Configuración de PEAP y EAP-FAST con ACS 5.2 y WLC

Contenido

Introducción **Prerequisites Requirements Componentes Utilizados Convenciones** Configurar Diagrama de la red **Suposición Configuration Steps** Configuración del servidor RADIUS Configurar recursos de red **Configurar** usuarios Definición de elementos de política Aplicar políticas de acceso Configurar la WLC Configure el WLC con los detalles del servidor de autenticación Configuración de las interfaces dinámicas (VLAN) Configuración de las WLAN (SSID) Configuración de la utilidad de cliente inalámbrico PEAP-MSCHAPv2 (usuario1) EAP-FAST (usuario2) Verificación Comprobar usuario1 (PEAP-MSCHAPv2) Verificar usuario2 (EAP-FAST) Troubleshoot Comandos para resolución de problemas Información Relacionada

Introducción

Este documento explica cómo configurar el controlador de LAN inalámbrico (WLC) para la autenticación EAP (Extensible Authentication Protocol) con el uso de un servidor RADIUS externo como Access Control Server (ACS) 5.2.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar realizar esta configuración:

- Tener un conocimiento básico del WLC y los Lightweight Access Points (LAPs)
- Tener un conocimiento funcional del servidor AAA

• Poseer un conocimiento profundo de las redes inalámbricas y de los problemas de seguridad inalámbrica

Componentes Utilizados

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

- Cisco 5508 WLC que ejecuta la versión 7.0.220.0 del firmware
- LAP de la serie 3502 de Cisco
- Suplicante nativo de Microsoft Windows 7 con controlador Intel 6300-N versión 14.3
- Cisco Secure ACS que ejecuta la versión 5.2
- Switch Cisco serie 3560

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 Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Estos son los detalles de configuración de los componentes utilizados en este diagrama:

- La dirección IP del servidor ACS (RADIUS) es 192.168.150.24.
- La dirección de la interfaz de administración y del administrador AP del WLC es 192.168.75.44.
- Los servidores DHCP dirigen 192.168.150.25.
- La VLAN 253 se utiliza en toda esta configuración. Ambos usuarios se conectan al mismo SSID "goa". Sin embargo, el usuario 1 está configurado para autenticarse mediante PEAP-MSCHAPv2 y el usuario 2 mediante EAP-FAST.
- Los usuarios se asignarán en la VLAN 253:
 - VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.1
 - VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

Suposición

- Los switches se configuran para todas las VLAN de Capa 3.
- Al servidor DHCP se le asigna un ámbito DHCP.
- Existe conectividad de capa 3 entre todos los dispositivos de la red.
- El LAP ya está unido al WLC.

- Cada VLAN tiene una máscara /24.
- ACS 5.2 tiene instalado un certificado autofirmado.

Configuration Steps

Esta configuración se divide en tres pasos de alto nivel:

- 1. <u>Configure el servidor RADIUS.</u>
- 2. <u>Configure el WLC.</u>
- 3. Configuración de la utilidad de cliente inalámbrico.

Configuración del servidor RADIUS

La configuración del servidor RADIUS se divide en cuatro pasos:

- 1. <u>Configure los recursos de red.</u>
- 2. Configurar usuarios.
- 3. Definir elementos de política.
- 4. Aplique políticas de acceso.

ACS 5.x es un sistema de control de acceso basado en políticas. Es decir, ACS 5.x utiliza un modelo de política basado en reglas en lugar del modelo basado en grupos utilizado en las versiones 4.x.

El modelo de políticas basadas en reglas ACS 5.x proporciona un control de acceso más potente y flexible en comparación con el antiguo enfoque basado en grupos.

En el modelo basado en grupos más antiguo, un grupo define la política porque contiene y une tres tipos de información:

- Información de identidad: esta información puede estar basada en la pertenencia a grupos AD o LDAP o en una asignación estática para usuarios internos de ACS.
- Otras restricciones o condiciones: restricciones de tiempo, restricciones de dispositivos, etc.
- Permisos: VLAN o niveles de privilegio de Cisco IOS[®].

El modelo de políticas de ACS 5.x se basa en reglas con el formato:

• Si la condición entonces resultado

Por ejemplo, utilizamos la información descrita para el modelo basado en grupos:

• Si identity-condition, restricted-condition, authorization-profile.

Como resultado, esto nos da la flexibilidad de limitar en qué condiciones se permite al usuario acceder a la red, así como qué nivel de autorización se permite cuando se cumplen condiciones específicas.

Configurar recursos de red

En esta sección, configuramos el cliente AAA para el WLC en el servidor RADIUS.

Este procedimiento explica cómo agregar el WLC como cliente AAA en el servidor RADIUS para que el WLC pueda pasar las credenciales del usuario al servidor RADIUS.

