Configurazione di PEAP e EAP-FAST con ACS 5.2 e WLC

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Configurazione Esempio di rete Presupposti Procedura di configurazione Configurazione del server RADIUS Configura risorse di rete Configura utenti Definizione degli elementi dei criteri Applica criteri di accesso Configurare il WLC Configurare il WLC con i dettagli del server di autenticazione Configurazione delle interfacce dinamiche (VLAN) Configurazione delle WLAN (SSID) **Configurare Wireless Client Utility** PEAP-MSCHAPv2 (utente1) EAP-FAST (utente 2) Verifica Verifica utente1 (PEAP-MSCHAPv2) Verifica utente2 (EAP-FAST) Risoluzione dei problemi Comandi per la risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene spiegato come configurare il controller WLC (Wireless LAN Controller) per l'autenticazione EAP (Extensible Authentication Protocol) con l'utilizzo di un server RADIUS esterno, ad esempio Access Control Server (ACS) 5.2.

Prerequisiti

Requisiti

Prima di provare la configurazione, verificare che siano soddisfatti 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

Componenti usati

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

- Cisco 5508 WLC con firmware versione 7.0.20.0
- Cisco serie 3502 LAP
- Supplicant nativo di Microsoft Windows 7 con driver Intel 6300-N versione 14.3
- Cisco Secure ACS con versione 5.2
- Cisco serie 3560 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

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Configurazione

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

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> ricerca dei comandi (solo utenti registrati).

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 192.168.150.24.
- L'indirizzo dell'interfaccia di gestione e AP-manager del WLC è 192.168.75.44.
- L'indirizzo dei server DHCP è 192.168.150.25.
- In questa configurazione, viene usata la VLAN 253. Entrambi gli utenti si connettono allo stesso SSID "goa". Tuttavia, l'utente 1 è configurato per l'autenticazione tramite PEAP-MSCHAPv2 e l'utente 2 tramite EAP-FAST.
- Gli utenti verranno assegnati alla VLAN 253:VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.1VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

Presupposti

- Gli switch sono configurati per tutte le VLAN di layer 3.
- Al server DHCP viene assegnato un ambito DHCP.
- Esiste una connettività di livello 3 tra tutti i dispositivi della rete.
- II LAP è già unito al WLC.
- Ogni VLAN ha una maschera /24.

• In ACS 5.2 è installato un certificato autofirmato.

Procedura di configurazione

Questa configurazione è suddivisa in tre fasi principali:

- 1. Configurare il server RADIUS.
- 2. Configurare il WLC.
- 3. Configurare Wireless Client Utility.

Configurazione del server RADIUS

La configurazione del server RADIUS è suddivisa in quattro passaggi:

- 1. Configurare le risorse di rete.
- 2. Configurare gli utenti.
- 3. Definire gli elementi dei criteri.
- 4. Applicare i criteri di accesso.

ACS 5.x è un sistema di controllo degli accessi basato su regole. ovvero ACS 5.x utilizza un modello di criteri basato su regole anziché il modello basato su gruppi utilizzato nelle versioni 4.x.

Il modello di policy basato su regole ACS 5.x offre un controllo dell'accesso più potente e flessibile rispetto al precedente approccio basato su gruppi.

Nel modello basato su gruppi meno recente, un gruppo definisce i criteri in quanto contiene e associa tre tipi di informazioni:

- Informazioni sull'identità: queste informazioni possono essere basate sull'appartenenza a gruppi AD o LDAP oppure su un'assegnazione statica per gli utenti ACS interni.
- Altre restrizioni o condizioni: restrizioni temporali, restrizioni per i dispositivi e così via.
- Autorizzazioni: livelli di privilegio per VLAN o Cisco IOS[®].

Il modello di policy di ACS 5.x si basa sulle seguenti regole:

• If condition then result

Ad esempio, vengono utilizzate le informazioni descritte per il modello basato su gruppi:

• If identity-condition, restricted-condition e authorization-profile.

Di conseguenza, questo ci offre la flessibilità di limitare a quali condizioni l'utente può accedere alla rete e quale livello di autorizzazione è consentito quando vengono soddisfatte condizioni specifiche.

Configura risorse di rete

In questa sezione viene configurato 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 dell'utente al server RADIUS.

Attenersi alla seguente procedura:

1. Dalla GUI di ACS, selezionare **Risorse di rete > Gruppi di dispositivi di rete > Posizione**, quindi fare clic su **Crea** (in basso).

cisco Cisco Secure ACS			
► 🚭 My Workspace	Network Resources > Network Device Groups > Location		
🗴 🅼 Network Resources	Network Device Groups		
 Network Device Groups Location 	Filter: 💽 Match if: 🗨 Go 🔻		
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Image: Name Description Image: All Locations All Locations		
Users and Identity Stores			
▹ Spolicy Elements			
► 🔂 Access Policies			
 Monitoring and Reports 			
🕞 😹 System Administration			

2. Aggiungere i campi obbligatori e fare clic su Invia

Device Group -	Seneral	
o Name:	LAB	
Description:	LAB Devices	
o Parent	All Locations	Select
Required field	lds	

