# Configurazione di un server RADIUS e di un WLC per l'assegnazione dinamica della VLAN

# Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Assegnazione dinamica di VLAN con server RADIUS Configurazione Esempio di rete Configurazione Procedura di configurazione Configurazione server RADIUS Configurazione dell'ACS con gli attributi VSA di Cisco Airespace per l'assegnazione dinamica della VLAN Configurazione dello switch per più VLAN **Configurazione WLC Configurazione Wireless Client Utility** Verifica Risoluzione dei problemi Informazioni correlate

# **Introduzione**

In questo documento viene spiegato il concetto di assegnazione dinamica delle VLAN. In questo documento viene descritto come configurare il controller WLC (Wireless LAN Controller) e un server RADIUS per assegnare dinamicamente i client WLAN (Wireless LAN) a una VLAN specifica.

# **Prerequisiti**

## **Requisiti**

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

- Conoscere a fondo i WLC e i Lightweight Access Point (LAP)
- Conoscenza funzionale del server AAA
- Conoscere a fondo le reti wireless e i problemi di sicurezza wireless

Conoscenze base di LWAPP (Lightweight AP Protocol)

### Componenti usati

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

- Cisco 4400 WLC con firmware release 5.2
- Cisco serie 1130 LAP
- Cisco 802.11a/b/g Wireless Client Adapter con firmware versione 4.4
- Cisco Aironet Desktop Utility (ADU) con versione 4.4
- Cisco Secure Access Control Server (ACS) con versione 4.1
- Cisco serie 2950 switch

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.

## **Convenzioni**

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

# Assegnazione dinamica di VLAN con server RADIUS

Nella maggior parte dei sistemi WLAN, ogni WLAN dispone di un criterio statico che viene applicato a tutti i client associati a un SSID (Service Set Identifier) o a una WLAN nella terminologia del controller. 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 WLAN supporta le reti di identità. Ciò consente alla rete di annunciare un singolo SSID, ma consente a utenti specifici di ereditare criteri QoS o di sicurezza diversi in base alle credenziali utente.

L'assegnazione dinamica della VLAN è una di queste funzionalità che permette a un utente wireless di accedere a una VLAN specifica in base alle credenziali fornite dall'utente. L'assegnazione degli utenti a una VLAN specifica viene gestita da un server di autenticazione RADIUS, ad esempio CiscoSecure ACS. Questa funzione può essere utilizzata, ad esempio, per fare in modo che l'host wireless rimanga sulla stessa VLAN su cui si sposta all'interno della rete di un campus.

Pertanto, quando un client tenta di associarsi a un LAP registrato con un controller, il LAP passa le credenziali dell'utente al server RADIUS per la convalida. Una volta completata l'autenticazione, il server RADIUS passa all'utente alcuni attributi IETF (Internet Engineering Task Force). Questi attributi RADIUS determinano l'ID VLAN da assegnare al client wireless. L'SSID (WLAN, in termini di WLC) del client non conta perché l'utente è sempre assegnato a questo ID VLAN predeterminato.

Gli attributi utente RADIUS utilizzati per l'assegnazione dell'ID VLAN sono:

- IETF 64 (Tipo tunnel) Impostare questa opzione su VLAN.
- IETF 65 (Tunnel Medium Type) Impostato su 802
- IETF 81 (Tunnel Private Group ID) Imposta su VLAN ID.

L'ID VLAN è a 12 bit e accetta un valore compreso tra 1 e 4094 inclusi. Poiché Tunnel-Private-Group-ID è di tipo stringa, come definito nella <u>RFC2868</u> per l'utilizzo con IEEE 802.1X, il valore intero dell'ID VLAN viene codificato come stringa. Quando vengono inviati questi attributi del tunnel, è necessario compilare il campo Tag.

Come indicato nella <u>RFC2868</u>, sezione 3.1: **II campo Tag è lungo un ottetto e serve a raggruppare gli attributi dello stesso pacchetto che fanno riferimento allo stesso tunnel.** I valori validi per questo campo sono compresi tra 0x01 e 0x1F inclusi. Se il campo Tag non è utilizzato, deve essere zero (0x00). Per ulteriori informazioni su tutti gli attributi RADIUS, consultare la <u>RFC</u> <u>2868</u>.

