Cisco Airespace VSAs on Microsoft IAS Radius Server Configuration Example

Document ID: 91392

Contents

Introduction Prerequisites Requirements Components Used Conventions Background Information Configure the IAS for Airespace VSAs Configure the WLC as an AAA Client on the IAS Configure the Remote Access Policy on the IAS Example Configuration Verify Troubleshoot Related Information Introduction

This document shows you how to configure a Microsoft Internet Authentication Service (IAS) server to support Cisco Airespace Vendor Specific Attributes (VSAs). The Vendor Code for Cisco Airespace VSAs is **14179**.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to configure an IAS server
- Knowledge of the configuration of Lightweight Access Points (LAPs) and Cisco Wireless LAN Controllers (WLCs)
- Knowledge of Cisco Unified Wireless Security Solutions

Components Used

The information in this document is based on these software and hardware versions:

- Microsoft Windows 2000 server with IAS
- Cisco 4400 WLC that runs software version 4.0.206.0
- Cisco 1000 Series LAPs
- 802.11 a/b/g wireless client adapter with firmware 2.5
- Aironet Desktop Utility (ADU) version 2.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Note: This document is intended to give the reader an example on the configuration required on the IAS server to support Cisco Airespace VSAs. The IAS server configuration presented in this document has been tested in the lab and works as expected. If you have trouble configuring the IAS server, contact Microsoft for help. Cisco TAC does not support Microsoft Windows server configuration.

This document assumes that the WLC is configured for basic operation and that the LAPs are registered to the WLC. If you are a new user trying to setup the WLC for basic operation with LAPs, refer to Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

In most wireless LAN (WLAN) systems, each WLAN has a static policy that applies to all clients associated with a service set identifier (SSID). Although powerful, this method has limitations because it requires clients to associate with different SSIDs in order to inherit different QoS and security policies.

However, the Cisco Wireless LAN Solution supports identity networking, which allows the network to advertise a single SSID and specific users to inherit different QoS or security policies based on their user profiles. The specific policies that you can control using identity networking include:

- **Quality of Service** When present in a RADIUS Access Accept, the QoS–Level value overrides the QoS value specified in the WLAN profile.
- ACL When the Access Control List (ACL) attribute is present in the RADIUS Access Accept, the system applies the ACL–Name to the client station after it authenticates. This overrides any ACLs that are assigned to the interface.
- VLAN When a VLAN Interface–Name or VLAN–Tag is present in a RADIUS Access Accept, the system places the client on a specific interface.
- WLAN ID When the WLAN–ID attribute is present in the RADIUS Access Accept, the system applies the WLAN–ID (SSID) to the client station after it authenticates. The WLAN ID is sent by the WLC in all instances of authentication except IPSec. In case of web authentication, if the WLC receives a WLAN–ID attribute in the authentication response from the AAA server, and it does not match the ID of the WLAN, authentication is rejected. Other types of security methods do not do this.
- **DSCP Value** When present in a RADIUS Access Accept, the DSCP value overrides the DSCP value specified in the WLAN profile.
- **802.1p–Tag** When present in a RADIUS Access Accept, the 802.1p value overrides the default specified in the WLAN profile.

Note: The VLAN feature only supports MAC filtering, 802.1X, and Wi–Fi Protected Access (WPA). The VLAN feature does not support web authentication or IPSec. The operating system's local MAC Filter database has been extended to include the interface name. This allows local MAC filters to specify which interface the client should be assigned. A separate RADIUS server can also be used, but the RADIUS server must be defined using the Security menus.

Refer to Configuring Identity Networking for more information on identity networking.

Configure the IAS for Airespace VSAs

In order to configure the IAS for Airespace VSAs, you need to complete these steps:

1. Configure the WLC as an AAA Client on the IAS

2. Configure the Remote Access Policy on the IAS

Note: The VSAs are configured under the Remote Access Policy.

Configure the WLC as an AAA Client on the IAS

Complete these steps in order to configure the WLC as an AAA client on the IAS:

1. Click **Programs > Administrative Tools > Internet Authentication Service** in order to launch IAS on the Microsoft 2000 server.



- 2. Right-click the Clients folder and choose New Client in order to add a new RADIUS client.
- 3. In the Add Client window, enter the name of the client and choose **RADIUS** as the Protocol. Then, click **Next**.