Viene visualizzata la seguente schermata:



3. Selezionate Tipo periferica (Device Type) > Crea (Create).

cisco Cisco Secure ACS			
🕨 🖌 My Workspace	Network Resources > Network Device Groups > Device Type > Create		
Network Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Device Group - General Name: 5508 Description: Wireless LAN Controller Parent All Device Types = Required fields	Select	
Users and Identity Stores			
Policy Elements			
Access Policies			
Monitoring and Reports			
 System Administration 			

4. Fare clic su **Invia**. Viene visualizzata la seguente schermata:

•	cisco Cisco Secure AC		
	🕨 🚭 My Workspace	rk Resources > Netw	ork Device Groups > Device Type
	Network Resources	work Device Group	S
	 Network Device Groups Location Device Type 	er:	Match if: Go 🔻
	Network Devices and AAA Clients	Name	 Description
	Default Network Device External RADIUS Servers	* All Device Type	All Device Types
	B Users and Identity Stores	<u>5508</u>	Wireless LAN Controller
	Solicy Elements		
	Access Policies		
	Monitoring and Reports		
	System Administration		

- 5. Selezionare Risorse di rete > Dispositivi di rete e client AAA.
- 6. Fare clic su Create (Crea) e immettere i dettagli come illustrato di

seguito:				
+ 🔂 My Workspace	Network Resources > Net	twark Devices and AAA Clerks > Create		
Idework Resources Network Device Groups Location Device Type Network Devices and AAAChents Default Network Device External RACIUS Servers Works and Identity Stores Works and Identity Stores Works Policy Elements Works Policy Elements Works Policy Elements Works Policy Elements Workshold Reports Workshold Reports Workshold Reports Workshold Reports Workshold Reports	Name: W. Description: W. Network Device Gr Location Device Type	C-5508 reless LAN Controller exps All Locations:LAB All Device Types:5508	Salect Salect	
	IP Address (* Single IP A 9 IP: 192 168 75	ddress C IP Range(s)	Authentication Options TACACS+ RADUS RADUS Shared Secret claco CoA part (1700 Enable KeyWrap Key Encryption Key: Nessage Authenticator Code Key: Key Input Format C ASCII © HEXAD	DECIMAL
	e - Required fields	i		

7. Fare clic su **Invia**. Viene visualizzata la seguente schermata:

Netwo	ork Devices					
Filter			Match It.	•	G0 🔻	
	Name	-	IP / Mask	NDG:Location	NDG:Device Type	Description
	WLC-5508		192.168.75.44/32	All Locations:LAB	All Device Types:5508	Wireless LAN Controller

Configura utenti

In questa sezione verranno creati utenti locali su ACS. Entrambi gli utenti (utente1 e utente2) vengono assegnati nel gruppo denominato "Utenti wireless".

1. Andare a Utenti e archivi identità > Gruppi di identità > Crea.

11 111 11 Cisco Secure ACS CISCO 🚮 My Workspace Users and identity Stores > Identity Groups > Create Network Resources General 28 Users and Identity Stores o Name: Wireless Users Description: Wireless Users authenticating over wireless Internal Identity Stores o Parent All Groups Select Users Hosts Required fields External Identity Stores LDAP Active Directory RSA SecurID Token Servers **RADIUS Identity Servers Certificate Authorities** Certificate Authentication Profile Identity Store Sequences So Policy Elements

2. Dopo aver fatto clic su Invia, la pagina avrà il seguente

as	petto)
au	ροιιο	' I

cisco Cisco Secure ACS			
🕨 🖑 My Workspace	Users and identity Stores > identity Groups		
Network Resources	Identity Groups		
Users and Identity Stores	Filter: 💌 Match it: 💌 Go 🔝		
Identity Groups			
Users	Name Description		
Hosts	* <u>All Groups</u> Identity Group Root		
LDAP	Wireless Users Wireless Users authenticating over wireless		
Active Directory			
RSASecuriD Token Servers RADIUS Identity Servers			
Certificate Authorities			
Certificate Authentication Profile			
 Policy Elements 			

3. Creare gli utenti **user1** e **user2**, quindi assegnarli al gruppo "Wireless Users".Fare clic su **Utenti e archivi identità > Gruppi di identità > Utenti >**

▶ 🚭 My Workspace	Users and identity Stores > Internal identity Stores > Users > Create
	General Image: An and the second se
External Identity Stores Certificate Authorities Certificate Authorities Identity Store Sequences	Password Information Password must Contain 4 - 32 characters
Q. Policy Elements Q. Access Policies	Password: Password: Password: Password:
 Monitoring and Reports System Administration 	Change password on next login User Information There are no additional identity attributes defined for user records

Crea.

