# Esempio di configurazione di ACS versione 5.2 e WLC per autenticazione WLAN

#### Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Configurare il WLC Configurazione di Cisco Secure ACS Verifica Risoluzione dei problemi

## Introduzione

Questo documento offre un esempio di configurazione per limitare l'accesso per utente a una LAN wireless (WLAN) in base all'identificatore del set di servizi (SSID).

## Prerequisiti

#### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione del controller WLC (Wireless LAN Controller) e del Lightweight Access Point (LAP) per un funzionamento di base
- Configurazione di Cisco Secure Access Control Server (ACS)
- Metodi LWAPP (Lightweight Access Point Protocol) e di sicurezza wireless

#### Componenti usati

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

- Cisco serie 5500 WLC con firmware versione 7.4.110
- Cisco serie 1142 LAP
- Cisco Secure ACS Server versione 5.2.0.26.11

## Configurazione

Per configurare i dispositivi per questa installazione, è necessario:

- 1. Configurare il WLC per le due WLAN e il server RADIUS.
- 2. Configurare Cisco Secure ACS.
- 3. Configurare i client wireless e verificare la configurazione.

#### **Configurare il WLC**

Completare questa procedura per configurare il WLC per questa configurazione:

 Configurare il WLC per inoltrare le credenziali dell'utente a un server RADIUS esterno. Il server RADIUS esterno (in questo caso Cisco Secure ACS) convalida quindi le credenziali utente e fornisce l'accesso ai client wireless. Attenersi alla seguente procedura: Selezionare Sicurezza > Autenticazione RADIUS dall'interfaccia utente del controller per visualizzare la pagina Server di autenticazione RADIUS.



Per definire i parametri del server RADIUS, fare clic su **New** (Nuovo). Questi parametri includono l'indirizzo IP, il segreto condiviso, il numero di porta e lo stato del server RADIUS. Le caselle di controllo Utente di rete e Gestione determinano se l'autenticazione basata su RADIUS è valida per gli utenti di rete e di gestione. In questo esempio viene utilizzato Cisco Secure ACS come server RADIUS con indirizzo IP 10.104.208.56.

#### cisco MONITOR WHAN: CONTROLLER AGRELESS SECURITY MEMOBINENT OCHNIANOS HELE ESEDEAC Security RADIUS Authentication Servers > New < Back Apply ...... Server Index (Priority) 1 . General + RADIUS Author Server 37 Address 10104.20555 Shared Securi Format 65.03 Shared Secret Enough Net David Multiplet Confirm Shared Secret \*\*\*\*\*\* Kury Weap Catigran to (TRO dummars for any that a key amplificant RODE Conver) Pert Banker 1:12 Ampulkies Received Robines Tashiari 📼 Server Status E Local EAP Support for RFC 3576 backled in Priority Order Server Tirosout 2 seconds Notwork User Z Cratile Entit 🗏 Erable Access Control Lists Planapament IP1cc incbie Wireless Protection Policies F Web Auth TrestSec 533 Advanced

Fare clic su Apply (Applica).

2. Completare questi passaggi per configurare una WLAN per il dipendente con SSID **dipendente** e l'altra WLAN per i collaboratori con SSID **collaboratore esterno**. Per creare una

WLAN, fare clic su **WLAN** dall'interfaccia utente del controller. Viene visualizzata la finestra WLAN. In questa finestra sono elencate le WLAN configurate sul controller.Per configurare una nuova WLAN, fare clic su **New** (Nuovo).In questo esempio viene creata una WLAN denominata Employee e l'ID WLAN è 1. Fare clic su **Applica**.

