Konfigurationsbeispiel für Cisco Airespace VSAs in Microsoft IAS Radius Server

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Hintergrundinformationen Konfigurieren des IAS für Airespace VSAs Konfigurieren des WLC als AAA-Client im IAS Konfigurieren der Remote-Zugriffsrichtlinie auf dem IAS Beispielkonfiguration Überprüfung Fehlerbehebung Zugehörige Informationen

Einleitung

In diesem Dokument wird die Konfiguration eines Microsoft Internet Authentication Service (IAS)-Servers zur Unterstützung der VSAs (Vendor Specific Attributes) von Cisco beschrieben. Der Vendor-Code für Cisco Airespace VSAs lautet **14179**.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Kenntnisse der Konfiguration eines IAS-Servers
- Kenntnis der Konfiguration von Lightweight Access Points (LAPs) und Cisco Wireless LAN Controllern (WLCs)
- Kenntnisse der Cisco Unified Wireless Security-Lösungen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Microsoft Windows 2000 Server mit IAS
- Cisco 4400 WLC mit Softwareversion 4.0.206.0
- LAPs der Cisco Serie 1000
- 802.11a/b/g Wireless Client-Adapter mit Firmware 2.5
- Aironet Desktop Utility (ADU) Version 2.5

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hinweis: Dieses Dokument soll dem Leser ein Beispiel für die Konfiguration geben, die auf dem IAS-Server zur Unterstützung von Cisco Application VSAs erforderlich ist. Die in diesem Dokument vorgestellte IAS-Serverkonfiguration wurde im Labor getestet und funktioniert wie erwartet. Wenn Sie Probleme beim Konfigurieren des IAS-Servers haben, wenden Sie sich an Microsoft, um Hilfe zu erhalten. Das Cisco TAC unterstützt die Microsoft Windows-Serverkonfiguration nicht.

In diesem Dokument wird davon ausgegangen, dass der WLC für den Basisbetrieb konfiguriert ist und dass die LAPs beim WLC registriert sind. Wenn Sie ein neuer Benutzer sind und versuchen, den WLC für den Basisbetrieb mit LAPs einzurichten, lesen Sie die Informationen zur <u>LAP-Registrierung (Lightweight AP) an einen Wireless LAN Controller (WLC)</u>.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions (Technische Tipps von Cisco zu Konventionen).</u>

Hintergrundinformationen

In den meisten WLAN-Systemen (WLAN) verfügt jedes WLAN über eine statische Richtlinie, die auf alle Clients angewendet wird, die einem Service Set Identifier (SSID) zugeordnet sind. Diese Methode ist zwar leistungsstark, bietet jedoch Einschränkungen, da Clients verschiedene SSIDs verknüpfen müssen, um unterschiedliche QoS- und Sicherheitsrichtlinien zu erben.

Die Cisco Wireless LAN-Lösung unterstützt jedoch Identitätsnetzwerke, die es dem Netzwerk ermöglichen, eine einzelne SSID und bestimmte Benutzer anzukündigen, um je nach ihren Benutzerprofilen unterschiedliche QoS- oder Sicherheitsrichtlinien zu erben. Die spezifischen Richtlinien, die Sie mithilfe von Identitätsnetzwerken steuern können, sind:

- Quality of Service Wenn der QoS-Level-Wert in einem RADIUS Access Accept vorhanden ist, überschreibt er den im WLAN-Profil angegebenen QoS-Wert.
- ACL Wenn das Attribut "Access Control List" (Zugriffssteuerungsliste) im RADIUS Access Accept (RADIUS-Zugriffsakzepte) vorhanden ist, wendet das System den ACL-Namen nach der Authentifizierung auf die Client-Station an. Dadurch werden alle der Schnittstelle zugewiesenen ACLs außer Kraft gesetzt.
- VLAN: Wenn ein VLAN-Schnittstellenname oder ein VLAN-Tag in einem RADIUS Access Accept vorhanden ist, platziert das System den Client auf einer bestimmten Schnittstelle.
- WLAN-ID: Wenn das WLAN-ID-Attribut im RADIUS Access Accept vorhanden ist, wendet das System die WLAN-ID (SSID) nach der Authentifizierung auf die Client-Station an. Die WLAN-

ID wird vom WLC in allen Authentifizierungsinstanzen außer IPSec gesendet. Wenn der WLC bei der Webauthentifizierung ein WLAN-ID-Attribut in der Authentifizierungsantwort des AAA-Servers erhält und es nicht mit der ID des WLAN übereinstimmt, wird die Authentifizierung abgelehnt. Andere Sicherheitsmethoden tun dies nicht.