Complete estos pasos:

1. Desde la GUI de ACS, vaya a **Network Resources** > **Network Device Groups** > **Location**, y haga clic en **Create** (en la parte inferior).

cisco Cisco Secure A	CS
► 🛃 My Workspace	Network Resources > Network Device Groups > Location
👻 🦣 Network Resources	Network Device Groups
 Network Device Groups Location 	Filter: Match if: Go 🔻
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name Description All Locations
B Users and Identity Stores	
Policy Elements Policy Elements	
► 🔂 Access Policies	
Monitoring and Reports	
🕞 🍕 System Administration	

2. Agregue los campos obligatorios y haga clic en Enviar.

A Name	LAD	
Description:		
Description.	LAB Devices	
o Parent:	All Locations	Select
Required field	lds	

Ahora verá esta pantalla:



3. Haga clic en **Tipo de dispositivo** > **Crear**.

cisco Cisco Secure A	CS	
🕨 🧐 My Workspace	Network Resources > Network Device Groups > Device Type > Create	
Network Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Device Group - General Image: 0 Name: 5508 Description: Wireless LAN Controller Image: 0 Parent: All Device Types Image: 0 Required fields	Select
Users and Identity Stores		
Policy Elements		
Access Policies		
Monitoring and Reports		
System Administration		

4. Haga clic en Submit (Enviar). Ahora verá esta pantalla:

cisco Cisco Secure A	CS		
► In the second sec	Network Resources > Network Device Groups > Device Type		
🔹 😝 Network Resources	Network Device Groups		
Network Device Groups Location Device Type	Filter: Match if: Go 🗢		
Network Devices and AAA Clients	Name Description		
Default Network Device External RADIUS Servers	* <u>All Device Types</u> All Device Types		
Users and Identity Stores	5508 Wireless LAN Controller		
Policy Elements			
Access Policies			
Monitoring and Reports			
System Administration			

- 5. Vaya a Recursos de red > Dispositivos de red y clientes AAA.
- 6. Haga clic en **Create** y rellene los detalles como se muestra aquí:

→ S MyWorkspace	Network Resources > Network Devices and AAA Clerks > Create				
Ketwork Resources Network Device Groups Location	o Name: WLC Description: Wre	-5508 less LAN Controller			
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Service	Network Device Grou Location Device Type	All Locations:LAB	Select Select		
Source and Identity Stores Source Elements Control Access Policies Monitoring and Reports	IP Address © Single IP Add 9 IP: 192 108 75 4	IP Address © Single IP Address © IP Range(s) 9 IP. [192 108 75.44		Authentication Options	
 System Administration 	e - Required felds		Ľ	CoA port 1700 Enable KeyWitap Key Encryption Key: Message Authenticator Code Key: Key Input Format C ASCII C HEXADECIMAL	

7. Haga clic en Submit (Enviar). Ahora verá esta pantalla:

	ark bences	1997				
ilter			 Match it. 	•	G0 🔻	
-	Name	•	IP / Mask	NDG:Location	NDG:Device Type	Description
	WLC-5508		192.168.75.44/32	All Locations:LAB	All Device Types:5508	Wireless LAN Controller

Configurar usuarios

En esta sección, crearemos usuarios locales en ACS. Ambos usuarios (usuario1 y usuario2) están asignados en un grupo denominado "Usuarios inalámbricos".

1. Vaya a Usuarios y almacenes de identidad > Grupos de identidad > Crear.

100 C. 100 C.	cisco Cisco Secure ACS				
	» 😚 My Workspace	Users and identity Stores > Identity Groups > Create			
	Network Resources	Coursed .			
	Users and Identity Stores	e Name: Wireless Users			
	Identity Groups	Description: Wireless Liters withorthroting over wireless			
	 Internal identity Stores 	Parent All Croupe Salart			
	Hosts	Required telds			
	+ External Identity Stores				
ŝ	Active Directory				
ŝ	RSA SecurID Token Servers				
	RADIUS Identity Servers				
語	Certificate Authentication Profile				
	Identity Store Sequences				
	» S. Policy Elements				

2. Una vez que haga clic en **Submit**, la página tendrá el siguiente aspecto:

cisco Cisco Secure Ad	CS		
🕨 🚓 My Workspace	Users and identity Stores > identity Groups		
Network Resources	Identity Groups		
Osers and identity Stores Identity Groups Internal Identity Stores Users Hosts External Identity Stores LDAP Activa Directory RSA SecuriD Token Servers RADIUS Identity Servers Certificate Authonities Certificate Authonities	Filter: 💽 Match it: 💽 Go 🔝		
	Name Description		
Identity Store Sequences			

- 3. Cree los usuarios user1 y user2 y asígnelos al grupo "Usuarios inalámbricos".
 - a. Haga clic en Usuarios y almacenes de identidad > Grupos de identidad > Usuarios > Crear.

