Esempio di configurazione del reindirizzamento della pagina iniziale del controller LAN wireless

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Premesse Installazione della rete Configurazione Passaggio 1. Configurare il WLC per l'autenticazione RADIUS tramite il server Cisco Secure ACS. Passaggio 2. Configurare le WLAN per il reparto amministrativo e operativo. Passaggio 3. Configurare Cisco Secure ACS in modo che supporti la funzione di reindirizzamento della pagina iniziale. Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene descritto come configurare la funzione di reindirizzamento della pagina iniziale sui Wireless LAN Controller.

Prerequisiti

Requisiti

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

- Conoscenza delle soluzioni di sicurezza LWAPP
- Informazioni su come configurare Cisco Secure ACS

Componenti usati

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

• Cisco serie 4400 Wireless LAN Controller (WLC) con firmware versione 5.0

- Cisco serie 1232 Light Weight Access Point (LAP)
- Cisco Aironet 802.a/b/g Adattatore client wireless con firmware versione 4.1
- Server Cisco Secure ACS con versione 4.1
- Qualsiasi server Web esterno di terze parti

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.

Premesse

Il reindirizzamento Web della pagina iniziale è una funzione introdotta con Wireless LAN Controller versione 5.0. Con questa funzione, l'utente viene reindirizzato a una particolare pagina Web dopo il completamento dell'autenticazione 802.1x. Il reindirizzamento si verifica quando l'utente apre un browser (configurato con una home page predefinita) o tenta di accedere a un URL. Al termine del reindirizzamento alla pagina Web, l'utente ha accesso completo alla rete.

Èpossibile specificare la pagina di reindirizzamento nel server RADIUS (Remote Authentication Dial-In User Service). Il server RADIUS deve essere configurato in modo da restituire l'attributo Cisco av-pair url-redirect RADIUS al controller LAN wireless dopo la riuscita autenticazione 802.1x.

La funzione di reindirizzamento Web della pagina iniziale è disponibile solo per le WLAN configurate per la sicurezza di layer 2 802.1x o WPA/WPA2.

Installazione della rete

Nell'esempio, un Cisco 4404 WLC e un Cisco serie 1232 LAP sono connessi tramite uno switch di layer 2. Anche il server Cisco Secure ACS (che agisce come server RADIUS esterno) è connesso allo stesso switch. Tutti i dispositivi si trovano nella stessa subnet.

Il LAP è inizialmente registrato sul controller. È necessario creare due WLAN: una per gli utenti del **reparto di amministrazione** e l'altra per gli utenti del **reparto operazioni**. Entrambe le LAN wireless utilizzano WPA2/ AES (per l'autenticazione viene utilizzato EAP-FAST). Entrambe le WLAN utilizzano la funzione di reindirizzamento della pagina iniziale per reindirizzare gli utenti agli URL della home page appropriati (su server Web esterni).

Nel documento viene usata questa impostazione di rete:



Cisco Secure ACS server

WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

La sezione successiva spiega come configurare i dispositivi per questa installazione.

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 <u>registrati</u>).

Per configurare i dispositivi in modo che utilizzino la funzionalità di reindirizzamento della pagina iniziale, completare la procedura seguente:

- 1. Configurare il WLC per l'autenticazione RADIUS tramite il server Cisco Secure ACS.
- 2. Configurare le WLAN per i reparti Admin e Operations.
- 3. <u>Configurare Cisco Secure ACS in modo che supporti la funzione di reindirizzamento della pagina iniziale.</u>

Passaggio 1. Configurare il WLC per l'autenticazione RADIUS tramite il server

Cisco Secure ACS.

Per inoltrare le credenziali dell'utente a un server RADIUS esterno, è necessario configurare il WLC.