- DSCP Value (DSCP-Wert): Wenn der Wert in einem RADIUS Access Accept vorhanden ist, überschreibt der DSCP-Wert den im WLAN-Profil angegebenen DSCP-Wert.
- 802.1p-Tag: Wenn der 802.1p-Wert in einem RADIUS Access Accept vorhanden ist, wird er über den im WLAN-Profil angegebenen Standardwert gesetzt.

Hinweis: Die VLAN-Funktion unterstützt nur MAC-Filterung, 802.1X und Wi-Fi Protected Access (WPA). Die VLAN-Funktion unterstützt keine Webauthentifizierung oder IPSec. Die lokale MAC-Filter-Datenbank des Betriebssystems wurde um den Schnittstellennamen erweitert. Auf diese Weise können lokale MAC-Filter festlegen, welche Schnittstelle dem Client zugewiesen werden soll. Ein separater RADIUS-Server kann ebenfalls verwendet werden, der RADIUS-Server muss jedoch mithilfe der Sicherheitsmenüs definiert werden.

Weitere Informationen zu Identitätsnetzwerken finden Sie unter Konfigurieren von Identitätsnetzwerken.

Konfigurieren des IAS für Airespace VSAs

Um den IAS für Airespace VSAs zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

- 1. Konfigurieren des WLC als AAA-Client im IAS
- 2. Konfigurieren der Remote-Zugriffsrichtlinie auf dem IAS

Hinweis: Die VSAs werden unter "Remote Access Policy" (Remote-Zugriffsrichtlinie) konfiguriert.

Konfigurieren des WLC als AAA-Client im IAS

Gehen Sie wie folgt vor, um den WLC als AAA-Client im IAS zu konfigurieren:

 Klicken Sie auf Programme > Verwaltung > Internet Authentication Service, um IAS auf dem Microsoft 2000-Server zu starten.



- 2. Klicken Sie mit der rechten Maustaste auf den Ordner **Clients**, und wählen Sie **Neuer Client** aus, um einen neuen RADIUS-Client hinzuzufügen.
- Geben Sie im Fenster Add Client (Client hinzufügen) den Namen des Clients ein, und wählen Sie RADIUS als Protokoll aus. Klicken Sie anschließend auf Weiter. In diesem Beispiel lautet der Client-Name WLC-1. Hinweis: Standardmäßig ist das Protokoll auf RADIUS festgelegt.

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

4. Geben Sie im Fenster Add RADIUS Client (RADIUS-Client hinzufügen) die Client-IP-Adresse, die Client-Vendor-Adresse und den geheimen Schlüssel ein. Nachdem Sie die Client-Informationen eingegeben haben, klicken Sie auf Fertig stellen. Dieses Beispiel zeigt einen Client mit dem Namen WLC-1 und der IP-Adresse 172.16.1.30, der Client-Anbieter ist auf Cisco und der Shared geheime Client 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 si	ignature attribute in the request	
Shared secret:	*****	
Confirm shared secret:	*****	
	< <u>B</u> ack Finisl	h Cancel

Mit diesen Informationen wird der WLC mit dem Namen WLC-1 als AAA-Client des IAS-Servers

hinzugefügt.

Action Year Year Year Year Year Year Address Protocol Client-Vendor Tree Friendy Name Address Protocol Client-Vendor Differits Friendy Name Address Protocol Client-Vendor Priends Remote Access Logging Tree Tree Client-Vendor Priends Remote Access Policies Tree Tree Tree	🐓 Internet Authentication Service				
Tree Friendly Name Address Protocol Client-Vendor Image: Strength and Protocol Service (Local) Image: Strength and Strengt and Strenge and Strength and Strength and Strength and	_ <u>A</u> ction View ← → € 🗊 💼 日	2			
Internet Authentication Service (Loca) Image: Service Access Logging Image: Service Access Policies Image: Service A	Tree	Friendly Name	Address	Protocol	Client-Vendor
	 Internet Authentication Service (Local) Cients Remote Access Logging Remote Access Policies 	WLC-1	172.16.1.30	RADIUS	<u>Osco</u>

Im nächsten Schritt wird eine Remote-Zugriffsrichtlinie erstellt und die VSAs konfiguriert.