My Workspace	Users and identity Stores > Internal identity Stores > Users > Create
Network Resources	General
Users and Identity Stores	🖉 🗢 Name: User1 Status: Enabled 💌 😕
Identity Groups	Description: PEAP:mschapv2 users
0596	 Identity Group: All Groups: Wireless Users Select
External Identity Stores Certificate Authorities Certificate Authorities Identity Store Sequences	Password Information Password must Contain 4 - 32 characters
S Policy Elements	Password: •••••
Access Policies	Confirm Pasewort
Monitoring and Reports	Change password on next login

b. De manera similar, cree user2.

cisco Cisco Secure A	CS
My Workspace	Users and identity Stores > Internal identity Stores > Users > Create
	General General Ø Name: User2 Description: EAPFAST user Ø Identity Group: All Groups:/Wireless Users Select Password Information Password must • Contain 4 - 32 characters
Identity Store Sequences	Password: Onfirm Password: Confirm Password: Change password on next login Change password on next login There are no additional identity attributes defined for user records P - Required fields

La pantalla tendrá el siguiente aspecto:

cisco Cisco Secure AC	:8			
🕨 🚭 My Workspace	Users and Identity Stores	> internal identity Store	s > Users	
► 🁦 Network Resources	Internal Users			
Busers and Identity Stores Identity Groups Internal Identity Stores Users Hosts External Identity Stores Certificate Authorities Certificate Authorities Identity Store Sequences	Filter: Match it: Go 🗢			
	C Status	User Name	 Identity Group 	Description
	□ ●	<u>user1</u>	All Groups:Wireless Users	PEAP:mschapv2 users
	□ 0	user2	All Groups:Wireless Users	EAPFAST user
Policy Elements				

Definición de elementos de política

Verifique que **Permit Access** esté configurado.

cisco Cisco Secure A	CS
🔸 🤯 My Workspace	Policy Elementa > Authorization and Permissions > Network Accesse > Asthorization Profiles
Network Resources	Authorization Profiles
Users and Identity Stores	Filter
Policy Elements	
Session Conditions Authorization and Permissions	Permit Access
 Network Access Authorization Profiles 	
Device Administration Named Permission Objects	
Access Policies	
Monitoring and Reports	
🕨 🍕 System Administration	

Aplicar políticas de acceso

En esta sección, seleccionaremos qué métodos de autenticación se utilizarán y cómo se configurarán las reglas. Crearemos reglas basadas en los pasos anteriores.

Complete estos pasos:

1. Vaya a Políticas de acceso > Servicios de acceso > Acceso a la red predeterminado > Editar: "Acceso a la red predeterminado".



2. Seleccione el método EAP que desea que autentiquen los clientes inalámbricos. En este ejemplo, utilizamos **PEAP- MSCHAPv2** y **EAP-FAST**.



Access Policies Access Services	
Envice Selection Rules O Default Device Admin O Default Network Access	Allow PEAP PEAP Inner Methods P Allow EAP-M3-CHAPv2
Authorization	Allow Password Change Retries:
System Administration	Allow FASSWold Change Retries: Allow EAP-FAST EAP-FAST inner Methods Allow EAP-ASS-CHAEPv2 If Allow Password Change Retries: If Allow Password Change Retries: If Allow EAP-OTC If Allow FASSWord Change Retries: If Allow FASSWOrd Inter Authenticated In-Band FAC Provisioning If Allow Authentheated In-Band FAC Provisioning If Allow Authentheated In-Band FAC Provisioning If Allow FASSWORD ALL Authentication Machine FAC Time To Live: If Allow FASSWORD ALL Authenticated Provisioning Authentheated In-Band FAC Provisioning If Allow FASSWORD ALL Authentication Machine FAC Time To Live: If Hours If Allow FASSWORD ALL AUTHENTIAL AUTHEN

- 3. Haga clic en Submit (Enviar).
- 4. Verifique el grupo de identidad que ha seleccionado. En este ejemplo, utilizamos **Internal Users**, que creamos en ACS. **Guarde los cambios.**



5. Para verificar el perfil de autorización, vaya a Access Policies > Access Services > Default Network Access > Authorization.

Puede personalizar en qué condiciones permitirá el acceso de los usuarios a la red y qué perfil de autorización (atributos) pasará una vez autenticado. Esta granularidad sólo está disponible en ACS 5.x. En este ejemplo, hemos seleccionado Location, **Device Type**, **Protocol**, **Identity Group** y EAP Authentication Method.

Access Policies > Access Services > Detail Network Access > Authorization Standard Policy/Excending Policy
Network Access Authorization Policy
Filter. Status - Match it Equais - Enabled - Clear Filter Go -
Image: Status Name Conditions Results ND0:Location Time And Date Authorization Profiles Hit Count
Matile fields Import / 1922 1888 150.24 / accordmin/Policy/hputAction.do Import / 1922 1888 150.24 / accordmin/Policy/hputAction.do Import / 100
Persuit Easined or no ensibled rule matches. Permit Access 0
Create

- 6. Haga clic en Aceptar y Guardar cambios.
- 7. El siguiente paso consiste en crear una regla. Si no se define ninguna regla, se permite al cliente el acceso sin condiciones.

Haga clic en **Create** > **Rule-1**. Esta regla es para usuarios del grupo "Usuarios inalámbricos".