In this example, the client name is WLC-1.

Note: By default, the protocol is set to RADIUS.

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

4. In the Add RADIUS Client window, enter the **Client IP address**, **Client–Vendor**, and **Shared** secret. After you enter the client information, click **Finish**.

This example shows a client named WLC-1 with an IP address of 172.16.1.30, the Client–Vendor is set to *Cisco*, and the Shared secret is *cisco*123:

ld RADIUS Client	
Client Information Specify information regarding	the client.
Client address (IP or DNS):	
172.16.1.30	<u>⊻</u> enty
Client-Vendor:	
Cisco	_
🔲 <u>C</u> lient must always send t	he signature attribute in the request
Shared secret:	****
Confirm shared secret:	*****
	< <u>B</u> ack Finish Cancel

With this information, the WLC named WLC-1 is added as AAA client of the IAS server.

🐤 Internet Authentication Service				_ 🗆 ×
Action View ← → 💽 📆 💼 🖽 🖆	2			
Tree	Friendly Name	Address	Protocol	Client-Vendor
Internet Authentication Service (Local) Internet Access Logging Remote Access Policies	<u></u> WLC-1	172.16.1.30	RADIUS	<u>Cisco</u>
	4			•

The next step is to create a Remote Access Policy and configure the VSAs.

Configure the Remote Access Policy on the IAS

Complete these steps in order to configure a new Remote Access Policy on the IAS:

1. Right-click **Remote Access Policies** and choose **New Remote AcceMSss Policy**.

The Policy Name window appears.

2. Enter the name of the policy and click **Next**.

Add Remote Access Policy	×
Policy 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 > Cancel	

3. In the next window, select the conditions for which the Remote Access Policy will apply. Click **Add** in order to select the conditions.

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 dialed by user Caling-Station-Id Phone number from which call originated Clent-Friendly-Name Friendly name for the RADIUS clent. (IAS only) Clent-IP-Address IP address of RADIUS clent. (IAS only) Clent-Vendor Manufacturer of RADIUS proxy or NAS. (IAS only) Clent-Vendor Time periods and days of week during which use Framed-Protocol The protocol to be used NAS-Identitier String identifying the NAS originating the request (IA NAS-PAddress IP address of the NAS originating the request (IA 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 Windowe-Groups Windowe groups that user belongs to
Add Eemove Edit	
< <u>B</u> ack <u>N</u> ext> Cancel	Add Cancel

- 4. From the Attribute types menu, select these attributes:
 - Client–IP–Address Enter the IP address of the AAA client. In this example, the WLCs IP address is entered so that the policy applies to packets from the WLC.

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

• Windows Groups Select the Windows group (the user group) for which the policy will apply. Here is an example:

roups:				
Name CAT-TD-2K\Test-Clients				
Add <u>B</u> emove				
	0K		Cancel	
d Remote Access Policy				
Conditions Determine the conditions to m	atch.			
Conditions Determine the conditions to m Specify the conditions to mate	atch. h.			
Conditions Determine the conditions to m Specify the conditions to mate <u>C</u> onditions:	atch. h. 72 16 1 30'' 4	ND		
Conditions Determine the conditions to m Specify the conditions to mato <u>Conditions:</u> Client-IP-Address matches "C Windows-Groups matches "C	atch. h. 72 16 1 30'' / AT-TD-2K\Te	AND est-Clients''		

X

This example shows only two conditions. If there are more conditions, add those conditions as well and click **Next**.

The Permissions window appears.

5. In the Permissions window, choose Grant remote access permission.

After you choose this option, the user is given access, provided the user matches the specified conditions (from step 2).

d R	emote Access Policy
Pe	ermissions 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
	O Deny remote access permission
	Z Back Next > Cancel

6. Click Next.

7. The next step is to set up the user profile.

Even though you might have specified that users should be denied or granted access based on the conditions, the profile can still be used if this policy's conditions are overridden on a per–user basis.

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

a. In order to configure the user profile, click **Edit Profile** on the User Profile window.

The Edit Dial-in Profile window appears.

