Ejemplo de Configuración de Wireless LAN Controller Splash Page Redirect

Contenido

Introducción **Prerequisites** Requirements Componentes Utilizados **Convenciones Antecedentes** Configuración de la red Configurar Paso 1. Configure el WLC para la autenticación RADIUS a través del servidor ACS seguro de Cisco. Paso 2. Configure las WLAN para el departamento de administración y operaciones. Paso 3. Configure Cisco Secure ACS para que admita la función de redirección de páginas de bienvenida. Verificación Troubleshoot Información Relacionada

Introducción

Este documento describe cómo configurar la función de redireccionamiento de la página de presentación en los Controladores de LAN Inalámbricos.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de las soluciones de seguridad LWAPP
- Conocimiento de cómo configurar Cisco Secure ACS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador de LAN inalámbrica (WLC) de Cisco serie 4400 que ejecuta la versión 5.0 del firmware
- Punto de acceso ligero (LAP) Cisco serie 1232
- Cisco Aironet 802.a/b/g Wireless Client Adapter que ejecuta la versión 4.1 del firmware
- Servidor Cisco Secure ACS que ejecuta la versión 4.1
- Cualquier servidor web externo de terceros

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte <u>Convenciones de Consejos TécnicosCisco para obtener más información sobre las</u> <u>convenciones del documento.</u>

Antecedentes

La redirección web de la página de bienvenida es una función introducida con Wireless LAN Controller versión 5.0. Con esta función, el usuario es redirigido a una página web determinada después de que se haya completado la autenticación 802.1x. La redirección se produce cuando el usuario abre un navegador (configurado con una página de inicio predeterminada) o intenta acceder a una URL. Una vez completada la redirección a la página web, el usuario tiene acceso completo a la red.

Puede especificar la página de redirección en el servidor del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS). El servidor RADIUS debe configurarse para devolver el atributo RADIUS de redirección URL de par AV de Cisco al controlador de LAN inalámbrica tras una autenticación 802.1x correcta.

La función de redireccionamiento web de la página de bienvenida solo está disponible para las WLAN configuradas para la seguridad 802.1x o WPA/WPA2 de capa 2.

Configuración de la red

En este ejemplo, un Cisco 4404 WLC y un Cisco 1232 Series LAP se conectan a través de un switch de capa 2. El servidor Cisco Secure ACS (que actúa como servidor RADIUS externo) también está conectado al mismo switch. Todos los dispositivos están en la misma subred.

El LAP se registra inicialmente en el controlador. Debe crear dos WLAN: una para los usuarios del **Departamento de Administración** y otra para los usuarios del **Departamento de Operaciones**. Ambas redes LAN inalámbricas utilizan WPA2/ AES (EAP-FAST se utiliza para la autenticación). Ambas WLAN utilizan la función Splash Page Redirect para redirigir a los usuarios a las URL de la página de inicio adecuada (en servidores web externos).

En este documento, se utiliza esta configuración de red:



Cisco Secure ACS server

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

En la siguiente sección se explica cómo configurar los dispositivos para esta configuración.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

<u>Nota:</u> Utilice la herramienta <u>Command Lookup</u> (sólo para clientes <u>registrados</u>) para obtener más información sobre los comandos utilizados en esta sección.

Complete estos pasos para configurar los dispositivos para utilizar la función de redirección de página de bienvenida:

- 1. Configure el WLC para la autenticación RADIUS a través del servidor ACS seguro de Cisco.
- 2. Configure las WLAN para los departamentos de administración y operaciones.
- 3. <u>Configure Cisco Secure ACS para que admita la función de redirección de páginas de bienvenida.</u>

Paso 1. Configure el WLC para la autenticación RADIUS a través del servidor ACS

seguro de Cisco.

El WLC necesita ser configurado para reenviar las credenciales del usuario a un servidor RADIUS externo.