Access Policies > Access Services > Default	Network Access > Authorization				
Standard Policy Exception Policy					
Network Access Authorization Petion					
Filter. Status	sco Secure ACS - Mozilla Firefox				×
	192.168.150.24 https://192.168.1	150.24/acsadmin/Policyli	nputAction.do		슈
I Status Plame NE			-		
No data to display	General				
	Name: Fole-1	Status: Enabled	• 0		
	Conditions	nd results are availa	t area of the poicy rules screen con ble here for use in policy rules.	trois which	
	MDG:Location:		All Device Trees 5500	Select	
	P NDG Device type	match	Padus	Select	
	V Manifer Groups	lin	All Groups Wireless Users	Select	
	Eap Authentication Method	ANY-			
	Eap Authonication Reenod Results Authorization Profiles: Permit Access Select Deselect OK Cancel		You may select multiple authorization pro defined in multiple profiles will use the va profile defined.	files. Attributes ive from the first	10
T Datast Fr	and the last last				
Create Duplicate Edit	Delete A Move to V			Cush	emize HitCount

8. Guarde los cambios. La pantalla tendrá el siguiente aspecto:

	COSSIS PRO	thorization Policy						
ater. St	atus	- Mate	ch it Equals 💽 Enat	io • bek	ear Filter Go 🔻			
Status	Name	NDG:Location	NDG Device Type	Condition Protocol	identity Group	Eap Authentication Nethod	Ress Authorizatio	its n Profil
•	Rule-1	in All Locations:LAB	In All Device Types 5508	match Radius	in All Groups:Wireless Users	-4117-	Permit Acce	22
Default		I no rules defined or r	no enabled rule matches.				Parmel Acco	55

Si desea que se denieguen los usuarios que no cumplan las condiciones, edite la regla predeterminada para que diga "denegar acceso".

9. Ahora definiremos las **reglas de selección de servicios**. Utilice esta página para configurar una política simple o basada en reglas para determinar qué servicio aplicar a las solicitudes entrantes. En este ejemplo, se utiliza una política basada en reglas.

E s	Statur 8				Filter: Status 💌 Match it: Equals 💌 Enabled 💌 Clear Filter 🛛 Go 🔝									
	Statute II	Vame	Protocol	litiona	Results Service	Hit Count								
	8	Rule-1	match Radius		Default Network Access	0								
	e <u>e</u>	Rule-2	match Tacacs		Default Device Admin	0								

Configurar la WLC

La configuración requiere estos pasos:

- 1. Configure el WLC con los detalles del servidor de autenticación.
- 2. Configure las interfaces dinámicas (VLAN).
- 3. Configure las WLAN (SSID).

Configure el WLC con los detalles del servidor de autenticación

Es necesario configurar el WLC para que pueda comunicarse con el servidor RADIUS para autenticar los clientes, y también para cualquier otra transacción.

Complete estos pasos:

- 1. En la GUI del controlador, haga clic en Security.
- 2. Introduzca la dirección IP del servidor RADIUS y la clave secreta compartida utilizada entre el servidor RADIUS y el WLC.

Esta clave secreta compartida debe ser la misma que la configurada en el servidor RADIUS.

cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMAND5	HELP	EEEDBACK
Security	RADIUS Authenti	cation Servers	s > New					
 AAA General RADDUS Authentication Accounting Falback TACACS+ LDAP Local Net Users MAC Fitesing Disabled Clients User Login Policies AP Policies Password Policies Local EAP Priority Order Certificate Access Control Lists Wireless Protection Policies 	Server Index (Priori Server IP Address Shared Secret Form Shared Secret Confirm Shared Sec Key Wrap Port Number Server Status Support for RFC 357 Server Timeout Network User Management IPSec	ty) at ret	1 × 192.168.150.2 ASCII •••••• •••••• (Designed for 1812 Enabled Enabled Ø Enable Ø Enable Enable	4 FIPS custome	ers and requires a	key wrap compli	ant RADI	US server)
Web Auth								

+ Advanced

Configuración de las interfaces dinámicas (VLAN)

Este procedimiento describe cómo configurar las interfaces dinámicas en el WLC.

Complete estos pasos:

1. La interfaz dinámica se configura desde la GUI del controlador, en la ventana **Controller** > **Interfaces**.

cisco		WLANs		WIRELESS	SECURITY	MANAGEMENT
Controller General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Nobility Management Ports NTP CDP Advanced	Interface: Unterface VLAN Id	s > New Name	vlan253 [253			

2. Haga clic en Apply (Aplicar).

Esto lo lleva a la ventana Edit (Editar) de esta interfaz dinámica (VLAN 253 aquí).

3. Introduzca la dirección IP y el gateway predeterminado de esta interfaz dinámica.

cisco			WIRELESS	<u>S</u> ECURITY	MANAGEMENT
Controller	Interfaces > Edit				
General Inventory Interfaces Interface Groups Multicast Network Routes > Internal DHCP Server	General Information Interface Name NAC Address Configuration Guest Lan	vlan253 00:24:97	1:09:53:cf		-
Ports NTP CDP	Quarantine Quarantine Vian Id Physical Information	[] 0			
Advanced	The interface is attache Enable Dynamic AP Management Interface Address	ed to a LAG.			_
	VLAN Identifier IP Address Netmask Gateway	253 192.168.153 255.255.255 192.168.153	1.81 5.0		
	DHCP Information Primary DHCP Server Secondary DHCP Server	19	2,168,150,25		-
	Access Control List ACL Name Note: Changing the Interfut temporarily disabled and some clients.	no ace peremeters thus may result	one causes the Wil in loss of conn	Alls to be ectivity for	

