# Esempio di configurazione di VSA Cisco Airespace su Microsoft IAS Radius Server

## Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Premesse Configurazione di IAS per VSA Airespace Configurare il WLC come client AAA su IAS Configurare i criteri di accesso remoto su IAS Esempio di configurazione Verifica Risoluzione dei problemi Informazioni correlate

### **Introduzione**

In questo documento viene spiegato come configurare un server Microsoft Internet Authentication Service (IAS) per supportare gli attributi specifici del fornitore (VSA) di Cisco Airespace. Il codice del fornitore per i VSA Cisco Airespace è **14179**.

# **Prerequisiti**

#### Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Informazioni sulla configurazione di un server IAS
- Conoscenza della configurazione dei Lightweight Access Point (LAP) e dei Cisco Wireless LAN Controller (WLC)
- Conoscenza delle soluzioni Cisco Unified Wireless Security

#### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Server Microsoft Windows 2000 con IAS
- Cisco 4400 WLC con software versione 4.0.206.0
- Cisco serie 1000 LAP
- scheda client wireless 802.11 a/b/g con firmware 2.5
- Aironet Desktop Utility (ADU) versione 2.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

**Nota:** questo documento intende fornire al lettore un esempio della configurazione richiesta sul server IAS per supportare le VSA Cisco Airespace. La configurazione del server IAS descritta in questo documento è stata testata in laboratorio e funziona come previsto. In caso di problemi durante la configurazione del server IAS, contattare Microsoft per assistenza. Cisco TAC non supporta la configurazione del server Microsoft Windows.

In questo documento si presume che il WLC sia configurato per il funzionamento di base e che i LAP siano registrati sul WLC. Se si è un nuovo utente che cerca di configurare il WLC per il funzionamento di base con i LAP, fare riferimento alla <u>registrazione di un Lightweight AP (LAP) su un Wireless LAN Controller (WLC)</u>.

#### **Convenzioni**

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> nei suggerimenti tecnici.

### Premesse

Nella maggior parte dei sistemi WLAN (Wireless LAN), ogni WLAN ha un criterio statico che si applica a tutti i client associati a un SSID (Service Set Identifier). Sebbene potente, questo metodo presenta delle limitazioni in quanto richiede ai client di associarsi a SSID diversi per ereditare criteri QoS e di sicurezza diversi.

Tuttavia, la soluzione Cisco Wireless LAN supporta le reti di identità, che consentono alla rete di annunciare un singolo SSID e a utenti specifici di ereditare diverse policy di sicurezza o QoS in base ai rispettivi profili utente. I criteri specifici che è possibile controllare utilizzando Identity Networking includono:

- Quality of Service: quando è presente in un'accettazione di accesso RADIUS, il valore del livello QoS sostituisce il valore QoS specificato nel profilo WLAN.
- ACL: quando l'attributo Access Control List (ACL) è presente in RADIUS Access Accept, il sistema applica l'ACL-Name alla stazione client dopo l'autenticazione. In questo modo si ignorano gli ACL assegnati all'interfaccia.
- VLAN: quando un nome di interfaccia VLAN o un tag VLAN è presente in un'accettazione di accesso RADIUS, il sistema posiziona il client su un'interfaccia specifica.
- ID WLAN: quando l'attributo WLAN-ID è presente nell'autorizzazione di accesso RADIUS, il sistema applica l'ID WLAN (SSID) alla stazione client dopo l'autenticazione. L'ID WLAN viene inviato dal WLC in tutte le istanze di autenticazione ad eccezione di IPSec. In caso di autenticazione Web, se il WLC riceve un attributo WLAN-ID nella risposta di autenticazione

dal server AAA e non corrisponde all'ID della WLAN, l'autenticazione viene rifiutata. Non è possibile utilizzare altri tipi di metodi di protezione.

- Valore DSCP: se presente in un'accettazione di accesso RADIUS, il valore DSCP sostituisce il valore DSCP specificato nel profilo WLAN.
- **802.1p-Tag**: quando è presente in un'accettazione di accesso RADIUS, il valore 802.1p sostituisce il valore predefinito specificato nel profilo WLAN.