Complete estos pasos para configurar el WLC para un servidor RADIUS externo:

- 1. Elija **Security** y **RADIUS Authentication** de la GUI del controlador para mostrar la página RADIUS Authentication Servers.
- 2. Haga clic en Nuevo para definir un servidor RADIUS.
- Defina los parámetros del servidor RADIUS en la página RADIUS Authentication Servers > New .Estos parámetros incluyen:Dirección IP de servidor RADIUSsecreto compartidonúmero de puertoEstado del servidor.

servidor		
		Sage Configuration Eing Logout Befresh
CISCO	MONITOR WLANS CONTRO	OLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Authentication S	ervers > New <back apply<="" td=""></back>
General	Server Index (Priority)	1
RADIUS 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	Dest Number	1412
▶ Access Control Lists	Port Number	1012
Wireless Protection Policies	Server Status	Enabled ×
▶ Web Auth	Support for RFC 3576	Enabled 💌
Advanced	Server Timeout	2 seconds
	Network User	🗷 Enable
	Management	Enable
	IPSec	Enable

Este documento utiliza el servidor ACS con una dirección IP de 10.77.244.196.

4. Haga clic en Apply (Aplicar).

Paso 2. Configure las WLAN para el departamento de administración y operaciones.

En este paso, configure las dos WLAN (una para el departamento de administración y otra para el departamento de operaciones) que los clientes utilizarán para conectarse a la red inalámbrica.

El SSID de WLAN para el departamento de administración será *Admin*. El SSID de WLAN para el departamento de operaciones será Operations (Operaciones).

Utilice la autenticación EAP-FAST para habilitar WPA2 como el mecanismo de seguridad de la capa 2 en ambas WLAN y la función de política web - Splash Page Web Redirect como el método

de seguridad de la capa 3.

Complete estos pasos para configurar la WLAN y sus parámetros relacionados:

- 1. Haga clic en **WLANs** de la GUI del controlador para mostrar la página WLANs.Esta página enumera las WLANs que existen en el controlador.
- 2. Haga clic en **Nuevo** para crear un nuevo

WLAN.						Save Co	ofiguration 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						

- Introduzca el nombre SSID de WLAN y el nombre de perfil en la página WLAN > New (WLAN > Nuevo).
- 4. Haga clic en Apply (Aplicar).
- 5. En primer lugar, crearemos la WLAN para el departamento de administración.Una vez creada una nueva WLAN, aparece la página WLAN > Edit (WLAN > Editar) para la nueva WLAN. En esta página, puede definir varios parámetros específicos para esta WLAN. Esto incluye políticas generales, políticas de seguridad, políticas de QOS y parámetros avanzados.
- 6. En Políticas generales, marque la casilla de verificación **Status** para habilitar la WLAN.

cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	Saya C COMMANDS	onfiguration Ei HELP	ng Logout <u>R</u> efr
WLANS WLANS WLANS Advanced	WLANS > General Profile f Type SSID Status Security Radio P Interfac Broaded	Edit Secur Name y Policies olicy ce est SSID	ity QoS Admin WLAN Admin I Enable Splash- (Modificati All admin I Enable	Advanced ed Page-Web-R ons done unde	edirect[WPA2 r security tab	2][Auth(802.1X) will appear after a] pplying the chan	ges.)	Apply

- 7. Haga clic en la pestaña Seguridad y, a continuación, haga clic en la pestaña Capa 2.
- 8. Elija **WPA+WPA2** en la lista desplegable Layer 2 Security.Este paso activa la autenticación WPA para la WLAN.
- 9. En Parámetros WPA+WPA2, active las casillas de verificación **Política WPA2** y **Cifrado AES**.

ahaha				_			Saye Co	sofiguration Ping	Logout Befre
CISCO	MONITOR	<u>W</u> LANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нецр	_
WLANS WLANS WLANS Advanced	WLANS > General Layer 2 Layer WPA+W WPA WPA2 WPA2 Auth	Edit Securit 2 Layer 2 Security PA2 Paramo Policy 2 Policy 2 Encryption Key Mgmt	y QoS 3 AAA Se WPA+WPA2 MAC Filtering eters Ø Ø 02.1	Advanced revers				< Back	Apply

- 10. Elija **802.1x** en la lista desplegable Auth Key Mgmt. Esta opción habilita WPA2 con autenticación 802.1x/EAP y cifrado AES para la WLAN.
- 11. Haga clic en la pestaña Layer 3 Security.
- Active la casilla Web Policy y, a continuación, haga clic en el botón de opción Splash Page Web Redirect. Esta opción activa la función de redireccionamiento web de la página de bienvenida.