Per configurare il WLC per un server RADIUS esterno, completare la procedura seguente:

- 1. Selezionare **Security** (Sicurezza) e **RADIUS Authentication** (Autenticazione RADIUS) dall'interfaccia utente del controller per visualizzare la pagina Server di autenticazione RADIUS.
- 2. Per definire un server RADIUS, fare clic su New (Nuovo).
- Definire i parametri del server RADIUS nella pagina Server di autenticazione RADIUS > Nuovo.Questi parametri includono:Indirizzo IP server RADIUSSegreto condivisoNumero portaStato

server		
- dudu cisco		Sage Configuration Bing Logout Befresh
CISCO	Bounder Torus Zoune	OFTER MINETERS JECONITY MEMORINENT COMMONDS HED.
Security	RADIUS Authentication S	Servers > New <back apply<="" td=""></back>
General	Server Index (Priority)	1 .
Authentication	Server IPAddress	10.77.244.196
TACACS+ LDAP	Shared Secret Format	ASCII 💌
Local Net Users MAC Filtering	Shared Secret	•••••
Disabled Clients User Login Policies AP Policies	Confirm Shared Secret	•••••
Local EAP	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Priority Order	Port Number	1012
Access Control Lists	Port Number	
 Wireless Protection Policies 	Server Status	Enabled .
Web Auth	Support for RFC 3576	Enabled .
▶ Advanced	Server Timeout	2 seconds
	Network User	R Enable
	Management	🕅 Enable
	IPSec	Enable

In questo documento viene usato il server ACS con indirizzo IP 10.77.244.196.

4. Fare clic su **Apply** (Applica).

Passaggio 2. Configurare le WLAN per il reparto amministrativo e operativo.

In questo passaggio vengono configurate le due WLAN (una per il reparto Amministratori e l'altra per il reparto Operazioni) che i client utilizzeranno per connettersi alla rete wireless.

L'SSID WLAN per il reparto Admin sarà *Admin*. L'SSID WLAN per il reparto operazioni sarà Operations (Operazioni).

Usare l'autenticazione EAP-FAST per abilitare WPA2 come meccanismo di sicurezza di layer 2 sia sulle WLAN che sulla funzione Web policy - Splash Page Web Redirect come metodo di

sicurezza di layer 3.

Per configurare la WLAN e i parametri correlati, completare la procedura seguente:

- 1. Fare clic su **WLAN** dall'interfaccia utente del controller per visualizzare la pagina WLAN.In questa pagina vengono elencate le WLAN esistenti sul controller.
- 2. Per creare una nuova WLAN, fare clic su New

(Nuovo).				_			Saye Co	nfiguration <u>P</u> ing I	Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs>	New						< Back	Apply
WLANS	Туре		WLAN						
Advanced	Profile Na	me	Admin						
	WLAN SSI	D	Admin						

- 3. Immettere il nome dell'SSID della WLAN e il nome del profilo nella pagina WLAN > Nuovo.
- 4. Fare clic su **Apply** (Applica).
- 5. Innanzitutto creiamo la WLAN per il reparto amministrativo.Dopo aver creato una nuova WLAN, viene visualizzata la pagina WLAN > Modifica per la nuova WLAN. In questa pagina è possibile definire vari parametri specifici per la WLAN. Sono inclusi i criteri generali, i criteri di sicurezza, i criteri QOS e i parametri avanzati.
- 6. Per abilitare la WLAN, in Criteri generali selezionare la casella di controllo Stato

olulo.									
cisco	MONITOR		CONTROLLER	WIRE ESS	SECURITY	MANAGEMENT	Sage Co	HELD	Logout <u>R</u> efree
WLANS WLANS WLANS Advanced	WLANS > General Profile Type SSID Status Securit Radio P Interfai Broadc	Edit Secur Name y Policies Policy ce ast SSID	ity QoS Admin WLAN Admin IC Enable Splash- (Modification) All admin IC Enable	Advanced ed Page-Web-Re ions done under	edirect[WPA:	2][Auth(802.1X)] will appear after ap	I pplying the chang	ges.)	Apply