**Nota:** la funzione VLAN supporta solo il filtro MAC, 802.1X e l'accesso protetto Wi-Fi (WPA). La funzionalità VLAN non supporta l'autenticazione Web o IPSec. Il database del filtro MAC locale del sistema operativo è stato esteso per includere il nome dell'interfaccia. In questo modo, i filtri MAC locali possono specificare l'interfaccia da assegnare al client. È possibile utilizzare anche un server RADIUS separato, ma il server RADIUS deve essere definito utilizzando i menu Security.

Per ulteriori informazioni sulle reti di identità, fare riferimento a <u>Configurazione di Identity</u> <u>Networking</u>.

# Configurazione di IAS per VSA Airespace

Per configurare gli IAS per le VSA Airespace, completare i seguenti passaggi:

- 1. Configurare il WLC come client AAA su IAS
- 2. Configurare i criteri di accesso remoto su IAS

Nota: le VSA sono configurate in Criteri di accesso remoto.

#### Configurare il WLC come client AAA su IAS

Completare questa procedura per configurare il WLC come client AAA sullo switch IAS:

 Per avviare IAS sul server Microsoft 2000, fare clic su Programmi > Strumenti di amministrazione > Servizio di autenticazione Internet.



- 2. Fare clic con il pulsante destro del mouse sulla cartella **Clients** e scegliere **New Client** per aggiungere un nuovo client RADIUS.
- Nella finestra Add Client, immettere il nome del client e scegliere RADIUS come protocollo. Fare quindi clic su Avanti.Nell'esempio, il nome del client è WLC-1.Nota: per impostazione predefinita, il protocollo è impostato su RADIUS.

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

4. Nella finestra Aggiungi client RADIUS, immettere l'indirizzo IP del client, il fornitore del client e il segreto condiviso. Dopo aver immesso le informazioni sul client, fare clic su Fine.Nell'esempio viene mostrato un client denominato WLC-1 con indirizzo IP 172.16.1.30, il client-fornitore è impostato su Cisco e il segreto condiviso è cisco123:

Add RADIUS Client		×
Client Information Specify information regarding the	client.	
Client a <u>d</u> dress (IP or DNS):		
172.16.1.30		Verify
Client-Vendor:		
Cisco		▼
Client must always send the s	ignature attribute in the request	
Shared secret:	*****	
Con <u>f</u> irm shared secret:	*****	
	< <u>B</u> ack	Finish Cancel

Con queste informazioni, il WLC denominato WLC-1 viene aggiunto come client AAA del server

IAS.

🐤 Internet Authentication Service				
_ <u>A</u> ction View   ← →   🔁 📆 💼 🖽 (	2			
Tree	Friendly Name	Address	Protocol	Client-Vendor
Tree Internet Authentication Service (Local)	Friendly Name	Address 172.16.1.30	Protocol RADIUS	Cient-Vendor Cisco

Il passaggio successivo consiste nella creazione di un criterio di accesso remoto e nella configurazione delle VSA.

#### Configurare i criteri di accesso remoto su IAS

Completare questi passaggi per configurare un nuovo criterio di accesso remoto sullo IAS:

- 1. Fare clic con il pulsante destro del mouse su **Criteri di accesso remoto** e scegliere **Nuovo criterio di Accesso remoto MSss**.Viene visualizzata la finestra Nome criterio.
- 2. Immettere il nome del criterio e fare clic su **Avanti**.

emote A	ccess Policy
licy Name	
Specify -	a friendly name for the policy.
A Remot meeting	e Access Policy is a set of actions which can be applied to a group of users certain conditions.
Analogou specify a You can	is to rules you can apply to incoming mail in an e-mail application, you can set of conditions that must be matched for the Remote Access Policy to apply. Then specify actions to be taken when the conditions are met.
<u>Policy</u> frie	endly name:
Airespac	e VSA
·	
	< Back Next > Can

 Nella finestra successiva selezionare le condizioni a cui verranno applicati i criteri di accesso remoto. Per selezionare le condizioni, fare clic su Add (Aggiungi).