## **Configurazione**

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

## Esempio di rete

Nel documento viene usata questa impostazione di rete:



Di seguito sono riportati i dettagli di configurazione dei componenti utilizzati nel diagramma:

- L'indirizzo IP del server ACS (RADIUS) è 172.16.1.1.
- L'indirizzo dell'interfaccia di gestione del WLC è 172.16.1.30.
- L'indirizzo dell'interfaccia AP-Manager del WLC è 172.16.1.31.
- L'indirizzo del server DHCP 172.16.1.1 viene usato per assegnare gli indirizzi IP al protocollo LWAPP. Il server DHCP interno sul controller viene utilizzato per assegnare l'indirizzo IP ai client wireless.
- VLAN10 e VLAN11 vengono usate in questa configurazione. L'utente 1 è configurato per essere inserito nella VLAN10 e l'utente 2 è configurato per essere inserito nella VLAN11 dal server RADIUS.Nota: questo documento mostra solo tutte le informazioni di configurazione relative a user1. Completare la stessa procedura descritta in questo documento per user2.
- Questo documento utilizza 802.1x con LEAP come meccanismo di sicurezza.Nota: Cisco consiglia di utilizzare metodi di autenticazione avanzati, come l'autenticazione EAP-FAST e EAP-TLS, per proteggere la WLAN. Questo documento utilizza LEAP solo per semplicità.

## **Configurazione**

Prima della configurazione, per questo documento si presume che il LAP sia già stato registrato sul WLC. Per ulteriori informazioni, fare riferimento agli <u>esempi di configurazione base di Wireless</u> <u>LAN Controller e Lightweight Access Point</u>. Per informazioni sulla procedura di registrazione utilizzata, consultare il documento sulla <u>registrazione di un Lightweight AP (LAP) su un Wireless</u> <u>LAN Controller (WLC)</u>.

## Procedura di configurazione

Questa configurazione è suddivisa in tre categorie:

- 1. Configurazione server RADIUS
- 2. Configurazione dello switch per più VLAN
- 3. Configurazione WLC
- 4. Configurazione Wireless Client Utility

#### **Configurazione server RADIUS**

Questa configurazione richiede i seguenti passaggi:

- Configurare il WLC come client AAA sul server RADIUS
- <u>Configurare gli utenti e gli attributi RADIUS (IETF) utilizzati per l'assegnazione dinamica della</u>
   <u>VLAN sul server RADIUS</u>

#### Configurare il client AAA per il WLC sul server RADIUS

In questa procedura viene illustrato come aggiungere il WLC come client AAA sul server RADIUS in modo che il WLC possa passare le credenziali utente al server RADIUS.

Attenersi alla seguente procedura:

- 1. Dalla GUI di ACS, fare clic su Network Configuration (Configurazione di rete).
- 2. Fare clic sulla sezione Add Entry (Aggiungi voce) nel campo Client AAA.
- 3. Immettere l'indirizzo IP e la chiave del client AAA.L'indirizzo IP deve essere l'indirizzo IP dell'interfaccia di gestione del WLC.Accertarsi che la chiave immessa sia la stessa configurata sul WLC nella finestra Security. Chiave segreta utilizzata per la comunicazione tra il client AAA (WLC) e il server RADIUS.
- 4. Selezionare **RADIUS (Cisco Airespace)** dal campo Autentica con per il tipo di autenticazione.

CISCO SYSTEMS	Network Configuration
and Universitätion -	Edit
User Setup	
Group Setup	Add AAA Client
Shared Profile Components	AAA Client Hestname WI C1400
Network Configuration	172.16.1.30
System Configuration	AAA Client IP Address
Configuration	Shared Secret cisco
Administration Control	RADIUS Key Wrap
Databases	Key Encryption Key
noon Posture	Message Authenticator Code
Validation	Key Input Format O ASCII O Hexadecimal
Reports and Activity	Authenticate Using RADIUS (Cisco Airespace)
Documentation	Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
·	Log Update/Watchdog Packets from this AAA Client
	Log RADIUS Tunneling Packets from this AAA Client
	Replace RADIUS Port info with Username from this AAA Client
	Match Framed-IP-Address with user IP address for accounting packets from this AAA Client
	Submit Submit + Apply Cancel

#### <u>Configurare gli utenti e gli attributi RADIUS (IETF) utilizzati per l'assegnazione dinamica della</u> <u>VLAN sul server RADIUS</u>

In questa procedura viene illustrato come configurare gli utenti nel server RADIUS e gli attributi RADIUS (IETF) utilizzati per assegnare gli ID VLAN a tali utenti.

