Ejemplo de Configuración de ACL por Usuario con Controladores de LAN Inalámbricos y Cisco Secure ACS

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Convenciones **Antecedentes** Diagrama de la red Configurar Configuración del controlador de LAN inalámbrica Cree una VLAN para los usuarios inalámbricos Configure el WLC para Autenticar con Cisco Secure ACS Cree una nueva WLAN para los usuarios inalámbricos Definir las ACL para los usuarios Configuración del servidor Cisco Secure ACS Configure el Wireless LAN Controller como Cliente AAA en Cisco Secure ACS Configuración del perfil de usuario y usuario en Cisco Secure ACS Verificación Troubleshoot Consejos de Troubleshooting Información Relacionada

Introducción

Este documento explica con un ejemplo cómo crear listas de control de acceso (ACL) en los WLC y aplicarlas a los usuarios dependientes con la autorización de RADIUS.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

 Conocimiento básico de cómo configurar un servidor Cisco Secure ACS para autenticar clientes inalámbricos

- Conocimiento de la configuración de los puntos de acceso ligeros (LAP) Cisco Aironet y de los controladores de LAN inalámbrica (WLC) de Cisco
- Conocimiento de las soluciones Cisco Unified Wireless Security

Componentes Utilizados

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

- Controlador de LAN inalámbrica de Cisco serie 4400 que ejecuta la versión 5.0.148.0
- Puntos de acceso ligeros (LAP) Cisco Aironet serie 1231
- Cisco Aironet 802.11 a/b/g Cisco Wireless LAN Client Adapter que ejecuta la versión 3.6
- Cisco Aironet Desktop Utility versión 3.6
- Servidor Cisco Secure ACS versión 4.1
- Cisco 2800 Series Integrated Services Router que ejecuta IOS[®] Versión 12.4(11)T
- Switch Catalyst de Cisco serie 2900XL que ejecuta la versión 12.0(5)WC3b

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.

Convenciones

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

Antecedentes

La lista de control de acceso (ACL) por usuario forma parte de Cisco Identity Networking. La solución Cisco Wireless LAN Solution admite redes de identidad que, aunque permite a la red anunciar un único SSID, también permite a usuarios específicos heredar diferentes políticas en función de sus perfiles de usuario.

La función ACL por usuario proporciona la capacidad de aplicar una ACL configurada en el controlador de LAN inalámbrica a un usuario según la autorización RADIUS. Esto se logra con el atributo específico del proveedor (VSA) Airespace-ACL-Name.

Este atributo indica el nombre de ACL que se aplicará al cliente. Cuando el atributo ACL está presente en RADIUS Access Accept, el sistema aplica el nombre ACL a la estación cliente después de que se autentica. Esto anula cualquier ACL que se asignen a la interfaz. Ignora la interfaz ACL asignada y aplica la nueva.

A continuación se muestra un resumen del formato de atributo de nombre de ACL. Los campos se transmiten de izquierda a derecha

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	б	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
+	+-+				+	+-+	+ - +	+	+	+ - +	+ - +	+ - +	⊢−+	+ - +	+ - +	++	+	+-+	+	+	+	+ - +		+	+ - +	+ - +	+-+	⊢ – +	⊢−+	+ +	+-+
		1	[yr	be					Le	eng	gtł	ı										Ve	enc	loi	r-1	٤d					
+	+ - +			+	+ - +	+ - +	+ - +	+	+	+ - +	+ - +	+ - +	+ - +	+ +	+ - +	+ - +	+ - +	+-+		+	+	+ - +		+	+ - +	+ - +	+ - +	+ - +	+ - +	+ +	+-+
		Ve	enc	loı	<u>-</u> 1	Id	((cor	ıt	.)						7	/er	ndo	or	ty	үрe	9		7	Ver	ndo	or	le	eng	gtŀ	n

Para obtener más información sobre Cisco Unified Wireless Network Identity Networking, refiérase a la sección <u>Configuración de Identidad Networking</u> del documento <u>Configuración de Soluciones de Seguridad</u>.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

En esta configuración, el WLC y el LAP del controlador del Wireless LAN se utilizan para proporcionar servicios inalámbricos a los usuarios del Departamento A y el Departamento B. Todos los usuarios inalámbricos utilizan una oficina WLAN (SSID) común para acceder a la red y se encuentran en la VLAN Office-VLAN.



El servidor Cisco Secure ACS se utiliza para autenticar usuarios inalámbricos. La autenticación EAP se utiliza para autenticar usuarios. El WLC, el LAP y el servidor Cisco Secure ACS están conectados con un switch de Capa 2 como se muestra.

El router R1 conecta los servidores en el lado cableado a través del switch de Capa 2 como se muestra. El router R1 también actúa como servidor DHCP, que proporciona direcciones IP a clientes inalámbricos de la subred 172.16.0.0/16.

Debe configurar los dispositivos para que esto ocurra:

El usuario1 del Departamento A sólo tiene acceso al servidor 172.16.1.100

El usuario 2 del Departamento B sólo tiene acceso al servidor 172.16.1.50

Para lograr esto, necesita crear 2 ACL en el WLC: uno para User1 y el otro para User2. Una vez que se crean las ACL, debe configurar el servidor Cisco Secure ACS para devolver el atributo de nombre ACL al WLC tras la autenticación exitosa del usuario inalámbrico. El WLC luego aplica la ACL al usuario y, por lo tanto, a la red se restringe según el perfil del usuario.

Nota: Este documento utiliza la autenticación LEAP para autenticar a los usuarios. Cisco LEAP es vulnerable a los ataques de diccionario. En las redes en tiempo real, se deben utilizar métodos de autenticación más seguros como EAP FAST. Dado que el objetivo del documento es explicar cómo configurar la función ACL por usuario, LEAP se utiliza para simplificar.

La siguiente sección proporciona instrucciones paso a paso para configurar los dispositivos para esta configuración.

<u>Configurar</u>

Antes de configurar la función ACL por usuario, debe configurar el WLC para el funcionamiento básico y registrar los LAPs en el WLC. Este documento asume que el WLC está configurado para el funcionamiento básico y que los LAPs están registrados en el WLC. Si usted es un usuario nuevo, que intenta configurar el WLC para el funcionamiento básico con los LAPs, consulte Registro de Lightweight AP (LAP) a un Controlador de LAN Inalámbrica (WLC).

Una vez registrados los LAP, complete estos pasos para configurar los dispositivos para esta configuración:

- 1. Configure el Wireless LAN Controller.
- 2. Configure el servidor Cisco Secure ACS.
- 3. Verifique la Configuración.

