# Exemplo de Configuração de Redirecionamento de Página Inicial do Controlador Wireless LAN

# Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Informações de Apoio Instalação de rede Configurar Etapa 1. Configure a WLC para autenticação RADIUS através do servidor Cisco Secure ACS. Etapa 2. Configure as WLANs para o departamento de Administração e Operações. Etapa 3. Configure o Cisco Secure ACS para suportar o recurso de redirecionamento da página inicial. Verificar Troubleshoot Informações Relacionadas

## **Introduction**

Este documento descreve como configurar a característica de redirecionamento da página de abertura nos Controllers de LAN Wireless.

## **Prerequisites**

## **Requirements**

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento das soluções de segurança LWAPP
- Conhecimento de como configurar o Cisco Secure ACS

#### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 4400 Series Wireless LAN Controller (WLC) com firmware versão 5.0
- Ponto de acesso leve (LAP) Cisco 1232 Series

- Adaptador de cliente sem fio Cisco Aironet 802.a/b/g que executa o firmware versão 4.1
- Servidor Cisco Secure ACS que executa a versão 4.1
- Qualquer servidor Web externo de terceiros

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

#### **Conventions**

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.</u>

# Informações de Apoio

O redirecionamento para a Web da Página de Abertura é um recurso introduzido com o Wireless LAN Controller Versão 5.0. Com esse recurso, o usuário é redirecionado para uma página da Web específica após a conclusão da autenticação 802.1x. O redirecionamento ocorre quando o usuário abre um navegador (configurado com uma home page padrão) ou tenta acessar um URL. Depois que o redirecionamento para a página da Web estiver concluído, o usuário terá acesso total à rede.

Você pode especificar a página de redirecionamento no servidor RADIUS (Remote Authentication Dial-In User Service). O servidor RADIUS deve ser configurado para retornar o atributo RADIUS Cisco av-pair url-redirect ao Wireless LAN Controller após a autenticação 802.1x bem-sucedida.

O recurso de redirecionamento da Web da página inicial está disponível apenas para WLANs configuradas para segurança da camada 2 802.1x ou WPA/WPA2.

## Instalação de rede

Neste exemplo, um Cisco 4404 WLC e um Cisco 1232 Series LAP são conectados através de um switch de Camada 2. O servidor Cisco Secure ACS (que atua como um servidor RADIUS externo) também está conectado ao mesmo switch. Todos os dispositivos estão na mesma sub-rede.

O LAP é registrado inicialmente na controladora. Você deve criar duas WLANs: uma para os usuários do **departamento de administração** e outra para os usuários do **departamento de operações**. Ambas as LANs sem fio usam WPA2/AES (EAP-FAST é usado para autenticação). As duas WLANs usam o recurso Splash Page Redirect para redirecionar os usuários para as URLs de Home Page apropriadas (em servidores Web externos).

Este documento utiliza a seguinte configuração de rede:



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

A próxima seção explica como configurar os dispositivos para essa configuração.

# **Configurar**

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Conclua estas etapas para configurar os dispositivos para usar o recurso de redirecionamento de página inicial:

- 1. Configure a WLC para autenticação RADIUS através do servidor Cisco Secure ACS.
- 2. Configure as WLANs para os departamentos de Administração e Operações.
- 3. <u>Configure o Cisco Secure ACS para suportar o recurso de redirecionamento de página</u> <u>inicial.</u>

### Etapa 1. Configure a WLC para autenticação RADIUS através do servidor Cisco

### Secure ACS.

A WLC precisa ser configurada para encaminhar as credenciais do usuário a um servidor RADIUS externo.

Conclua estes passos para configurar o WLC para um servidor RADIUS externo:

- 1. Escolha **Security** e **RADIUS Authentication** na GUI do controlador para exibir a página RADIUS Authentication Servers.
- 2. Clique em New para definir um servidor RADIUS.
- Defina os parâmetros do servidor RADIUS na página Servidores de autenticação RADIUS > Novo.Esses parâmetros incluem:Endereço IP do servidor RADIUSshared secretnúmero da portaStatus do servidor