Analogamente, create

cisco Cisco Secure A	CS
My Workspace	Users and identity Stores > Internal identity Stores > Users > Create
All Network Resources	Connect
👻 🎬 Users and Identity Stores (2000)	Status: Enabled P
Identity Groups	Description: EAPFAST user
 Internal Identity Stores Usero 	Identity Group: All Groups: Wireless Users Select
Edemail identity Stores Certificate Authorities Certificate Authorities Identity Store Sequences	Password Information Password must • Contain 4 - 32 characters
Policy Elements	O Password: +++++
► Case Solicies	O Confirm Password:
Monitoring and Reports	Change password on next login
System Administration	User Information There are no additional identity attributes defined for user records • - Required fields

user2. schermo avrà il seguente aspetto:

cisco Cisco Secure ACS				
🕨 🚭 My Workspace	Users and Identity Store	es > Internal identity Store	es > Users	
► Network Resources	Internal Users			
General Mentity Stores Identity Groups	Filter:	• Match it	▼ G0 マ	
 Internal Identity Stores 	Status	User Name	 Identity Group 	Description
Users Hosts External Identity Stores Certificate Authorities Certificate Authentication Profile Identity Store Sequences	□ ●	user1	All Groups:Wireless Users	PEAP:mschapv2 users
	□ 0	user2	All Groups:Wireless Users	EAPFAST user
Policy Elements				

Definizione degli elementi dei criteri

Verificare che l'opzione Permit Access sia impostata.

cisco Cisco Secure A	ACS
🖌 💮 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
Interview Resources	Authorization Profiles
Users and Identity Stores	Filter Match It Go V
👻 🎭 Policy Elements	
Session Conditions Authorization and Permissions	Permit Access
 Network Access Authorization Profiles 	
Device Administration Named Permission Objects	
Access Policies	
► 🔝 Monitoring and Reports	
🖌 🍇 System Administration	

Applica criteri di accesso

In questa sezione verranno selezionati i metodi di autenticazione da utilizzare e la modalità di configurazione delle regole. Le regole verranno create in base ai passaggi precedenti.

Attenersi alla seguente procedura:

 Selezionare Access Policies > Access Services > Default Network Access > Edit: "Default Network Access".

cisco Cisco Secure A	ICS
🕨 🥵 My Workspace	Access Policies > Access Services > Default Network Access > Edit "Default Network Access"
+ 🎲 Network Resources	
Busers and Identity Stores	General Allowed Protocols
► Sp. Policy Elements	Name: Default Network Access
🔹 🛼 Access Policies	Description: Default Network Access Service
Access Services Service Selection Rules	Service Type : Network Access -
Dafault Device Admin	Policy Structure
Default Network Access	Identity Identity
► Ø deleterne	Group Mapping
 Monitoring and Reports 	Authorization
🕨 🍇 System Administration	

2. Selezionare il metodo EAP che si desidera venga autenticato dai client wireless. Nell'esempio vengono utilizzati PEAP- MSCHAPv2 e EAP-FAST.

cisco Cisco Secure A	CS
 My Workspace 	Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"
 My Workspace Network Resources Users and Identity Stores Policy Elements Policy Elements Access Policies Access Services Service Selection Rules Default Device Admin Default Network Access Identity Authorization Ø deleteme Monitoring and Reports System Administration 	Access Palicies > Access Services > Default Network Access > Edit "Default Network Access" General Allowed Protocols Process Host Lookup Authentication Protocols P Allow PAP/ASCII Allow CHAP Allow CHAP Allow MS-CHAPv1 Allow MS-CHAPv2 Allow EAP-MD5 Allow EAP-TL8 Allow LEAP Allow EAP-TL8 Allow EAP-FAST
	Preferred EAP protocol LEAP

- 🔝 Access Policies	
Access Services H Service Selection Rules O Default Device Admin O Default Device Admin O Default Network Access Idemity Authorization Ø deleteme Monitoring and Reports Ø System Administration	✓ ✓ Allow PEAP PEAP Inner Methods ✓ ✓ Allow EAP-MS-CHAPv2 ✓ Allow Password Change Retries: 1 ✓ Allow EAP-GTC ✓ Allow Password Change Retries: 1
	 Allow EAP-FAST EAP-FAST Inner Methods Allow EAP-MS-CHAPv2 Allow Password Change Retries: 3 Allow EAP-GTC Allow TLS-Renegotiation Use PACs Don't Use PACs Tunnel PAC Time To Live: 90 Days Proactive PAC update will occur after 10 % of PAC Time To Live has expired Proactive PAC update will occur after 10 % of PAC Time To Live has expired Allow Authenticated in-Band PAC Provisioning Server Returns Access Accept After Authenticated Provisioning Allow Machine Authentication Machine PAC Time To Live: 1 Hours 1 Hours 2

- 3. Fare clic su Invia.
- 4. Verificare il gruppo di identità selezionato. In questo esempio, viene utilizzato **Internal Users**, creato su ACS. **Salvare** le

modifiche	

Single re	t selection C Rule based result selection
lentity Source	nternal Users Select
	 Advanced Options
	tauthentication failed Reject 💌
	fuser not found Reject 💌
	f process failed Drop 💌
	lote: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests wi a rejected

5. Per verificare il profilo di autorizzazione, selezionare Access Policies > Access Services > Default Network Access > Authorization (Policy di accesso > Servizi di accesso > Accesso di rete predefinito).Èpossibile personalizzare in base a quali condizioni sarà consentito l'accesso degli utenti alla rete e in quali profili di autorizzazione (attributi) sarà possibile passare dopo l'autenticazione. Questa granularità è disponibile solo in ACS 5.x. In questo

esempio sono stati selezionati Location, **Device Type**, **Protocol**, **Identity Group** e **EAP Authentication**

Method.