Konfigurieren der Remote-Zugriffsrichtlinie auf dem IAS

Gehen Sie wie folgt vor, um eine neue Remote Access Policy für den IAS zu konfigurieren:

- 1. Klicken Sie mit der rechten Maustaste auf **Remote Access Policies (Remote-Zugriffsrichtlinien)**, und wählen Sie **New Remote AccessMS Policy (Neue Remote-Zugriffsrichtlinien)** aus.Das Fenster Policy Name (Richtlinienname) wird angezeigt.
- 2. Geben Sie den Namen der Richtlinie ein, und klicken Sie auf **Weiter**.

cy Name Specify a friendly name for the poli	icy.
A Remote Access Policy is a set of meeting certain conditions.	f actions which can be applied to a group of users
Analogous to rules you can apply to specify a set of conditions that mus You can then specify actions to be	to incoming mail in an e-mail application, you can st be matched for the Remote Access Policy to apply e taken when the conditions are met.
Policy friendly name:	
Airespace VSA	
·	
	Z Back Nevt > Car

3. Wählen Sie im nächsten Fenster die Bedingungen aus, für die die Remote-Zugriffsrichtlinie gilt. Klicken Sie auf **Hinzufügen**, um die Bedingungen auszuwählen.

Add Remote Access Policy 🔀 Conditions Determine the conditions to match.	Select Attribute 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 dialed by user Calling-Station-Id Phone number from which call originated Client-Friendly-Name Friendly name for the RADIUS client. (IAS only) Client-PAddress IP address of RADIUS client. (IAS only) Client-Paddress IP address of RADIUS client. (IAS only) Client-Paddress IP address of RADIUS client. (IAS only) Client-Paddress In periods and days of weak during which use Framed-Protocol The periods and days of weak during which use NAS-Hort/Time-Restric Time periods and days or weak during which use NAS-Hort/Time Sting identifying the NAS originating the request NAS-Port-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 Bemove Edit	Add Cancel

4. Wählen Sie im Menü Attributtypen die folgenden Attribute aus: **Client-IP-Adresse** - Geben Sie die IP-Adresse des AAA-Clients ein. In diesem Beispiel wird die IP-Adresse der WLCs eingegeben, sodass die Richtlinie für Pakete vom WLC

	Client-IP-Address ? 🗙	
	<u>Type a word or a wild card (for example, abc.*):</u>	
	172.16.1.30	
	· · · · · · · · · · · · · · · · · · ·	
	OK Cancel	
gilt.		Windows

Groups: Wählen Sie die Windows-Gruppe (die Benutzergruppe) aus, für die die Richtlinie gilt. Hier ein

	📲 Groups		? ×
	The following groups are currently in this	s condition.	
	<u>G</u> roups:		
	Name		
	CAT-TD-2K\Test-Clients		
	Add <u>R</u> emove		
		OK L	Cancel
Baisnial.			Cancer

Add Remote Access Policy	×
Conditions Determine the conditions to match.	
Specify the conditions to match.	
Londitions: Client-IP-Address matches "172-16-1-30" AND	
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
A <u>d</u> d <u>R</u> emove <u>E</u> dit < <u>B</u> ack <u>N</u> ext > Canc	cel

Dieses Beispiel zeigt nur zwei Bedingungen. Wenn es weitere Bedingungen gibt, fügen Sie auch diese Bedingungen hinzu, und klicken Sie auf **Weiter**. Das Fenster Berechtigungen wird angezeigt.