						Sage Co	nfiguration   Bing   I	Logout   Befresh
cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	RADIUS Authentic	ation Server	s > New				< 8ack	Apply
General	Server Index (Prior	ity) 1	•		_			
Authentication	Server IPAddress	10.2	7.244.196					
TACACS+   LDAP	Shared Secret Form	nat As	:H 💌					
Local Net Users MAC Filtering	Shared Secret	•••	••					
Disabled Clients User Login Policies AP Policies	Confirm Shared Se	cret 🚥	••					
Local EAP	Key Wrap		Designed for F	IPS customers	and requires a ke	y wrap complian	t RADIUS server)	
<ul> <li>Priority Order</li> <li>Access Control Lists</li> </ul>	Port Number	101	2					
Wireless Protection     Policies	Server Status	End	abled 💌					
▶ Web Auth	Support for RFC 35	76 En	abled 💌					
▶ Advanced	Server Timeout	2	seconds					
	Network User	RE	nable					
	Management	R E	nable					
	IPSec		nable					

Este documento usa o servidor ACS com um endereço IP 10.77.244.196.

4. Clique em Apply.

#### Etapa 2. Configure as WLANs para o departamento de Administração e Operações.

Nesta etapa, você configura as duas WLANs (uma para o departamento de administração e outra para o departamento de operações) que os clientes usarão para se conectar à rede sem fio.

O SSID da WLAN para o departamento de administração será *Admin*. O SSID da WLAN para o departamento de operações será Operações.

Use a autenticação EAP-FAST para habilitar a WPA2 como o mecanismo de segurança da Camada 2 nas WLANs e a política da Web - recurso Redirecionamento da Web para Página Inicial como o método de Segurança da Camada 3.

Conclua estes passos para configurar a WLAN e seus parâmetros relacionados:

- 1. Clique em **WLANs** na GUI do controlador para exibir a página WLANs.Esta página lista as WLANs que existem na controladora.
- 2. Clique em New para criar uma nova

WLAN.				_		Save Co	nfiguration Ping	Logout Refresh
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > New						< Back	Apply
* WLANS	Туре	WLAN						
Advanced	Profile Name	Admin						
	WLAN SSID	Admin						

- 3. Insira o nome SSID da WLAN e o nome do perfil na página WLANs > New (WLANs > Novo).
- 4. Clique em Apply.
- 5. Primeiro, vamos criar a WLAN para o departamento de administração.Quando você criar uma nova WLAN, a página WLAN > Edit da nova WLAN será exibida. Nesta página, você pode definir vários parâmetros específicos para esta WLAN. Isso inclui políticas gerais, políticas de segurança, políticas de QOS e parâmetros avançados.
- 6. Em General Policies (Regras gerais), marque a caixa de seleção Status para habilitar a



- 7. Clique na guia **Security** e, em seguida, clique na guia **Layer 2**.
- 8. Escolha WPA+WPA2 na lista suspensa Layer 2 Security. Esta etapa habilita a autenticação

WPA para a WLAN.

9. Em WPA+WPA2 Parameters, marque as caixas de seleção WPA2 Policy e AES

Encryption.				
	MONITOR WILANS CONTROLLER WIRELESS SECURITY MANAG		upper about the second	Logout Hefre
CISCO	MONITOR MUNICIPAL MARKETER MARKETERS SECORTI MEMORY	ЗЕМЕНТ СОММИНОЗ	nege	
WLANS	WLANs > Edit		< Back	Apply
VLANS	General Security Qus Auvanceu			
Advanced	Layer 2 Layer 3 ARR Servers			
	Layer 2 Security WPA+WPA2			
	MAC Filtering			
	WPA+WPAZ Parameters			
	WPA2 Policy 🗹			
	WPA2 Encryption RAES TKIP			
	Auth Key Mgmt 802.1X			

- 10. Escolha **802.1x** na lista suspensa Auth Key Mgmt. Esta opção habilita a WPA2 com autenticação 802.1x/EAP e criptografia AES para a WLAN.
- 11. Clique na guia Layer 3 Security.
- 12. Marque a caixa **Web Policy** e clique no botão de opção **Splash Page Web Redirect**.Essa opção ativa o recurso de redirecionamento da Web para a página inicial.