Edit Dial-in Profile			? ×
Authentication Dial-in Constraints	Encryption IP	Adva	anced
Disconnect if idle for		1] min.
Restrict maximum session to: I min. Restrict access to the following days and times:			
	<u>E</u> dit		
■ Restrict <u>D</u> ial-in to this num ■■ <u>R</u> estrict Dial-in media: —	ber only:		
☐ FDDI ☐ Token Ring ☐ Wireless - IEEE 802.11 ☐ Wireless - Other ☐ Cable			-
	ОК	Cancel	Apply

b. Click the **Authentication** tab, then choose the authentication method that is used in the WLAN.

This example uses Unencrypted Authentication (PAP,SPAP).

Edit Dial-in Profile		? ×		
Dial-in Constraints) IP	Multilink		
Authentication	Encryption	Advanced		
Check the authentication methods which are allowed for this connection.				
Encrypted Authentication (CHAP) Unencrypted Authentication (PAP, SPAP) Unauthenticated Access Allow remote PPP clients to connect without negotiating any authentication method.				

c. Click the **Advanced** tab. Remove all the default parameters and click **Add**.

Edit Dial-in Profile		ĺ	? ×
Dial-in Constraints	∫ IP) Multilink	ļ
Authentication	Encryption	Advanced	
Access Server.	n attributes to be return	ned to the Remote	
Parameters:	Vendor	Value	_
•		<u>[</u>	1
Add <u>R</u> emove	e <u>E</u> dit		
	or 1 (Coursel 1 Acres	
			,

d. From the **Add Attributes** window, select **Service–Type**, then choose the **Login** value from the next window.

ADIU <u>S</u> attributes:			Enumerable Attribute Information	
Name	Vendor	Description	4.0.5. 4	
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	J	
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	6	
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	Attribute value	
Tunnel-Type	RADIUS Standard	Tunneling protocols to be used	Autowe value.	
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	Cance
USR-AT-Call-Output-Filter	U.S. Robotics, I	Description not available		Cance
USR-AT-Input-Filter	U.S. Robotics, I	Description not available		_
USR-AT-Output-Filter	U.S. Robotics, I	Description not available		
4		•		

e. Next, you need to select the Vendor-Specific attribute from the RADIUS attributes list.

Add Attributes		<u>?</u> ×	fultivalued Attribute Information	
To add an attribute to the Prof RADIU <u>S</u> attributes:	ile, select the attribut	e and block Add	Attribute name: Vendor-Specific	
Name Reply-Message Service-Type Turnel-Assignment-ID Turnel-Clerk-Auth-ID Turnel-Medum-Type Turnel-Preference Turnel-Preference Turnel-Preference Turnel-Preference Turnel-Server-Auth-ID Turnel-Server-Auth-ID 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 Turnel-Server-Endpt Turnel-Server-Endpt Turnel-Server-Endpt Turnel-Server-Endpt USR-AT-Cal-Input-Filter USR-AT-Cal-Input-Filter USR-AT-Output-Filter	Vendor RADIUS Standard RADIUS Standard Cisco Microsoft U.S. Robotics, L. U.S. Robotics, L. U.S. Robotics, L. U.S. Robotics, L. U.S. Robotics, L.	Description Message to be displayed to user when authenticat Type of service user has requested Turnel to which a session is to be assigned Name used by the tunnel inhibitor during the authen IP address of the initiator end of the tunnel Turnsport medium to use when creating a tunnel to Password for authenticating to a remote perver Relative preference assigned to each turnel when Group ID for a particular tunneled 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 user's dia-in properties Description not available Description not available Description not available	Attribute number: 26 Attribute format: DetetString Attribute values: Vendor Value	Move JJ Move Do Esmov Est
		Add Close	05	Cance

f. In the next window, click **Add** in order to select a new VSA.

The Vendor–Specific Attribute Information window appears.

- g. Under Specify network access server vendor, choose Enter Vendor Code.
- h. Enter the Vendor Code for Airespace VSAs. The Vendor Code for Cisco Airespace VSAs is **14179**.
- i. Because this attribute conforms with the RADIUS RFC specification for VSAs, choose **Yes. It conforms.**

Vendor-Specific Attribute Information
Attribute name: Vendor-Specific
Specify network access server vendor. O Select from list: RADIUS Standard Image: Enter Vendor Code: 14179
Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.
Configure <u>A</u> ttribute
OK Cancel

- j. Click Configure Attribute.
- k. In the Configure VSA (RFC compliant) window, enter the Vendor–assigned attribute number, the Attribute format and the Attribute value, which depend on the VSA that you want to use.