 Wählen Sie im Fenster "Berechtigungen" die Option Remotezugriffsberechtigung erteilen aus.Nachdem Sie diese Option ausgewählt haben, erhält der Benutzer Zugriff, sofern der Benutzer die angegebenen Bedingungen erfüllt (aus Schritt 2).

d R	emote Access Policy
Pe	missions
	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.
	If a user matches the specified conditions:
	Grant remote access permission
	Upeny remote access permission
	< Back Next > Cancel

- 6. Klicken Sie auf Weiter.
- 7. Im nächsten Schritt wird das Benutzerprofil eingerichtet.Obwohl Sie angegeben haben, dass Benutzern aufgrund der Bedingungen der Zugriff verweigert oder gewährt werden soll, kann das Profil trotzdem verwendet werden, wenn die Bedingungen dieser Richtlinie pro Benutzer überschrieben

werden.

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 Cancel

Um das Benutzerprofil zu konfigurieren, klicken Sie im Fenster Benutzerprofil auf **Profil bearbeiten**.Das Fenster "Profil für die Einwahl bearbeiten" wird

lit Dial-in Profile			?	×
Authentication	Encryption	A	dvanced	ıĒ.
Dial-in Constraints	IP	- T	Multilink	ίŀ
Disconnect if idle for:		1	🚽 min.	
Restrict <u>m</u> aximum ses	sion to:	1	≍ min.	H
Restrict access to the	following days and tin	nes: ——		н
	<u>E</u> dit			
🔲 Restrict <u>D</u> ial-in to this	number only:			11
<u>R</u> estrict Dial-in media:				
FDDI			<u> </u>	н
Token Ring	11			11
			•	
				-1 -
		_		

angezeigt.

n Sie auf die Registerkarte **Authentifizierung**, und wählen Sie die im WLAN verwendete Authentifizierungsmethode aus.In diesem Beispiel wird die unverschlüsselte Authentifizierung (PAP, SPAP)

Dial-in Constraints IP Multilink						
Authentication Encryption Advanced	j					
Check the authentication methods which are allowed for this connection. Extensible Authentication Protocol Select the EAP type which is acceptable for this policy. Protected EAP (PEAP) Configure	Check the authentication methods which are allowed for this connection. Extensible Authentication Protocol Select the EAP type which is acceptable for this policy. Protected EAP (PEAP) Configure					
 Microsoft Encrypted Authentication version <u>2</u> (MS-CHAP v2) Microsoft Encrypted Authentication (MS-CHAP) Encrypted Authentication (CHAP) 	 Microsoft Encrypted Authentication version <u>2</u> (MS-CHAP v2) Microsoft Encrypted Authentication (MS-CHAP) 					
✓ Unencrypted Authentication (PAP, SPAP)						
Unauthenticated Access Allow remote PPP clients to connect without negotiating any authentication method.						
OK Cancel <u>Apply</u>						

en Sie auf die Registerkarte **Erweitert**. Entfernen Sie alle Standardparameter, und klicken Sie auf

Authentication Encryption Advanced pecify additional connection attributes to be returned to the Remote ccess Server. arameters: Name Vendor Value Add Remove Edit	Dial-in Constraints) IP) Mu	ultilink
pecify additional connection attributes to be returned to the Remote ccess Server. arameters: Name Vendor Value Image: Imag	Authentication	Encryption	Advo	anceo
ccess Server. arameters: Name Vendor Value	pecify additional conne	ction attributes to be	returned to the Ren	note
Name Vendor Value	Access Server.			
Add	arameters. Name	Vendor	Value	
Add	Hamo	Vondor	Yalao	
Add				
I► Add <u>R</u> emove <u>E</u> dit				
Add				
Add <u>R</u> emove <u>E</u> dit				
Add Remove Edit				
Add				
Add <u>R</u> emove <u>E</u> dit				
Add <u>H</u> emove <u>E</u> dit	41			
	•			Þ
	▲ Add	nove <u>E</u> dit		Þ
	▲ 	nove <u>E</u> dit		Þ
	 ▲<u>dd</u> 	nove <u>E</u> dit		
	 ▲<u>dd</u> 	nove <u>E</u> dit		
	A <u>d</u> d	nove <u>E</u> dit		Þ

Hinzufügen

len Sie im Fenster Attribute hinzufügen die Option Servicetyp aus, und wählen Sie anschließend im nächsten Fenster den Anmeldungswert aus.