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

- 13. Haga clic en la pestaña AAA Servers.
- 14. En Servidores de autenticación, elija la dirección IP del servidor correspondiente en la lista desplegable Servidor

cisco	Saye Configuration Bing Monitor Wlans Controller Wireless Security Management Commands Help	Logout <u>R</u> efi
WLANS WLANS WLANS Advanced	WLANs > Edit < Back	Apply

En este ejemplo, 10.77.244.196 se utiliza como servidor RADIUS.

- 15. Haga clic en Apply (Aplicar).
- 16. Repita los pasos del 2 al 15 para crear la WLAN para el departamento de operaciones.La página WLANs (WLANs) muestra las dos WLANs que ha creado.

				Sa <u>v</u> e C	onfiguration Ping Logout Befresh
CISCO	MONITOR WLANS CONTROL	LER WIRELE	SS SECURITY MANAGE	EMENT COMMANDS	HELD
WLANs	WLANs				New
WLANS	Profile Name	Туре	WLAN SSID	Admin Status	Security Policies
Advanced	Admin	WLAN	Admin	Enabled	[WPA2][Auth(802.1X)], Splash-Page
	Operations	WLAN	Operations	Enabled	[WPA2][Auth(802.1X)], Splash-Page

Observe que las políticas de seguridad incluyen la redirección de la página de bienvenida.

Paso 3. Configure Cisco Secure ACS para que admita la función de redirección de páginas de bienvenida.

El siguiente paso es configurar el servidor RADIUS para esta función. El servidor RADIUS necesita realizar una autenticación EAP-FAST para validar las credenciales del cliente y, tras una autenticación exitosa, redirigir al usuario a la URL (en el servidor web externo) especificada en el atributo RADIUS *url-redirect* de par AV de Cisco.

Configuración de Cisco Secure ACS para la autenticación EAP-FAST

Nota: Este documento asume que el controlador de LAN inalámbrica se agrega a Cisco Secure ACS como cliente AAA.

Complete estos pasos para configurar la autenticación EAP-FAST en el servidor RADIUS:

1. Haga clic en **Configuración del Sistema** de la GUI del servidor RADIUS y luego elija **Configuración de Autenticación Global** en la página Configuración del Sistema.

CiscoSecure ACS - Microsoft Internet Explorer	X
Elle Edit Yew Favorites Iools Help	Links ** Close
Address 👩 http://127.0.0.1:1065/	• 🔁 •
System Configuration	×
Select	Help
Image: Service Control Image: Service Control <t< th=""><th> Service Central Leastna Cash Fernant Central Leastna Cash Fernant Central Add Statement Managements Add Statement Add Statement</th></t<>	 Service Central Leastna Cash Fernant Central Leastna Cash Fernant Central Add Statement Managements Add Statement Add Statement
	(Back to Teo)
a)	internet
🎗 Start 🔯 🈹 🕴 CiscoSecure ACS - Mic	😏 7:57 PM

 Desde la página de configuración de Autenticación Global, haga clic en Configuración EAP-FAST para ir a la página de configuración de EAP-FAST.

- Lating of the	.0.0.1:1065/	• 🔂 👳
eo Systems dudu	System Configuration	Σ
liner 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-

 Desde la página EAP-FAST Settings, marque la casilla de verificación Allow EAP-FAST para habilitar EAP-FAST en el 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 Composents Setup Network Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Config	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	 Help EAP-FAST Configuration Page Use this page to configure EAP-FAST authentication settings. CAP-FAST Settings Client initial measures Authority ID Jafe Authority ID Jafe Allers assigness in Sand PAC provisioning Allers machine systematication Allers tatafasts session thread CAP-TAST Sectings Allers EAP-FAST Settings Allers EAP-FAST To enable EAP-FAST authentication, select this check base. Active Master Key TR – Enter a value for the amount of time that a master key is used to generate new Pertected Access Credentials (PACe), bithes the the term of the set CTP bit date date and Pertected Access Credentials (PACe).
Online Documentation	Allow Stateless session resume Authorization PAC TTL 1 hours Allowed inner methods REAP-GTC REAP-MSCHAPV2 EAP-TLS Submit Submit + Restart Cancel	 Under the lowe (TTL) defined have the Master Key is generated. 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. 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. 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.
		internet
🌯 Start 🔂 🍎	CiscoSecure ACS - Mic	👮 7:58 PM