Nota: Este documento trata la configuración requerida en el lado inalámbrico. El documento asume que la configuración por cable está en su lugar.

Configuración del controlador de LAN inalámbrica

En Wireless LAN Controller, debe hacer lo siguiente:

- Cree una VLAN para los usuarios inalámbricos.
- Configure el WLC para autenticar a los usuarios inalámbricos con Cisco Secure ACS.

- Cree una nueva WLAN para los usuarios inalámbricos.
- Defina las ACL para los usuarios inalámbricos.

Cree una VLAN para los usuarios inalámbricos

Para crear una VLAN para los usuarios inalámbricos, complete estos pasos.

- 1. Vaya a la GUI del WLC y elija **Controller > Interfaces**. Aparece la ventana Interfaces. Esta ventana muestra las interfaces que están configuradas en el controlador.
- 2. Haga clic en Nuevo para crear una nueva interfaz dinámica.
- En la ventana Interfaces > Nuevo, introduzca el nombre de la interfaz y el identificador de VLAN. A continuación, haga clic en Apply (Aplicar). En este ejemplo, la interfaz dinámica se denomina Office-VLAN y el ID de VLAN se asigna

Q • ○ • ⊡ ⊇ ☆ P	📌 😁 📀	\$ E							🧗 - 8 ×
cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Saye C COMMANDS	onfiguration <u>P</u> ing HELP	Logout Refresh
Controller	Interface	s > New						< Back	Apply
General Inventory	Interface	Name 0	ffice-VLAN						\smile
Interfaces Internal DHCP Server	VLAN Id	2	0						
Mobility Management Ports									
Master Controller Mode									
Network Time Protocol									
▶ QoS ▶ CDP									

4. En la ventana Interfaces > Edit, ingrese la dirección IP, la máscara de subred y el gateway predeterminado para la interfaz dinámica. Asígnela a un puerto físico del WLC e introduzca la dirección IP del servidor DHCP. A continuación, haga clic en Aplicar.

cisco		YLAN'S (ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Saya C COMMANDS	enfiguration <u>P</u> ing Loj HELP	gout <u>R</u> efrei
CISCO Controller General Inventory Interfaces Internal DHCP Server Mobility Management Ports Master Controller Mode Network Time Protocol QQS CDP	MONITOR M Interfaces > General Info Interface Nation MAC Address Interface Address Interface Address Netmask Gateway Physical Info Port Number	Edit ermation me s Idress ier	Office-V 00:06:0 20 172 255 172	WIRELESS		MANAGEMENT	COMMANDS	HELP	Apply
	Configuratio Quarantine DHCP Inform Primary DHC Secondary D Access Cont ACL Name Note: Changing temporarily disi some clients.	n P Server HCP Server rol List the Interfe abled and i	ar ner be parameters thus may result	16.1.75 causes the Wi in loss of conr]] LANs to be rectivity for				

Para este ejemplo, estos parámetros se utilizan para la interfaz Office-VLAN: Office-VLAN

```
IP address: 172.16.1.25
Netmask: 255.255.0.0
Default gateway: 172.16.1.75 (sub-interface on Router R1)
Port on WLC: 1
DHCP server: 172.16.1.75
```

Configure el WLC para Autenticar con Cisco Secure ACS

El WLC debe configurarse para reenviar las credenciales del usuario a un servidor RADIUS externo (en este caso, Cisco Secure ACS). Luego, el servidor RADIUS valida las credenciales del usuario y devuelve el atributo de nombre de ACL al WLC tras la autenticación exitosa del usuario inalámbrico.

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

- 1. Elija Seguridad y Autenticación RADIUS en la GUI del controlador para mostrar la página Servidores de Autenticación RADIUS. A continuación, haga clic en Nuevo para definir un servidor RADIUS.
- Defina los parámetros del servidor RADIUS en la página Servidores de autenticación RADIUS > Nuevo. Estos parámetros incluyen la dirección IP del servidor RADIUS, el secreto compartido, el número de puerto y el estado del servidor.

Security RADIUS Authentication Servers > New < Back AAA Server Index (Priority) I General Server Index (Priority) I Adhentication Server IPAddress 10.77.244.196 Accounting Server IPAddress 10.77.244.196 Accounting Shared Secret Format ASCII LDAP Shared Secret Shared Secret User Login Policies Shared Secret Image: Confirm Shared Secret User Login Policies Confirm Shared Secret Image: Confirm Shared Secret View Login Policies Secret Image: Confirm Shared Secret Priority Order Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server) Access Control Lists Port Number 1812 IPSec Certs Server Status Enabled Wireless Protection Policies Support for RFC 3576 Enabled Web Auth Support for RFC 3576 Enabled		m Eing	nfiguration HELP	COMMANDS	MANAGEMENT	SECURITY	LLER WIRELESS	WLANS CONTR	
AAA Server Index (Priority) 1 General RADius Server IPAddress Authentication Accession 10.77.244.196 Authentication Accession Server IPAddress Authentication Accession Server IPAddress IDAP Shared Secret Format ASCII Local Net Users Shared Secret Image: Confirm Shared Secret User Logn Policies Confirm Shared Secret Image: Confirm Shared Secret V Local EAP Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server) Priority Order Port Number 1012 IPSec Certs Server Status Enabled Wireless Protection Support for RFC 3576 Enabled Veb Auth Support for RFC 3576 Enabled	Apply	Back	< 8a				ervers > New	Authentication S	urity RADIU
Authentication Server IPAddress 10.77.244.196 Accounting Shared Secret Format ASCII IDAP Shared Secret Format ASCII LDAP Shared Secret Image: Shared Secret Format MAC Filtering Shared Secret Image: Shared Secret Format Disabled Clients Confirm Shared Secret Image: Secret Format Viser Login Policies Confirm Shared Secret Image: Secret Format Local EAP Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server) Priority Order Port Number 1812 IPSec Certs Server Status Imabled Imabled Wireless Protection Support for RFC 3576 Imabled Imabled Veb Auth Support for RFC 3576 Imabled Imabled CIDS Retransmit Timeout 20					_		1 💌	idex (Priority)	AA Server General RADIUS
Local Net Users Shared Secret MAC Filtering Shared Secret Disabled Clients Confirm Shared Just Logal Policies Secret > Local EAP Key Wrap > Priority Order (Designed for FIPS customers and requires a key wrap compliant RADIUS server) > Priority Order Port Number > IPSec Certs Server Status Wireless Protection Server Status Policies Support for RFC 3576 Enabled Enabled > CIDS Retransmit Timeout							ASCII •	ecret Format	Authentication Server Accounting TACACS+ Shared
User Login Policies AP Policies Local EAP Priority Order Priority Order Access Control Lists Port Number IPSec Certs Wireless Protection Policies Web Auth CIDS Retransmit Timeout Server Status Server Status Retransmit Timeout Server Status Server Status Serv							••••	ecret	Local Net Users MAC Filtering Shared Disabled Clients
> Local EAP Key Wrap Designed for FIPS customers and requires a key wrap compliant RADIUS server) > Priority Order Port Number 1812 > IPSec Certs Server Status Enabled Image: Compliant RADIUS server) > Wireless Protection Server Status Enabled Image: Compliant RADIUS server) > Web Auth CIDS Retransmit Timeout							•••••	Shared	User Login Policies Confirm AP Policies Secret
Access Control Lists Port Number 1812 IPSec Certs Server Status Enabled I Wireless Protection Support for RFC 3576 Enabled I Veb Auth Support for RFC 3576 Enabled I		; server)	RADIUS SE	y wrap complian	s and requires a ke	FIPS customer	(Designed for	P	ocal EAP Key Wr riority Order
IPSec Certs Server Status Enabled Wireless Protection Policies Support for RFC 3576 Enabled Web Auth CIDS Retransmit Timeout 30							1812	iber	ccess Control Lists Port Nu
Policies Support for RFC 3576 Enabled Web Auth CIDS Retransmit Timeout 20 seconds							Enabled x	tatus	PSec Certs Server
CIDS Retransmit Timeout 30 seconds							Enabled	for RFC 3576	olicies /eb Auth Suppor
No. Southas							30 seconds	nit Timeout	IDS Retran
Network User 🗵 Enable							Enable	User	Netwo
Management 🕅 Enable							🗷 Enable	nent	Manag
IPSec 🖸 Enable							🗇 Enable		IPSec