Add Attributes Image: Control of the statubute and click Add FADIUS attributes: Image: Control of the statubute and click Add ReplyMessage FADIUS Standard Message to be displayed to user when authenicating Service:Type FADIUS Standard Turnel to which a session in to be assigned Turnel-Clent-Endpt FADIUS Standard Turnel to which a session in to be assigned Turnel-Clent-Endpt FADIUS Standard Turnel to which a session in to be assigned Turnel-Preserve: Endpt FADIUS Standard Turnel to which a session in to be assigned Turnel-Preserve: Endpt FADIUS Standard Turnel to which a session in to be assigned Turnel-Preserve: Endpt FADIUS Standard Turnel to which a session in to be assigned Turnel-Preserve: Endpt FADIUS Standard Turnel period to the serve end of the turnel Turnel-Server: Endpt FADIUS Standard Name used by the turnel terminator during the authen Turnel-Server: Endpt FADIUS Standard Name used by the turnel terminator during the authen Turnel-Server: Endpt FADIUS Standard Name used by the turnel terminator during the authen Turnel-Server: Endpt FADIUS Standard Name used by the turnel terminator during the authen Turnel-Server: Endpt FADIUS Standard Turnel gerococh to be used Usend-Specific FADIUS Standard	ч	uJ.				
To add an attribute to the Profile, select the attribute and click Add FADIUS statibute: Name Vendor Description ReplyMessage RADIUS Standed Message to be displayed to user when autheritocht ServiceType Attribute Information Image: ServiceType Turnel-Assignment/D RADIUS Standed Turnel to which a session is to be assigned Attribute name: Turnel-CientSuthID RADIUS Standed Turnel to which a session is to be assigned Attribute name: Turnel-Message RADIUS Standed Transport medum to use when creating a turnel to main onto server Attribute number: Turnel-Preference RADIUS Standed Transport medum to use when creating a turnel to main onto server Attribute number: Turnel-Preference RADIUS Standed Transport medum to use when creating a turnel to emption during the auther Immediate formed server Turnel-Preference RADIUS Standed Name used by the turnel termined outring the auther Immediate formed server Turnel-Preference RADIUS Standed Name used by the turnel termined outring the auther Immediate formed server Turnel-Preference RADIUS Standed Used to support propriate Auther Immediate formed server Turnel-Preference RADIUS Standed Used to support propriate Auther Immediat	A	ld Attributes		<u>? ×</u>		
Name Vendor Description Reply-Message RADIUS Standard Message to be diplayed to user when authenicating Service-Type RADIUS Standard Tunnel Assignment/D RADIUS Standard Tunnel to which a session is to be assigned Tunnel-Cleint-Subh/D RADIUS Standard Innel to which a session is to be assigned Attribute number: Tunnel-Cleint-Subh/D RADIUS Standard Innel to which a session is to be assigned Attribute number: Tunnel-Reserved RADIUS Standard Innel to which a session is to be assigned to each tunnel to tunnel the server authon outing the authen interview server authon to use when creating a tunnel to tunnel-frameword or authon to use when creating a tunnel to tunnel-frameword matching the tunnel terminator during the authenticating the authenticating the authenticating the authenticating the authenticating the tunnel terminator during the authenticating the authenticatin		To add an attribute to the Prof RADIU <u>S</u> attributes:	ile, select the attribute	e and click Add	Enumerable Attribute Information	2 ×
		Name ReplyMessage Service:Type Tunnet-Client-Endpt Tunnet-Client-Endpt Tunnet-Password Tunnet-Password Tunnet-Password Tunnet-Put-Group-ID Tunnet-Server-Auth-ID Tunnet-Server-Endpt Tunnet-Type Vendor-Specific Cisco-AV-Pair Ignore-User-Dialin-Properties USR-AT-Cal-Input-Filter USR-AT-Cal-Input-Filter USR-AT-Cal-Input-Filter USR-AT-Cal-Input-Filter USR-AT-Cal-Input-Filter USR-AT-Cal-Input-Filter USR-AT-Cal-Input-Filter	Vendor RADIUS Standard RADIUS Standard Cisco Microsoft 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 turneled ession Name used by the tunnel terminator during the auth IP address of the server end of the tunnel Tunneling protocols to be used Used to support proprietary NAS features Cisco AV Pair VSA Ignore the user's dial-in properties Description not available Description not avai	Attribute name: Service-Type Attribute number: 6 Attribute format: Enumerator Attribute value: Loon OK Cancel	-

Als Nächstes müssen Sie das **anbieterspezifische** Attribut aus der RADIUS-Attributliste auswählen.