For setting the WLAN-ID on a per-user basis:

- ♦ Attribute Name Airespace–WLAN–Id
- **Vendor-assigned attribute number**;
- Attribute Format Integer/Decimal
- ◊ Value WLAN–ID

Example 1

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

For setting the QoS profile on a per–user basis:

- ◊ Attribute Name Airespace–QoS–Level
- \diamond Vendor–assigned attribute number¢
- ♦ Attribute Format Integer/Decimal
- ◊ Value Silver; 1 Gold; 2 Platinum; 3 Bronze

Example 2

Configure VSA (RFC compliant)		? ×
Vendor-assigned attribute number:		
Attribute format:		
_ Decimal		•
Attri <u>b</u> ute value: 3		
	OK Can	icel

For setting the DSCP Value on a per–user basis:

- ♦ Attribute Name Airespace–DSCP
- **Vendor-assigned** attribute aumber£
- **Attribute Format** Integer/Decimal
- **Value** DSCP Value

Example 3

Configure VSA (RFC compliant)	? ×
Vendor-assigned attribute number:	
3	
<u>A</u> ttribute format:	
Decimal	-
Attri <u>b</u> ute value:	
46	
OK Ca	ancel

For setting the 802.1p–Tag on a per–user basis:

- ♦ Attribute Name Airespace–802.1p–Tag
- **Vendor-assigned attribute number**^m
- Attribute Format Integer/Decimal
- ♦ Value 802.1p–Tag

Example 4

Configure VSA (RFC compliant)	? ×
Vendor-assigned attribute number:	
4	
<u>A</u> ttribute format:	
Decimal	
Attri <u>b</u> ute value:	
5	
	OK Cancel

For setting the Interface (VLAN) on a per-user basis:

- ◊ Attribute Name Airespace–Interface–Name
- ◊ Vendor–assigned attribute number¥
- **Attribute Format** String
- ◊ **Value** Interface–Name

Example 5

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

For setting the ACL on a per–user basis:

- ♦ Attribute Name Airespace–ACL–Name
- **Vendor-assigned attribute number**
- **Attribute Format** String
- ♦ Value ACL–Name

Example 6

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

- 8. Once you have configured the VSAs, click **OK** until you see the User profile window.
- 9. Then, click **Finish** in order to complete the configuration.

You can see the new policy under Remote Access Policies.

🐤 Internet Authentication Service			_ 🗆 ×
_ <u>A</u> ction View ← → 🗈 🖬 😼 😭			
Tree	Name	Order	
Internet Authentication Service (Local) Clients Remote Access Logging Remote Access Policies	S Airespace VSA	1	

Example Configuration

In this example, a WLAN is configured for web authentication. Users are authenticated by the IAS RADIUS server, and the RADIUS server is configured to allot QoS policies on a per–user basis.

I			Save Co	nfiguration Ping Logout
	MONITOR WLANS CO	NTROLLER WIRELESS SECURITY MANA	SEMENT COMMANDS	HELP
	WLANs > Edit			< Back App
	WLAN ID	1		
ups VIAN	WLAN SSID	SSID-WLC2		
	General Policies		Security Policies	
	Radio Policy	All 💌	Lavar 2 Saturity	None
	Admin Status	C Enabled	Layer 2 Sourity	MAC Filtering
	Session Timeout (secs)	0		,
	Quality of Service (QoS)	Silver (best effort) 💌	Layer 3 Security	None
	WMM Policy	Disabled W		Web Policy *
	7920 Phone Support	Client CAC Limit 🔲 AP CAC Limit		Authentication O Passt
	Broadcast SSID	Enabled	Preauthentication	none v
	Aironet IE	Enabled	AC	
	Allow AAA Override	✓ Enabled	* Web Policy cannot and L2TP.	be used in combination with
	Client Exclusion	Enabled ** 60	** When client exclu	sion is enabled, a timeout va
	DHCP Server	Override	to reset excluded di	ents) onted by 10xx APs
	DHCP Addr. Assignment	Required	Crist is not sup	and of toxy are
	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 tions.		
	Radius Servers			
	23.3	Authentication Servers Accounting Servers		
	Server 1	10:172.16.1.1. Port:1812 V Done V		

As you can see from this window, web authentication is enabled, the authentication server is 172.16.1.1, and AAA override is also enabled on the WLAN. The default QoS setting for this WLAN is set to Silver.