11 11 11							Logout Estrect
CISCO	MONITOR MLANE (	CONTROLLER WORELESS SEV	CURTY MANAGEMENT	CONVANCE HELF	ESEDBACK		
WLANs	WLANs > New			_		< Back	Apply
<ul> <li>WILANS WLANS</li> <li>WLANS</li> <li>WLANS</li> <li>WLANS</li> </ul>	Type Profile Name SSID ID	et.Al m Employee Employee					

Selezionare la finestra **WLAN > Modifica** e definire i parametri specifici della WLAN: Dalla scheda Protezione di layer 2, selezionare **802.1x**. Per impostazione predefinita, l'opzione Protezione di livello 2 è 802.1x. Ciò consente l'autenticazione 802.1 x/Extensible Authentication Protocol (EAP) per la WLAN.

cisco	BONITOR WINNE CONTROLLER AURELESS SECURITY MENABEMENT OCHMANOS HELE ESSENCY	ada raudawana Dala rafara Dauara
WLANs	WLANs > Edit 'Employee'	< Back Apply
* WLANS WLANS F Advanced	Ceneral Security QaS Advanced Layer 2 Layer 3 AAA Servers	
	Layer 2 Security ( With Letter 4g )	
	Park Premieron Premi Premieron Premieron Premi	
	WPA I WPAZ Parameters	
	WP07 Policy (v) WP02 Encryption (v)Ants ETYOP Authentication Key Management	
	002.2.4 M Tesha CCKM Englise PSK Tesha	
	Post Notes 2 Web Poly: manet in continuous in accordantia with Plant 2 Sectorement local durithms is not expended, with Plant 2010/ITE a manifestion for action installant Plant	

Dalla scheda Server AAA, selezionare il server RADIUS appropriato dall'elenco a discesa in Server RADIUS. Gli altri parametri possono essere modificati in base ai requisiti della rete WLAN. Fare clic su **Apply** (Applica).

			Sage Centryunation Engl Legeut Betreah
cisco	MONITOR MLANE CONTROLLER AGRELESS SECUR	TY NEVADENELT CONVENCE HELF RECORDS	
WLANs	WLANs > Edit 'Employee'		< Back Apply
WLANS WLANS	General Security QoS Advanced		
⊁ Advanced	Layer 2 Layer 3 AAA Servers		
	Select AAA servers below to override use of default se	ervers on this WLKN	Î.
	REPORT OF A REPORT OF A REPORT OF A REPORT	Star 1 bur	
	Antipute Antipute	According Servers Servers tors	- *
	141 Tantiwa	Frank Survey Loss a	
	August 1 19110-104-210-10, N	AT 8.2 m T-64 m	
	Smar 2 tore	• 7.K. H	
	Second Bone	· 2-04 ·	
	Secur 5 tota		
	Server 6 Bale	- T.C	
	Radius Server Accounting		
	Interim Update 🔄		
	Local EAP Authentication		
	e [	н	· · ·
	Fost Notes 2 Biol Talica menot in second in conduction with Many		
	<ul> <li>Web story conner be ones in completence with these she is discriminant local substance is not connected with these shell.</li> </ul>	WITE A REACTION OF A CONTRACT OF A REACTION OF A	

Analogamente, per creare una WLAN per i collaboratori esterni, ripetere i passaggi da b a d.

#### Configurazione di Cisco Secure ACS

Sul server Cisco Secure ACS è necessario:

- 1. Configurare il WLC come client AAA.
- 2. Creare il database utenti (credenziali) per l'autenticazione basata su SSID.
- 3. Abilitare l'autenticazione EAP.

Completare questi passaggi su Cisco Secure ACS:

- 1. Per definire il controller come client AAA sul server ACS, selezionare **Risorse di rete > Dispositivi di rete e client AAA** dall'interfaccia utente di ACS. In Dispositivi di rete e client AAA, fare clic su **Crea**.
- 2. Quando viene visualizzata la pagina Configurazione di rete, definire il nome del WLC, l'indirizzo IP e il segreto condiviso e il metodo di autenticazione (RADIUS).