Attenersi alla seguente procedura:

- 1. Dalla GUI di ACS, fare clic su **User Setup** (Configurazione utente).
- 2. Nella finestra Impostazione utente, immettere un nome utente nel campo Utente e fare clic su

Aggiungi/Modifica.

Cisco Systems	User Setup
	Select
User Setup	
Group Setup	User: User1
Shared Profile Components	Find Add/Edit
Network Configuration	List users beginning with letter/number:
System Configuration	
Interface Configuration	0123456789
Madministration Control	List all users
Databases	Remove Dynamic Users
Posture Validation	
Network Access Profiles	💡 Back to Help
Reports and Activity	
Documentation	

3. Nella pagina Modifica immettere le informazioni utente necessarie, come illustrato di seguito:

CISCO SYSTEMS	User Setup
antilitina antilitina a	Edit
User Setup	User: User1
Setup Shared Profile Components	C Account Disabled
Network Configuration	Supplementary User Info
System Configuration	Real Name User1
Interface Configuration	Description User1
Administration Control	
Databases	User Setup 🤶
BBBB Posture Validation	Password Authentication:
Network Access Profiles	CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)
Reports and Activity	Password •••••
Online Documentation	Confirm Password
	Separate (CHAP/MS-CHAP/ARAP)
	Password •••••••••
	Confirm Password
	When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

In questo diagramma, si noti che la password fornita nella sezione Impostazione utente deve essere la stessa fornita sul lato client durante l'autenticazione dell'utente.

- 4. Scorrere la pagina Modifica e individuare il campo Attributi RADIUS IETF.
- 5. Nel campo Attributi RADIUS IETF, selezionare le caselle di controllo accanto ai tre attributi Tunnel e configurare i valori degli attributi come mostrato di seguito:

CISCO SYSTEMS	User Setup		
	Failed attempts since login: 0	last successful	
User Setup	Reset current failed	d attempts count	
Group Setup	on submit		
Shared Profile Components			- 1
Network Configuration	Download	able ACLs 🤶	
System Configuration	Assign IP ACL:	VPN_Access	
Configuration		a	٦
Administration Control	IETF RADIU	S Attributes 🦿	-
	🗹 [064] Tunnel-Type		
Jul Databases	Tag 1 💽 Value	VLAN 💽	
Posture Validation	Tag 2 💌 Value		
Network Access	🗹 (065) Tunnel-Medium-1	Гуре	
Profiles	Tag 1	▼ Value 802 ▼	
Reports and Activity	Tag 2	▼ Value	
	🗹 (081) Tunnel-Private-G	iroup-ID	
	Tag 🚺 💌 Val	lue 10	
	Tag 2 💌 Val	lue	
			_]]

**Nota:** nella configurazione iniziale del server ACS, gli attributi RADIUS IETF potrebbero non essere visualizzati.Per abilitare gli attributi IETF nella finestra di configurazione utente, scegliere **Configurazione interfaccia > RADIUS (IETF)**.Selezionare quindi le caselle di controllo relative agli attributi **64, 65 e 81** nelle colonne Utente e Gruppo.



Nota: affinché il server RADIUS assegni dinamicamente il client a una VLAN specifica, è necessario che l'ID VLAN configurato nel campo IETF 81 (Tunnel-Private-Group-ID) del server RADIUS sia presente sul WLC.Selezionare la casella di controllo dell'attributo Per Utente TACACS+/RADIUS in Configurazione interfaccia > Opzioni avanzate per abilitare il server RADIUS per le configurazioni per utente.Inoltre, poiché il protocollo LEAP viene utilizzato come protocollo di autenticazione, assicurarsi che sia abilitato nella finestra Configurazione di sistema del server RADIUS, come mostrato di seguito:



# System Configuration

*************************	Cisco client initial message:
User J Setup	PEAP session timeout (minutes): 120
Group Setup	Enable Fast Reconnect: 🔽
Shared Profile Components	EAP-FAST EAP-FAST Configuration
Network Configuration	ΕΔΡ-ΤΙ S
System Configuration	Allow EAP-TLS
Interface Configuration	Select one or more of the following options:
Administration	Certificate CN comparison
Databases	EAP-TLS session timeout (minutes): 120
Posture Validation	
Network Access Profiles	LEAP Allow LEAP (For Aironet only)
Reports and Activity	EAP-MD5
Documentation	Allow EAP-MD5
	AP EAP request timeout (seconds): 20

# Configurazione dell'ACS con gli attributi VSA di Cisco Airespace per l'assegnazione dinamica della VLAN

Nelle versioni più recenti di ACS, è possibile anche configurare l'attributo Cisco Airespace [VSA (specifico del fornitore)] per assegnare a un utente autenticato con un nome di interfaccia VLAN (non l'ID VLAN), in base alla configurazione utente su ACS. A tale scopo, eseguire la procedura descritta in questa sezione.