On the IAS RADIUS server, a Remote Access Policy is configured which returns the QoS attribute Bronze in the RADIUS accept request. This is done when you configure the VSA specific to the QoS attribute.

Configure VSA (RFC compliant)		? ×
Vendor-assigned attribute number:		
2		
<u>A</u> ttribute format:		
Decimal		•
Attri <u>b</u> ute value:		
3		
	ОК	Cancel

See the Configure the Remote Access Policy on the IAS section of this document for detailed information on how to configure a Remote Access Policy on the IAS server.

Once the IAS server, the WLC, and the LAP are configured for this setup, the wireless clients can use web authentication in order to connect.

Verify

Use this section to confirm that your configuration works properly.

When the user connects to the WLAN with a user ID and password, the WLC passes the credentials to the IAS RADIUS server which authenticates the user against the conditions and the user profile configured in the Remote Access Policy. If the user authentication is successful, the RADIUS server returns a RADIUS accept request which also contains the AAA override values. In this case, the QoS policy of the user is returned.

You can issue the **debug aaa all enable** command in order to see the sequence of events that occurs during authentication. Here is a sample output:

(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 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..... 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 70
resultCode.....
protocolUsed.....
0x00000008
proxvState Wed Apr 18 18:14:24 2007: Wed Apr 18 18:14:24 2007: Wed Apr 18 18:14:24 2007: 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-Typ
 AVP[01] Service-Type..... Wed Apr 18 18:14:24 2007: 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 proxyState..... Wed Apr 18 18:15:08 2007: Wed Apr 18 18:15:08 2007: 00:40:96:AC:E6:57-00:00 Packet contains 8 AVPs (not shown) Wed Apr 18 18:15:08 2007: Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Successful transmission of Authentication Pack (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:
 Packet contains 3 AVPs:

 Wed Apr 18 18:15:08 2007:
 AVP[01] Airespace /
 AVP[01] Airespace / QOS-Level..... 0x0000003 (3) (4 bytes) Wed Apr 18 18:15:08 2007: 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 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: AVP[01] User-Name..... Wed Apr 18 18:15:12 2007: User-VLAN10 (11 bytes) Wed Apr 18 18:15:12 2007: AVP[02] Nas-Port..... 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) 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) Wed Apr 18 18:15:12 2007: AVP[10] Tunnel-Group-Id..... 0x3230 (12848) (2 bytes) AVP[11] Acct-Status-Type..... Wed Apr 18 18:15:12 2007: 0x0000001 (1) (4 bytes) AVP[12] Calling-Station-Id..... Wed Apr 18 18:15:12 2007: 20.0.0.1 (8 bytes) AVP[13] Called-Station-Id..... Wed Apr 18 18:15:12 2007: 172.16.1.30 (11 bytes)

As you can see from the output, the user is authenticated. Then, AAA override values are returned with the RADIUS accept message. In this case, the user is given the QoS policy of Bronze.

You can verify this on the WLC GUI as well. Here is an example:

Or Clients > Detail < Back		MONITOR WLANS CONTR	OLLER WIRELESS SEC	URITY MANAGEMENT COM	Save Configuration Ping Logout
Arry broker Client Properties AP Properties MAC Address 00:40:96:ac:e6:57 AP Address 00:0b:85:5b:fb:d0 PSS is APS is APS is APS is APS is Clouds IP Address 20:0.0.1 AP Name ap:5b:fb:d0 Port Number 1 VLAN SJD SJD-WIC2 Port Number 1 WLAN SJD SJD-WIC2 Port Number 1 VLAN SJD SJD-WIC2 ULS Servers OCK Version CCXV3 802:11 Authentication Open System E2E Version Not Supported Reason Code 0 Mobility Role Local Status Code 0 Mobility Role Local Status Code 0 Policy Manager State RUN CP Poli Request Not Implemented Policy Type N/A PBCC Not Implemented Policy Type N/A PBCC Not Implemented Policy Type N/A Timeout 0 Resortity Policy Completed Yes Chanel Agility Not Implemented Policy Type N/A Timeout 0 Quality of Service Properties WIM State Disabled QS Level Bronze Dif Servi Code Point (DSC) disabled	or	Clients > Detail			< Back Link Test Remo
Hiss roller MAC Address 00:40:96:ac:e6:57 AF Address 00:0b:85:5b:fb:d0 PS IP Address 20.0.0.1 AP Name ap:5b:fb:d0 PS User Name User-VLANIO AP Type 802.11a m Rogue APS ie APS ie Cleards te Cleards Interface internal Status Associated 11ab/d Radios VLAN ID 20 Association ID 1 11b/d Radios CCX Version CCXv3 802.11 Authentication Open System 11b/d Radies Not Supported Reason Code 0 0 Mobility Pole N/A CF Pollable Not Implemented Policy Manager State RUN CF Pollable Not Implemented Security Information Security Policy Completed Yes Channel Agiity Not	iary	Client Properties		AP Properties	
B75 IP Address 20.0.0.1 AP Name ap:5b:fb:d0 B75 User Name User-VLAN10 AP Type 602.11a B75 Port Number 1 WLAN SSID SSID-WLC2 C Rogues Interface internal Status Associated L1b/g Radios VLAN ID 20 Association ID 1 L1b/g Radios VLAN ID 20 Association ID 1 L1b/g Radios VLAN ID CCXV3 802.11 Authentication Open System L2C Version CCXV3 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 Policy Type N/A Phole WEP State WEP Disable Security Policy Completed Yes Channel Agilty Not Implemented Policy Type N/A WEP State WEP Disable Quality of Service Propertise N/A WEP Disable VEP State Qof Level Bronze Diff Serv Code Point (DSCP) disabled	tics roller	MAC Address	00:40:96:ac:e6:57	AP Address	00:0b:85:5b:fb:d0
BSS is a APS in R Aguet APS is Clearistic is C Request Las Radios ta		IP Address	20.0.0.1	AP Name	ap:5b:fb:d0
Port Number 1 WLAN SSID SSID-WLC2 in Regue APS is Clearts Interface internal Status Associated Lia Radios Lia Radios Lia Radios BUD/g Radios MUS Servers 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 Pollable Not Implemented Security Information Security Completed Yes Channel Agility Not Implemented Policy Type N/A Timeout 0 0 0 EAP Type N/A Timeout 0 0 0 Policy Type N/A Timeout 0 0 0 Policy Type N/A Timeout 0 0 0 0 Policy Of Service Propertize Disabled Disabled Disabled Disabled Disabled Disabled Disabled	ess APr	User Name	User-VLAN10	AP Type	802.11a
ab Cleants Interface internal Status Associated 11 a Radios VLAN ID 20 Association ID 1 11 b/g Radios CCX Version CCXV3 802.11 Authentication Open System 11 b/g Radios CCX Version CCXV3 802.11 Authentication Open System 11 b/g Radios CCX Version Not Supported 8eason Code 0 11 b/g Radios Local CP Pollable Not Implemented 11 b/g Radios N/A CF Pollable Not Implemented Policy Manager State RUN CF Pollable Not Implemented Policy Manager State RUN CF Poll Request Not Implemented Policy Type N/A Channel Agility Not Implemented Policy Type N/A Timeout 0 EAP Type N/A WMM State Disabled Versite Versite Versite Quality of Service Properties Bronze Disabled Bronze Versite Versite Versite Diff Serv Code Point (DSCP) disabled Bronze Versite Versite Ver	in Rogue APs	Port Number	1	WLAN SSID	SSID-WLC2
Lit Rediosi VLAN ID 20 Association ID 1 Lit b/g Radiosi CCX Version CCXv3 802.11 Authentication Open System Lit S 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 Pollable Not Implemented Security Information Yes Short Preamble Not Implemented Security Policy Completed Yes Channel Agility Not Implemented Policy Type N/A Timeout 0 1 EAP Type N/A WEP State WEP Disable WEP Disable Quality of Service Propertis- Bisabled QoS Level Bronze VER State VER State<	e Clients c Rogues	Interface	internal	Status	Associated