- 4. Haga clic en Apply (Aplicar).
- 5. Las interfaces configuradas tendrán el siguiente aspecto:

uluulu cisco	MONITOR	WLANs	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	COMMAN	IDS HELP	FEEDBACK	
Controller	Interfaces	5							
Inventory	Interface	Name	VLAN Identifier	IP Addres	s Interfa	ce Type I	Dynamic AP	Hanagement	
Interfaces	manageme	nt	75	192.168.75	.44 Static	1	Enabled		
Interface Groups	service-por	t	N/A.	0.0.0.0	Static	1	Not Supported		
Multicast	virtual		N/A	1.1.1.1	Static	1	Not Supported		
Network Routes	vlan253		253	192.168.15	3.81 Dynami	ic t	Disabled		
Internal DHCP Server									
Mobility Management									
Ports									
▶ NTP									
▶ CDP									
Advanced									

Configuración de las WLAN (SSID)

Este procedimiento explica cómo configurar las WLANs en el WLC.

Complete estos pasos:

- 1. Desde el controlador GUI, vaya a **WLANs** > **Create New** para crear una nueva WLAN. Se muestra la ventana New WLANs (Nuevas WLAN).
- 2. Introduzca la información de ID de WLAN y SSID de WLAN.

Puede introducir cualquier nombre como SSID de WLAN. Este ejemplo utiliza **goa** como el SSID de WLAN.

cisco		WLANS	CONTROLLER	W]RELESS	SECURITY	MANAGEMENT	COMMAND
WLANS WLANS WLANS Advanced	WLANS > Type Profile Na SSID ID	New me	QOB QOB 1	-			

3. Haga clic en Apply para ir a la ventana Edit del objetivo WLAN.





aneral 9	Security	QoS Adva	inced			
Layer 2	Layer 3	AAA Servers	use of default server	s on this WLAN		
Radius Serv Radius Se	rers srver Overwr	ite interface 🗆 t	Inabled		LDAP Server 1	None
Server 1 Server 2 Server 3		Aut TP No	thentication Servers Enabled :192.168.150.24, Port:1 one one	Accounting Consbled B12 × None × × None × × None ×	g Servers Server 3 Server 3	None
Local EAP A Local EAP Authentica	athenticati Authenticati ation priori	on DN Enabled Ity order for				
Not U	boet		Order Used For Au	thentication		

WLANs > Edit 'goa'

meral Security	QoS Advanced	
Allow AAA Override	Enabled	DHCP
Coverage Hole Detection	Enabled	DHCP Server Override
Enable Session Timeout		
Aironet IE	P Enabled	DHCP Addr. Assignment 🏼 Required
Diagnostic Channel	Finabled	Management Frame Protection (MFP)
1Pv6 Enable ²		and other protocial distribution
Override Interface ACL	None -	MEP Client Protection - [Disabled]
P2P Blocking Action	Disabled -	DTIM Period (in beacon intervals)
Client Exclusion 2	Enabled	802.11a/n (1 - 255) 1
Maximum Allowed	0	802.11b/g/n (1 - 255) 1
Chente =		NAC
Static IP Tunneling 12	Cnabled	NAC State None +
Channel Scanning Defe	er	Load Balancing and Band Select
Scan Defer Priority	0 1 2 3 4 5 6 7	Client Load Balancing
		Client Band Select 4
Scan Defer Time(msecs)	100	Passive Client

Configuración de la utilidad de cliente inalámbrico

PEAP-MSCHAPv2 (usuario1)

En nuestro cliente de prueba, utilizamos el suplicante nativo de Windows 7 con una tarjeta Intel 6300-N que ejecuta la versión de controlador 14.3. Se recomienda probar con los controladores más recientes de los proveedores.

Complete estos pasos para crear un perfil en Windows Zero Config (WZC):

- 1. Vaya a Control Panel > Network and Internet > Manage Wireless Networks.
- 2. Haga clic en la pestaña Add.
- 3. Haga clic en Crear manualmente un perfil de red.



4. Agregue los detalles según lo configurado en el WLC.

Nota: El SSID distingue entre mayúsculas y minúsculas.

5. Haga clic en Next (Siguiente).

letwork name:	609		
Security type:	WPA2-Enterprise		
Encryption type:	AES 🔹		
Security Key:		Hide characters	
Start this connec	tion automatically		
Connect even if Warning: If you	the network is not broadcasting select this option, your computer's privacy	/ might be at risk.	