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 dated by user           Called-Station-Id         Phone number from which call originated           Clent-Friendly-Name         Friendly name for the RADIUS clent. (IAS only)           Clent-PAddress         IP address of RADIUS clent. (IAS only)           Clent-Vendor         Manufacturer of RADIUS clent. (IAS only)           Clent-Vendor         Manufacturer of RADIUS clent. (IAS only)           Clent-Vendor         The periods and days of week during which use           Framed-Photocol         The protocol to be used           NAS-Identitier         String identifying the NAS originating the request           NAS-Identitier         String identifying the NAS originating the request           NAS-Port-Type         Type of physical port used by the NAS originating           Service-Type         Type of service user has requested           Tunnel-Type         Tunneling protocols to be used           Windows-Groups         Windows groups that user belongs to
Add Eemove Ech	×¥
< <u>B</u> ack <u>N</u> ext> Cancel	Add Cancel

4. Dal menu Tipi di attributo, selezionare i seguenti attributi: **Client-IP-Address**: immettere l'indirizzo IP del client AAA. Nell'esempio, viene immesso l'indirizzo IP del WLC, in modo che il criterio venga applicato ai pacchetti provenienti dal

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

Windows: selezionare il gruppo di Windows (il gruppo di utenti) a cui applicare il criterio. Di seguito è riportato un

308 Groups	? ×
The following groups are currently in this condition.	
<u>G</u> roups:	
Name	
CAT-TD-2K\Test-Clients	
<u>Aga</u> <u>H</u> emove	
ΩK	Cancel
esempio	

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"	ł
A <u>d</u> d <u>R</u> emove <u>E</u> dit	
< <u>B</u> ack <u>N</u> ext> Can	cel

In questo esempio vengono illustrate solo due condizioni. Se sono presenti altre condizioni, aggiungerle e fare clic su **Avanti**.Viene visualizzata la finestra Autorizzazioni.

 Nella finestra Autorizzazioni scegliere Concedi autorizzazione di accesso remoto.Dopo aver scelto questa opzione, all'utente viene concesso l'accesso, purché soddisfi le condizioni specificate (dal passaggio 2).

id Rem	ote Access Policy
Permi	sions
D	etermine whether to grant or deny remote access permission.
Y	ou can use a Remote Access Policy either to grant certain access privileges to a
g	roup of users, or to act as a filter and deny access privileges to a group of users.
lf	a user matches the specified conditions:
6	Grant remote access permission
0	
`	
	( Rock Nout ) Concel

- 6. Fare clic su Next (Avanti).
- 7. Il passaggio successivo consiste nell'impostare il profilo utente. Anche se è stato specificato che l'accesso agli utenti deve essere negato o concesso in base alle condizioni, il profilo può comunque essere utilizzato se le condizioni di questo criterio vengono ignorate per ogni utente.

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

Per configurare il profilo utente, fare clic su **Modifica profilo** nella finestra Profilo utente.Viene visualizzata la finestra Modifica profilo chiamate in

dit Dial-in Profile			? ×
Authentication	Encryption	) Adva	anced
Dial-in Constraints	IP IP		ultilink [
Disconnect if idle for:		1	min.
Restrict <u>m</u> aximum session	n to:	1 🛓	] min.   -
Restrict access to the fo	llowing days and tin	nes:	
	<u>E</u> dit		
Restrict Dial-in to this nu	mber only:		
🗖 🗖 <u>R</u> estrict Dial-in media: —	-		
FDDI			
Token Ring			
Wireless - IEEE 802.11			
	ОК	Cancel	Apply
-			

ingresso.

clic sulla scheda **Authentication** (Autenticazione), quindi selezionare il metodo di autenticazione utilizzato nella WLAN.In questo esempio viene utilizzata l'autenticazione non crittografata