**Nota:** in questa sezione viene usata la versione ACS 4.1 per configurare l'attributo VSA di Cisco Airespace.

Configurazione del gruppo ACS con l'opzione Cisco Airespace VSA Attribute

Attenersi alla seguente procedura:

- 1. Dalla GUI di ACS 4.1, fare clic su **Interface Configuration** (Configurazione interfaccia) dalla barra di navigazione. Quindi, selezionare **RADIUS (Cisco Airespace)** dalla pagina Configurazione interfaccia per configurare l'opzione dell'attributo Cisco Airespace.
- Dalla finestra RADIUS (Cisco Airespace), selezionare la casella di controllo Utente (se necessario, la casella di controllo Gruppo) accanto a Aire-Interface-Name per visualizzarla nella pagina User Edit. Fare quindi clic su Invia.



- 3. Andare alla pagina Modifica dell'utente 1.
- 4. Dalla pagina User Edit, scorrere verso il basso fino alla sezione **Cisco Airespace RADIUS Attributes**. Selezionare la casella di controllo accanto all'attributo **Aire-Interface-Name** e specificare il nome dell'interfaccia dinamica da assegnare al completamento dell'autenticazione utente.In questo esempio viene assegnata alla VLAN **di amministrazione**.

CISCO SYSTEMS	User Setup	
	L Date exceeds.	
User Setup Group Setup Setup Shared Profile Components Network Configuration System Configuration	May 💽 2 Failed attempts exceed: 5 Failed attempts since last successful login: 0 Reset current failed attempts count on submit	2009
Configuration	Downloadable ACLs	?
Administration Control	Assign IP ACL: VPN_Acces	55
Posture Validation	Cisco Airespace RADIUS Attributes	?
Network Access Profiles	☑ [14179\005] Aire-Interface-Name	
Reports and Activity	ladmin	
Documentation		

5. Fare clic su Invia.

## Configurazione dello switch per più VLAN

Per consentire l'uso di più VLAN sullo switch, è necessario usare questi comandi per configurare la porta dello switch connessa al controller:

- 1. Switch(config-if)#switchport mode trunk
- 2. Switch(config-if)#switchport trunk encapsulation dot1q

**Nota:** per impostazione predefinita, la maggior parte degli switch consente tutte le VLAN create sullo switch tramite la porta trunk.

Questi comandi variano per uno switch Catalyst con sistema operativo (CatOS).

Se allo switch è collegata una rete cablata, è possibile applicare la stessa configurazione alla porta dello switch che si connette alla rete cablata. Ciò consente la comunicazione tra le stesse VLAN nella rete cablata e wireless.

**Nota:** in questo documento non viene descritta la comunicazione tra VLAN. Questo aspetto esula tuttavia dalle finalità del presente documento. Per il routing tra VLAN, è necessario usare uno

switch di layer 3 o un router esterno con configurazioni VLAN e trunking appropriate. La configurazione del routing tra VLAN è spiegata in diversi documenti.

#### **Configurazione WLC**

Questa configurazione richiede i seguenti passaggi:

- Configurare il WLC con i dettagli del server di autenticazione
- <u>Configurazione delle interfacce dinamiche (VLAN)</u>
- Configurazione delle WLAN (SSID)

Configurare il WLC con i dettagli del server di autenticazione

Ènecessario configurare il WLC in modo che possa comunicare con il server RADIUS per autenticare i client e anche per qualsiasi altra transazione.