	mm/ D x O Cetter E C X Coro Source ACS	*			A + 0
X 🕒 Shara Browser WebEc •					
cisco EvAL(Days left: 5)	CS		ecular	acalomplais (Primary)	Log Out About Help
	Network Resources > Network Devices and AAA Clamb > Create       • Name:     D074       Description:     Retwork Device Groups       Location     All Locatore       Device Type     All Device Types       # Address     IP Range(s)       • IP:     10.100.98.4	Seec.	Authentikation Options  TACACS+ Charad Secret Ingris Connect Device Ingrey Connect Supp RHOUS Ingres Secret ROUS CoAppt: 1710 Ingrestive Key/Wap Key Encryption Key Ingrestive Key	ort and Grange of	
Concerns of the second second					

3. Selezionare **Utenti e archivi identità > Gruppi di identità** dalla GUI di ACS. Creare i rispettivi gruppi per dipendente e appaltatore e fare clic su **Crea**. In questo esempio il nome del

gruppo creato è Dipendenti.

🗲 🍙 🕝 http://10.184.208.56/scrade	mm/ D + O Centric E d X 6 Cisco Secure A	cs ×		A 🛨 🗉
× Shara Browner, WebEr •				
altable Cisco Secure A	CS		ecautoin	acatemptete (Primary) Log Out About Help
CISCO EVAL(Days left: 5)				
<ul> <li>St MyWorkspace</li> </ul>	Users and Identity Stones > Hantity Groups > Create			
+ (5) Network Resources	General			
- 🗃 Users and Identity Stores	<ul> <li>Name: Employees</li> </ul>			
Herety Groupe	Description:			
<ul> <li>Internal identity blanes</li> <li>Users</li> </ul>	Parent All Scores	(Report)		
Hosts	0 - Descrived fields	(1000)		
<ul> <li>External Identity Stores</li> </ul>				
LDAP				
RSASecuriD Taken Senera				
RADIUS Identity Servers				
Certificate Authorities				
Certificate Authentication Profile				
<ul> <li>A Brits Elements</li> </ul>				
a Ch. Access Datates				
- Di Masitaina pari Danasta				
> 1 somering and Reports				
<ul> <li>S Bysten Administration</li> </ul>				
	Submit Carcel			

4. Selezionare Utenti e archivi identità > Archivi identità interni. Fare clic su Create (Crea) e immettere il nome utente. Inserirli nel gruppo corretto, definirne la password e fare clic su Invia.In questo esempio viene creato un utente denominato employee1 nel gruppo Employee. Analogamente, creare un utente denominato appaltatore1 nel gruppo appaltatori.

and the state of t	(BC) Lips Was had	and the second s	
(-) (-) (-) (-) (-) (-) (-) (-) (-) (-)	In/ D + O Cettre. E C X Circo Secur ACS X		6 2 9
X Stars Browner WebEr -			
alitatia Cisco Secure Al	CS	***	dmin acatemptate (Primary) Log Out About Help
CISCO EVAL(Days left: 5)			
» ∰ M/Workspace	Users and Identity Stores > Internal Bentity Stores > Users > Greate		
> (5) Nelwork Resources	and a		
- A Users and Identity Stores	General Tracket a C		
Henth Groups	•Name: empoyee1 Danue: Chables • 0		
<ul> <li>Internal Identity Stores</li> </ul>	Description:		
Users	Clidenthy Group: Al Groups Employee Balact		
<ul> <li>External Identity Stores</li> </ul>	Password Information	Enable Password Information	
LDAP	Password must	Password must.	
Active Directory	<ul> <li>Contain 4 - 32 characters</li> </ul>	<ul> <li>Contain 4 - 32 characters</li> </ul>	
RSA Security Taken Servers RADIUS Identity Servers			
Certificate Authorities	· Password.	Enable Password:	
Certificate Authentication Profile	Confirm Passwort:	Confirm Password:	
Nersh Store Sequences	Change password on next login		
<ul> <li>QV PolicyElements</li> </ul>	User Information		
* 🔁 Access Policies	There are no additional identity attributes defined for user records		
<ul> <li>Monitoring and Reports</li> </ul>	G = Required fields		
System Administration			
	×1		
	Submit Carcel		

5. Selezionare Elementi dei criteri > Condizioni di rete > Filtri stazioni finali. Fare clic su Crea.



Immettere un nome significativo e nella scheda **Indirizzo IP** immettere l'indirizzo IP del WLC. In questo esempio i nomi sono Dipendente e Appaltatore.