- 7. Fare clic sulla scheda **Protezione** e quindi sulla scheda **Layer 2**.
- 8. Selezionare **WPA+WPA2** dall'elenco a discesa Protezione di layer 2.Questo passaggio consente di abilitare l'autenticazione WPA per la WLAN.
- 9. In Parametri WPA+WPA2 selezionare le caselle di controllo **Criterio WPA2** e **Crittografia AES**.

	ac i Edu
CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANs WLANs > Edit < Back	pply

- 10. Selezionare **802.1x** dall'elenco a discesa Auth Key Mgmt. Questa opzione abilita WPA2 con autenticazione 802.1x/EAP e crittografia AES per la WLAN.
- 11. Fare clic sulla scheda Protezione di livello 3.
- 12. Selezionare la casella **Criteri Web**, quindi fare clic sul pulsante di opzione **Reindirizzamento Web pagina iniziale**.Questa opzione attiva la funzione Web Redirect della pagina iniziale.

						Sa <u>v</u> e Co	nfiguration Ping	Logout <u>R</u> efre
CISCO	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	_
WLANS WLANS WLANS Advanced	WLANS > Edit General Secur Layer 2 Lay Layer 3 Security Web Policy Authenticatio Passthrough Conditional 1 Splash Page Preauthenticatio ACL	ity QoS er 3 AAA Se None 2 in Web Redirect Web Redirect None ¥	Advanced				< Back	Apply

- 13. Fare clic sulla scheda **Server AAA**.
- 14. In Server di autenticazione scegliere l'indirizzo IP del server appropriato dall'elenco a discesa Server

cisco	Sage Configuration Bing Logout B MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS WLANS > Advanced	WLANs > Edit < Back

Nell'esempio, 10.77.244.196 viene usato come server RADIUS.

15. Fare clic su **Apply** (Applica).

1

 Ripetere i passaggi da 2 a 15 per creare la WLAN per il reparto operazioni.Nella pagina WLAN sono elencate le due WLAN

create.							
սիսիս					Sa <u>v</u> e Co	onfiguration Ping	Logout <u>R</u> efresh
CISCO	MONITOR WLANS CO	NTROLLER WIRELI	ESS SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs						New
WLANS WLANS	Profile Name	Туре	WLAN SSID		Admin Status	Security Policies	
Advanced	Admin	WLAN	Admin		Enabled	[WPA2][Auth(802.1	X)], Splash-Page
	Operations	WLAN	Operations		Enabled	[WPA2][Auth(802.1	X)], Splash-Pagr

I criteri di protezione includono il reindirizzamento della pagina iniziale.

Passaggio 3. Configurare Cisco Secure ACS in modo che supporti la funzione di reindirizzamento della pagina iniziale.

Il passaggio successivo consiste nella configurazione del server RADIUS per questa funzionalità. Il server RADIUS deve eseguire l'autenticazione EAP-FAST per convalidare le credenziali del client e, se l'autenticazione ha esito positivo, per reindirizzare l'utente all'URL (sul server Web esterno) specificato nell'attributo RADIUS di *reindirizzamento URL a* coppia av Cisco.

Configurazione di Cisco Secure ACS per l'autenticazione EAP-FAST

Nota: in questo documento si presume che il controller LAN wireless sia stato aggiunto al Cisco

Secure ACS come client AAA.

Completare questa procedura per configurare l'autenticazione EAP-FAST nel server RADIUS:

1. Fare clic su **Configurazione del sistema** dall'interfaccia utente del server RADIUS, quindi scegliere **Configurazione autenticazione globale** dalla pagina Configurazione del sistema.



 Dalla pagina di impostazione dell'autenticazione globale, fare clic su Configurazione EAP-FAST per accedere alla pagina di impostazione di EAP-FAST.