A	dd Attributes		<u>? ×</u>	ŀ	Multivalued Attribute Information	? ×
	To add an attribute to the Prof RADIU <u>S</u> attributes:	ile, select the attribut	e and click Add		Attribute name: Vendor-Specific	
	RADIUS attributes: Name Reply-Message Service-Type Turnel-Assignment-ID Turnel-Clent-Endpt Turnel-Clent-Endpt Turnel-Password Turnel-Password Turnel-Password Turnel-Password Turnel-Server-Auth-ID Turnel-Server-Endpt Turnel-Server-Endpt Turnel-Server-Endpt Turnel-Server-Endpt Turnel-Server-Endpt Turnel-Server-Endpt Turnel-Server-Endpt Turnel-Server-Endpt Turnel-Server-Endpt Turnel-Server-Endpt Turnel-Server-Endpt Server-Disin-Properties USR-ACCM-Type	Vendor RADIUS Standard RADIUS Standard	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 tunnel Transport medium to use when creating a tunnel to 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 turnel Turneling protocols to be used Used to support proprietay NAS features Cisco AV Pair VSA Ignore the user's dai-in properties Description not available		Vendor-Specific Attribute number: 26 Attribute format: OctetString Attribute values: Vendor Value Ma	love Up ve <u>D</u> own Add
	USR-AT-Call-Output-Filter USR-AT-Input-Filter USR-AT-Output-Filter II	U.S. Robolics, I., U.S. Robolics, I., U.S. Robolics, I.,	Description not available Description not available Description not available <u>A</u> dd Close			Edit

Klicken Sie im nächsten Fenster auf **Hinzufügen**, um ein neues VSA auszuwählen.Das Fenster Herstellerspezifische Attributinformationen wird angezeigt.Wählen Sie unter Anbieter für Netzwerkzugriffsserver angeben die Option **Anbietercode eingeben aus**.Geben Sie den Vendor Code für Airespace VSAs ein. Der Vendor-Code für Cisco Airespace VSAs lautet **14179**.Da dieses Attribut der RADIUS RFC-Spezifikation für VSAs entspricht, wählen Sie **Yes (Ja)** aus. **Es**

Vendor-Specific	
Specify network access s	erver vendor.
Select from list:	RADIUS Standard 💌
Enter Vendor Code:	14179
vendor specific attributes.	ute conforms to the RADIUS RFC specification for
 Specify whether the attributes vendor specific attributes. Yes. It conforms. No. It does not conform 	ute conforms to the RADIUS RFC specification for m.
 Specify whether the attributes vendor specific attributes. Yes. It conforms. No. It does not conform Configure Attribute 	ute conforms to the RADIUS RFC specification for m.

auf Attribut konfigurieren. Geben Sie im Fenster Configure VSA (RFC-konform) (VSA

Sie

konfigurieren) (RFC-konform) die vom Anbieter zugewiesene Attributnummer, das Attributformat und den Attributwert ein, die von dem VSA abhängen, das Sie verwenden möchten.So legen Sie die WLAN-ID auf Benutzerbasis fest:**Attributname** - AirRespace-WLAN-ID**Vom Anbieter zugewiesene Attributnummer**: 1**Attributformat** - Integer/Dezimal**Wert** -WLAN-ID**Beispiel 1**

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

So legen Sie das

QoS-Profil auf Benutzerbasis fest:**Attributname** - Airespace-QoS-Level**Vom Anbieter zugewiesene Attributnummer**: 2**Attributformat** - Integer/Dezimal**Wert**: 0 - Silver; 1 - Gold; 2 -Platinum; 3 - Bronze**Beispiel 2**

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

So legen Sie den

DSCP-Wert auf Benutzerbasis fest: Attributname - Airespace-DSCPVom Anbieter zugewiesene Attributnummer - 3Attributformat - Integer/DezimalWert - DSCP-WertBeispiel 3

	Configure VSA (RFC compliant)	
	Vendor-assigned attribute number:	
	3	
	Attribute format:	
	Decimal	
	Attri <u>b</u> ute value:	
	46	
		-
•		So legen S