 Las casillas de verificación Usuario de red y Administración determinan si la autenticación basada en RADIUS se aplica a los usuarios de administración y de red. Este ejemplo utiliza Cisco Secure ACS como el servidor RADIUS con la dirección IP 10.77.244.196. Haga clic en Apply (Aplicar).

Cree una nueva WLAN para los usuarios inalámbricos

A continuación, debe crear una WLAN a la que los usuarios inalámbricos puedan conectarse. Para crear una nueva WLAN, complete estos pasos:

- 1. Desde la GUI del controlador de LAN inalámbrica, haga clic en WLAN. Esta página enumera las WLANs que existen en el controlador.
- Elija New para crear una nueva WLAN. Ingrese el ID de WLAN, el Nombre del Perfil y el SSID de WLAN para el WLAN, y haga clic en Aplicar. Para esta configuración, cree una oficina WLAN.

😋 • 🕑 • 💽 🖻 🏠	A 📌 🙆 🔕 🖗 🖉	920496,87			NO PARTY			🥂 – 8 ×
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	Sage Co COMMANDS	nfiguration <u>B</u> ing HELP	Logout Befresh
WLANs	WLANs > New						< Back	Apply
WLANS	WLAN ID	1 💌						
AP Groups VLAN	Profile Name	Office						
	WLAN SSID	Office						
]	

3. Una vez que crea una nueva WLAN, aparece la página WLAN > Edit para la nueva WLAN. En esta página, puede definir varios parámetros específicos de esta WLAN que incluyen políticas generales, seguridad, QoS y parámetros avanzados.

cisco	Sage Configuration Bing Logout Bet MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs	WLANs > Edit Apply
r WLANS WLANS AP Groups VLAN	General Security QoS Advanced Profile Name Office WLAN SSID Office WLAN Status F Enabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface office-vian BroadCast SSID F
	Faat Notes I CKIP is not supported by 10xx model APs 3 AREAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 5 Client MRP is not active unless WIPA2 is configured

Marque **Estado de WLAN** en Políticas generales para habilitar la WLAN. Elija la interfaz adecuada en el menú desplegable. En este ejemplo, utilice la interfaz **Office-vlan**. Los demás parámetros de esta página se pueden modificar según los requisitos de la red WLAN.

 Elija la ficha Seguridad. Elija 802.1x en el menú desplegable Seguridad de Capa 2 (ya que es una autenticación LEAP). Elija el tamaño de clave WEP adecuado en los parámetros 802.1x.

ANe	WI ANES Edit	Apple
/LANs WLANs AP Groups VLAN	General Security QoS Advanced Layer 2 Layer 3 AAA Servers	a p p n s
	Layer 2 Security 802.1X MAC Filtering 802.1X Parameters	
	802.11 Data Encryption Type Key Size	
	East Notes	
	1 CKIP is not supported by 10xx model APs 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded 5 Client MFP is not active unless WPA2 is configured	client

5. En la ficha Security (Seguridad), elija la subficha AAA server (Servidor AAA). Elija el servidor AAA que se utiliza para autenticar clientes inalámbricos. En este ejemplo, utilice el servidor ACS 10.77.244.196 para autenticar clientes inalámbricos.



 Elija la pestaña Avanzadas. Marque Allow AAA Override para configurar la invalidación de la política de usuario a través de AAA en una LAN inalámbrica.

cisco	Sage Configuration Bing Logout B MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS WLANS AP Groups VLAN	WLANs > Edit < Back Apply General Security QoS Advanced Allow AAA Override Enabled DHCP Override H-REAP Local Switching % Enabled DHCP & Coverride Override Session Timeout (secs) 1800 DHCP Addr. Assignment Required Aironet IE IF Enabled DHCP Addr. Assignment Required Override Interface ACL None Enabled Defrastructure MFP If (Global MFP Disabled) Override Interface ACL F Enabled MFP Client Optional Protection 1
	Foot Notes 1 CKIP is not supported by 10xx model APs 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients 5 Client MPP is not active unless WPA2 is configured

Cuando se habilita la invalidación de AAA y un cliente tiene parámetros de autenticación de LAN inalámbrica AAA y controlador de LAN inalámbrica de Cisco en conflicto, el servidor AAA realiza la autenticación del cliente. Como parte de esta autenticación, el sistema operativo mueve a los clientes de la VLAN LAN inalámbrica predeterminada de la solución LAN inalámbrica de Cisco a una VLAN devuelta por el servidor AAA y predefinida en la configuración de la interfaz del controlador LAN inalámbrico de Cisco, que sólo ocurre cuando se configura para el filtrado MAC, 802.1X y/o el funcionamiento WPA. En todos los casos, el sistema operativo también utiliza QoS, DSCP, valores de etiquetas de prioridad 802.1p y ACL proporcionados por el servidor AAA, siempre y cuando estén predefinidos en la configuración de la interfaz del controlador LAN inalámbrico de Cisco.