	1.0.1:1065/	s 🛃 🖻
Croco Systems	System Configuration	2
Ebune 1	EAP Configuration	Pelp
Setup	PEAP Allow EAP-MSCHAPv2 Allow EAP-GTC	Use this page to specify settings for various authentication grotacols. • CAP Conferencies
Shared Profile Components Net work Configuration	Allow Posture Validation Allow EAP-TLS	• PEAP • CAP_FAXX • CAP_FAXX • CAP_FIX3 • CAP_FIX2 • CAP_FIX2
System Configuration	Select one or more of the following options: E Certificate SAN comparison Certificate CN comparison	APEAP Report Timesat MS-CMAP Conference
Administration Control	E Certificate Binary comparison EAP-TLS session timeout (minutes): 120	EAP Configuration EAP is a flexible requestivespanse protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of another protocol such as UDP, 002.1x or RADDUS and supports
Network Access Profiles	PEAP session timeout (minutes): 120 Enable Fast Reconnect: R	multiple "authentication" types. [back to Top] PEAP
Contine Documentation	EAP-FAST EAP-FAST Configuration	PEAP is the outer layer protocol for the secure tunnel.
	EAP-TLS	Noder FEM is a contribute-based suction to completed. FEM authoritization can occur only after you have completed the required steps on the ACS Certificate Setup page.
	Select one or more of the following options:	 Allow EAP MSCHAPv2 — Use to enable EAP-MSCHAPv2 within MS PEAP authentic stone. Enable this protocol for any reportary that supports MS- CMAPV2 and the store of the store of

3. Dalla pagina Impostazioni EAP-FAST, selezionare la casella di controllo **Consenti EAP-FAST** per abilitare EAP-FAST nel server RADIUS.

CiscoSecure ACS - N	Scrosoft Internet Explorer	<u>=161 ×</u>
Ele Edt Yew Fg	ronites Iools Help	Links 🍄 🤷
Address http://127.0	0.0.1:1065/	💽 🛃 🐼
Crees Systems	System Configuration	
User Setup	EAP-FAST Configuration	EAP-FAST Configuration Page
Group Setup	EAP-FAST Settings	Use this page to configure EAD-FAST authentication settings.
Bhareditroffs Components Configuration Configuration	AP-FAST Active master key TTL active master key TTL amonths Tunnel PAC TTL amonths Client initial message: tacwebacs Authority ID Info: tacwebacs Authority ID Info: Allow anonymous in-band PAC provisioning Allow authenticated in-band PAC provisioning Accept client on authenticated provisioning Require client certificate for provisioning	EAP-FAST Sections Elimit initial measure Authority ID Lafe Allers assegments in kind DAC provisioning Allers assegments in kind DAC provisioning Allers assegments in kind DAC provisioning Allers assesting to the add DAC provisioning Allers assesting asthern to atlen Allers assesting asthern to atlen EAP-TAST section asthern to atlen EAP-TAST section association EAP-FAST sections EAP-FAST sections EAP-FAST sections EAP-FAST sections
Network Access Prodies Reports and Activity Online Documentation	Allow Machine Authentication Machine PAC TTL I weeks Allow Stateless session resume Authorization PAC TTL I hours Allowed inner methods REAP-GTC REAP-MSCHAPV2 EAP-TLS Submit Submit + Restart Cancel	 Active Naster Key TIL Enter a value for the amount of time that a master key is used to generate new Protected Access Credentials (PACs), lithen the time to live (TIC) defined for the Master Key sepires, the master key is considered retired and a new master key is generated. Retired master key TIL Enter a value for the amount of time that PACs generated using a ratired master key are acceptable for EAP-FAST authomic atom with an end-user client gains network access using a PAC based on articed master key. ACS sends a new PAC to the end-user client. Tanael PAC TIL Enter a value for the amount of time that a PAC is before it expires and master key. ACS credit of the end-user client. Tanael PAC TIL Enter a value for the amount of time that a PAC is used the Tunnel PAC has not expired, new PAC creation and assignment is automatic. If the master key used to generate the Tunnel PAC has not expired, new PAC creation and assignment is automatic. If the master key used to generate the Tunnel PAC has not expired.
		j j j j j j j j j j j j j j j j j j j
🐮 Start 🔯 🥭	CiscoSecure ACS - Mic	💆 7:58 PM

