor-assigned attribute number:		
5		
Attribute format:		
String		-
Attri <u>b</u> ute value:		
vlan10		
·		
	OK Can	cel

Om ACL op een per-

gebruiker-basis in te stellen:**Naam** van **kenmerk**—Airespace-ACL-naam**Toewijzingsnummer** van de verkoper—6**Opmaak**-string van **kenmerkenWaarde**—ACL-naam**Voorbeeld 6** 

Configure VSA (RFC compliant)		? ×
Vendor-assigned attribute number:		
6		
Attribute format:		
String		<b>_</b>
Attri <u>b</u> ute value:		
ACL1		
· · · · · · · · · · · · · · · · · · ·		
	OK	Cancel

- 8. Nadat u de VSA's hebt ingesteld, klikt u op **OK** totdat u het venster Gebruikersprofiel ziet.
- 9. Klik vervolgens op **Voltooien** om de configuratie te voltooien.U kunt het nieuwe beleid zien onder het beleid voor toegang op afstand.

🐤 Internet Authentication Service				
Action View   ← → 🗈 🖬 🔩 😭				
Tree	Name	Order		
Internet Authentication Service (Local) Clients Remote Access Logging Remote Access Policies	Rirespace VSA	1		

### **Configuratievoorbeeld**

In dit voorbeeld wordt een WLAN geconfigureerd voor web-verificatie. Gebruikers worden geauthentiseerd door de IAS RADIUS-server en de RADIUS-server is ingesteld om het QoSbeleid per gebruiker toe te wijzen.

A A A A A A A A A A A A A A A A A A A			Save Co	anguradon Ping Logout Refres	
AL. AL. PROPERTY	MONITOR WLANS CO	NTROLLER WIRELESS SECURITY MANA	GEMENT COMMANDS	HELP	
MLANS	WLANs > Edit			< Back Apply	
WLANS WLANS	WLAN ID WLAN SSID	1 SSID-WLC2			
AP Groups VLAN	General Policies		Security Policies		
	Radio Policy Admin Status	All 💌	Layer 2 Security	None	
	Session Timeout (secs) Quality of Service (QoS) WMM Policy	0 Silver (best effort)	Layer 3 Security	None	
	7920 Phone Support Broadcast SSID	Client CAC Limit AP CAC Limit	Preauthenticatio	Authentication      Passthrough     none	
	Aironet IE Allow AAA Override	Enabled	* Web Policy cannot be used in combination with IPsec and L2TP.		
	Client Exclusion DHCP Server	Enabled ** 60     Timeout Value (secs)     Override	** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients) *** CKIP is not supported by 10xx APs		
	DHCP Addr. Assignment	Required			
	MFP Version Required	1			
	MFP Signature Generation H-REAP Local Switching	Global MFP Disabled)			
	* H-REAP Local Switching and FORTRESS authentice	not supported with IPSEC, L2TP, PPTP, CRANITE tions.			
	Radius Servers				
		Authentication Servers Accounting Servers			

Zoals u vanuit dit venster kunt zien, is Web Authenticatie ingeschakeld, is de authenticatieserver 172.16.1.1 en AAA Override is ook ingeschakeld op het WLAN. De standaard QoS-instelling voor dit WLAN wordt ingesteld op Silver.

Op de IAS RADIUS-server is een beleid voor externe toegang ingesteld dat de QoS-eigenschap Bronze in de RADIUS-modus accepteert. Dit gebeurt wanneer u de VSA die specifiek is voor de QoS eigenschap configureren.

Configure VSA (RFC compliant)	?	×
Vendor-assigned attribute number:		1
2		
Attribute format:		
Decimal	▼	
Attri <u>b</u> ute value:		,
3		
		1
	OK Cancel	

Zie het <u>Configureren van het beleid voor externe toegang in de IAS-</u>sectie van dit document voor gedetailleerde informatie over de manier waarop u een Afstandstoegangsbeleid op de IAS-server kunt configureren.

Zodra de IAS-server, de WLC en de LAP voor deze instelling zijn geconfigureerd, kunnen de draadloze klanten gebruik maken van web-authenticatie om verbinding te maken.

## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Wanneer de gebruiker zich met een gebruikersid en een wachtwoord op WLAN aansluit, geeft de WLC de referenties door aan de IAS RADIUS-server die de gebruiker authenticeert aan de hand van de voorwaarden en het gebruikersprofiel die in het afstandstoegangsbeleid zijn ingesteld. Als de gebruikersverificatie succesvol is, retourneert de RADIUS-server een RADIUS accepteert een aanvraag die ook de AAA-omzeilingswaarden bevat. In dit geval wordt het QoS-beleid van de gebruiker geretourneerd.