Nella scheda CLI/DNIS, lasciare CLI come -ANY- e immettere DNIS come \*<SSID>. In questo esempio, il campo DNIS viene immesso come \*Dipendente in quanto questo filtro della stazione terminale viene utilizzato per limitare l'accesso solo alla WLAN del dipendente. L'attributo DNIS definisce l'SSID a cui l'utente può accedere. Il WLC invia l'SSID nell'attributo DNIS al server RADIUS.Ripetere gli stessi passaggi per il filtro Stazione finale terzista.



6. Selezionare Elementi criteri > Autorizzazioni e autorizzazioni > Accesso alla rete > Profili di autorizzazione. Deve essere presente un profilo predefinito per Permit Access.

X Shere Browner Webbs •	n/ D + Q Centricu B d X Cisco Securi ACS X		n ☆®
CISCO CISCO Secure Al CISCO EVAL(Days left b)	CS and	min acatemptote (Primary)	Log Cut About Help
» G MyWorkspace	Policy Bernetia > Authorization and Permissions > Televork Accessa > Authorization Profiles		
<ul> <li>(5) Network Resources</li> </ul>	Authorization Profiles	Stawing 1-1 of 1	0 • perpage 00
<ul> <li>B Users and Identity Stores</li> </ul>	Filter: Velsh it: 🔹 🐨		
<ul> <li>Q&gt; Policy Elements</li> <li>Encoder Constitues</li> </ul>	Name + Destriction		
Date and Time	Fermit Access		
Custom * Nation: Canditiane End Statum Fitars Device Fitars Device PetiFitars * Authorization and Permissions * Nation: Access Patrimeter * Device Administration * Device Administration * Named Permission Objects * Cost Policies * Cost Po			
	Create Duplicate Edit Delate	H e Page	1 of 1 10 11

7. Selezionare Criteri di accesso > Servizi di accesso > Regole selezione servizi. Fare clic su Personalizza. Aggiungere eventuali condizioni appropriate. In questo esempio viene utilizzato il protocollo Radius come condizione di corrispondenza.Fare clic su Crea. Denominare la regola. Selezionare Protocollo, quindi Raggio.In Risultati scegliere il servizio di Access appropriato. In questo esempio viene lasciato come Accesso di rete predefinito.

Webpage Dialog		X
@ https://10.104.208.56/acsadmin/P	olicyInputAction.do	😮 Certificate error
Customize Conditions Available: ACS Host Name Compound Condition Device Filter Device IP Address Device Port Filter End Station Filter NDG:Device Type NDG:Location Time And Date UseCase	Selected:  Protocol	
OK Cancel		

Cisco Secure ACS Webpage Dialog	×
Attps://10.104.208.56/acsadmin/PolicyInputAction.do	😮 Certificate error
General	
Name: Rule-4 Status: Enabled 👻 \Theta	
The Customize button in the lower right area of the policy rules screen controls conditions and results are available here for use in policy rules.	which policy
Conditions	
Protocol: match   Radius  Select	
Results	
Service: Default Network Access 👻	
	Неір

8. Selezionare Criteri di accesso > Servizi di accesso > Accesso di rete predefinito > Identità. Scegliere Selezione risultati singoli e Origine identità come utenti interni.

		and the second s	A CONTRACTOR OF	interinterior A
(-) (-) (-) (-) (-) (-) (-) (-) (-) (-)	min/ D + O Cetter. E d X 6 Circ	o Secure ACS ×		ର <del>ସ</del> ାସ
× Shere Browner WebEc •				
alitate Cisco Secure A	CS		acautoin	acalemplate (Primary) Log Out About Help
CISCO EVAL(Days left: 5)				
» ∰ MyWorkspace	Access Policies > Access Services > Default M	Wwark Access > Merily		
+ (52 Nelwork Resources	Sincle result selectory — Role tony	of result sales from		
+ 2 Users and identity Stores	Identity Source: Indential Uners	( galant )		
<ul> <li>Qv PolicyElements</li> </ul>	Hend Core			
- 🐍 Access Policies	<ul> <li>Advanced Options</li> </ul>			
* Access Services				
1 Service Selection Rules				
O DefaultDevice Admin				
Authorization				
<ul> <li>O Default Network Access</li> </ul>				
Autorization				
<ul> <li>Monitoring and Reports</li> </ul>				
+ R System Administration				
	State Channel - Official Channel			
	saw charges Uscart Charg	019		

