Ejemplo de Restringir Acceso WLAN Basado en SSID con WLC y Cisco Secure ACS Configuration

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Antecedentes Configuración de la red Configurar Configurar la WLC Configurar la WLC Configura el cliente inalámbrico y verifique Troubleshoot Comandos para resolución de problemas Información Relacionada

Introducción

Este documento proporciona un ejemplo de configuración para restringir el acceso por usuario a una WLAN basada en el SSID (Service Set Identifier).

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar el controlador de LAN inalámbrica (WLC) y el punto de acceso ligero (LAP) para el funcionamiento básico
- Conocimientos básicos sobre cómo configurar Cisco Secure Access Control Server (ACS)
- Conocimiento del protocolo de punto de acceso ligero (LWAPP) y de los métodos de seguridad inalámbrica

Componentes Utilizados

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

- WLC de la serie 2000 de Cisco que ejecuta firmware 4.0
- LAP de la serie 1000 de Cisco
- Cisco Secure ACS Server versión 3.2
- Adaptador de cliente inalámbrico Cisco 802.11a/b/g que ejecuta firmware 2.6
- Cisco Aironet Desktop Utility (ADU) versión 2.6

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

<u>Antecedentes</u>

Con el uso del acceso WLAN basado en SSID, los usuarios pueden ser autenticados según el SSID que utilizan para conectarse a la WLAN. El servidor Cisco Secure ACS se utiliza para autenticar a los usuarios. La autenticación ocurre en dos etapas en Cisco Secure ACS:

- 1. autenticación EAP
- 2. Autenticación SSID basada en las restricciones de acceso a la red (NAR) en Cisco Secure ACS

Si la autenticación basada en EAP y SSID se realiza correctamente, el usuario puede acceder a la WLAN o, de lo contrario, el usuario se desasocia.

Cisco Secure ACS utiliza la función NARs para restringir el acceso del usuario en función del SSID. Un NAR es una definición que se hace en Cisco Secure ACS de condiciones adicionales que se deben cumplir antes de que un usuario pueda acceder a la red. Cisco Secure ACS aplica estas condiciones usando la información de los atributos enviados por sus clientes AAA. Aunque hay varias maneras de configurar los NAR, todos se basan en la información de atributo coincidente enviada por el cliente AAA. Por lo tanto, debe entender el formato y el contenido de los atributos que sus clientes AAA envían si desea emplear NAR efectivos.

Al configurar un NAR, puede elegir si el filtro funciona positiva o negativamente. Es decir, en el NAR se especifica si se permite o deniega el acceso a la red, en base a una comparación de la información enviada por los clientes AAA a la información almacenada en el NAR. Sin embargo, si un NAR no encuentra información suficiente para funcionar, de forma predeterminada se deniega el acceso.

Puede definir un NAR para un usuario o grupo de usuarios específico y aplicarlo a él. Refiérase al <u>Informe Técnico sobre Restricciones de Acceso a la Red</u> para obtener más información.

Cisco Secure ACS admite dos tipos de filtros NAR:

1. Filtros basados en IP: los filtros NAR basados en IP limitan el acceso según las direcciones IP del cliente de usuario final y el cliente AAA. Consulte <u>Acerca de los Filtros NAR basados</u>

en IP para obtener más información sobre este tipo de filtro NAR.

2. Filtros no basados en IP: los filtros NAR no basados en IP limitan el acceso basándose en la comparación simple de cadenas de un valor enviado desde el cliente AAA. El valor puede ser el número de ID de línea de llamada (CLI), el número de servicio de identificación de número marcado (DNIS), la dirección MAC u otro valor que se origine en el cliente. Para que este tipo de NAR funcione, el valor en la descripción de NAR debe coincidir exactamente con lo que se envía desde el cliente, incluido el formato que se utilice. Por ejemplo, (217) 555-4534 no coincide con 217-555-4534. Refiérase a Acerca de los Filtros NAR No Basados en IP para obtener más información sobre este tipo de filtro NAR.

Este documento utiliza los filtros no basados en IP para realizar la autenticación basada en SSID. Un filtro NAR no basado en IP (es decir, un filtro NAR basado en DNIS/CLI) es una lista de ubicaciones de punto de acceso/llamada permitidas o denegadas que puede utilizar en la restricción de un cliente AAA cuando no tiene una conexión basada en IP establecida. La función NAR no basada en IP generalmente utiliza el número CLI y el número DNIS. Hay excepciones en el uso de los campos DNIS/CLI. Puede introducir el nombre SSID en el campo DNIS y realizar una autenticación basada en SSID. Esto se debe a que el WLC envía en el atributo DNIS, el nombre SSID, al servidor RADIUS. Por lo tanto, si genera DNIS NAR en el usuario o en el grupo, puede crear restricciones SSID por usuario.

Si utiliza RADIUS, los campos NAR enumerados aquí utilizan estos valores:

- Cliente AAA: se utiliza NAS-IP-address (atributo 4) o, si no existe NAS-IP-address, NAS-identificador (atributo RADIUS 32).
- **Puerto**: se utiliza el puerto NAS (atributo 5) o, si el puerto NAS no existe, el ID de puerto NAS (atributo 87).
- CLI: se utiliza el identificador de estación de llamada (atributo 31).
- DNIS: se utiliza el ID de estación llamada (atributo 30).

Refiérase a <u>Restricciones de Acceso a la Red</u> para obtener más información sobre el uso de NAR.