		Save Configuration   Ping	Logout   <u>R</u> efre
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT	COMMANDS HELP	_
WLANS WLANS WLANS Advanced	General       Security       QoS       Advanced         Layer 2       Layer 3       AAA Servers         Layer 3       Security       None         Image: Web Policy 4       Image: Authentication         Image: Passthrough       Image: Conditional Web Redirect         Image: Splash Page Web Redirect       Preauthentication         ACL       None	< Back	Apply

- 13. Clique na guia Servidores AAA.
- 14. Em Authentication Servers (Servidores de autenticação), escolha o endereço IP do servidor apropriado na lista suspensa Server

abab	Sage Configuration   Ping   Logo	ut i <u>B</u> el
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANs	WLANs > Edit A	pply
* WLANS	General Security QoS Advanced	
WLANs	Layer 2 Layer 3 AAA Servers	
Advanced	-	
	Select AAA servers below to override use of default servers on this WLAN	
	Radius Servers LDAP Servers	
	Authentication Servers Accounting Servers Server 1 None	
	Enabled Server 2 None	
	Server 1P:10.77.244.196, Port:1812 None  Server 3 None	
	2 None ·	
	Server None  None  None	
	Local EAP Authentication	
	Local EAP Authentication Enabled	
	Authentication priority order for	1
	web-auth user	
	٠	

Neste exemplo, 10.77.244.196 é usado como o servidor RADIUS.

- 15. Clique em Apply.
- Repita as etapas 2 a 15 para criar a WLAN para o departamento de operações. A página WLANs lista as duas WLANs que você criou

chou.									
							Sa <u>v</u> e C	onfiguration Ping	Logout Refresh
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нецр	
WLANs	WLANs								New
WLANS	Profile Na	me	Ту	pe WL	AN SSID		Admin Status	Security Policies	
Advanced	Admin		WL	AN Adr	nin		Enabled	[WPA2][Auth(802.)	LX)], Splash-Page
	Operations		WL	AN Ope	trations		Enabled	[WPA2][Auth(802.)	LX)], Splash-Pagr

Observe que as políticas de segurança incluem o redirecionamento da página inicial.

# Etapa 3. Configure o Cisco Secure ACS para suportar o recurso de redirecionamento da página inicial.

A próxima etapa é configurar o servidor RADIUS para esse recurso. O servidor RADIUS precisa executar a autenticação EAP-FAST para validar as credenciais do cliente e, após a autenticação bem-sucedida, redirecionar o usuário para a URL (no servidor Web externo) especificada no atributo RADIUS *url-redirect* Cisco av-pair.

#### Configurar o Cisco Secure ACS para autenticação EAP-FAST

**Observação:** este documento pressupõe que o Wireless LAN Controller foi adicionado ao Cisco Secure ACS como um cliente AAA.

Conclua estas etapas para configurar a autenticação EAP-FAST no servidor RADIUS:

1. Clique em **System Configuration** na GUI do servidor RADIUS e escolha **Global Authentication Setup** na página System

CiscoSecure ACS - Microsoft Internet Explorer	
Ele Edit Yew Favorites Iools Help	Links <sup>39</sup> Close
Agdress 1 http://127.0.0.1:1065/	- 🔁 😡
Address http://127.0.0.1:1005/	Service Central     Service Central     Service Central     Service Central     Control     Contro     Control     Contro     Control     Control
Poster Validation Network Access Poster Reports and Activity Online Decomentation	Saretice Ceadral Salect to open the page from which you can stop or restart Cisco Secure ACS services. (Brick to Top) Logging Salect to configure various Cisco Secure ACS reports and customize the type of information that is logged. (Brick to Top) Date Format Ceatrol Salect to configure the date format, either month/day/year or day/month/year, for CSV files and Service Logs and in the GUI. (Brick to Top)

 Na página de configuração Autenticação global, clique em Configuração EAP-FAST para ir para a página de configurações EAP-FAST.

- Lating of the	.0.0.1:1065/	• 🔂 👳
en Sverens dada.	System Configuration	Σ
liter 1	EAP Configuration	P Help
Steep Broop Setup Shared Profile Components Network Configuration System Configuration Interface Configuration Administration	PEAP         Allow EAP-MSCHAPv2         Allow EAP-GTC         Allow Posture Validation         Allow EAP-TLS         Select one or more of the following options:         E Certificate SAN comparison         E Certificate CN comparison         E Certificate Binary comparison	Use this page to specify settings for various authentication protocols. • EAP Configuration • PSAP • EAP FASIS • E
Control External User Databases Posture Validation Network Access Profiles Reports and	EAP-TLS session timeout (minutes): 120 Cisco client initial message: PEAP session timeout (minutes): 120 Enable Fast Reconnect:	EAP Configuration EAP is a flexible request-response protocol for arbitrary authentic ation information (RFC 2284), EAP is layered on top of another protocol such as UOP, 002.1x or RADDUS and supports multiple "authentication" types. [back to Top] PEAP
ine omentation	EAP-FAST EAP-FAST Configuration	PEAP is the outer layer protocol for the secure tunnel
	EAP-TLS III Allow EAP-TLS Select one or more of the following options:	authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.  Allow EAP-MSCHAPv2 — Use to anable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS-

 Na página Configurações de EAP-FAST, marque a caixa de seleção Permitir EAP-FAST para habilitar o EAP-FAST no servidor RADIUS.