- 4. Configure los valores TTL (Time-to-Live) de clave maestra activa/retirada como desee o establézcalos en el valor predeterminado, como se muestra en este ejemplo.El campo Información de ID de autoridad representa la identidad textual de este servidor ACS, que un usuario final puede utilizar para determinar con qué servidor ACS se autenticará. Rellenar este campo es obligatorio.El campo Mensaje de visualización inicial del cliente especifica un mensaje que se enviará a los usuarios que se autentiquen con un cliente EAP-FAST. La longitud máxima es de 40 caracteres. Un usuario sólo verá el mensaje inicial si el cliente de usuario final admite la visualización.
- 5. Si desea que ACS realice el aprovisionamiento de PAC en banda anónimo, marque la casilla de verificación **Permitir el aprovisionamiento de PAC en banda anónimo**.
- 6. La opción Allowed inner methods determina qué métodos EAP internos pueden ejecutarse dentro del túnel EAP-FAST TLS. Para el aprovisionamiento en banda anónimo, debe habilitar EAP-GTC y EAP-MS-CHAP para la compatibilidad con versiones anteriores. Si selecciona Permitir el aprovisionamiento de PAC en banda anónimo, debe seleccionar EAP-MS-CHAP (fase cero) y EAP-GTC (fase dos).
- 7. Haga clic en Submit (Enviar).Nota: Para obtener información detallada y ejemplos sobre cómo configurar EAP-FAST con aprovisionamiento de PAC en banda anónimo y aprovisionamiento en banda autenticado, consulte <u>Ejemplo de Configuración de EAP-FAST</u> <u>con Controladores LAN Inalámbricos y Servidor RADIUS Externo</u>.

Configure la base de datos User y defina el atributo url-redirect RADIUS

Este ejemplo configura el nombre de usuario y la contraseña del cliente inalámbrico como Usuario1 y Usuario1, respectivamente.

Complete estos pasos para crear una base de datos de usuarios:

- 1. En la GUI de ACS en la barra de navegación, elija User Setup.
- 2. Cree un nuevo usuario inalámbrico, y luego haga clic en Add/Edit para ir a la página Edit de este

 (b) Constructions of the product of the pro	usuario.		
We way way and a group way and	Fig. Edt. Vew Fa	encroscot ancernet explorer	-101 A
 	Address Al John 19	0.0.1-10%	• 6 •
Cites Striker User Setup Solar Main Solar Solar	advant hall white a		
State Hep Image: State Hep Image: State Image: State Hep Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State Image: State	Cinco Systems	User Setup	×
 	db. db.	Select	Help
🥶 Internet	Viser Setop SharedFooffe Composeds Configuration Configuration	User: User1 Find Add/Edit List users beginning with letter/number: ABSERTSVVVVV QARSSE Ust all users Remove Dynamic Users	<list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item>
	2		🔮 Internet

3. En la página User Setup Edit (Edición de la configuración de usuario), configure Real Name (Nombre real) y Description (Descripción), así como los parámetros Password (Contraseña), como se muestra en este ejemplo.Este documento utiliza la base de datos interna de ACS para la autenticación de contraseña.

http://127	.0.0.1:1065/	X
o Storeus	User Setup	
walled.	Edit	Help
Jeer Jeerp Iroup Jerop hared/Profile composed composed interface configuration interface configuration demonstration demonstration configuration Configuration Configuration	User: User1 (New User) Account Disabled Supplementary User Info Real Name Description User Setup Password Authentication:	Account Disabled Ordeting, a Username Supplementary, Disc July Passmed Anthentication Camp, to mitch the user is assigned Caliback Clent UP, Advers Assignment Advanced Sattless Nutwork Access Restrictions Main_Seation Oration Main_Seation Main_Seation Main_Seation Main_Seation Market Access Restrictions Main_Seation Main_Seation Main_Seation Main_Seation Main_Seation Maches_Seation Maches_Seation
etwork Access rofiles teperts and activity Inline Jocumentation	ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP)	TETE RADIUS Attributes RADIUS Yeader Sectific Attributes Account Disabled States Select the Account Disabled check box to disable this account clear the check box to enable the account. (Back to Tra)
	Password Confirm Password Submit Cancel	Beleting a Username 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 current user account from the database, click Delete. When asked to