So legen Sie das

802.1p-Tag auf Benutzerbasis fest: Attributname - Airespace-802.1p-TagVom Anbieter zugewiesene Attributnummer - 4Attributformat - Integer/DezimalWert: 802.1p-TagBeispiel 4

Configure VSA (RFC compliant)
Vendor-assigned attribute number:
4
Attribute format:
Decimal
Attribute value:
5
UK Lancel
So legen Sie

Schnittstelle (VLAN) auf Benutzerbasis fest: Attributname - Airespace-Interface-NameVom Anbieter zugewiesene Attributnummer: 5Attributformat - ZeichenfolgeWert -SchnittstellennameBeispiel 5

Configure ¥SA (RFC compliant)		? ×	1
⊻endor-assigned attribute number:			
5			
Attribute format:			
String		•	
Attri <u>b</u> ute value:			
vlan10			
	OK	Cancel	

So legen Sie die

ACL auf Benutzerbasis fest: **Attributname** - Airespace-ACL-Name**Vom Anbieter zugewiesene Attributnummer** - 6**Attributformat** - Zeichenfolge**Wert** - ACL-Name**Beispiel 6**

	? ×
	•
OK	Cancel
	OK

- 8. Wenn Sie die VSAs konfiguriert haben, klicken Sie auf **OK**, bis das Fenster Benutzerprofil angezeigt wird.
- 9. Klicken Sie anschließend auf **Fertig stellen**, um die Konfiguration abzuschließen.Die neue Richtlinie wird unter "Remote Access Policies" (Remote-Zugriffsrichtlinien) angezeigt.

🐤 Internet Authentication Service		
Action View 🛛 🗢 → 💽 🔢 😼 😭		
Tree	Name	Order
Internet Authentication Service (Local) Clients Remote Access Logging Remote Access Policies	Arespace VSA	

Beispielkonfiguration

In diesem Beispiel wird ein WLAN für die Webauthentifizierung konfiguriert. Die Benutzer werden vom IAS RADIUS-Server authentifiziert, und der RADIUS-Server ist so konfiguriert, dass QoS-Richtlinien auf Benutzerbasis zugewiesen werden.

				inguration Fing Coyour
A resultion	MONITOR WLANS CO	NTROLLER WIRELESS SECURITY MANAC	SEMENT COMMANDS	HELP
√s	WLANs > Edit			< Back Appl
5	WLAN ID	1		
Ns roups VLAN	WLAN SSID	SSID-WLC2		
	General Policies		Security Policies	
	Radio Policy	All	Laura 2 Canualty	Nana
	Admin Status	C Enabled	Layer 2 Security	MAC Filtering
	Session Timeout (secs)	0		- Hard Finding
	Quality of Service (QoS)	Silver (best effort)	Layer 3 Security	None 💌
	WMM Policy	Disabled 2		🕑 Web Policy *
	7920 Phone Support	Client CAC Limit 📋 AP CAC Limit		Authentication O Passthr
	Broadcast SSID	C Enabled	Preauthentication	none 💌
	Aironet IE	C Enabled	* Web Policy cannot	he used in combination with TD
	Allow AAA Override	✓ Enabled	and L2TP.	be used in combination with p
	Client Exclusion	Enabled ** 60 Timeout Value (secs)	** When client exclu zero means infinity(ision is enabled, a timeout valu will require administrative over
	DHCP Server	Override	to reset excluded cli *** CKIP is not sup	ents) ported 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.		
	Radius Servers			
		Authentication Servers Accounting Servers		
	Carvar 1	10:172 16 1 1. Port:1912 W Done W		

Wie Sie in diesem Fenster sehen, ist die Webauthentifizierung aktiviert, der Authentifizierungsserver ist 172.16.1.1, und AAA-override ist auch im WLAN aktiviert. Die QoS-Standardeinstellung für dieses WLAN ist auf Silver eingestellt.

Auf dem IAS RADIUS-Server wird eine Remote Access Policy konfiguriert, die das QoS-Attribut Bronze in der RADIUS Accept-Anforderung zurückgibt. Dies geschieht, wenn Sie das für das QoS-Attribut spezifische VSA konfigurieren.