- 4. Configurare i valori TTL (Time-to-Live) della chiave master attiva/ritirata in base alle esigenze oppure impostarli sul valore predefinito, come illustrato in questo esempio.II campo Authority ID Info (Informazioni ID autorità) rappresenta l'identità testuale del server ACS, che un utente finale può utilizzare per determinare il server ACS da autenticare. Compilare questo campo è obbligatorio.II campo Messaggio iniziale di visualizzazione client specifica il messaggio da inviare agli utenti che eseguono l'autenticazione con un client EAP-FAST. La lunghezza massima è di 40 caratteri. Il messaggio iniziale verrà visualizzato solo se il client dell'utente finale supporta la visualizzazione.
- 5. Se si desidera che ACS esegua la preparazione anonima della PAC in banda, selezionare la casella di controllo **Consenti preparazione anonima della PAC in banda**.
- 6. L'opzione Allowed inner methods determina i metodi EAP interni che possono essere eseguiti all'interno del tunnel EAP-FAST TLS. Per il provisioning in banda anonimo, è necessario abilitare EAP-GTC e EAP-MS-CHAP per la compatibilità con le versioni precedenti. Se si seleziona Consenti preparazione PAC in banda anonima, è necessario selezionare EAP-MS-CHAP (fase zero) e EAP-GTC (fase due).
- 7. Fare clic su **Invia**.**Nota:** per informazioni dettagliate ed esempi su come configurare EAP FAST con il provisioning in-band PAC anonimo e il provisioning in-band autenticato, fare riferimento all'<u>esempio di autenticazione EAP-FAST con i controller LAN wireless e la configurazione del server RADIUS esterno.</u>

Configurare il database utente e definire l'attributo RADIUS di reindirizzamento URL

In questo esempio il nome utente e la password del client wireless vengono configurati rispettivamente come Utente1 e Utente1.

Per creare un database utenti, effettuare i seguenti passaggi:

- 1. Dalla GUI di ACS nella barra di navigazione, scegliere User Setup (Configurazione utente).
- 2. Creare un nuovo utente senza fili e quindi fare clic su Aggiungi/Modifica per accedere alla pagina Modifica

Ele Edt Yew Fg	vorites Iools Help	Links ** Cose
Address 🔄 http://127.0	0.0.1:1065/	🛃 🔁 😡
Cinco Syntems	User Setup	×
addinaddina	Select	Help
User Setup Corosp Setup Dared Profile Configuration Surren Configuration Surren Configuration Configuration Configuration Configuration Configuration Configuration Pother Pothe	User: User1 Find Add/Edit List users beginning with letter/number: ABSPBTTYYTT DPDETTYTT DATES List all users Remove Dynamic Users Red to bulp	 Yest Safata and External Over Databases Herding a Sectific User in the ACS Internal Oxtabases Adding a User to the ACS Internal Oxtabases Adding a User to the ACS Internal Oxtabases Listing AU User answer that Regin with a Databases Changing a User answer in the ACS Internal Oxtabases Changing a User answer in the ACS Internal Oxtabases Changing a User answer in the ACS Internal Oxtabases Changing a User answer in the ACS Internal Oxtabases Demicro Dynamic User User Setup anables you to configure individual user information, add users, and delete users in the database. User Setup and External User Oxtabases Befire ACS can authenticate users with an external user databases You must have the database up and running on the enternal server. For anample, if you are using taken card authentication, your taken server must be running and pergerty configuration. You must have configuration overrifes Group Setup configuration. You must have configuration overrifes Group Setup configuration is an external User Oxtabases section. Notes User Setup configuration overrifes Group Setup configuration. Providuate database, usernames cannot be located or listed here until the user has succersfully authenticated inc. External user database modification must be done from within the external user database. User Setup for groups in the ACS internal database. Notes: User Setup forms the ACS internal database for within the external user database. User Setup forms the ACS internal database. Notes: User Setup forms that database for user information, add user database. (Buck no Trog) Finding a Specific User in the ACS Internal Database. Finding a Specific User in the ACS Internal Databases
		of the username in the Uneer field, add an astarisk (*) as a wildcard, and click. Field. From the list of usernames displayed. click the username whose information you want to view or change.