Attenersi alla seguente procedura:

- 1. Dalla GUI del controller, fare clic su Security (Sicurezza).
- 2. Immettere l'indirizzo IP del server RADIUS e la chiave privata condivisa utilizzata tra il server RADIUS e il WLC.La chiave privata condivisa deve essere la stessa configurata nel server RADIUS in Configurazione di rete > Client AAA > Aggiungi voce. Di seguito è riportato un esempio di finestra del

CISCO	MONITOR MLANS CONTRO	LLER WIRELESS SECURITY MANAGEMENT COMMAN	IDS HELP
Security	RADIUS Authentication S	ervers > New	< Back Apply
AAA General RADIUS Authentication Accounting Palback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number		compliant RADIUS server)
Local EAP Priority Order Certificate Access Control Lists Wireless Protection Policies	Server Status Support for RPC 3576 Server Timeout Network User Management IPSec	Enabled Enabled Enable Enable Enable Enable Enable	

#### Configurazione delle interfacce dinamiche (VLAN)

In questa procedura viene spiegato come configurare le interfacce dinamiche sul WLC. Come spiegato in precedenza in questo documento, l'ID VLAN specificato nell'attributo Tunnel-Private-Group ID del server RADIUS deve esistere anche nel WLC.

Nell'esempio, l'utente 1 viene specificato con l'ID tunnel-gruppo privato di 10 (VLAN =10) sul

server RADIUS. Vedere la sezione <u>Attributi RADIUS IETF</u> della finestra Impostazione utente 1.

In questo esempio, è possibile vedere la stessa interfaccia dinamica (VLAN=10) configurata nel WLC. Dalla GUI del controller, nella finestra Controller > Interfacce, viene configurata l'interfaccia dinamica.

ahaha		- CONTROLLER		SECTIBITY	MARAGEMENT	Saya Co	nfiguration   Eing	Logout   <u>B</u> efresh
Controller	Interfaces > New	N	WINELESS	Jecorari	NUMBER	COMMITS	< Back	Apply
General Inventory Interfaces	Interface Name VLAN Id	vlan10 10						
Network Routes  Internal DHCP Server  Mobility Management								
Ports NTP								
<ul> <li>Advanced</li> </ul>								

- 1. Fare clic su **Apply** (Applica) in questa finestra.Viene visualizzata la finestra Edit (Modifica) di questa interfaccia dinamica (qui VLAN 10).
- 2. Immettere l'indirizzo IP e il gateway predefinito dell'interfaccia

dinamica.								
cisco	MONITOR MU	ANS CONTROLLE	R WIRELESS	SECURITY	MONAGEMENT	Saye C COMMANDS	enfiguration Ding	Cogout   Befresh
CISCO Controller General Inventory Interfaces Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP CDP Advanced	MONITOR WU Interfaces > E General Inform Interface Name MAC Address Configuration Guest Lan Quarantine Quarantine Quarantine Via Physical Inform Port Number Backup Port Active Port	ANS CONTROLLE	R WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HEU"	Apply
	Interface Adds VLAN Identifier IP Address Netmask Gateway DHCP Informa Primary DHCP Secondary DHC	ress	0 72.18.1.10 55.255.0.0 72.18.1.30 172.16.1.30					

**Nota:** poiché in questo documento viene usato un server DHCP interno sul controller, il campo del server DHCP primario di questa finestra punta all'interfaccia di gestione del WLC stesso. Ai client wireless è inoltre possibile utilizzare un server DHCP esterno, un router o lo

stesso server RADIUS come server DHCP. In questi casi, il campo del server DHCP primario punta all'indirizzo IP del dispositivo utilizzato come server DHCP. Per ulteriori informazioni, consultare la documentazione del server DHCP in uso.

3. Fare clic su Apply (Applica).A questo punto, si è configurati con un'interfaccia dinamica nel WLC. Analogamente, è possibile configurare diverse interfacce dinamiche nel WLC. Tuttavia, tenere presente che lo stesso ID VLAN deve essere presente anche nel server RADIUS perché la VLAN specifica possa essere assegnata al client.

#### Configurazione delle WLAN (SSID)

In questa procedura viene spiegato come configurare le WLAN nel WLC.