Ec	dit Dial-in Profile		? ×		
	Dial-in Constraints	IP	Multilink		
	Authentication	Encryption	Advanced		
	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)				
			Conigure		
	Microsoft Encrypted	Microsoft Encrypted Authentication version <u>2</u> (MS-CHAP v2)			
	I <u>Microsoft Encrypted</u>	Authentication (MS-CHAP	)		
	Encrypted Authentica	Encrypted Authentication (CHAP)			
	🔽 Unencrypted Authen	Unencrypted Authentication (PAP, SPAP)			
	Unauthenticated Access	· · · · · · · · · · · · · · · · · · ·			
	Allow remote <u>PPP</u> clients to connect without negotiating any authentication method.				
		OK Ca	ncel Annlu		
P).					

e clic sulla scheda Avanzate. Rimuovete tutti i parametri di default e fate clic su Aggiungi

Dial-in Constraints	l l	P Ì	Multilink	
Authentication	Encry	ption	Advanced	ł
Specify additional conne Access Server. Parameters:	ection attributes	to be returned t	o the Remote	
Name	Vendor	Va	lue	
▲ 	move	Edit		Þ

finestra **Aggiungi attributi**, selezionare **Service-Type**, quindi scegliere il valore **Login** dalla finestra

#### successiva.

\dd Attributes		<u>? ×</u>	1	
To add an attribute to the Prof	ile, select the attribut	e and click Add		
RADIUS attributes:			Enumerable Attribute Information ?	х
Name	Vendor	Description		
Reply-Message	RADIUS Standard	Message to be displayed to user when authenticati	Attribute name:	
Service-Type	RADIUS Standard	Type of service user has requested	Service-Type	_
Tunnel-Assignment-ID	RADIUS Standard	Tunnel to which a session is to be assigned		
Tunnel-Client-Auth-ID	RADIUS Standard	Name used by the tunnel initiator during the authen	Altibute 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	b b	
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	All the test setue:	
Tunnel-Type	RADIUS Standard	Tunneling protocols to be used	Autore vare.	-
Vendor-Specific	RADIUS Standard	Used to support proprietary NAS features	Login	-
Cisco-AV-Pair	Cisco	Cisco AV Pair VSA		
Ignore-User-Dialin-Properties	Microsoft	Ignore the user's dial-in properties		
USR-ACCM-Type	U.S. Robotics, I	Description not available		
USR-AT-Call-Input-Filter	U.S. Robotics, I	Description not available	OK Cancel	
USR-AT-Call-Output-Filter	U.S. Robotics, I	Description not available		
USR-AT-Input-Filter	U.S. Robotics, I	Description not available		
USR-AT-Output-Filter	U.S. Robotics, I	Description not available		
•		E E E E E E E E E E E E E E E E E E E		
		Add Dose		

Quindi, selezionare l'attributo **specifico del fornitore** dall'elenco degli attributi RADIUS.