Rs CCX Version CCXV3 802.11 Authentication Open System E2E Version Not Supported Reason Code 0 Mobility Role Local Status 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 Yes Channel Agility Not Implemented Security Policy Completed Yes Channel Agility Not Implemented Policy Type N/A Timeout 0 Encryption Cipher None WEP State WEP Disable Quality of Service Propertise Fornze VMM State Disabled QoS Level Bronze Bronze Diff Serv Code Point (DSCP) disabled	11a Radios	VLAN ID	20	Association ID	1
E2E Version Not Supported Reason Code 0 Mobility Role Local Status Code 0 Mobility Role Local CF Pollable Not Implemented Policy Manager State RUN CF Poll Request Not Implemented Security Information PBCC Not Implemented Security Policy Completed Yes Channel Agility 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 Timeout 0 Quality of Service Propertics Bronze VMM State Disabled Opi Level Bronze Disabled US	ts	CCX Version	CCXv3	802.11 Authentication	Open System
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 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 WEP State WEP Disable VMM State Disabled Disabled US US Optic Service Propert (DSCP) disabled US US US Optif Serv Code Point (DSCP) disabled US US US	US Servers	E2E Version	Not Supported	Reason 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 Channel Agility Not Implemented Policy Type N/A Timeout 0 Encryption Cipher None WEP State WEP Disable EAP Type N/A Security Policy Complete Yes Ogs Level Disabled WIM State Disabled Opticy Code Point (DSCP) disabled Verse Verse		Mobility Role	Local	Status Code	0
Policy Manager State RUN CF Poli Request Not Implemented Security Information Short Preamble Not Implemented Security Policy Completed Yes Channel Agility Not Implemented Security Policy Type N/A Channel Agility Not Implemented Policy Type N/A Timeout 0 Encryption Cipher N/A WEP State WEP Disable Quality of Service Properties WMM State Disabled OoS Level Bronze Diff Serv Code Point (DSCP) disabled		Mobility Peer IP Address	N/A	CF Pollable	Not Implemented
Security Information Short Preamble 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 Ver State Ver State WMM State Disabled Bronze Ver State Ver State Diff Serv Code Point (DSCP) disabled Ver State Ver State		Policy Manager State	RUN	CF Poll Request	Not Implemented
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 WEP State WEP Disable Quality of Service Properties Usabled Vertice Properties Vertice Properties WMM State Disabled Disabled Vertice Properties Diff Serv Code Point (DSCP) disabled Vertice Properties		Security Information		Short Preamble	Not Implemented
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		Security Policy Completed	Yaz	PBCC	Not Implemented
Pointy type None 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		Policy Type	N/A	Channel Agility	Not Implemented
EAP Type N/A Quality of Service Properties WMM State Disabled QoS Level Diff Serv Code Point (DSCP)		Encryption Cipher	None	Timeout	0
Quality of Service Properties WMM State Disabled QoS Level Bronze Diff Serv Code Point (DSCP) disabled		EAP Type	N/A	WEP State	WEP Disable
WMM State Disabled QoS Level Bronze Diff Serv Code Point (DSCP) disabled		Quality of Service Properties			
QoS Level Bronze Diff Serv Code Point (DSCP) disabled		WMM State	Disabled		
Diff Serv Code Point (DSCP) disabled		QoS Level	Bronze		
		Diff Serv Code Point (DSCP)	disabled		
802.1p Tag disabled		802.1p Tag	disabled		
					Internet

Note: The default QoS profile for this SSID is Silver. However, because AAA override is selected and the user is configured with a QoS profile of Bronze on the IAS server, the default QoS profile is overridden.

Troubleshoot

You can use the **debug aaa all enable** command on the WLC to troubleshoot the configuration. An example of the output of this debug in a working network is shown in the Verify section of this document.

Note: Refer to Important Information on Debug Commands before you use debug commands.

Related Information

- Cisco Wireless LAN Controller Configuration Guide, Release 4.0
- Restrict WLAN Access based on SSID with WLC and Cisco Secure ACS Configuration Example
- Wireless Product Support
- Technical Support & Documentation Cisco Systems

Contacts & Feedback | Help | Site Map

© 2013 – 2014 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.