Attenersi alla seguente procedura:

- 1. Dalla GUI del controller, selezionare **WLAN > New** (Nuova) per creare una nuova WLAN.Viene visualizzata la finestra Nuove WLAN.
- Immettere l'ID WLAN e le informazioni sull'SSID WLAN.Èpossibile immettere qualsiasi nome come SSID WLAN. In questo esempio viene usato VLAN10 come SSID WLAN.

cisco	MONITOR WLANS		WIRELESS	SECURITY	Management	C <u>O</u> MMANDS	HELP	Cogost Berresi
WLANs	WLANs > New						< Back	Apply
WLANS	Туре	WLAN	v 💌					
Advanced	Profile Name	VLAN	10					
	SSID	VLAN	10					
	ID	3	-					

3. Per accedere alla finestra Modifica di WLAN SSID10, fare clic su **Apply** (Applica)

27140	WLAINS > Edit	< Back	Appl
WLANs WLANs	General Security	Qo5 Advanced	
Advanced	Profile Name	VLAN10	
	Туре	WLAN	
	SSID	VLAN10	
	Status	F Enabled	
	Security Policies	[WPA2][Auth(882.1X)] (Modifications done under security tab will appear after applying the changes.)	
	Radio Policy	Al	
	Interface	management -	
	Broadcast SSID	₽ Enabled	

cisco	MONITOR WLAN	IS <u>C</u> ONTROL	LER WIRE	LESS <u>S</u> ECURITY	MANAGEMENT	Sale Co C <u>O</u> MMANDS	nfiguration   <u>P</u> ing   HELP	Logout   3
WLANs	WLANs > Edit						< Back	Apply
WLANS WLANS	General Sec	curity Qo	S Advar	iced				
Advanced	Layer 2	ayer 3 🛛 🗛	A Servers	1				
	Layer 2 Secu	urity Z 802.1X	: Filtering	×				
	802.1X Parame	eters						
	802.11 Data	Encryption	Type F WEP	Key Size				

In genere, in un controller LAN wireless, a ciascuna WLAN viene eseguito il mapping a una VLAN (SSID) specifica in modo che un utente specifico appartenente alla WLAN venga inserito nella VLAN mappata. Questa mappatura viene in genere eseguita nel campo Interface Name (Nome interfaccia) della finestra SSID della

WLAN.

cisco	Sage Configurati MONITOR WLAN: CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	on Eing Logout Befre					
WLANs	WLANs > Edit	Back Apply					
WLANS WLANS	General Security QoS Advanced						
▶ Advanced	Layer 2 Layer 3 AAA Servers						
	Select AAA servers below to override use of default servers on this WLAN	÷					
	Radius Servers LDAP Servers						
	Authentication Servers Accounting Servers Server 1 None - F Enabled Server 2 None -						
	Server 1 1P:172.16.1.1, Port:1012 • None • Server 3 None •						
	Server 2 None None I						
	Server 3 None None						
	Local EAP Authentication						
	Local EAP Authentication Enabled						
	Authentication priority order for web-auth user						
	> LOCAL Up RADIUS						

Nell'esempio riportato, è compito del server RADIUS assegnare un client wireless a una VLAN specifica dopo la riuscita dell'autenticazione. Non è necessario mappare le WLAN a un'interfaccia dinamica specifica sul WLC. Oppure, anche se il mapping tra la WLAN e l'interfaccia dinamica viene eseguito sul WLC, il server RADIUS ignora questo mapping e assegna l'utente che passa attraverso la WLAN alla VLAN specificata nel campo user **Tunnel-Group-Private-ID** nel server RADIUS.

4. Selezionare la casella di controllo **Consenti sostituzione AAA** per sostituire le configurazioni WLC con il server RADIUS.

5. Abilitare l'opzione Allow AAA Override nel controller per ciascuna WLAN (SSID) configurata.

LANs	WLANs > Edit		< Back Ap
WLANS WLANS	General Security	QoS Advanced	
normiceo	Allow AAA Override	F Enabled	DHCP
	Coverage Hole Detection Enable Session Timeout	F Enabled	DHCP Server 🗖 Override
		Session Timeout (secs)	DHCP Addr. Assignment 🗖 Required
	Aironet IE	R Enabled	Management Frame Protection (MFP)
	Diagnostic Channel	Enabled	
	IPv6 Enable		Infrestructure MFP IF (Global MFP Disabled)
	Override Interface ACL	None -	MFP Client
	P2P Blocking Action	Disabled	Protection & Optional -
	Client Exclusion 4	F Enabled 60	DTIM Period (in beacon intervals)
	HREAP	Teneous value (secs	
	H-REAR Local Switching		602.110/n (1 - 255) 1
	Learn Client IP Address	E Enabled	002.110/g/i (1 · 200) [1
	COSTI CIGIN IF MUSICIS	** chaoled	
			State L Enabled