- 6. Fare clic su OK, quindi su Salva modifiche.
- Il passaggio successivo consiste nella creazione di una regola. Se non viene definita alcuna regola, al client viene consentito l'accesso senza condizioni.Selezionate Crea (Create) > Regola-1 (Rule-1). Questa regola è destinata agli utenti del gruppo "Utenti wireless".

Access Policies > Access Services > D	efault Network Access > Authorization				
Standard Policy Exception Policy					
Network Access Authorization P	lettine				1
Filter: Status	Cisco Secure ACS - Mobilia Firefor	61.52		×	
E	- 192168150.24 Https://192	168.150.24/acsadmin/Polic	cylinputAction.do	合	
I Status Reame N	£		-		
No data to display	General				
	Name: Rule-1	Status: Enabled	- 0		
	The Customize policy condition	e button in the lower rights and results are ava	ght area of the policy rules screen cor Ilable here for use in policy rules.	ntrois which	
	VDG:Location:	in	All Locations LAB	Select	
	VDG:Device Type:	in	All Device Types 5500	Select	
	Protocol:	match	Radus	Select	
	Identity Group:	in	MI Groups Wireless Users	Select	
	Eap Authentication Met	hod: ANY-			
	Results Authorization Profiles: Permit Access Select Deselect		You may select multiple authorization pro defined in multiple profiles will use the vi profile defined.	ofiles. Attributes alue from the first	
" E Dataat r	r Gancer			1190	
Create * Duplicate * Ed	tt Delete A Move te	×		Customiza	HtCount

8. Salvare le modifiche. Lo schermo avrà il seguente aspetto:

l.

		RECEIVED FORCY						
iter. St	atus	- Nato	ch if. Equals 💽 Enat	led - Cie	ear Filler Go 🔫			
Status	Name	NDG:Location	NDG Device Type	Condition Protocol	identity Group	Eap Authentication Method	Resi	ults on Profile
	Rulo-1	in All Locations:LAB	In All Device Types 5508	match Radius	in All Groups:Wireless Users	-487-	Permit Acco	222
Dstaut	_	The rules defined or r	ne enabled rule matches.				Permit Acc	855

Se si desidera negare agli utenti che non soddisfano le condizioni, modificare la regola predefinita in "nega accesso".

9. Verranno ora definite **le regole di selezione del servizio**. Utilizzare questa pagina per configurare un criterio semplice o basato su regole per determinare il servizio da applicare alle richieste in ingresso. In questo esempio viene utilizzato un criterio basato su

Filter	Stat	15 ¥	Natch if	Equals + Enabled + C	learFilter 🛛 Go 🗍 🐱	
		Status	Name	Conditions	Results	Hit Count
1			Rule-1	match Radius	Default Network Access	0
2			Rule-2	match Tacacs	Default Device Admin	0

Configurare il WLC

Questa configurazione richiede i seguenti passaggi:

- 1. Configurare il WLC con i dettagli del server di autenticazione.
- 2. Configurare le interfacce dinamiche (VLAN).
- 3. Configurare le 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 per qualsiasi altra transazione.

Attenersi alla seguente procedura:

- 1. Dalla GUI del controller, fare clic su Security (Sicurezza).
- 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 uguale a quella configurata nel server RADIUS.

cisco	MONITOR WLAN		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Security	RADIUS Auther	ntication Server	s > New					
 AAA General RADIUS Authentication Accounting Falbook TACACS+ LDAP Local Net Users MAC Fibring Disabled Clients User Login Policies AP Policies Password Policies 	Server Index (Pr Server IP Addres Shared Secret Fo Shared Secret Confirm Shared S Key Wrap Port Number Server Status	ionity) s rmat Secret	1 x 192.168.150.1 ASCII x (Designed for 1812 Enabled x	24 r FIPS custom	ers and requires a	key wrap compl	iant RADI	IUS server)
Local EAP	Support for RFC	3576	Enabled -					
Priority Order	Server Timeout		2 aecono	la l				
Certificate	Network User		🗹 Enable					
Access Control Lists	Management		🗷 Enable					
Wireless Protection Policies	IPSec		Enable					
Web Auth								
Advanced								

Configurazione delle interfacce dinamiche (VLAN)

In questa procedura viene descritto come configurare le interfacce dinamiche sul WLC.

Attenersi alla seguente procedura:

1. L'interfaccia dinamica viene configurata dalla GUI del controller nella finestra Controller >

cisco		WLANS		WIRELESS	SECURITY	MANAGEMENT
CISCO Controller General Inventory Interfaces Interface Groups Multicast Network Routes	MONITOR Interfaces ULAN Id	wLANS s > New Name	Vlen253	WIRELESS	SECORITY	MANAGEMENT
 Internal DHCP Server Mobility Management Ports NTP CDP Advanced 						

Interfacce.