6. Haga clic en **Cambiar la configuración de la conexión** para volver a verificar la configuración.



7. Asegúrese de que tiene **PEAP** habilitado.

goa Wireless Network Properties	23		
Connection Security			
Security type: WPA2-Enterprise			
Encryption type: AES -			
	,		
Choose a network authentication method:			
Microsoft: Protected EAP (PEAP) Settings]		
Remember my credentials for this connection each			
diffe Thribyged off			
Advanced settings			
ОК	Cancel		

goa Wireless Network Properties		
Connection Security		
Security type:	WPA2-Enterprise	
Encryption type:	AES	
Choose a network aut Microsoft: Protected I Remember my creatine I'm logged on Advanced settings	hentication method: EAP (PEAP) Settings dentials for this connection cach	
	OK Cancel	

8. En este ejemplo, no estamos validando el certificado del servidor. Si marca esta casilla y no puede conectarse, intente desactivar la función y vuelva a realizar la prueba.

Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities;
AAA Certificate Services
AddTrust External CA Root
Class 3 Public Primary Certification Authority
Class 3 Public Primary Certification Authority
DigiCert Assured ID Root CA
DigiCert High Assurance EV Root CA
DST Root CA X3
4 III III III III III III III III III I
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Enable Fast Reconnect
Enforce Network Access Protection
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK Cancel

9. También puede utilizar sus credenciales de Windows para iniciar sesión. Sin embargo, en este ejemplo no vamos a usar eso. Click OK.

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

10. Haga clic en **Advanced settings** para configurar el nombre de usuario y la contraseña.

goa Wireless Network Pr	operties	23	
Connection Security			
Security type:	WPA2-Enterprise		
Encryption type:	AES 💌		
Choose a network aut	hentication method:		
Microsoft: Protected B	Microsoft: Protected EAP (PEAP)		
Remember my credentials for this connection each time I'm logged on			
Advanced settings			
	OK Car	ncel	

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

Windows Security
Save credentials Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).
user1
OK Cancel

La utilidad de cliente ya está lista para conectarse.

EAP-FAST (usuario2)

En nuestro cliente de prueba, utilizamos el suplicante nativo de Windows 7 con una tarjeta Intel 6300-N que ejecuta la versión de controlador 14.3. Se recomienda probar con los controladores más recientes de los proveedores.

Complete estos pasos para crear un perfil en WZC:

- 1. Vaya a Control Panel > Network and Internet > Manage Wireless Networks.
- 2. Haga clic en la pestaña Add.
- 3. Haga clic en Crear manualmente un perfil de red.

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

4. Agregue los detalles según lo configurado en el WLC.

Nota: El SSID distingue entre mayúsculas y minúsculas.

5. Haga clic en Next (Siguiente).

Enter information	for the wireless network you want to add	
Network name:	goa	
Security type:	WPA2-Enterprise	
Encryption type:	AES 💌	
Security Key:	Hide char	racters
Start this conne	tion automatically	
Connect even if the network is not broadcasting Warning: If you select this option, your computer's privacy might be at risk.		

6. Haga clic en Cambiar la configuración de la conexión para volver a verificar la configuración.

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

7. Asegúrese de que EAP-FAST está activado.

Nota: De forma predeterminada, WZC no tiene EAP-FAST como método de autenticación. Tiene que descargar la utilidad de un proveedor externo. En este ejemplo, como se trata de una tarjeta Intel,

tenemos Intel PROSet instalado en el sistema.

goa Wireless Network Pr	operties
Connection Security	
Security type: Encryption type:	WPA2-Enterprise AES
Choose a network aut Cisco: EAP-FAST Microsoft: Smart Card Microsoft: Protected B Cisco: LEAP Cisco: PEAP Cisco: PEAP Cisco: EAP-FAST Intel: EAP-SIM Intel: EAP-SIM Intel: EAP-AKA Advanced settings	or other certificate AP (PEAP)
	OK Cancel

goa Wireless Network Properties	23
Connection	
Security type: WPA2-Enterprise	
Encryption type: AES -	
Choose a network authentication method:	
Cisco: EAP-FAST Settings	
Remember my credentials for this connection each time I'm logged on	
Advanced settings	
OK Car	ncel

8. Habilite Allow automatic PAC provisioning y asegúrese de que la opción Validate server certificate esté desactivada.

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

9. Haga clic en la ficha **Credenciales de usuario** e introduzca las credenciales del usuario 2. También puede utilizar sus credenciales de Windows para iniciar sesión. Sin embargo, en este ejemplo no vamos a usar eso.

EAP-FAST Prop	oerties				? X
Connection	User Credentials	Authentication	About		
O Use o	ertificate on this o	omputer			
O Use o	one-time password				
O Use V	Windows username	and password			
Prom	pt automatically fo	r username and	password		
O Use s	saved username a	nd password			
Userna	ame: us	er2			
Passwo	ord: •	••••			
Confirm	m password:				
			\mathbf{r}		
			ОК	Cancel	Help

10. Click OK.

EAP-FAST Properties
Connection User Credentials Authentication About
Select authentication method:
Any method Configure
Enable Fast Reconnect
OK Cancel Help

La utilidad de cliente ya está lista para conectarse para el usuario 2.

Nota: Cuando el usuario 2 intenta autenticarse, el servidor RADIUS enviará una PAC. Acepte la PAC para completar la autenticación.



Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Comprobar usuario1 (PEAP-MSCHAPv2)

Desde la GUI del WLC, vaya a Monitor > Clients, y seleccione la dirección MAC.

lient Properties		_	AP Properties	
MAC Address	00:24:d7:ae:f1:98		AP Address	2c:3f:38:c1:3c:f0
IP Address	192.165.153.107		AP Name	3502e
Client Type	Regular		AP Type	802.11an
User Neme	user1		WLAN Profile	904
Port Number	13		Status	Associated
Interface	vlan253		Association ID	1
VLAN ID	253		802.11 Authentication	Open System
CCX Version	CCXv4		Reason Code	1
E2E Version	E2Ev1		Status Code	0
Mobility Role	Local		CF Pollable	Not Implemented
Mobility Peer IP Address	N/A		CF Poll Request	Nat Implemented
Policy Nanager State	RUN		Short Preamble	Not Implemented
Management Frame Protection	No		PBCC	Not Implemented
UpTime (Sec)	12		Channel Agility	Nat Implemented
Power Save Node	OFF		Re-authentication timeout	86365
Current TxRateSet	6.0,9.0,12.0,18.0,24.0,3	6.0,45.0,54.	Remaining Re-authentication timeout	0
Data RateSet	ŭ		WEP State	WEP Enable
ecurity Information				
Security Policy Completed	Yes			
Policy Type	REN (WPA2)			
Encryption Cipher	CCMP (AES)			

Estadísticas RADIUS WLC:

PEAP

Access

RUN

EAP Type

SNNP NAC State

dius NAC State



Registros de ACS:

- 1. Complete estos pasos para ver los recuentos de aciertos:
 - a. Si verifica los registros dentro de los 15 minutos de la autenticación, asegúrese de actualizar el conteo de aciertos.

E a mai	no Cole	action field	line			
Filter	: Stat.	.6 -] Match if:	Equals - Enabled - Clea	ar Filter 🛛 🐨	
		Status	Name	Conditions Protocol	Results Service	Hit Cour
1		•	Rule-1	match Radius	Default Network Access	1
	-	0	Rule-2	match Tacaca	Dofault Device Admin	0

b. Tiene una pestaña para Recuento de visitas en la parte inferior de la misma página.

Access Palo	ies > Access Services > I	Default Network Access > Ast	norization				
Standard P	Policy Exception Policy	ı					
Network	Access Authorization	Policy					
Filter: 9	talus	Match if: Equals	 Enabled 	💌 Clear Filter 🛛 Go 🖙			
Name	NDG:Location	NDG:Device Type	Conditi Protecol	ons Identity Group	Eap Authentication Method	Results Authorization Profiles	Hit Count
Rule-1	in All Locations LAB	in All Device Types:5508	match Radius	in All Groups:Wireless Users	-ANY-	Permit Access	1
4							Л
faut	If no rules define	d or no enabled rule matche	18.			Permit Access	V
Create	- Duplicate • E	dit Delete ^ Mov	ve to 🗵			Customize	HitCount

2. Haga clic en **Supervisión e informes** y aparecerá una ventana emergente Nuevo. Vaya a **Autenticaciones - Radio - Hoy**. También puede hacer clic en **Detalles** para verificar qué regla de selección de servicio se aplicó.

1.5.2	Launch Interactive Vener
Shewing Rays 1 of 1 First Prev Head Lord	Cote Page 6e
AAA Protocol > RADIUS Authentication	
Authentication Status : Pass er Fail Dote : January 29, 2012 05:40 PM - January 29, 2012 05:10 PM (Lost 30 Minutes) Let	t Hourt 1Last 12 Hours Tedax Yestenlav Last 7 Dava Last 30 Dava)
Generated on January 29, 2012 6:10:42 PM EST	
Relad ✓-Fas X-Fat S-Cide for details R =House over item for additional information	
Logged At RADIUS NAS Details Usemanie MAC/1P Access Seni	ce Authentication Network Device NAS IP Address NAS Port ID CTS Security Group ACS Instance
Jan 29,12 6:07:37.943 PM 2 9, user1 00:24:d7.as-f1.98 Default Notesek /	KERRR PEAP (EAP MISCHAPV2) WLC 5508 192 158 75.44 SALIL-ACS52

Verificar usuario2 (EAP-FAST)

Desde la GUI del WLC, vaya a **Monitor** > **Clients**, y seleccione la dirección MAC.

Clients > Detail

-	Client Properties			AP Properties	
I	MAC Address	001241d71aetf1198		AP Address	2cr3fr38rc1r3crf0
I	1P Address	192.168.153.111		AP Name	3502e
I	Client Type	Regular		AP Type	802.11an
I	User Name	user2		WLAN Profile	goa
I	Port Number	13		Status	Associated
I	Interface	vlan253		Association ID	1
I	VLAN ID	253		802.11 Authentication	Open System
1	CCX Version	CCXV4		Reason Code	1
	E2E Version	E2Ev1		Status Code	0
	Mobility Role	Local		CF Pollable	Not Implemented
	Mobility Peer IP Address	N/A		CF Poll Request	Not Implemented
I	Policy Manager State	RUN		Short Preamble	Not Implemented
1	Management Frame Protection	No		PBCC	Not Implemented
	UpTime (Sec)	29		Channel Agility	Not Implemented
	Power Save Mode	OFF		Re-authentication timeout	86392
	Current TxRateSet	m15		Remaining Re-authentication	0
		6.0,9.0,12.0,18.0,24	.0,36.0,48.0,54.	timeout	
	Data RateSet	0		WEP State	WEP Enable
1	Security Information				
	Security Policy Completed	Yes			
	Policy Type	RSN (WPA2)			
	Encryption Cipher	CCMP (AES)			
	EAP Type	EAP-FAST			
	SNMP NAC State	Access			
	Radius NAC State	R11N			