CiscoSecure ACS - N	Scrosoft Internet Explorer	<u>= 10   ×</u>
Ele Edt Yew Fg	vonkes Iools Help	Links 🍄 🤷
Address http://127./	0.0.1:1065/	💌 🛃 60
Cisco Storens	System Configuration	
Uger Setup Uger Setup Daved Profile Composents Network Configuration Con	EAP-FAST Configuration  EAP-FAST Settings  EAP-FAST  Active master key TTL  Active master key TTL  Retired master key TTL  Tunnel PAC TTL  Client initial message:  Authority ID Info:  Allow anonymous in-band PAC provisioning  Allow authenticated in-band PAC provisioning  Allow authenticated in-band PAC provisioning  Require client certificate for provisioning  Allow Machine Authentication  Machine PAC TTL  Weeks	<ul> <li>Help</li> <li>EAP-FAST Configuration Page</li> <li>Use this page to configure EAP-FAST authentication settings.</li> <li>CAP-FAST Settings</li> <li>Client initial measures</li> <li>Authority ID Jafe</li> <li>Authority ID Jafe</li> <li>Allers assigness in Sand PAC provisioning</li> <li>Allers machine systematication</li> <li>Allers tatalons session thread</li> <li>CAP-TAST Sectings</li> <li>Allers EAP-FAST - To enable EAP-FAST authentication, select this check base.</li> <li>Active Haster Key TR - Enter a value for the amount of time that a master key is used to generate new Portected Access Credentials (PACe), when the the termine of the port of the fact of the set of</li></ul>
Online Documentation	Allow Stateless session resume Authorization PAC TTL 1 hours Allowed inner methods REAP-GTC REAP-MSCHAPV2 EAP-TLS Submit Submit + Restart Cancel	<ul> <li>Under the lowe (TTL) defined have the Master Key is generated.</li> <li>Retered master key TIL -Enter a value for the amount of time that PACs generated using a retired master key is capability for EAD-FAST authentication. When an end-user client gains network access using a PAC based on a retired master key. ACS sends a new PAC to the end-user client.</li> <li>Tennel PAC TIL - Enter a value for the amount of time that a PAC is used on a retired master key. ACS sends a new PAC to the end-user client.</li> <li>Tennel PAC TIL - Enter a value for the amount of time that a PAC is used baffore it explores and must be repliced. If the master key used to generate the Tunnel PAC expired, automatic, if the master key used to generate the Tunnel PAC expired, automatic, or amound provisioning must be used to provide the end-user client with a new PAC.</li> </ul>
		internet
🌯 Start 🔂 🍎	CiscoSecure ACS - Mic	👮 7:58 PM

- 4. Configure os valores TTL (Time-to-Live) da chave mestra ativa/desativada conforme desejado ou defina-a com o valor padrão conforme mostrado neste exemplo.O campo Authority ID Info (Informações de ID da autoridade) representa a identidade textual desse servidor ACS, que um usuário final pode usar para determinar em qual servidor ACS será autenticado. O preenchimento deste campo é obrigatório.O campo Mensagem de exibição inicial do cliente especifica uma mensagem a ser enviada aos usuários que se autenticam em um cliente EAP-FAST. O comprimento máximo é de 40 caracteres. Um usuário verá a mensagem inicial apenas se o cliente do usuário final suportar a exibição.
- 5. Se desejar que o ACS execute o fornecimento de PAC anônimo dentro da banda, marque a caixa de seleção **Permitir fornecimento de PAC anônimo dentro da banda**.
- 6. A opção Allowed inner methods determina quais métodos EAP internos podem ser executados dentro do túnel EAP-FAST TLS. Para provisionamento anônimo em banda, você deve habilitar EAP-GTC e EAP-MS-CHAP para compatibilidade com versões anteriores. Se você selecionar Permitir fornecimento de PAC anônimo em banda, deverá selecionar EAP-MS-CHAP (fase zero) e EAP-GTC (fase dois).
- Clique em Submit. Observação: para obter informações detalhadas e exemplos sobre como configurar o EAP FAST com o provisionamento PAC In-band anônimo e o provisionamento In-band autenticado, consulte <u>Autenticação EAP-FAST com controladores LAN sem fio e</u> <u>Exemplo de Configuração de Servidor RADIUS Externo</u>.