 Nella pagina Modifica della configurazione utente, configurare il nome reale e la descrizione, nonché le impostazioni della password, come illustrato in questo esempio. In questo documento viene usato il database interno ACS per l'autenticazione tramite password.

Edt Vew Fr	Microsoft Internet Lipplorer	
ss A http://127	10.0.1:1065/	10
tes Statems	User Setup	
<u> </u>	Edit	Help
User Setup Setup Satup Shared/Inoffle Components Network Configuration	User: User1 (New User) Account Disabled Supplementary User Info	Account Disabled Ordeling a Username Supplementary Day Days Password Authentication Calitate Calitate Calitate Calitate Calitate Calitate Calitate Calitate Calitate
System Configuration Interface Configuration Configuration Control	Real Name Description	Six Devels, Access, Res Dictions Has: Seasteen Unein, Devels Access, Disable Oversila adde, ACLa Advanced, IACAC2 - Sattlines IACAC2 - Cashle Control IACAC3 - Cashle Control
External User Databases Posture Validation Network Access Profiles	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not chacked.)	IACACS - Dethesed Parameet IACACS - Shell Command: Antherization Command: Antherization, Society Statement, Control Contr
Activity Online Documentation	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP)	Account Disabled Status Select the Account Disabled check box to disable this account clear the check box to enable the account.
	Password Confirm Password Submit Cancel	Beleting a Username The Delete botton appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete . When asked to confirm your action. click De .

- 4. Scorrere la pagina verso il basso per modificare gli attributi RADIUS.
- 5. Selezionare la casella di controllo [009\001] cisco-av-pair.
- 6. Immettere queste coppie di av Cisco nella casella di modifica [009\001] cisco-av-pair per specificare l'URL a cui l'utente viene reindirizzato:url-redirect=http://10.77.244.196/Admin-Login.html

Cisco Systems	User Setup	[
	(useu iut senukass anu senukuun cherius such as routers)	- Help
User Setup	Password	Account Disabled
Group Setup	Password	Ordetting a Unername Supplementary User Infe
Shared Profile Components	Cisco Airespace RADIUS Attributes	Cassward Authentication Group to which the user is assigned Callback
Network Configuration	[14179/005] Aire-Interface-Name	Cleant IP Address Assignment Advanced Settings
System Configuration		Max Session Max Session
Configuration		Account Disable Dismissional Disable
Administration Centrel	Cisco IOS/PIX 6.x RADIUS Attributes	Advanced IACACS - Settings TACACS - Enable Control TACACS - Enable Resourced
Databases	₩ [009\001] cisco-av-pair	TACACS - Outbound Password TACACS - Shell Command Authorization
Porture Validation	ur1- redirect=http://10.77.244.196/	Command Authorization for Network Device Hanagement Applications TACACS - Unknewn Services TACACS - Unknewn Services
Network Access Profiles	Admin-login.html	RADIUS Vendor Saccific Attributes
Reports and Activity	×	
Documentation		Account Disabled Status
		the check box to enable the account.
	💡 Back to Help	[Back to Top]
		Deleting a Username
	Submit Delete Cancel	The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the

Questa è la home page degli utenti del reparto di amministrazione.

- 7. Fare clic su Invia.
- 8. Ripetere questa procedura per aggiungere User2 (utente del reparto operazioni).
- 9. Ripetere i passaggi da 1 a 6 per aggiungere al database altri utenti del reparto di amministrazione e del reparto operazioni. **Nota:** gli attributi RADIUS possono essere configurati a livello di utente o di gruppo su Cisco Secure ACS.

Verifica

Per verificare la configurazione, associare un client WLAN del reparto di amministrazione e del reparto operazioni alle WLAN appropriate.