Quando l'override AAA è abilitato e un client ha parametri di autenticazione WLAN AAA e controller in conflitto, l'autenticazione del client viene eseguita dal server AAA (RADIUS). Come parte di questa autenticazione, il sistema operativo sposta i client su una VLAN restituita dal server AAA. Questa impostazione è predefinita nella configurazione dell'interfaccia del controller.Ad esempio, se la WLAN aziendale utilizza principalmente un'interfaccia di gestione assegnata alla VLAN 2 e l'override AAA restituisce un reindirizzamento alla VLAN 100, il sistema operativo reindirizza tutte le trasmissioni client alla VLAN 100 anche se la porta fisica a cui è assegnata la VLAN 100. Quando l'override AAA è disabilitato, tutte le impostazioni predefinite di autenticazione del client corrispondono alle impostazioni dei parametri di autenticazione del controller e l'autenticazione viene eseguita dal server AAA solo se la WLAN del controller non contiene parametri di autenticazione specifici del client.

#### **Configurazione Wireless Client Utility**

In questo documento viene usato ADU come utility client per la configurazione dei profili utente. Questa configurazione utilizza anche LEAP come protocollo di autenticazione. Configurare l'ADU come mostrato nell'esempio di questa sezione.

Per creare un nuovo profilo, dalla barra dei menu ADU scegliere Gestione profili > Nuovo.

Il client di esempio è configurato per far parte di SSID VLAN10. Questi diagrammi mostrano come configurare un profilo utente su un client:

Cisco Aironet Desktop Utility - Current Profile:	Default 🛛 💽
Current Status Profile Management Diagnostics	
Default LAP	<u>N</u> ew
Ext.Web	Modily
	Remove
	Activate
Details	
Network Type: Security Mode:	Import
Network Name 1 (SSID1):	Export
Network Name 2 (SSID2):	Scan.
Network Name 3 (SSID3):	
Auto Select Profiles	Order Profiles

Profile N	anagemer	nt		? 🛛
General	Security 4	Advance	a]	
~ Profil	e Settings			
	Profile	Name:	vlan10	
	Client	Name:	wcs	
Netw	ork Names		·····	
		SSID1:	vlan10	
		SSID2:		
		SSID3:		
	* * * *			
				Cancel

Security Options			585
WPA/WPA2/CCKM WPA/	AWPA2/CCKM EAP Type: LEAP		~
wPA/wPA2 Passphrase			
802.1x	802.1x EAP Type LEAP	$\geq$	¥
Pre-Shared Key (Static WEP)			
None			
Configure	Allow Association to Mixed Cells Locked Profile		
Group Policy Delay:	60 🗘 sec		

# **Verifica**

Attivare il profilo utente configurato nell'ADU. In base alla configurazione, viene richiesto di immettere un nome utente e una password. È inoltre possibile indicare all'ADU di utilizzare il nome utente e la password di Windows per l'autenticazione. Il client può ricevere l'autenticazione in diverse opzioni. È possibile configurare queste opzioni nella scheda Protezione > Configura del profilo utente creato.

Nell'esempio precedente, l'utente 1 è assegnato alla VLAN10 come specificato nel server RADIUS.

In questo esempio vengono utilizzati il nome utente e la password specificati dal client per ricevere l'autenticazione e per essere assegnati a una VLAN dal server RADIUS:

- Nome utente = utente1
- Password = utente1

Nell'esempio viene mostrato come richiedere il nome utente e la password alla VLAN10 SSID. Il nome utente e la password vengono immessi nell'esempio seguente:

Current Status Pro	one Management Diagnostics	
Default		New
Ext.Web		Modify
Vian10		Remove
ter Wireless N	etwork Password	Activate
network		Import
Jser Name :	user1	Export Scan
network Jser Name : Password :	user1	Export Scan
Jser Name : Password : .og on to :	user1 •••••	Import Export Scan Order Profiles
Jser Name : Password : .og on to : Card Name :	user1 ••••• Cisco Aironet 802.11a/b/g Wireless Adapter	Import Export Scan Order Profiles

Se l'autenticazione e la convalida corrispondente hanno esito positivo, verrà visualizzato il messaggio di stato Operazione riuscita.