#### Configure o banco de dados do Usuário e defina o atributo url-redirect RADIUS

Este exemplo configura o nome de usuário e a senha do cliente sem fio como User1 e User1, respectivamente.

Conclua estas etapas para criar um banco de dados de usuário:

- 1. Na GUI do ACS na barra de navegação, selecione User Setup.
- 2. Crie um novo usuário sem fio e clique em Add/Edit para ir para a página Edit deste

#### usuário.

Cinco Syntems	User Setup	Ð
Annual User Setup      User Group Group DaredProffe Configuration      Configuration       Config	Select User: User1 Find Add/Edit List users beginning with letter/number: ABSELSES PSESTING DIR 2 45 5 2 8 2 List all users Remove Dynamic Users Back to help	<ul> <li>Help</li> <li>Store Safer, and External Over Databases</li> <li>Finding a Sociality User in the ACS Internal Database.</li> <li>Adding a User Is the ACS Internal Outsbase.</li> <li>Unting Usersames in the ACS Internal Outsbase.</li> <li>Unting Usersames in the ACS Internal Outsbase.</li> <li>User Safer a Usersame in the ACS Internal Outsbase.</li> <li>Refere ACS can authenticate users in the ACS Internal Outsbase.</li> <li>Before ACS can authenticate users with an external user database.</li> <li>You must have the database. User Safer and External User Database.</li> <li>You must have the database users in the ACS Internal Outsbase.</li> <li>You must have the database users in the auternal user database.</li> <li>You must have the database users in the external user database.</li> <li>You must have the database users in the External User Databases.</li> <li>You must have the database users in the External User Databases.</li> <li>You must have the database users in the External User Databases.</li> <li>You must have the database users of authentication, your taken server must be running and properly configured.</li> <li>You must have configuration overrides Group Setup configuration.</li> <li>Make User Setup configuration overrides Group Setup configuration.</li> <li>Make user fatting configuration overrides Group Setup configuration is external user database interest in the ACS internal database for users database interest in the ACS internal database for users database interest in the ACS internal database.</li> <li>User Setup Setup Setup Setup in the Configuration, and accounting properties.</li> <li>Make User Setup Setup Inter You configuration, and accounting properties.</li> <li>Make User Setup Setup Setup is configured to a setup setup in the auternal user database. User Setup Setup</li></ul>

3. Na página User Setup Edit, configure Real Name e Description, bem como as configurações de Password, conforme mostrado neste exemplo.Este documento usa o banco de dados interno do ACS para autenticação de senha.

Edit Yow Fa	vorites Iools Help	Links
Etp://127.	0.0.1:1065/	
to Systems	User Setup	
K. AN	Edit	Help
Uzer Setup Group	User: User1 (New User)	Account Disabled     Orieliting a Upersone
Dared Profile Components	Account Disabled	Computer which the user is assigned     Computer which the user is assigned
Network Configuration	Supplementary User Info	Clent IP: Address Assignment     Advanced Settings
System Configuration	Real Name Description	Destructs Access Residictions     Han Section     Under Operation     Access Disable
Administration		Overslandsble ALLs     Advanced JACAGS - Sattings     TACAGS - Cashle Control
External User Databases	User Setup	IACACS - Enable Parament     IACACS - Outbound Parament     IACACS - Shell Command Authorization
Posture Validation	Password Authentication: ACS Internal Database	Command Anthonization for Network Device Nanagement Audications     IACACS - Unknown Services     ISTE RADIUS Attributes
lebrork Access voliles	CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)	RADIUS Yeadar Specific Atteleates
Activity Online	Password .	Account Disabled Status
Jocumentation	Password (CHUD 045-CHUD (4D4D)	Select the Account Disabled check box to disable this account; clear the check box to enable the account.
	Decement	Back to Trail
	Confirm	Deleting a Username The Delete button appears only when you are editing an existing user
	Submit Cancel	account, not when you are adding a new user account. To delete the current user account from the database, click <b>Delete</b> . When asked to confirm your action, click <b>OK</b> .