7. Elija los otros parámetros en función de los requisitos de la red. Haga clic en Apply (Aplicar).

Definir las ACL para los usuarios

Debe crear dos ACL para esta configuración:

• ACL1: Para proporcionar acceso al User1 al servidor solamente 172.16.1.100

• ACL2: Para proporcionar acceso al usuario 2 al servidor 172.16.1.50 solamente Complete estos pasos para configurar las ACL en el WLC:

- Desde la GUI del WLC, elija Security > Access Control Lists. Aparecerá la página Listas de control de acceso. Esta página enumera las ACL configuradas en el WLC. También le permite editar o quitar cualquiera de las ACL. Para crear una nueva ACL, haga clic en Nuevo.
- 2. Esta página le permite crear nuevas ACL. Ingrese el nombre de la ACL y haga clic en

Aplicar. Una vez que se crea la ACL, haga clic en Editar para crear reglas para la ACL.

3. El usuario1 sólo debe poder acceder al servidor 172.16.1.100 y se le debe denegar el acceso a todos los demás dispositivos. Para ello, debe definir estas reglas.Refiérase al <u>Ejemplo de Configuración de ACL en el Controlador de LAN Inalámbrico</u> para obtener más información sobre cómo configurar ACL en los Controladores de LAN Inalámbricos.

cisco	MONT	TOR W	LANS CONTR		WIRELESS	SE		MANAGEMENT	Saya C COMMANDS	onfiguration HELP	Eing	Logout R	ef
Security	Acce	ss Con	trol Lists > E	dit					< 6	lack	Add Nev	v Rule	I
General RADIUS	Gene	ral s List Nam	e User	L									
Accounting + TACACS+	Seq	Action	Source IP/M	ask	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction		
LDAP Local Net Users MAC Filtering	٦	Permit	172.16.0.0 255.255.0.0	/	172.16.1.100 255.255.255.255	′	Any	Any	Αογ	Any	Inbound		
Disabled Clients User Login Policies AP Policies	2	Permit	172.16.1.100 255.255.255.2	55	172.16.0.0 255.255.0.0	1	Any	Any	Any	Any	Outbound		
Local EAP	L												
Priority Order													
 Access Control Lists Access Control Lists CPU Access Control Lists 													
IPSec Certs													
Wireless Protection Policies													
Web Auth													
> CIDS													

 Del mismo modo, debe crear una ACL para el usuario 2, que permite el acceso del usuario 2 al servidor 172.16.1.50 solamente. Esta es la ACL requerida para User2.

cisco	MONI	TOR W	(LANs <u>C</u> O	NTROLI	LER	WIRELESS	SE	CURITY M	GNAGEMENT		HELP	Eing	Logout <u>R</u> efre
Security	Acce	ss Cor	ntrol Lists	> Edit						< 8.a	ck	Add New	v Rule
▼ AAA General ▼ RADIUS	Gene	ral s List Nam	ie l	lser2									
Authentication Accounting	Seq	Action	Source If	P/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	
LDAP Local Net Users MAC Filtering	4	Permit	172.16.0.0) , .0	1	172.16.1.50 255.255.255.255	, [/]	Any	Any	Απγ	Αηγ	Inbound	۰
Disabled Clients User Login Policies AP Policies	2	Permit	172.16.1.5 255.255.2	0 55.255	1	172.16.0.0 255.255.0.0	1	Any	Any	Any	Απγ	Outbound	٠
Local EAP													
Priority Order													
 Access Control Lists Access Control Lists CPU Access Control Lists 													
IPSec Certs													
Wireless Protection Policies													
▶ Web Auth													
▶ CIDS													

Ahora ha configurado el controlador de LAN inalámbrica para esta configuración. El siguiente paso es configurar el servidor Cisco Secure Access Control para autenticar a los clientes inalámbricos y devolver el atributo ACL Name al WLC tras la autenticación exitosa.

Configuración del servidor Cisco Secure ACS

Para que Cisco Secure ACS pueda autenticar clientes inalámbricos, debe completar estos pasos:

- Configure el Wireless LAN Controller como un cliente AAA en Cisco Secure ACS.
- Configure los usuarios y los perfiles de usuario en Cisco Secure ACS.

Configure el Wireless LAN Controller como Cliente AAA en Cisco Secure ACS

Para configurar el Wireless LAN Controller como cliente AAA en Cisco Secure ACS, complete estos pasos:

 Haga clic en Configuración de red > Agregar cliente AAA. Aparece la página Agregar cliente AAA. En esta página, defina el nombre del sistema WLC, la dirección IP de la interfaz de administración, Shared Secret y Authenticate Using Radius Airespace. Aquí tiene un ejemplo:

Cisco Systems	Network Configuration	×
ad brad bra	Edit	Help 🗧
User Setup Graup Setup Shared Profile Components Components Configuration Sprice Configuration	Add AAA Client AAA Client Hostname wlc AAA Client IP Address 10.77.244.210 Shared Secret cisco	AAA Client Hestmane AAA Client Hestmane AAA Client HE Address Shared Secret tistmark Device Group RADUIS Key Yman Authenticale Using Single Connect TACACS - AAA Client Log Update/Watchdeg Darkets from this AAA Client Log SADUIS Towneling Parkets from this AAA Client Replace RADUIS Devt info with Username from this AAA Client Mathentical IP-Address with user IP address IP-Address with user IP address IP-Address with user IP address IP-Address with user IP
Control External User Dutabases Posture Validation Network Access Reports and Reports and	Key Encryption Key Message Authenticator Code Key Key Input Format Authenticate Using RADIUS (Cisco Airespace)	AAA Client Hestname The AAA Client Hostnama is the name scripted to the AAA client. [Back to Top]
Ordine Documentation	Single Connect TACACS+ AAA Client (Record stop in accounting on failure) Log Update/Watchdog Packets from this AAA Client Log RADIUS Tunneling Packets from this AAA Client	AAA Client IP Address The AAA Client IP Address is the IP address assigned to the AAA client.
	Replace RADIUS Port info with Username from this AAA Client Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	If you want to designate more than one AAA client with a single AAA client entry in ACE, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press Enter.
	P Back to Help	You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.160.13.1

Nota: El secreto compartido configurado en Cisco Secure ACS debe coincidir con el secreto compartido configurado en el WLC bajo **Servidores de Autenticación RADIUS > Nuevo**.