Quindi, è necessario verificare che il client sia assegnato alla VLAN corretta in base agli attributi RADIUS inviati. A tale scopo, effettuare i seguenti passaggi:

- 1. Dalla GUI del controller, selezionare Wireless > AP.
- 2. Fare clic su **Client**, visualizzato nell'angolo sinistro della finestra Access Point (AP).Vengono visualizzate le statistiche

client.											
cisco	MONITOR WLAN		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Eing 1	Logout	T E et	resh
Monitor	Clients							Entrie	s 1 - 4	of 4	
Summary	Current Filter	None	[Change filts	er] (Show All)							
Access Points											
Statistics	Client MAC Addr	AP Name		WLAN	Profile	Protocol	Status	Auth	Port	WGR	8
► CDP	00:21:5c:09:08:dd	AP1130		Unkno	MD	802.11a	Probing	No	2	No	
Rogues	00:21:5c:50:3a:1f	AP1130		VLAN1	0	802.11g	Associated	Yes	z	No	
Clients											
Multicast											

3. Fare clic su **Details** (Dettagli) per identificare i dettagli completi del client, come l'indirizzo IP, la VLAN a cui è assegnato e così via.In questo esempio vengono visualizzati i seguenti

#### dettagli del client

utonto1	•	
ULCIILC I		

utente1:						
cisco	MONITOR WILANS CONT	ROLLER WIRELESS	SECURITY	MANAGEMENT COM	Save Contiguration   Eng   MANDS HELP	Logout   <u>R</u> efre
Monitor	Clients > Detail			< Back	Apply Link Test	Remove
Summary Access Points	Client Properties			AP Properties		
Statistics	MAC Address	00:21:50:50:3a:1f		AP Address	00:15:c7:ab:55:90	
▶ CDP	IP Address	17.18.1.35		AP Name	AP1130	
Rogues	Client Type	Regular		AP Type	802.11g	
Clients	User Name	User1		WLAN Profile	VLAN10	
Multicast	Port Number	2		Status	Associated	
	Interface	vlan10		Association ID	1	
	VLAN ID	10		802.11 Authentication	Open System	
	CCX Version	CCXv4		Reason Code	0	
	E2E Version	E2Ev1		Status Code	0	
	Mobility Role	Local		CF Pollable	Not Implemented	
	Mobility Peer IP Address	N/A		CF Poll Request	Not Implemented	
	Policy Manager State	RUN		Short Preamble	Implemented	
	Mirror Mode	Disable -		PBCC	Not Implemented	
	Management Frame Protection	No		Channel Agility	Not Implemented	
	Conveitu Information			Timeout	1800	
	security information			WEP State	WEP Disable	
	Security Policy Completed	Yes				
	Policy Type	802.1X				
	Encryption Cipher	WEP (104 bits)				
	EAP Type	LEAP				
	NAC State	Access				

Da questa finestra è possibile osservare che il client è assegnato alla VLAN10 in base agli attributi RADIUS configurati sul server RADIUS. Nota: se l'assegnazione della VLAN dinamica è basata sull'impostazione dell'attributo VSA di Cisco Airespace, il nome dell'interfaccia la visualizzerà come admin, come mostrato nell'esempio, nella pagina dei dettagli del client.

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

 debug aaa events enable: questo comando può essere usato per garantire il corretto trasferimento degli attributi RADIUS al client tramite il controller. Questa parte dell'output di debug garantisce la corretta trasmissione degli attributi RADIUS:

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]:
attribute 64, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]:
attribute 65, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:
attribute 81, vendorId 0, valueLen 3
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:
attribute 79, vendorId 0, valueLen 32
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute
(code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18
4a 27 65 69 6d e4 05 f5
.....J'eim...00000010: d0 98 0c cb 1a 0c 8a 3c
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]:
attribute 1, vendorId 9, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]:
attribute 25, vendorId 0, valueLen 28
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]:
attribute 80, vendorId 0, valueLen 16
```

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Type 16777229
should be 13 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222
should be 6 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57
setting dot1x reauth timeout = 1800
```

 Questi comandi possono essere utili anche: debug dot1x aaa enableabilitazione pacchetti debug aaa

# Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Nota: l'assegnazione della VLAN dinamica non funziona per l'autenticazione Web da un WLC.

## Informazioni correlate

- <u>Autenticazione EAP con server RADIUS</u>
- <u>Cisco LEAP</u>
- Guida alla configurazione di Cisco Wireless LAN Controller, versione 4.0
- Documentazione e supporto tecnico Cisco Systems