- 2. Fare clic su **Apply** (Applica).Viene visualizzata la finestra Edit (Modifica) di questa interfaccia dinamica (qui VLAN 253).
- 3. Immettere l'indirizzo IP e il gateway predefinito dell'interfaccia

cisco	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMEN
Controller	Interfaces	> Edit				
General Inventory Interfaces	General In	formatio	in	3		-
Interface Groups Multicast	NAC Addr	ess	00:24:	97:69:63:cf		
Network Routes	Configurat	ion				
Mobility Management	Guest Lan					
Ports	Quarantine	t Man Id				
> NTP > CDP	Physical In	formatio	on			
Advanced	The interfa	oce is attac	hed to a LAG.			
	Manageme	Address				
	VLAN Iden	tifier	253			
	IP Address		192.168.1	53.81		
	Netmask		255.255.2	55.0		
	Gateway		192.168.1	53.1		
	DHCP Info	rmation				_
	Primary D	HCP Serve	۰ [192.168.150.25		
	Secondary	DHOP Ser	rver			
	Access Co	ntrol List	t			_
	ACL Name		1	none 💽		
	Note: Changi temporarily d some clients.	ng the Inte lisabled an	inface paramate d thus may resu	rs causes the Wi It in loss of conr	LANS to be rectivity for	

dinamica.

- 4. Fare clic su **Apply** (Applica).
- 5. Le interfacce configurate avranno il seguente aspetto:

cisco	MONITOR	<u>WLANs</u>	WIRELESS	<u>s</u> ecurity	MANAGEMENT	COMMAN	NDS HELP	FEEDBACK	
Controller	Interfaces	1							
General									
Inventory	Interface	Name	VLAN Identifier	IP Address	s Interfa	се Туре	Dynamic AP	Management	
Interfaces	manageme	nt	75	192.168.75	44 Static		Enabled		
Interface Groups	service-por	t	N/A.	0.0.0.0	Static		Not Supported		
Multicast	virtual		N/A	1.1.1.1	Static		Not Supported		
Network Routes	<u>vlan253</u>		253	192,168,153	5.61 Dynamic	:	Disabled		-
Internal DHCP Server									
Mobility Management									
Ports									
▶ NTP									
CDP									
Advanced									

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 > Create New** (Crea nuova) per creare una nuova WLAN. Viene visualizzata la finestra Nuove WLAN.
- 2. Immettere l'ID WLAN e le informazioni sull'SSID WLAN.Èpossibile immettere qualsiasi nome come SSID WLAN. In questo esempio viene usato **goa** come SSID della

uluulu cisco		<u>W</u> LANs		W]RELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS
WLANS WLANS Advanced	WLANS > Type Profile Na SSID ID	New ms	WLAA goo goo 1				

WLAN.

3. Per accedere alla finestra Edit (Modifica) dell'obiettivo WLAN, fare clic su **Apply** (Applica).

cisco	MONITOR MLANS		WIRELESS		MANAGEMENT	COMMANDS	HELP
WLANs	WLANs > Edit 'g	oa'					
✓ WLANS	General Secu	ity QoS	Advanced				
 Advanced AP Groups 	Profile Name Type SSID Status Security Policies Radio Policy Interface/Interfac Group(G) Multicast Man Fea Broadcast SSID	gos WLAN goos [WPA2)((Modificati (Modificati (All e vian253 ture □ cnable E cnable	ed (Auth(802.1X ions done under v d d	+ CCKM)] r security tab (wil appear after ap	splying the chang	yes.)

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY
WLANs	WLANs > Edit 'goa'
WLANs MLANs Advanced	General Security QoS Advanced Layer 2 Layer 3 AAA Servers Layer 2 Security 9 WFA+WFA2
	WPA+WPA2 Parameters WPA Policy
	WPA2 Policy R WPA2 Encryption R AES TKIP Auth Key Mgmt 802.1X+CCKN •

WLANs > Edit 'goa'

General Layer 2	Security	QoS Advan AAA Servers				
Radius S Radius	A servers be ervers Server Overw	low to override u rite interfece □ _{En}	se of default servers	on this WLAN	LDAP Serve Server 1	None v
Server Server Server	71 72 73	Auth V p IP: Non	entication Servers nabled 192.168.150.24, Port:18 19	Accounting Servers Image: Complete Image: Complete	Server 2 Server 3	None 💌
Local EA Local E Authent web-au	P Authenticati SAP Authenticati fication prior th user	ion Ion Enabled ity order for			•	
No 4	ot Used		Order Used For Aut	hentication		