Add Attributes			? ×	ľ	Multivalued Attribute Information	? ×
To add an attribute to the Profi RADIU <u>S</u> attributes:	ie, select the attribute	and click Add			Attribute name: Vendor-Specific	
Name	Vendor	Description			áltribute number:	
Heply-Message	RADIUS Standard	Message to be displayed to user when authentica	-			
Service-Type Transit Assistant (D	RADIUS Standard	Type of service user has requested			20	
Turmel-Assignment-ID	RADIUS Standard	I unnel to which a session is to be assigned.				
Tunnel Clent Endet	RADIUS Standard	Name used by the tunner initiator during the author ID address of the initiates and of the tunnel	1		Attribute format:	
TurnerClencenapt	RADIUS Standard	Transport medium is use when creation a brond if			OctetString	
TurnelReenund	RéDILIS Standard	Password for authentication to a remote resear	·			
Tunnel-Preference	BADILIS Standard	Relative preference assigned to each turnel when			Attribute values:	
Tunnel-Pyt-Group-ID	BADIUS Standard	Group ID for a particular tunneled session			Mandar Maker	Maria Ha
Tunnel-Server-Auth-ID	RADIUS Standard	Name used by the tunnel terminator during the aut	- C.		vendor value	Move Db
Tunnel-Server-Endpt	RADIUS Standard	IP address of the server end of the tunnel				Hour Bown
Tunnel-Type	RADIUS Standard	Tunneling protocols to be used			-	nues <u>p</u> osn
Vendor-Specific	RADIUS Standard	Used to support proprietary NAS features				bbd
Cisco-AV-Pair	Cisco	Cisco AV Pair VSA			L	- <u></u>
Ignore-User-Dialin-Properties	Microsoft	Ignore the user's dial-in properties				Removo
USR-ACCM-Type	U.S. Robolics, I	Description not available			-	Tipunako
USR-AT-Call-Input-Filter	U.S. Robotics, I	Description not available				5.0
USR-AT-Call-Output-Filter	U.S. Robotics, I	Description not available			-	Enn
USR-AT-Input-Filter	U.S. Robolics, I	Description not available	22 I.			
USR-AT-Output-Filter	U.S. Hobolics, I	Description not available	_ لئے			
1 I I I I I I I I I I I I I I I I I I I		<u>`</u>				
		Add Close			0K	Cancel

Per selezionare una nuova VSA, fare clic su Add (Aggiungi) nella finestra successiva.Viene visualizzata la finestra Informazioni attributi specifici del fornitore.In Specificare il fornitore del server di accesso alla rete, scegliere Immettere il codice fornitore.Immettere il codice del fornitore per le VSA Airespace. Il codice del fornitore per i VSA Cisco Airespace è 14179.Poiché questo attributo è conforme alla specifica RFC RADIUS per le VSA, scegliere Sì. È

Vendor-Specific	
pecify network access se	rver vendor.
Select from list:	RADIUS Standard
Enter Vendor Code: pecify whether the attribute endor specific attributes.	14179 te conforms to the RADIUS RFC specification fo
<ul> <li>Enter Vendor Code:</li> <li>pecify whether the attributendor specific attributes.</li> <li>Yes. It conforms.</li> <li>No. It does not conform.</li> </ul>	14179 te conforms to the RADIUS RFC specification fo

Fare clic

conforme.

su Configura attributo.Nella finestra Configure VSA (RFC compliant), immettere il numero di

attributo assegnato dal fornitore, il formato dell'attributo e il valore dell'attributo, che dipendono dal VSA che si desidera utilizzare.Per impostare l'ID WLAN per singolo utente:**Nome attributo**: Airespace-WLAN-Id**Numero attributo assegnato dal fornitore**\_\_\_1Formato attributo: intero/decimaleValore: WLAN-IDEsempio 1

Configure ¥SA (RFC compliant)		? >
Vendor-assigned attribute number:		
1		
<u>A</u> ttribute format:		
Decimal		-
Attri <u>b</u> ute value:		
2		
	ОК	Cancel

profilo QoS per singolo utente:**Nome attributo**: Airespace-QoS-Level**Numero attributo assegnato dal fornitore**—2**Formato attributo**: intero/decimale**Valore**—0 - Argento; 1 - Oro; 2 platino; 3 - Bronzo**Esempio 2** 

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

valore DSCP per singolo utente:**Nome attributo**: Airespace-DSCP**Aumber attributo assegnato** dal fornitore—3Formato attributo: intero/decimaleValore: valore DSCPEsempio 3

C	Configure VSA (RFC compliant)	
	Vendor-assigned attribute number:	
	3	
	<u>A</u> ttribute format:	
	Decimal 💌	
	Attri <u>b</u> ute value:	
	46	
		-
•	OK Cancel	

Per impostare il tag

802.1p per ogni utente: Nome attributo: Airespace-802.1p-TagNumero attributo assegnato dal fornitore: 4Formato attributo: intero/decimaleValore—Tag 802.1pEsempio 4