U kunt **debug a** uitgeven **allen toelaat** opdracht om de opeenvolging van gebeurtenissen te zien die tijdens authenticatie plaatsvindt. Hier wordt een voorbeelduitvoer weergegeven:

```
(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
Wed Apr 18 18:14:24 2007:
                      resultCode.....0
Wed Apr 18 18:14:24 2007:
                      protocolUsed.....0x0000008
Wed Apr 18 18:14:24 2007:
                       proxyState.....
                       28:1F:00:00:00:00-00:00
Wed Apr 18 18:14:24 2007:
                       Packet contains 2 AVPs:
                          AVP[01] Service-Type.....
Wed Apr 18 18:14:24 2007:
                          0x0000006 (6) (4 bytes)
Wed Apr 18 18:14:24 2007:
                          AVP[02] Airespace / WLAN-Identifier.....
```

0x0000000 (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 resultCode.....0 Wed Apr 18 18:14:24 2007: protocolUsed.....0x0000008 proxyState..... Wed Apr 18 18:14:24 2007: Wed Apr 18 18:14:24 2007: 29:1F:00:00:00:00-00:00 Packet contains 2 AVPs: Wed Apr 18 18:14:24 2007: AVP[01] Service-Type..... Wed Apr 18 18:14:24 2007: 0x0000006 (6) (4 bytes) Wed Apr 18 18:14:24 2007: AVP[02] Airespace / WLAN-Identifier..... 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 proxyState.... Wed Apr 18 18:15:08 2007: Wed Apr 18 18:15:08 2007: 00:40:96:AC:E6:57-00:00 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 0...2W.\*.W8...]Y 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 ...20.0.0.1..172 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 1a 00 46 3f cf 1b 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 172.16.1.1 for mobile 00:40:96:ac:e6:57 receiveId = 0 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.....0x0000001 Wed Apr 18 18:15:08 2007: proxyState..... 00:40:96:AC:E6:57-00:00 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) Wed Apr 18 18:15:08 2007: AVP[02] Service-Type..... 0x00000001 (1) (4 bytes) AVP[03] Class..... Wed Apr 18 18:15:08 2007: DATA (30 bytes) Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Applying new AAA override for station

00:40:96:ac:e6:57 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) AVP[02] Nas-Port..... Wed Apr 18 18:15:12 2007: 0x00000001 (1) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[03] Nas-Ip-Address..... 0xac10011e (-1408237282) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[04] NAS-Identifier.... 0x574c4332 (1464615730) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[05] Airespace / WLAN-Identifier..... 0x00000001 (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) AVP[07] Acct-Authentic..... Wed Apr 18 18:15:12 2007: 0x00000001 (1) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[08] Tunnel-Type..... 0x0000000d (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..... Wed Apr 18 18:15:12 2007: 0x00000001 (1) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[12] Calling-Station-Id..... 20.0.0.1 (8 bytes) Wed Apr 18 18:15:12 2007: AVP[13] Called-Station-Id..... 172.16.1.30 (11 bytes)

Zoals u aan de uitvoer kunt zien, is de gebruiker echt gemaakt. Vervolgens worden AAAoverwinningswaarden teruggegeven met het RADIUS-bericht. In dit geval krijgt de gebruiker het QoS-beleid van Bronze.

U kunt dit ook controleren op de WLC GUI. Hierna volgt een voorbeeld:

			RITY MANAGEMENT COM	Save Configuration Ping Logout
nitor	Clients > Detail	CLER TIRELESS SECO		< Back Link Test Remo
mmary	Client Properties		AP Properties	
tistics	MAC Address	00:40:96:ac:e6:57	AP Address	00:0b:85:5b:fb:d0
orts	IP Address	20.0.0.1	AP Name	ap:5b:fb:d0
reless	User Name	User-VLAN10	AP Type	802.11a
nown Rogue APs	Port Number	1	WLAN SSID	SSID-WLC2
Rogue Clients Adhoc Rogues 802.11a Radios 802.11b/g Radios Clients RADIUS Servers	Interface	internal	Status	Associated
	VLAN ID	20	Association ID	1
	CCX Version	CCXv3	802.11 Authentication	Open System
	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
	and the second sec		Short Preamble	Not Implemented
	Security Information		PBCC	Not Implemented
	Security Policy Completed	Yes	Channel Agility	Not Implemented
	Policy Type	N/A	Timeout	0
	Encryption Cipher	None	WEP State	WEP Disable
	EAP Type	N/A		
	Quality of Service Properties			
	WMM State	Disabled		
	QoS Level	Bronze		
	Diff Serv Code Point (DSCP)	disabled		
	802.1p Tag	disabled		
	Average Data Rate	disabled		

**Opmerking:** het standaard QoS-profiel van deze SSID is Silver. Omdat AAA-Override echter is geselecteerd en de gebruiker is ingesteld met een QoS-profiel van Bronze op de IAS-server, wordt het standaard QoS-profiel overschreven.

### Problemen oplossen

U kunt het **debug-**venster gebruiken **en** het **allen inschakelen** van de WLC om de configuratie problemen op te lossen. Een voorbeeld van de uitvoer van dit debug in een werknetwerk wordt weergegeven in het gedeelte <u>Verifiëren</u> van dit document.

**Opmerking:** Raadpleeg <u>Belangrijke informatie over debug Commands</u> voordat u **debug**opdrachten gebruikt.

# Gerelateerde informatie

- <u>Configuratie-gids voor Cisco draadloze LAN-controllers, release 4.0</u>
- WLAN-toegang beperken op basis van SSID met WLC en Cisco Secure ACSconfiguratievoorbeeld
- Ondersteuning voor wireless producten
- Technische ondersteuning en documentatie Cisco Systems