	0.000
and how overhee in Enabled	DHCP
Coverage Hole Detection M Enabled	DHCP Server Override
nable Bession Timeout	
Gronet IE Penabled	DHCP Addr. Assignment P Required
Nagnostic Channel Enabled	Management Frame Protection (MFP)
Pv6 Enable 2	and the second of the second
Override Interface ACL None -	MPP Client Protection 2 Disabled -
2P Blocking Action Disabled -	DTIM Period (in beacon intervals)
Dient Exclusion 2 Enabled	802.11a/n (1 - 255) 1
Assimum Allowed	802.11b/g/n (1 - 255) 1
Diente 🖣 👘	NAC
Static IP Tunneling 😰 🗆 Enabled	NAC State None -
Channel Scanning Defer	Load Balancing and Band Select
can Defer Priority 0 1 2 3 4 5 6 7	Client Load Balancing

Configurare Wireless Client Utility

PEAP-MSCHAPv2 (utente1)

WLANs > Edit 'goa'

Nel nostro client di test, utilizziamo Windows 7 Native Supplicant con una scheda Intel 6300-N con versione del driver 14.3. È consigliabile eseguire il test utilizzando i driver più recenti dei fornitori.

Completare questa procedura per creare un profilo in Windows Zero Config (WZC):

- 1. Selezionare Pannello di controllo > Rete e Internet > Gestisci reti wireless.
- 2. Fare clic sulla scheda Aggiungi.
- 3. Fare clic su **Crea manualmente un profilo di rete**.



- 4. Aggiungere i dettagli come configurato sul WLC.**Nota:** per SSID viene fatta distinzione tra maiuscole e minuscole.
- 5. Fare clic su **Next** (Avanti).

		٦
Network name:	goa	
Security type:	WPA2-Enterprise	
Encryption type:	AES 👻	
Security Key:	Hide characters	;
Start this connect	tion automatically	
Connect even if	the network is not broadcasting	
Warning: If you	select this option, your computer's privacy might be at risk.	

6. Fare clic su **Cambia impostazioni di connessione** per ricontrollare le impostazioni.

I Manually connect to a wireless network	
Successfully added goa	
Change connection settings Open the connection properties so that I can change the settings.	
	Close

7. Assicurarsi che PEAP sia

goa Wireless Network Properties	23
Connection Security	
Security type: WPA2-Enterprise Encryption type: AES	
Choose a network authentication method: Microsoft: Protected EAP (PEAP) Settings Remember my credentials for this connection each time I'm logged on	
Advanced settings	
ок Са	ncel

goa Wireless Network Properties
Connection
Security type: WPA2-Enterprise
Encryption type: AES -
Choose a network authentication method: Microsoft: Protected EAP (PEAP) Settings Remember my credentials for this connector coord time I'm logged on Advanced settings
OK Cancel

8. In questo esempio il certificato server non viene convalidato. Se si seleziona questa casella e non è possibile connettersi, provare a disabilitare la funzionalità e ripetere il

Validate server certificate	
Connect to these servers:	
Trusted Root Certification Authorities:	
AAA Certificate Services	-
AddTrust External CA Root	=
Class 3 Public Primary Certification Authority	
Class 3 Public Primary Certification Authority	
DigiCert Assured ID Root CA	
Digicert High Assurance EV Root CA	
	•
certification authorities.	
Select Authentication Method:	Configure
Select Authentication Method: Secured password (EAP-MSCHAP v2)	
Select Authentication Method: Secured password (EAP-MSCHAP v2)	
Select Authentication Method: Secured password (EAP-MSCHAP v2) Carteria Enable Fast Reconnect Enforce Network Access Protection	
Select Authentication Method: Secured password (EAP-MSCHAP v2) Cartering Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV	
Select Authentication Method: Secured password (EAP-MSCHAP v2) Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	,

9. In alternativa, è possibile utilizzare le credenziali di Windows per eseguire l'accesso. Tuttavia, in questo esempio non useremo questo metodo. Fare clic su

E/	AP MSCHAPv2 Properties
	When connecting:
	Automatically use my Windows logon name and password (and domain if any).
	OK Cancel

10. Per configurare il nome utente e la password, fare clic su **Advanced settings** (Impostazioni avanzate).

goa Wireless Network Properties	X
Connection Security	
Security type: WPA2-Enterprise Encryption type: AES	
Choose a network authentication method: Microsoft: Protected EAP (PEAP) Settings 	
Remember my credentials for this connection each time I'm logged on	
Advanced settings	
OK Ca	ncel

Advanced settings							
802.1X settings 802.11 settings							
Specify authentication mode:							
User authentication Save credentials							
Delete credentials for all users							
Enable single sign on for this network							
Perform immediately before user logon							
Perform immediately after user logon							
Maximum delay (seconds): 10							
Allow additional dialogs to be displayed during single sign on							
This network uses separate virtual LANs for machine and user authentication							
OK Cancel							

Windows Security	
Save crede	ntials
Saving your cre when you're no	edentials allows your computer to connect to the network ot logged on (for example, to download updates).
11/2	user1
	•••••
	OK Cancel

L'utilità Client è pronta per la connessione.

EAP-FAST (utente 2)

Nel nostro client di test, utilizziamo Windows 7 Native Supplicant con una scheda Intel 6300-N con versione del driver 14.3. È consigliabile eseguire il test utilizzando i driver più recenti dei fornitori.