- 4. Role a página para baixo para modificar os atributos RADIUS.
- 5. Marque a caixa de seleção [009\001] cisco-av-pair.
- 6. Insira este Cisco av-pair na caixa de edição [009\001] cisco-av-pair para especificar a URL para a qual o usuário é redirecionado:url-redirect=http://10.77.244.196/Admin-Login.html

Cisco Systems	User Setup	[
	(useu iur benuPass anu benuAutri cirents such as routers)	- Help
User Setup	Password	Account Disabled
Group Setup	Password	Deleting a Uvername     Supplementary User Info
SharedProfile Components	Cisco Airespace RADIUS Attributes	Cassword Authentication     Group to which the user is assigned     Callback     Callback
Network Configuration	[14179'005] Aire-Interface-Name	Clean IP Address Assignment     Advanced Settings
System Configuration		Construction Access Access for the Opens     Construction of the Opense     Construction of the Opense     Construction of the Opense
Configuration		Account Disable     Dormloadakin ACLs
Administration Centrel	Cisco IOS/PIX 6.x RADIUS Attributes	Advanced TACACS+ Settings     TACACS+ Enable Control     TACACS+ Enable Control     TACACS+ Enable Control
Databases	₩ [009\001] cisco-av-pair	TACACS - Outbound Passwerd     TACACS - Shell Command Authorization
Posture Validation	ur1- redirect=http://10.77.244.196/	Examinant Authorization for Network Device Hanagement Applications     TACACS-Unknown Service     XNN PROVE AUTOMATIC
Network Access Profiles	Admin-login.html	BADEUS Vendor-Seccific Attributes
Reports and Activity	×	
and 1 Online		Account Disabled Status
Documentation		Select the Account Disabled check box to disable this account; clear the check box to enable the account.
	P Back to Help	(Back to Tou)
		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

Esta é a página inicial dos usuários do departamento Admin.

- 7. Clique em Submit.
- 8. Repita este procedimento para adicionar User2 (usuário do departamento de operações).
- Repita as etapas de 1 a 6 para adicionar mais usuários do departamento Admin e do departamento Operações ao banco de dados. Observação: os atributos RADIUS podem ser configurados no nível do usuário ou do grupo no Cisco Secure ACS.

# **Verificar**

Para verificar a configuração, associe um cliente WLAN do departamento de Administração e do departamento de Operações às WLANs apropriadas.

Quando um usuário do departamento Admin se conecta ao Wireless LAN Admin, o usuário é solicitado a fornecer as credenciais 802.1x (credenciais EAP-FAST no nosso caso). Quando o usuário fornecer as credenciais, a WLC as passará para o servidor Cisco Secure ACS. O servidor Cisco Secure ACS valida as credenciais do usuário em relação ao banco de dados e, após uma autenticação bem-sucedida, retorna o atributo url-redirect para o Wireless LAN Controller. A autenticação está concluída neste estágio.

🛜 Cisco Aironet Desktop Utility	y - Current Profile: Admin	2 🔀					
Action Options Help							
Current Status Profile Management	Diagnostics						
Profile Name:	Admin						
Línk 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 o usuário abre um navegador da Web, ele é redirecionado para a URL da página inicial do departamento de administração. (Essa URL é retornada à WLC através do atributo cisco-avpair). Após o redirecionamento, o usuário tem acesso total à rede. Aqui estão as capturas de tela:



As mesmas sequências de eventos ocorrem quando um usuário do departamento de operações se conecta às operações da WLAN.

🖻 Cisco Aironet	Desktop Utility	y - Current Profi	le: Operations	? 🗙
<u>Action Options H</u> e	lp			
Current Status Pro	ofile Management	Diagnostics		
CISCO SYSTEMS				
ահուսին	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	



## **Troubleshoot**

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Você pode usar os comandos a seguir para solucionar problemas de configuração.

 show wlan wlan\_id — Exibe o status dos recursos de redirecionamento da Web para uma WLAN específica.Aqui está um exemplo:

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

 debug dot1x events enable — Habilita a depuração de mensagens de pacote 802.1x.Aqui está um exemplo:

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 — Ativa a saída de depuração de todos os eventos aaa.Aqui está
um exemplo:
```

```
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: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
       dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
       vlanIfName: '', aclName: '
```

## Informações Relacionadas

- Guia de configuração de Cisco Wireless LAN Controller, versão 5.0
- Exemplo de configuração de autenticação da Web para o controlador da LAN sem fio
- Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers
- Página de Suporte Wireless
- Suporte Técnico e Documentação Cisco Systems

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.