Quando un utente del reparto di amministrazione si connette all'amministratore LAN wireless, all'utente vengono richieste credenziali 802.1x (credenziali EAP-FAST nel caso specifico). Una volta che l'utente ha fornito le credenziali, il WLC le passa al server Cisco Secure ACS. Il server Cisco Secure ACS convalida le credenziali dell'utente a fronte del database e, se l'autenticazione ha esito positivo, restituisce l'attributo url-redirect al controller LAN wireless. Autenticazione completata in questa fase.

😤 Cisco Aironet Desktop Utility	y - Current Profile: Admin		? 🗙
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
Profile Name:	Admin		
Link Status:	Not Associated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149	
Server Based Authentication:	None	Data Encryption: AES	
IP Address:	10.77.244.221		
Signal Strength		Good	
		Advanced	

Quando l'utente apre un browser Web, viene reindirizzato all'URL della home page del reparto Admin. (Questo URL viene restituito al WLC tramite l'attributo cisco-av-pair). Dopo il reindirizzamento, l'utente ha accesso completo alla rete. Ecco gli screenshot:



Le stesse sequenze di eventi si verificano quando un utente del reparto operazioni si connette alle operazioni WLAN.

😤 Cisco Aironet Desktop Utility	y - Current Profile: O	perations ?	×
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
Profile Name:	Operations		
Link Status:	Authenticated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149	
Server Based Authentication:	EAP-FAST	Data Encryption: AES	
IP Address:	10.77.244.221		
Signal Strength:		Good	
		Advanced	



Risoluzione dei problemi

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

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

Per risolvere i problemi relativi alla configurazione, è possibile utilizzare i comandi seguenti.

 show wlan id_wlan: visualizza lo stato delle funzionalità di reindirizzamento Web per una particolare WLAN.Di seguito è riportato un esempio:

• • • •	
WLAN Identifier	1
Profile Name	Admin
Network Name (SSID)	Admin
Web Based Authentication	Disabled
Web-Passthrough	Disabled
Conditional Web Redirect	Disabled
Splash-Page Web Redirect	Enabled

 debug dot1x events enable: abilita il debug dei messaggi pacchetto 802.1x.Di seguito è riportato un esempio:

Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to
 mobile 00:40:96:ac:dd:05 (EAP Id 16)

- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from mobile 00:40:96:ac:dd:05
- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from
 mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43)
- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for mobile 00:40:96:ac:dd:05
- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800

seconds, got from WLAN config.

- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05
 setting dot1x reauth timeout = 1800
- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry
 for station 00:40:96:ac:dd:05 (RSN 2)
- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf
 to PMKID cache for station 00:40:96:ac:dd:05
- Fri Feb 29 10:27:16 2008: New PMKID: (16)
- Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca fb fa 8e 3c
- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK
 lifetime can take care of same.
- Fri Feb 29 10:27:16 2008: Including PMKID in M1 (16)
- Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca fb fa 8e 3c
- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to mobile 00:40:96:ac:dd:05

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while
in Authenticating state for mobile 00:40:96:ac:dd:05
```

 debug aaa events enable: abilita l'output di debug di tutti gli eventi aaa.Di seguito è riportato un esempio:

```
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
    Authentication Packet (id 103) to 10.77.244.196:1812, proxy state
    00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from
   RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
   Authentication Packet (id 104) to 10.77.244.196:1812, proxy state
    00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from
   RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
    'http://10.77.244.196/Admin-login.html' set
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for
    station 00:40:96:ac:dd:05
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station
    00:40:96:ac:dd:05
      source: 4, valid bits: 0x0
      gosLevel: -1, dscp: 0xfffffff, dot1pTaq: 0xffffffff, sessionTimeout: -1
      dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
      vlanIfName: '', aclName: '
```

Informazioni correlate

- Guida alla configurazione di Cisco Wireless LAN Controller, versione 5.0
- <u>Esempio di configurazione dell'autenticazione Web del controller LAN wireless</u>
- Esempio di configurazione dell'autenticazione Web esterna con i controller LAN wireless
- Pagina di supporto wireless
- 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).