Configure VSA (RFC compliant)	? ×
Vendor-assigned attribute number:	
4	
, Attribute format:	
	<b>_</b>
Attribute value:	
S	
	innent I
	Denimenseten
	Per impostare

l'interfaccia (VLAN) per singolo utente: Nome attributo: Airespace-Interface-NameNumero attributo assegnato dal fornitore-5Formato attributo: StringValue - Interface-NameEsempio

	Configure VSA (RFC compliant)	]
	Vendor-assigned attribute number:	
	5	
	<u>A</u> ttribute format:	
	String	
	Attri <u>b</u> ute value:	
	vlan10	
	OK Cancel	
5		Per impostare

Per impostare

l'ACL in base all'utente: Nome attributo: Airespace-ACL-NameNumero attributo assegnato dal fornitore—6Formato attributo: StringValue: ACL-NameEsempio 6

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

- 8. Dopo aver configurato le VSA, fare clic su **OK** fino a visualizzare la finestra del profilo utente.
- 9. Quindi, fare clic su Finish (Fine) per completare la configurazione.È possibile visualizzare il nuovo criterio in Criteri di accesso remoto.

🐤 Internet Authentication Service			l X
Action View 🖉 🖙 🔁 🖬 😼 😭			
Tree	Name	Order	_
<ul> <li>Provide Authentication Service (Local)</li> <li>☐ Clients</li> <li>☐ Remote Access Logging</li> <li>④ ♥ Remote Access Policies</li> </ul>	Airespace VSA	1	

#### Esempio di configurazione

Nell'esempio, una WLAN è configurata per l'autenticazione Web. Gli utenti vengono autenticati dal server RADIUS IAS e il server RADIUS è configurato per allocare i criteri QoS per singolo utente.



Come si può vedere da questa finestra, l'autenticazione Web è abilitata, il server di autenticazione è 172.16.1.1 e sulla WLAN è abilitata anche la sostituzione AAA. L'impostazione predefinita di QoS per questa WLAN è Silver.

Sul server RADIUS IAS, è configurato un criterio di accesso remoto che restituisce l'attributo QoS Bronze nella richiesta di accettazione RADIUS. A tale scopo, è necessario configurare la VSA specifica per l'attributo QoS.

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

Per informazioni dettagliate su come configurare un criterio di accesso remoto sul server IAS, vedere la sezione <u>Configurazione</u> del criterio di accesso remoto<u>sullo</u> IAS di questo documento.

Una volta configurati il server IAS, il WLC e il LAP per questa configurazione, i client wireless possono utilizzare l'autenticazione Web per connettersi.

### **Verifica**

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Quando l'utente si connette alla WLAN con un ID utente e una password, il WLC passa le credenziali al server IAS RADIUS che autentica l'utente in base alle condizioni e al profilo utente configurati nei criteri di accesso remoto. Se l'autenticazione dell'utente ha esito positivo, il server RADIUS restituisce una richiesta di accettazione RADIUS contenente anche i valori di sostituzione AAA. In questo caso, viene restituito il criterio QoS dell'utente.

Èpossibile usare il comando **debug aaa all enable** per visualizzare la sequenza di eventi verificatisi durante l'autenticazione. Di seguito è riportato un esempio di output:

(Ci	sco (	Cont	troller) >	debug	g 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
					mobil	Le 28:1f:00:00:00:00	
Wed	Apr	18	18:14:24	2007:	Autho	orizationResponse: 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:	
Wed	Apr	18	18:14:24	2007:		AVP[01] Service-Type	
						0x0000006 (6) (4 bytes)	
Wed	Apr	18	18:14:24	2007:		AVP[02] Airespace / WLAN-Identifier	
						$0 \times 00000000$ (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 29:1F:00:00:00:00-00:00 Wed Apr 18 18:14:24 2007: Packet contains 2 AVPs: Wed Apr 18 18:14:24 2007: AVP[01] Service-Type..... 0x0000006 (6) (4 bytes) AVP[02] Airespace / WLAN-Identifier..... Wed Apr 18 18:14:24 2007: 0x00000000 (0) (4 bytes) Wed Apr 18 18:15:08 2007: Unable to find requested user entry for User-VLAN10 Wed Apr 18 18:15:08 2007: AuthenticationRequest: 0xa64c8bc Wed Apr 18 18:15:08 2007: Callback.....0x8250c40 Wed Apr 18 18:15:08 2007: protocolType.....0x0000001 proxyState..... 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 Wed Apr 18 18:15:08 2007: 00000000: 01 1a 00 68 00 00 00 00 00 00 00 00 00 00 00 00 ...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 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 resultCode.....0 protocolUsed.....0x00000001 proxyState..... Wed Apr 18 18:15:08 2007: 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 3 AVPs: AVP[01] Airespace / QOS-Level..... Wed Apr 18 18:15:08 2007: 0x0000003 (3) (4 bytes) Wed Apr 18 18:15:08 2007: AVP[02] Service-Type..... 0x00000001 (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: Wed Apr 18 18:15:12 2007: AVP[01] User-Name..... User-VLAN10 (11 bytes) Wed Apr 18 18:15:12 2007: AVP[02] Nas-Port..... 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..... 0x0000001 (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: 0x000000d (13) (4 bytes) AVP[09] Tunnel-Medium-Type..... Wed Apr 18 18:15:12 2007: 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) 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)

Come si può vedere dall'output, l'utente è autenticato. I valori di sostituzione AAA vengono quindi restituiti con il messaggio di accettazione RADIUS. In questo caso, all'utente viene data la politica QoS del Bronzo.

Èpossibile verificarlo anche sull'interfaccia utente del WLC. Di seguito è riportato un esempio:

	MONITOR WLANS CONTR	OLLER WIRELESS SECU	RITY MANAGEMENT COMM	IANDS HELP	
nitor	Clients > Detail			< Back Link Test Remov	
nmary	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	
own Rogue APs	Port Number	1	WLAN SSID	SSID-WLC2	
dhoc Rogues	Interface	internal	Status	Associated	
2.11a Radios	VLAN ID	20	Association ID	1	
lients	CCX Version	CCXv3	802.11 Authentication	Open System	
ADIUS Servers	E2E Version	Not Supported	Reason Code	0	
	Mobility Role	Local	Status Code	0	
	Mobility Peer IP Address	N/A	CF Pollable	Not Implemented	
	Policy Manager State	RUN	CF Poll Request	Not Implemented	
	Regulty Information		Short Preamble	Not Implemented	
	security information		PBCC	Not Implemented	
	Security Policy Completed	Yes	Channel Agility Timeout WEP State	Not Implemented	
	Policy Type	N/A		0 WEP Disable	
	Encryption Cipher	None			
	EAP Type	N/A			
	Quality of Service Propert	es			
	WMM State	Disabled			
	QoS Level	Bronze			
	Diff Serv Code Point (DSCP)	disabled			
	802.1p Tag	disabled			
	Average Data Rate	disabled			

**Nota:** il profilo QoS predefinito per questo SSID è Silver. Tuttavia, poiché è stata selezionata la sostituzione AAA e l'utente è configurato con un profilo QoS Bronze sul server IAS, il profilo QoS predefinito viene sostituito.

### Risoluzione dei problemi

Per risolvere i problemi di configurazione, è possibile usare il comando **debug aaa all enable** sul WLC. Nella sezione <u>Verifica</u> di questo documento viene mostrato un esempio dell'output di questo debug in una rete funzionante.

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> prima di usare i comandi di **debug**.

## Informazioni correlate

- Guida alla configurazione di Cisco Wireless LAN Controller, versione 4.0
- Esempio di limitazione dell'accesso WLAN in base al SSID con WLC e Cisco Secure ACS
- <u>Supporto dei prodotti wireless</u>
- Documentazione e supporto tecnico Cisco Systems