Selezionare **Criteri di accesso > Servizi di accesso > Accesso alla rete predefinito > Autorizzazione.** Fare clic su **Personalizza** e aggiungere le condizioni Personalizzate. In questo esempio vengono utilizzati, nell'ordine, Identity Group, NDG:Device Type e End Station Filter.



Fare clic su **Crea**. Assegnare un nome alla regola e scegliere il gruppo di identità appropriato in Tutti i gruppi. Nell'esempio, questo valore è Employee.

Cisco Secure ACS Webpage Dialog	Cisco Secure ACS Webpage Dalog
Carificate en	🍘 hetpes/12.224.200. 🖬 /acca devies Plataarek Davies Grouph Fleg utilations da Prosentat Data, a tarea Filmer Eductity Groupe Eductity (m. 🧕 O
	Network Device Groups
General	FRAC • MAKE IC • 🖂 🐨
Name, Rue-2 Status: Enabled +	
The Customize button in the inversion area of the policy raise access controls which anisy	Name   Description
conditions and results are available here for use in policy rules.	O • A GOLDE HEAD OWNERDON
	Contractor
Conditions Reserve	
Cartering Group	
Constitution state with a failed	and Alexandra and Alexandra States
	🧭 https://ILTIL.IIL.W/www.init/Febarat.fe/entropy.Physical-tex.in/texatories.com/entropy.fe/entropy.fe/entropy.go. 2011/10/2011
Pasadas Professional Annual	Remone being trouge
	TOPE LABOR I III
You may select multiple authorization profiles . Atributes	A Desize Total A Desize Upper
protie defined.	(* ma
Robert Present	
Sweet Depends	
	LINER HIDOLER, MAR LINER, CONTRACTOR AND
	DE General Celes

Fare clic sul pulsante di opzione **Employee End Stn Filter** o immettere il nome immesso al punto 1b nella sezione "Configurazione del WLC".

Ę	Cisco Secure ACS Webpage Dialog						
	遵 https	://10.104.208.56/acsadmin/N	IARsLPInputAction.do?listType=EndStatio	n	Certificate error		
	End Station Filters			Showing 1-2 of 2 50	▼ per page Go		
	Filter:	<ul> <li>Match if:</li> </ul>	🗕 🐨				
		Name 🔺	Description				
	0	Contractor End Stn Filter					
	۲	Employee End Stn Filter					
	Crea	te Duplicate Edit	Delete	I Page	1 of 1 🕨 🕅		
	OK C	ancel			Help		

Selezionare la casella di controllo Consenti accesso.

Cisco Secure ACS Webpage Dialog		<b></b> X
https://10.104.208.56/acsadmin/NetworkAccessLPInputAction.do		💈 Certificate error
Authorization Profiles	Showing 1-2 of 2 50	▼ per page Go
Filter: 🔹 Match if: 🔹 Go 🗢		
Name  Description		
DenyAccess		
Permit Access		_
Create Duplicate Edit Delete	I Page	1 of 1 🕨 🔛
		Help
		Help

Ripetere gli stessi passaggi descritti in precedenza anche per le regole collaboratori esterni.

Assicurarsi che l'azione predefinita sia **Nega accesso**. Dopo aver completato il passaggio e, le regole dovrebbero essere simili a quelle riportate nell'esempio seguente:



La configurazione è terminata. Dopo questa sezione, il client deve essere configurato di conseguenza con l'SSID e i parametri di sicurezza per potersi connettere.

## Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## Risoluzione dei problemi

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