- 4. Desplácese hacia abajo en la página para modificar los atributos RADIUS.
- 5. Marque la casilla de verificación [009\001] cisco-av-pair.
- 6. Ingrese estos pares AV de Cisco en el cuadro de edición [009\001] cisco-av-pair para especificar la URL a la que se redirige al usuario:url-redirect=http://10.77.244.196/Admin-Login.html

Cisco Systems	User Setup	[
	(useu iur benueass anu benueurn cirents such as routers)	- Help
User Setup	Password •••••	Account Disabled
Group Setup	Password	Osleting a Username Supalementary User Infe
Shared Profile Components	Cisco Airespace RADIUS Attributes	Passward Authentication Group to relich the user is assigned Callback
Network Configuration	[141794005] Aire-Interface-Name	Clent IP. Address Assignment Advanced Settinge
System Configuration		Cettymen Access res for the term Man Sensions Usage Owntas
Configuration		Account Disable Describe adable ACLs
Administration Centrel	Cisco IOS/PIX 6.x RADIUS Attributes 🙎	Advanced TACAS+ Settings TACAS+ Enable Central TACAS+ Enable Sensered
Databases	🕅 [009\001] cisco-av-pair	TACACS - Outbrand Password TACACS - Shell Command Authorization
Validation	ur1- redirect=http://10.77.244.196/	Command Authorization for Network Device Management Applications TACS Unknown Services TETE ROUTS Attracted
Network Access Profiles	Admin-login.html	RADIUS Vender-Szecific Attributes
Reports and Activity	<u>×</u>	
min Online		Account Disabled Status
Documentation		Select the Account Disabled check box to disable this account clear the check box to enable the account.
	💡 Back to Help	[Bask 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

Esta es la página de inicio de los usuarios del departamento de administración.

- 7. Haga clic en Submit (Enviar).
- 8. Repita este procedimiento para agregar el usuario 2 (usuario del departamento de operaciones).
- 9. Repita los pasos del 1 al 6 para agregar más usuarios del departamento de administración y del departamento de operaciones a la base de datos. **Nota:** Los atributos RADIUS se pueden configurar en el nivel de usuario o de grupo en Cisco Secure ACS.

Verificación

Para verificar la configuración, asocie un cliente WLAN del departamento de administración y del departamento de operaciones a sus WLAN apropiadas.

Cuando un usuario del departamento de administración se conecta con el administrador de LAN inalámbrica, se le solicitan credenciales 802.1x (credenciales EAP-FAST en nuestro caso). Una vez que el usuario proporciona las credenciales, el WLC pasa esas credenciales al servidor ACS seguro de Cisco. El servidor Cisco Secure ACS valida las credenciales del usuario contra la base de datos y, tras una autenticación satisfactoria, devuelve el atributo url-redirect al controlador de LAN inalámbrica. La autenticación se ha completado en esta etapa.

😤 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			

Cuando el usuario abre un navegador web, se le redirige a la URL de la página de inicio del departamento de administración. (Esta URL se devuelve al WLC a través del atributo cisco-av-pair). Después de la redirección, el usuario tiene acceso completo a la red. Estas son las capturas de pantalla:



Las mismas secuencias de eventos se producen cuando un usuario del departamento de operaciones se conecta a las operaciones de WLAN.

😨 Cisco Aironet Desktop Utility	y - Current Profile: Operatio	ons	? 🗙
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	



Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

Puede utilizar los siguientes comandos para solucionar problemas de configuración.

 show wlan wlan_id: muestra el estado de las funciones de redirección web para una WLAN determinada.Aquí tiene un ejemplo:

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: habilita la depuración de mensajes de paquetes 802.1x.Aquí tiene un ejemplo:

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: habilita la salida de depuración de todos los eventos aaa.Aquí tiene un ejemplo:

```
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: '
```

Información Relacionada

- Guía de configuración de controlador de LAN inalámbrica de Cisco, versión 5.0
- Ejemplo de Configuración de la Autenticación Web del Controlador LAN Inalámbrico
- Ejemplo de configuración de autenticación web externa con controladores de LAN inalámbrica
- Página de Soporte de Red Inalámbrica
- Soporte Técnico y Documentación Cisco Systems

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).