2. Haga clic en Enviar+Aplicar.

Configuración del perfil de usuario y usuario en Cisco Secure ACS

Para configurar los usuarios en Cisco Secure ACS, complete estos pasos:

 Elija User Setup en la GUI de ACS, ingrese el nombre de usuario y haga clic en Add/Edit. En este ejemplo, el usuario es User1.



 Cuando aparezca la página Configuración de usuario, defina todos los parámetros específicos del usuario. En este ejemplo, se configuran el nombre de usuario, la contraseña, la información de usuario adicional y los atributos RADIUS porque sólo necesita estos parámetros para la autenticación EAP.

Cisco Systems	User Setup	×
adbodbo	Edit	Help
User Setup Group Setup	User: UserA (New User)	Account Disabled Deloting a Dormane Supplementary User Info Password Authentication From to which the user is assigned
Vergoneets Network Configuration System Configuration Interface Configuration	Supplementary User Info Real Name User 1 Description	Callback Client IP: Address Assignment Advanced Settings Network Access Restrictions Has Sessions Usage Ouelas Account Disable Downloadable ACLs Account Of Settings
Administration Centrel External User Databases Pestase Pestase Profiles	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)	TACACS - Enable Control TACACS - Enable Control TACACS - Enable Control TACACS - Duthousd Parsword TACACS - Self Contrant Authorization Control Authorization for Network Device Management Applications TACACS - Unknown Services IETE RADIUS Attributes RADIUS Yendor-Suecific Attributes
Reports and Activity Deline Documentation	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Confirm	Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account. [Rack to Tap] Deleting a Username
	Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.	The Delete botton appears only when you are editing an existing uper account, not when you are adding a new uper account. To delete the current user account from the database, click Delete. When asked to confirm your action, click DK. [Back to Top]
	Group to which the user is assigned: Submit Cancel	Supplementary User Info Type the applicable information in any supplemental user information borees that appear. To add or chance fields, click Interface Type the applicable information in any supplemental user information

Desplácese hacia abajo hasta que vea los atributos RADIUS de Cisco Airespace específicos para el usuario. Verifique el **Aire-ACL-Name** para habilitar el ACS para que devuelva el nombre ACL al WLC junto con la respuesta de autenticación exitosa. Para User1, cree una ACL User1 en el WLC. Introduzca el nombre de ACL como User1.

😋 • 🗇 • 💽 🖻	수 🕼 🚖 🗢 😓 🖬	🥂 – 8 ×
Cinco Systems	User Setup	X
dbdb	Date exceeds:	Help
User Setup Setup Setup Shared Profile Components Network Configuration Septem Configuration	Sep 9 2007 Failed attempts exceed: 5 Failed attempts since last successful login: 0 Reset current failed attempts count on submit	Account Disabled Belatina a Berniane Supplementary User Info Password Arthentication Grapp to which the user is assigned Callback Client IP Address Assignment Advanced Settings Natural Access Restrictions Max Session Brage Quartas Access Disable Downloadable ACLs
Administration Centrel Databases Postare Validation Wetwork Access Profile:	Cloce Airespace RADIUS Attributes	Advanced TACACS+ Settings TACACS+ Enable Control TACACS+ Enable Parsword TACACS+ Settleward Parsword TACACS+ Shell Command Authorization Command Authorization for Network Device Management Applications TACACS+ Unknown Services TACACS+ Unknown Services RADIUS Vendor: Specific Attributes
Reports and Activity Online Documentation	[14179/004] Aire-802.1P-T ag [0 [14179/005] Aire-Interface-Name [14179/006] Aire-AcLName [USer1 [14179/006] Aire-AcLName [USer1 [14179/006] Aire-AcLName [USer1 [14179/006] Aire-AcLName [USer1	Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account. [Ack to Ten] Deleting a Username The Delete buttos appears only when you are editing an emisting user account, not when you are adding a new user account. To delete the content, not when you are adding a new user account. To delete the content user account from the database, click Delete. When asked to confirm your action, click DK. [Eack to Ten] Supplementary User Info
	Submit Cancel	Type the applicable information in any supplemental user information boxes that appear. To add or chance fields, click Interface

3. Repita el mismo procedimiento para crear User2 como se muestra aquí.

Cisco Systems	User Setup				
-dlb-dlb-	Select	Help			
User Stared Profile Shared Profile </th <th>Select User: User2 Find Add/Edit List users beginning with letter/number: ABCPEFSSIIVYXXII QIIIISSIIVYXXII QIIIISS List all users Remove Dynamic Users 2 bek to Help</th> <th> Help Person and a factor of these Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rational Rationants Person a factor of the ACS Internal Rational Rationants Person a factor of the ACS Internal Rational Rationants Person ACS and the ACS Internal Rational Rationants Person ACS and the ACS Internal Rational Rationants Person Rationant Rationant Rationants Person Rationant Rationant Rationants Person Rationant Rationants Person Rationants Person Rationants Person Rationant Rationants Person Rationants<!--</th--></th>	Select User: User2 Find Add/Edit List users beginning with letter/number: ABCPEFSSIIVYXXII QIIIISSIIVYXXII QIIIISS List all users Remove Dynamic Users 2 bek to Help	 Help Person and a factor of these Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rational Rationants Person a factor of the ACS Internal Rational Rationants Person a factor of the ACS Internal Rational Rationants Person ACS and the ACS Internal Rational Rationants Person ACS and the ACS Internal Rational Rationants Person Rationant Rationant Rationants Person Rationant Rationant Rationants Person Rationant Rationants Person Rationants Person Rationants Person Rationant Rationants Person Rationants<!--</th-->			
0 · O · E E ·	 A ≠ € ⊗ 5 B 	🕅 - 5 ×			
Cisco Systems	User Setup	×			
adbad ba	Edit	Help E			
User Setup Group Setup Setup Setup Setup Setup Setup Configuration Setup Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration	User: UserA (New User) Account Disabled Supplementary User Info Real Name User2 Description User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS-	Account Disabled Beletima a Distributed Supplementary User Info Supplementary User Info Destroard Authentication Comp to which the user is assigned Calback Client IP Address Assignment Advanced Settings Network Access Restrictions Max Sessions Unage Quetas Network Access Restrictions Max Sessions Disable Aftact Advanced TACACS - Settings TACACS - Inable Password TACACS - Inable Password TACACS - Undersmod Password TACACS - RADIUS Attributes			
Reports and Activity Documentation	Password Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned: Submit Cancel	Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account. [hack to Tee] Deleting a Username The Delete buttos appears only when you are editing as existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When added to certifing your action, click OK. [hack to Tee] Supplementary User Info Type the applicable information in any supplemental user information			