Per creare un profilo in WZC, completare i seguenti passaggi:

- 1. Selezionare Pannello di controllo > Rete e Internet > Gestisci reti wireless.
- 2. Fare clic sulla scheda Aggiungi.
- 3. Fare clic su **Crea manualmente un profilo di rete**.

HOW Q	o you want to add a network?
-	Manually create a network profile
	This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).
4	Create an ad hoc network This creates a temporary network for sharing files or an Internet connection

- 4. Aggiungere i dettagli come configurato sul WLC.**Nota:** per SSID viene fatta distinzione tra maiuscole e minuscole.
- 5. Fare clic su **Next** (Avanti).

Network name:			
Network name.	goa		
Security type:	WPA2-Enterprise 🔹		
Encryption type:	AES 👻		
Security Key:		Hide characters	
Start this connec	tion automatically		
Connect even if	the network is not broadcasting		
Warning: If you	select this option, your computer's priva	cy might be at risk.	

6. Fare clic su **Cambia impostazioni di connessione** per ricontrollare le impostazioni.

Manually connect to a wireless network	
Successfully added goa	
Change connection settings Open the connection properties so that I can change the settings.	
	Close

7. Assicurarsi che EAP-FAST sia abilitato.**Nota:** per impostazione predefinita, WZC non dispone di EAP-FAST come metodo di autenticazione. È necessario scaricare l'utility da un fornitore esterno. In questo esempio, poiché si tratta di una scheda Intel, Intel PROSet è installato sul

Security type:	WPA2-Enterprise
Encryption type:	AES 🔻
Choose a network at Cisco: EAP-FAST Microsoft: Smart Ca Microsoft: Protected Cisco: LEAP Cisco: PEAP Cisco: PEAP Cisco: EAP-FAST Intel: EAP-SIM Intel: EAP-TTLS Intel: EAP-AKA	rd or other certificate d EAP (PEAP)
Advanced setting	IS

sistema.

goa Wireless Network Properties					
Connection					
Security type: WPA2-Enterprise					
Encryption type: AES -					
Choose a network authentication method:					
Cisco: EAP-FAST Settings Remember my credentials for this connection each time I'm logged on					
Advanced settings					
OK Cancel					

8. Abilitare Consenti preparazione automatica PAC e verificare che Convalida certificato server sia

deselezionato.

EAP-FAST Properties
Connection User Credentials Authentication About
Use anonymous outer identity anonymous Use Protected Access Credentials (PAC) Allow automatic PAC provisioning
PAC Authority: None Import
Validate server certificate
AAA Certificate Services AddTrust External CA Root Class 3 Public Primary Certification Authority Class 3 Public Primary Certification Authority Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA DigiCert High Assurance EV Root CA DST Root CA X3
Do not prompt user to authorize new servers or trusted certification authorities. OK Cancel Help

9. Fare clic sulla scheda **Credenziali utente** e immettere le credenziali dell'utente 2. In alternativa, è possibile utilizzare le credenziali di Windows per eseguire l'accesso. Tuttavia, in questo esempio non useremo questo metodo.

EAP-FAST Properties	2 ×						
Connection User Credentia	Authentication About						
Use certificate on this computer							
Use one-time password							
C Use Windows userna	O Use Windows username and password						
Prompt automatically	y for username and password						
Use saved username	e and password						
Username:	user2						
Password:	•••••						
Confirm password:	•••••						
	₹						
OK Cancel Help							

10. Fare clic su **OK**.

EAP-FAST Properties	? ×
Connection User Credentials Authentication About	
Select authentication method:	
Any method 🔹	Configure
Enable Fast Reconnect	
Enable Posture validation	
OK Car	Help

L'utilità Client è ora pronta per la connessione per l'utente 2.

Nota: quando l'utente 2 tenta di eseguire l'autenticazione, il server RADIUS invia una PAC. Accettare la PAC per completare l'autenticazione.



Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Verifica utente1 (PEAP-MSCHAPv2)

Dalla GUI del WLC, selezionare **Monitor > Clients**, quindi selezionare l'indirizzo MAC.

01	i	-	-	D .	- 4	-	:1
6	161	113	~	5	61	/CI	Ш

Client Properties			AP Properties		
Г	MAC Address	00:24:d7:ae:f1:98		AP Address	2c:3f:38:c1:3c:f0
I	IP Address	192.165.153.107		AP Name	3502e
I	Client Type	Regular		AP Type	802.11an
I	User Neme	user1		WLAN Profile	904
	Port Number	13		Status	Associated
I	Interface	vian253		Association ID	1
L	VLAN ID	253		802.11 Authentication	Open System
	CCX Version	CCXv4		Reason Code	1
	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 Nanager State	RUN		Short Preamble	Not Implemented
	Management Frame Protection	No		PBCC	Not Implemented
	UpTime (Sec)	12		Channel Agility	Nat Implemented
	Power Save Node	OFF		Re-authentication timeout	86365
	Current TxRateSet			Remaining Re-authentication	0
		6.0,9.0,12.0,15.0,24.0,3	6.0,45.0,54.	timeout	_
	Data RateSet	a		WEP State	WEP Enable
	oculty Information				