Registros de ACS:

- 1. Complete estos pasos para ver los recuentos de aciertos:
 - a. Si verifica los registros dentro de los 15 minutos de la autenticación, asegúrese de actualizar el conteo de HIT.

Servi	ce Sele	ection Pol	licy					
Filter	Stat	JS 🔻	Match It	Equals 🔹	Enabled 🔹	Clear Filter	Go 🔻	
	E	Status	Name	Protocol	Conditions		Results Service	Hit Cour
1			Rule-1	match Radius			Default Network Access	3
2	Г		Rule-2	match Tacacs			Default Device Admin	0

b. Tiene una pestaña para **Recuento de visitas** en la parte inferior de la misma página.

Access Authorization R	Policy					
atus	Match if: Equals	 Enabled 	🔹 Clear Filter 🛛 😨			
NDG:Location	NDG:Device Type	Conditi Protocol	ons Identity Group	Eap Authentication Method	Results Authorization Profiles	Hit Coun
in All Locations:LAB	in All Device Types:5508	match Radius	in All Groups: Wireless Users	-ANY-	Permit Access	2
	eccess Authorization I alus NDG:Location in All Locations:LAB	Access Authorization Policy alus Match It: Equals NDG:Location NDG:Device Type in All Locations:LAB in All Device Types:5508	codess Authorization Policy alus Match it: Equals Enabled Conditi NDG:Location NDG:Device Type Protocol in All Locations:LAB in All Device Types:5508 match Radius	Locess Authorization Policy alus ■ Match it: Equals ■ Enabled ■ Clear Filter Go ▼ Conditions NDG:Location NDG:Device Type Protocol Identity Group in All Locations:LAB in All Device Types:5508 match Radius in All Groups:Wireless Users	eccese Authorization Policy alus ▼ Match it: Equals ▼ Enabled ▼ Clear Filter Go ▼ Conditions NDG:Location NDG:Device Type Protocol Identity Group Eap Authentication Method in All Locations:LAB in All Device Types:5508 match Radius in All Groups:Wireless Users -ANY-	codese Authorization Policy alus Match it: Equals Enabled Cenditions Conditions Results NDG:Location NDG:Device Type Protocol Identity Group Eap Authentication Method Authorization Profiles In All Locations:LAB In All Device Types:5508 match Radius In All Groups:/Wireless Users -NY- Permit Access

2. Haga clic en **Supervisión e informes** y aparecerá una ventana emergente Nuevo. Vaya a **Autenticaciones - Radio - Hoy**. También puede hacer clic en **Detalles** para verificar qué regla de selección de servicio se aplicó.

2 2 2										La	anch Interactive	Vewer 5
Showing Pag	c 1 of 1		1000	ration frees	ment Last	1 Get	to Page: Ge					
AAA Protocol > RAI	US Auther	ntication										
Authentication Status : Date :	Pass or Fail January 29, 2	2012 05:5	3 PM	January 29, 3	2012 06:23 PM (La	st 30 Ninutes <u>Last Hour</u> L	ast 12 Hours Today Yesterday	Last 7 Days (Las	: 30 D #(n)			
Generated on January	29, 2912 6:23	17 PM E	ST									
Reicad	A +Chia for a	state 1	-Head	an over iters	for additional inform	nation						
Logged At	RACIUS Status	NAS Falure	Details	Usemana	MAC/IP Address	Access Service	Authentication Method	Natwork Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS INS
Jan 29,12 6.19 27 270	FM 4		14	uper2	99-24-d7-ap-f1-98	Default Network Access	EAP-FAST (EAP-MSCHAP42)	WLC-5508	192.168.75.44			SALL-A
Jan 29,12 6:07:37:943	PM 🖌		4	user1	00-24-d7-ae-f1-98	Default Network Access	PEAP (EAP-MSCHAPV2)	WLC-5508	192 168 75.44			SALIL-A

Troubleshoot

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

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

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

- 1. Si experimenta cualquier problema, ejecute estos comandos en el WLC:
 - **debug client** <*mac add of the client*>
 - debug aaa all enable
 - show client detail *<mac addr>* : verifique el estado del administrador de políticas.
 - show radius auth statistics Verifique el motivo de la falla.
 - debug disable-all Desactiva los debugs.
 - clear stats radius auth all Borrar estadísticas de radio en el WLC.

2. Verifique los registros en el ACS y anote el motivo de la falla.

Información Relacionada

• <u>Soporte Técnico y Documentación - Cisco Systems</u>

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).