🔕 • 😒 🖻 🗐	6 🖉 🔅 🗢 🔕 🖻	🕂 – 🕫 🕹 🖓 – 🖉
Cisco Systems	User Setup	X
-dbdb	Date exceeds:	Help 🗧
User Setup Greup Stap Shared Profile Composents Metwork Configuration Splem Configuration	Sep 9 2007 Failed attempts exceed: Failed attempts since last successful login: 0 Reset current failed attempts count on submit	Account Disabled Belisting a Unerganet Supplementary User Info Password Authon Scattin Group to which the user is assigned Callback Clean LIP Address Assignment; Advanced Settings Instruct Access Restrictions Han Sessions Using Operate Account Disable Downloadable Acts
Administration Centrel	Cisco Airespace RADIUS Antributes	Advanced TACACS+ Settings TACACS+ Settings TACACS+ Settings TACACS+ Factors
Pestareal User Databases Postare Validation Profile:	[14179/002] Aize-QoS-Level [8ronze [14179/003] Aize-DSCP [0	TACACS - Outbound Password TACACS + Shell Command Authorization Cammand Authorization for Network Device Management Applications TACACS + Unknown Specific For Network Device Management Applications TACACS + Unknown RADIUS Yeador-Specific Attributes
Reports and Activity	[14179404] Aire-802.1P-Tag	Account Disabled Status
Documentation	[14179'005] Aize-Interface-Name	Select the Account Disabled check box to disable this account; clear the check box to enable the account.
(14179006) Aize-Act.Nane	Defeting a Vername
		The Delete button appears only when you are editing an existing user account, not whon you are adding a new user account. To delete the current user account from the database, click Delete . When asked to confirm your action, click CK .
	💡 Back to Melp	[Back to Tap]
		Supplementary User Info
	Submit Cancel	Type the applicable information in any supplemental user information

4. Haga clic en Configuración del sistema y Configuración de autenticación global para asegurarse de que el servidor de autenticación esté configurado para realizar el método de autenticación EAP deseado. En la configuración EAP, elija el método EAP adecuado. Este ejemplo utiliza autenticación LEAP. Haga clic en Enviar cuando haya terminado.

😋 • 😔 - 🖻 🖻	수 1 · · · · · · · · · · · · · · · · · ·	🕂 – 8 ×
Cisco Sestens	System Configuration	×
	PEAP	🚔 Help 🏠
User	Allow EAP-MSCHAPv2	
CGIsseab	Allow EAP-GTC	Use this page to specify settings for various authentication protocols.
Graup Setup	C Allow Posture Validation	EAD Configuration
Shared Profile Components	Allow EAP-TLS	EAP-FAST
Paul Network	Select one or more of the following options:	• LEAP
Configuration	F Certificate SAN comparison	• EAP-HOS
Sasten Sasten	I Certificate CN comparison	APLAP Regest Intent HS-CHAP Configuration
- Mill courses actor	F Certificate Binary comparison	
Configuration	EAP-TI S session timeout (minutes): 120	
Administration		EAP Configuration
	Cisco client initial message:	EAP is a flexible request-response protocol for arbitrary
Databases	PEAP session timeout (minutes): 120	authentication information (RPC 2204). EAP is layered on top of another protocol such as UDP, 802.1x or RADIUS and supports
[mana] Pestere	Cuble Fact Descent	multiple "authentication" types.
Const Validation	Enable Fast Reconnect: IP	iback to Teol
Profile:	EAP-FAST	PEAD
Reports and	EAP-EAST Configuration	
Activity		PEAP is the euter layer protocol for the secure tunnel.
Documentation	EAP-TLS	the static section had also been at the
	Allow EAP-TLS	authentication can occur only after you have completed the required steps
	Select one or more of the following options:	to the ACS Centificate Setup page.
	M Certificate SAN comparison	Allow EAP-MSCHAPv2 - Use to anable EAP-MSCHAPv2 within MS PEAP
	R Certificate CN comparison	authentication. Enable this protocol for any repository that supports MS+ CHAPv2, such as Microsoft AD, and the ACS Internal Database.
	Rectificate Binary comparison	
	EAP-TLS session timeout (minutes): 120	 Allow EAP-GTC — Use to enable EAP-GTC within Cisce PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.
-	LEAP	Allow Porture Validation Use to snakle the PEAP (EAP-TLV) anotacal for
	Allow LEAP (For Aironet only)	· posture validation of Hetwork Admission Control (NAC) clients.
	Submit Submit + Restart Cancel	 Allow EAP-TLS - Use to enable the EAP-TLS protocol as an additional inner method for PEAP. The PEAP/EAP-TLS feature stocody leverage the existing *

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Intente asociar un cliente inalámbrico con el Lightweight AP con la autenticación LEAP para verificar si la configuración funciona como se esperaba.

Nota: Este documento asume que el perfil del cliente está configurado para la autenticación LEAP. Refiérase a <u>Uso de la Autenticación EAP</u> para obtener más información sobre cómo configurar el 802.11 a/b/g Wireless Client Adapter para la autenticación LEAP.

Una vez que se activa el perfil del cliente inalámbrico, se solicita al usuario que proporcione el nombre de usuario/contraseña para la autenticación LEAP. Esto es lo que sucede cuando el usuario1 intenta autenticarse en el LAP.

Enter Wireless Network Password			
Please enter your LE network	AP username and password to log on to the wireless		
User Name :	User1		
Password :	•••••		
Log on to :			
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter		
Profile Name :	Office OK Cancel		

El Lightweight AP y luego el WLC transfieren las credenciales del usuario al servidor RADIUS externo (Cisco Secure ACS) para validar las credenciales. El servidor RADIUS compara los datos con la base de datos del usuario y, tras la autenticación exitosa, devuelve el nombre ACL configurado para el usuario al WLC. En este caso, la ACL User1 se devuelve al WLC.