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNNP NAC State	Access
Rediue NAC State	RUN

Statistiche RADIUS WLC:

(Cisco Controller) >show radius auth statistics	
Authentication Servers:	
Server Index	1
Server Address	192.168.150.24
Msg Round Trip Time	1 (msec)
First Requests	8
Retry Requests	0
Accept Responses	1
Reject Responses	0
Challenge Responses	7
Malformed Msgs	0
Bad Authenticator Msgs	0
Pending Requests	0
Timeout Requests	0
Unknowntype Msgs	0
Other Drops	0
Log ACS:	

1. Completare questi passaggi per visualizzare i conteggi visite:Se si controllano i registri entro 15 minuti dall'autenticazione, assicurarsi di aggiornare il numero di



accessi.

parte inferiore della stessa pagina è presente una scheda per **Conteggio** visite.

letwork /	Access Authorization I	Policy					
Filter: St	tatus	▼ Match if: Equals	 Enabled 	💌 Clear Filter 🛛 Go 💌			
Name	NDG:Location	NDG:Device Type	Conditi Protocol	ions Identity Group	Eap Authentication Method	Results Authorization Profiles	HitCou
Rule-1	in All Locations 1.48	in All Device Types:5508	match Radius	in All Groups:Wireless Users	-ANY-	Permit Access	1
							л

 Fare clic su Monitoraggio e report per visualizzare una nuova finestra popup. Andare su Autenticazioni -Radius -Today. È inoltre possibile fare clic su Dettagli per verificare quale regola di selezione del servizio è stata applicata.



Verifica utente2 (EAP-FAST)

Dalla GUI del WLC, selezionare Monitor > Clients, quindi selezionare l'indirizzo MAC.

Client Properties			AP Properties		
MAC Address	001241d71aetf1198		AP Address	2013ft3810113ctf0	
IP Address	192.168.153.111		AP Name	3502e	
Client Type	Regular		AP Type	802.11an	
User Name	user2		WLAN Profile	00a	
Port Number	13		Status	Associated	
Interface	vlan253		Association ID	1	
VLAN ID	253		802-11 Authentication	Open System	
CCX Version	CCXV4		Reason Code	1	
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	Not Implemented	
Management Frame Protection	No		PBCC	Not Implemented	
UpTime (Sec)	29		Channel Agility	Not Implemented	
Power Save Mode	OFF		Re-authentication timeout	86392	
Current TxRateSet	m15 6.0,9.0,12.0,18.0,24	.0,36.0,48.0,54.	Remaining Re-authentication timeout	0	
Deta RateSet	0	ai	ai WEP State WEP 8		

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

Log ACS:

1. Completare questi passaggi per visualizzare i conteggi visite:Se si controllano i registri entro 15 minuti dall'autenticazione, assicurarsi di aggiornare il numero di accessi

Filter	Stat	JS 🔻	Match It.	Equals - Enabled - C	Clear Filter Go 🗢		
	E	Status	Name	Conditions	Results Service	Hit Coun	
1	E		Rule-1	match Radius	Default Network Access	3	
2	Г		Rule-2	match Tacacs	Default Device Admin	0	

a parte inferiore della stessa pagina è presente una scheda per **Conteggio** visite.



 Fare clic su Monitoraggio e report per visualizzare una nuova finestra popup. Andare su Autenticazioni -Radius -Today. È inoltre possibile fare clic su Dettagli per verificare quale regola di selezione del servizio è stata applicata.

2 · · · · · · · · · · · · · · · · · · ·											Las	anch Interactive	Viewer 1
Show	ng Page 1	of 1					Get	o Page: Ge					
UAA Protocol	> RADIUS	Authent	tication										
Authentication 8 Jate : Generated on Ja Relead	Status : Par Jan muary 29, 2	us or Fail usery 29, 2 912 6:23:1	012 05:53 7 PM ES	T MA	lanuary 29, 3	012 06:23 PM (La	at 30 Nitrutes <u>Last Hour</u> <u>L</u>	aat 12 Hours Today Yesferday	Last 7 Days (Last	<u>20 Deye</u>)	00000		1990)
Logged	iai 🤏 -c	RACIUS Status	NAS D	Netails	Usemane	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	C15 Security Group	ACS IN
Logged Jan 29,12 6.19	un Munc 1 At 27 270 PM	RACIUS Status	NAS D	letails	Usemame user2	MAC/IP Address 10.25-d7-ap-f1.98	Access Service Default Network Access	Authentication Method EAP-FAST (EAP-MSCH4P42)	Natwork Davica	NAS IP Address 192.168.75.44	NAS Port ID	C1S Security Group	ACS INS

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

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

- In caso di problemi, usare questi comandi sul WLC:debug client <mac add of the client>debug aaa all enableshow client detail <mac addr> - Verificare lo stato di policy manager.show radius auth statistics - Verifica il motivo dell'errore.debug disable-all -Disattiva i debug.clear stats radius auth all: cancella le statistiche sul raggio del WLC.
- 2. Verificare i log nel server ACS e annotare il motivo dell'errore.

Informazioni correlate

Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).