Configure VSA (RFC compliant)	? ×
Vendor-assigned attribute number:	
Attribute format:	
Attribute value:	
la	
	OK Cancel

Detaillierte Informationen zur Konfiguration einer <u>Remote-Zugriffsrichtlinie auf dem IAS-</u>Abschnitt dieses Dokuments finden Sie im Abschnitt Konfigurieren der Remote-Zugriffsrichtlinie.

Sobald der IAS-Server, der WLC und die LAP für diese Konfiguration konfiguriert sind, können die Wireless-Clients die Webauthentifizierung verwenden, um eine Verbindung herzustellen.

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Wenn der Benutzer über eine Benutzer-ID und ein Kennwort eine Verbindung zum WLAN herstellt, übergibt der WLC die Anmeldeinformationen an den IAS RADIUS-Server, der den Benutzer anhand der Bedingungen und des Benutzerprofils authentifiziert, die in der Remote-Zugriffsrichtlinie konfiguriert wurden. Wenn die Benutzerauthentifizierung erfolgreich ist, gibt der RADIUS-Server eine RADIUS-Annahmeanforderung zurück, die auch die AAA-Überschreibungswerte enthält. In diesem Fall wird die QoS-Richtlinie des Benutzers zurückgegeben.

Sie können den Befehl **debug aa all enable** ausführen, um die Ereignissequenz anzuzeigen, die während der Authentifizierung auftritt. Hier sehen Sie eine Beispielausgabe:

```
(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:
                         structureSize.....70
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.....
```

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 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 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..... 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 31User-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 bcF?.....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 00z.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) Wed Apr 18 18:15:12 2007: AVP[06] Acct-Session-Id..... 4626602c/00:40:96:ac:e6:57/16 (29 bytes) Wed Apr 18 18:15:12 2007: AVP[07] Acct-Authentic..... 0x00000001 (1) (4 bytes) AVP[08] Tunnel-Type..... Wed Apr 18 18:15:12 2007: 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) Wed Apr 18 18:15:12 2007: AVP[11] Acct-Status-Type..... 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)

Wie Sie in der Ausgabe sehen können, wird der Benutzer authentifiziert. Anschließend werden AAA-Überschreibungswerte mit der Meldung RADIUS accept (RADIUS akzeptieren) zurückgegeben. In diesem Fall erhält der Benutzer die QoS-Richtlinie von Bronze.

Sie können dies auch auf der WLC-GUI überprüfen. Hier ein Beispiel:

<u>.</u>	MONITOR WLANS CONTR	OLLER WIRELESS SECU	JRITY MANAGEMENT COMM	IANDS HELP
nitor	Clients > Detail			< Back Link Test Remo
imary	Client Properties		AP Properties	
istics ntroller	MAC Address	00:40:96:ac:e6:57	AP Address	00:0b:85:5b:fb:d0
Ports	IP Address	20.0.0.1	AP Name	ap:5b:fb:d0
eless	User Name	User-VLAN10	AP Type	802.11a
Known Rogue APs Rogue Clients Adhoc Rogues 802.11a Radios 002.11b/g Radios Clients RADIUS Servers	Port Number	1	WLAN SSID	SSID-WLC2
	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
	Requity Information		Short Preamble	Not Implemented
	Securicy 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		

Hinweis: Das Standard-QoS-Profil für diese SSID ist Silver. Da jedoch AAA-Überschreibungen ausgewählt und der Benutzer mit einem QoS-Profil von Bronze auf dem IAS-Server konfiguriert ist, wird das standardmäßige QoS-Profil überschrieben.

Fehlerbehebung

Sie können den Befehl **debug aa all enable** auf dem WLC verwenden, um die Konfiguration zu beheben. Ein Beispiel für die Ausgabe dieses Debuggens in einem funktionierenden Netzwerk finden Sie im Abschnitt <u>Überprüfen</u> dieses Dokuments.

Hinweis: Beachten Sie <u>vor der</u> Verwendung von **Debug-**Befehlen die <u>Informationen</u> zu <u>Debug-</u><u>Befehlen</u>.

Zugehörige Informationen

- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 4.0
- Einschränken des WLAN-Zugriffs auf der Basis der SSID mit WLC und Cisco Secure ACS -Konfigurationsbeispiel
- <u>Wireless-Produktunterstützung</u>
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>