Cisco Aironet Desktop Utilit	y - Current Profile	: Office-TSWEB	2×
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
nullinullin Profile Name:	Office-TSWEB		
Link Status:	Authenticated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 64	
Server Based Authentication:	LEAP	Data Encryption: WEP	
IP Address:	172.16.0.14		
Signal Strength:		Excellent	
		Advanced	
	TE BIKU HUHUHUHU KU		

El controlador de LAN inalámbrica aplica esta ACL al usuario1. Esta salida de ping muestra que User1 sólo puede acceder al servidor 172.16.1.100, pero no a ningún otro dispositivo.

```
D:\Documents and Settings\Administrator>ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time=3ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 3ms, Average = 1ms
D:\Documents and Settings\Administrator>ping 172.16.1.50
Pinging 172.16.1.50 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

De manera similar, cuando el usuario 2 intenta acceder a la WLAN, el servidor RADIUS, tras la autenticación exitosa, devuelve el usuario de ACL2 al WLC.

Enter Wireless Network Password		
Please enter your LE network	AP username and password to log on to the wireless	
User Name :	User2	
Password :	•••••	
Log on to :		
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter	
Profile Name :	Office	
	OK Cancel	

Authentication Status	? - 🗆
Card Name: Cisco Aironet 802.1	1a/b/g Wireless Adapter
Profile Name: Office-TSWEB	
Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Skipped because the domain name was not configured

El controlador de LAN inalámbrica aplica esta ACL al usuario 2. Esta salida de ping muestra que el usuario 2 sólo puede acceder al servidor 172.16.1.50, pero no a ningún otro dispositivo.

```
D:\Documents and Settings\Administrator>ping 172.16.1.50
Pinging 172.16.1.50 with 32 bytes of data:
Reply from 172.16.1.50: bytes=32 time=3ms TTL=255
Reply from 172.16.1.50: bytes=32 time=18ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Ping statistics for 172.16.1.50:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 18ms, Average = 5ms
D:\Documents and Settings\Administrator>ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Troubleshoot

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

En Wireless LAN Controller, también puede utilizar estos comandos debug para resolver problemas de autenticación AAA

- debug aaa all enable: configura el debug de todos los mensajes AAA
- debug dot1x packet enable: habilita la depuración de todos los paquetes dot1x
- debug client <MAC Address> —Habilita la depuración del cliente inalámbrico

Este es un ejemplo del comando debug aaa all enable

Nota: Algunas de las líneas de la salida se han movido a la segunda línea debido a restricciones de espacio.

```
Thu Aug 16 14:42:54 2007: AuthenticationReguest: 0xblab104

      Thu Aug 16 14:42:54 2007:
      Callback.....0x85ed228

      Thu Aug 16 14:42:54 2007:
      protocolType....0x00140001

Thu Aug 16 14:42:54 2007:

      Thu Aug 16 14:42:54 2007:
      proxyState.....00:40:96:AF:3E:93-03:01

      Thu Aug 16 14:42:54 2007:
      Packet contains 16 AVPs (not shown)

Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet
   (id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99 b4 19 27 28 eb 5f 35 9c
   ....-4.....'(._5.
Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73 65 72 31 1f 13 30 30 2d
   .....user1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46 2d 33 45 2d 39 33 1e 20
  40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35 2d 35 42 2d 46 42 2d 44
  00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65 2d 54 53 57 45 42 05 06
   0:Office-TSWEB..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1a
   .....M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00 00 01 06 06 00 00 00
  ...7c.....
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d 06 00 00 13 40 06 00
   . . . . . . . = . . . . . @ . .
Thu Aug 16 14:42:54 2007: 0000080: 00 00 0d 41 06 00 00 00 06 51 04 32 30 4f 27 02
   ....Q.200'.
Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d 87 9d 0b f9 dd e5 39 0d
   Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96 dc c3 55 ff 7c 51 4e 75
  .....#....U.|QNu
Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56 43 3d 30 2e 31 3b 50 12
   ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0 c6 2f 5e f5 65 e9 3e 2d
   ..;5<sup>^</sup>..../<sup>^</sup>.e.>-
Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4 27 e6 d4 0e 1b 8e 5d 19
  ...6.1j.'....].
Thu Aug 16 14:42:54 2007: 00000010: 60 lc c2 16 4f 06 03 01 00 04 18 0a 53 56 43 3d
   ....O.....SVC=
Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb 90 ec 48 9b fb d7 ce ca
   0.1;P.1...H....
Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09
                                                             ;d...
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=11
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=11
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Access-Challenge received from RADIUS server
   10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007: structureSize.....104
                               resultCode.....255
Thu Aug 16 14:42:54 2007:
Thu Aug 16 14:42:54 2007:
                               protocolUsed.....0x0000001
Thu Aug 16 14:42:54 2007:
                               proxyState....
  00:40:96:AF:3E:93-03:01
```

Thu Aug 16 14:42:54 2007: Packet contains 3 AVPs (not shown) Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xblab104 Thu Aug 16 14:42:54 2007: Callback.....0x85ed228 Thu Aug 16 14:42:54 2007: protocolType.....0x00140001 Thu Aug 16 14:42:54 2007: proxyState..... 00:40:96:AF:3E:93-03:02 Thu Aug 16 14:42:54 2007: Packet contains 16 AVPs (not shown) Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Successful transmission of Authentication Packet (id 2) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00 Thu Aug 16 14:42:54 2007: 00000000: 01 02 00 c0 38 b6 b2 20 ff 5b f2 16 64 df 02 618....[..d..a Thu Aug 16 14:42:54 2007: 00000010: cf f5 93 4b 01 07 75 73 65 72 31 1f 13 30 30 2d ...K..User1..00-Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46 2d 33 45 2d 39 33 1e 20 40-96-AF-3E-93.. Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35 2d 35 42 2d 46 42 2d 44 00-0B-85-5B-FB-D Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65 2d 54 53 57 45 42 05 06 0:Office.. Thu Aug 16 14:42:54 2007: 00000050: 00 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1aM....wlc. Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00 00 01 06 06 00 00 00 ...7c.... Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d 06 00 00 01 13 40 06 00 = @ . . Thu Aug 16 14:42:54 2007: 0000080: 00 00 0d 41 06 00 00 06 51 04 32 30 4f 17 01 ...A....Q.200.. Thu Aug 16 14:42:54 2007: 00000090: 01 00 15 11 01 00 08 0f 14 05 65 1b 28 61 c9 75e.(a.u Thu Aug 16 14:42:54 2007: 000000a0: 73 65 72 31 18 0a 53 56 43 3d 30 2e 31 3b 50 12 ser1..SVC=0.1;P. Thu Aug 16 14:42:54 2007: 000000b0: 05 ba 6b af fe a4 b0 d1 a2 94 f8 39 80 ca 3c 96 Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8 6c 07 8e fb 58 84 8d f6=].1...X... Thu Aug 16 14:42:54 2007: 00000010: 33 6d 93 21 08 06 ff ff ff ff 4f 27 02 01 00 25 3m.!...8 Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 1e 33 b5 4e 69 90 e7 84 25% Thu Aug 16 14:42:54 2007: 00000030: 42 a9 20 ac 84 33 9f 87 ca dc c9 b3 75 73 65 72 B....3....user Thu Aug 16 14:42:54 2007: 00000040: 31 1a 3b 00 00 00 09 01 35 6c 65 61 70 3a 73 65 1.;....5leap:se Thu Aug 16 14:42:54 2007: 00000050: 73 73 69 6f 6e 2d 6b 65 79 3d 29 80 1d 2c 1c 85 ssion-key=).... Thu Aug 16 14:42:54 2007: 00000060: db 1c 29 7e 40 8a b8 93 69 2a 55 d2 e5 46 89 8b ...)~@...i*U..F.. Thu Aug 16 14:42:54 2007: 00000070: 2c 3b 65 49 3e 44 cf 7e 95 29 47 54 1a 1f 00 00 ,;eI>D.~.)GT.... Thu Aug 16 14:42:54 2007: 0000080: 00 09 01 19 61 75 74 68 2d 61 6c 67 6f 2d 74 79auth-algo-ty Thu Aug 16 14:42:54 2007: 00000090: 70 65 3d 65 61 70 2d 6c 65 61 70 1a 0d 00 00 37 pe=eap-leap....7 Thu Aug 16 14:42:54 2007: 000000a0: 63 06 07 55 73 65 72 31 19 14 43 41 43 53 3a 30 c..User1..CACS:0 Thu Aug 16 14:42:54 2007: 000000b0: 2f 39 2f 61 34 64 66 34 64 32 2f 31 50 12 9a 71 /9/a4df4d2/1P..q Thu Aug 16 14:42:54 2007: 000000c0: 09 99 7d 74 89 ad af e5 c8 b1 71 94 97 d1 ..}t....q... Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=2 Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=2 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93

Access-Accept received from RADIUS server

10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3 Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800 Thu Aug 16 14:42:54 2007: structureSize.....236 Thu Aug 16 14:42:54 2007: resultCode.....0 Thu Aug 16 14:42:54 2007: protocolUsed.....0x0 0000001 Thu Aug 16 14:42:54 2007: proxyState.....00: 40:96:AF:3E:93-03:02 Thu Aug 16 14:42:54 2007: Packet contains 6 AVPs: Thu Aug 16 14:42:54 2007: AVP[01] Framed-IP-Address.....0xffffffff (-1) (4 bytes) Thu Aug 16 14:42:54 2007: AVP[02] EAP-Message.....DATA (37 bytes) Thu Aug 16 14:42:54 2007: AVP[03] Cisco / LEAP-Session-Key...DATA (16 bytes) Thu Aug 16 14:42:54 2007: AVP[04] Airespace / ACL-Name.....User1 (5 bytes) Thu Aug 16 14:42:54 2007: AVP[05] Class.....CACS:0/9/a4df4d2/1 (18 bytes) Thu Aug 16 14:42:54 2007: AVP[06] Message-Authenticator.....DATA (16 bytes) Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Applying new AAA override for station 00:40:96:af:3e:93 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Override values for station 00:40:96:af:3e:93 source: 4, valid bits: 0x400 gosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName:User1 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Inserting new RADIUS override into chain for station 00:40:96:af:3e:93

Puede utilizar una combinación del comando **show wlan summary** para reconocer cuál de sus WLAN emplea autenticación del servidor RADIUS. A continuación, puede ver el comando **show client summary** para ver qué direcciones MAC (clientes) se autentican correctamente en las WLAN RADIUS. También puede relacionar esto con los registros de intentos fallidos o intentos fallidos de Cisco Secure ACS.

Cisco recomienda que pruebe las configuraciones de ACL con un cliente inalámbrico para asegurarse de que las ha configurado correctamente. Si no funcionan correctamente, verifique las ACL en la página web de ACL y verifique que los cambios de ACL se hayan aplicado a la interfaz del controlador.

También puede utilizar estos comandos show para verificar su configuración:

 show acl summary: para mostrar las ACL configuradas en el controlador, utilice el comando show acl summary.

Aquí tiene un ejemplo:

(Cisco Controller)	>show acl	summary
ACL Name		Applied
Userl		Yes
User2		Yes

• show acl detailed <ACL_Name>: muestra información detallada sobre las ACL

configuradas.Aquí tiene un ejemplo:**Nota:** Algunas de las líneas de la salida se han movido a la segunda línea debido a restricciones de espacio.

Source Destination Source Port Dest Port I Dir IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action __ ___ ____ _____ ____ ____ 1 In 172.16.0.0/255.255.0.0 172.16.1.100/255.255.255.255 Any 0-65535 0-65535 Any Permit 2 Out 172.16.1.100/255.255.255 172.16.0.0/255.255.0.0 Any 0-65535 0-65535 Any Permit (Cisco Controller) >show acl detailed User2 Source Destination Source Port Dest Port I Dir IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action __ ___ ____ ---- ----- ----- -----1 In 172.16.0.0/255.255.0.0 172.16.1.50/255.255.255 0-65535 0-65535 Any Permit Anv 2 Out 172.16.1.50/255.255.255.255 172.16.0.0/255.255.0.0 Any 0-65535 0-65535 Any Permit

Cisco Controller) >show acl detailed User1

 show client detail <MAC Address of the client> - Muestra información detallada sobre el cliente inalámbrico.

Consejos de Troubleshooting

Utilice estos consejos para resolver problemas:

- Verifique en el controlador que el servidor RADIUS está en estado activo y no en modo de espera o desactivado.
- En el controlador, verifique si el servidor RADIUS se elige en el menú desplegable de la WLAN (SSID).
- Verifique si el servidor RADIUS recibe y valida la solicitud de autenticación del cliente inalámbrico.
- Verifique los informes de Autenticaciones Pasadas e Intentos Fallidos en el servidor ACS para lograr esto. Estos informes están disponibles en Informes y actividades en el servidor ACS.

Información Relacionada

- ACL en Controladores de LAN Inalámbricos: Reglas, limitaciones y ejemplos
- Ejemplo de Configuración de ACL en el Controlador de LAN Inalámbrica
- Ejemplo de Configuración de Filtros MAC con Controladores de LAN Inalámbricos (WLC)
- Guía de configuración del controlador inalámbrico de LAN de Cisco, versión 5.2
- 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).