Dado que el WLC envía en el atributo DNIS y el nombre SSID, puede crear restricciones SSID por usuario. En el caso del WLC, los campos NAR tienen estos valores:

- Cliente AAA: dirección IP WLC
- puerto —*
- CLI —*
- DNIS:*nombre de usuario

El resto de este documento proporciona un ejemplo de configuración sobre cómo lograr esto.

Configuración de la red

En este ejemplo de configuración, el WLC se registra en el LAP. Se utilizan dos WLAN. Una WLAN es para los usuarios del departamento de administración y la otra para los usuarios del departamento de ventas. Los clientes inalámbricos A1 (usuario administrador) y S1 (usuario de ventas) se conectan a la red inalámbrica. Debe configurar el WLC y el servidor RADIUS de tal manera que el usuario administrador A1 pueda acceder solamente al **administrador** de WLAN y se le restrinja el acceso a las **ventas de** WLAN y el usuario de ventas S1 debería poder acceder a las **ventas de la WLAN** y debería tener acceso restringido al **administrador de la WLAN**. Todos los usuarios utilizan la autenticación LEAP como método de autenticación de Capa 2.

Nota: Este documento asume que el WLC está registrado en el controlador. Si es nuevo en el WLC y no sabe cómo configurar el WLC para el funcionamiento básico, consulte <u>Registro del</u> <u>Lightweight AP (LAP) en un Wireless LAN Controller (WLC)</u>.



WLC Management Interface IP address : 172.16.1.30/16 WLC AP-Manager Interface IP address: 172.16.1.31/16 Cisco Secure ACS server IP address: 172.16.1.60/16

SSID for the Admin department users : Admin SSID for Sales department users: Sales

Configurar

Para configurar los dispositivos para esta configuración, debe:

- 1. Configure el WLC para los dos WLANs y el servidor RADIUS.
- 2. Configure Cisco Secure ACS.
- 3. Configure los clientes inalámbricos y verifique.

Configurar la WLC

Complete estos pasos para configurar el WLC para esta configuración:

 El WLC debe configurarse para reenviar las credenciales del usuario a un servidor RADIUS externo. El servidor RADIUS externo (Cisco Secure ACS en este caso) valida las credenciales del usuario y proporciona acceso a los clientes inalámbricos. Complete estos pasos:Elija Security > RADIUS Authentication en la GUI del controlador para mostrar la página RADIUS Authentication Servers

3 · 3 · 2	🚯 🔎 👷 🧭 🍰 * Address 🔊 https://172.16.1.30/screens/fre 🗹 🔂 Go 🛛 Links ** Norton Antibinus 🚱 • 🦓 – 6 ×
Enses Storres	Save Configuration Ping Logout Refresh MONITOR WEAK: CONTROLLER WIRELESS SECTIPITY MANAGEMENT COMMANDS HELD
Security	RADIUS Authentication Servers Apply New
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Call Station ID Type IP Address 💌 Credentials Caching 📄 Use AES Key Wrap 📄 Network User Management Server Index Server Address Port Admin Status
Access Control Lists	
Web Auth Certificate	
Wireless Protection Policies Trusted AP Policies Roque Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	
Web Login Page	
CIDS Sensors Shunned Clients	
https://172.16.1.30/screens/h	rameSecurity.html 🔒 🕲 Internet

Haga clic en **Nuevo** para definir los parámetros del servidor RADIUS.Estos parámetros incluyen la dirección IP del servidor RADIUS, el secreto compartido, el número de puerto y el estado del servidor. Las casillas de verificación Network User and Management determinan si la autenticación basada en RADIUS se aplica a los usuarios de red y de administración. Este ejemplo utiliza Cisco Secure ACS como el servidor RADIUS con la dirección IP 172.16.1.60.

	@ / % @ @ @	Address 🕘 https://172.16.1.30/screens/frc 🌱 🛃 Go	Save Configuration Ping Logout Refres
A	MONITOR WLANS CONTR	OLLER WIRELESS SECURITY MANAGEMENT	COMMANDS HELP
Security	RADIUS Authentication Ser	rvers > New	< Back Apply
AAA General	Server Index (Priority)	1	
RADIUS Authentication RADIUS Accounting	Server IPAddress	172.16.1.60	
MAC Filtering Disabled Clients	Shared Secret Format	ASCII 💌	
User Login Policies AP Policies	Shared Secret	•••••	
Access Control Lists	Confirm Shared	[
Web Auth Certificate	Secret		
Wireless Protection Policies	Key Wrap		
Rogue Policies Standard Signatures	Port Number	1812	
Custom Signatures Signature Events	Server Status	Enabled 💌	
Client Exclusion Policies AP Authentication / MFP	Support for RFC 3576	Enabled 💌	
Protection	Retransmit Timeout	2 seconds	
Web Login Page			
CIDS	Network User	🗹 Enable	
Shunned Clients	Management	Enable	
A	<u>.</u>		A

Haga clic en Apply (Aplicar).

2. Configure una WLAN para el departamento de administración con SSID Admin y la otra WLAN para el departamento de ventas con SSID Sales. Para hacerlo, complete estos pasos:Haga clic en WLAN en la GUI para crear una WLAN. Aparece la ventana WLAN. Esta ventana enumera las WLAN configuradas en el controlador.Haga clic en Nuevo para configurar una WLAN nueva.Este ejemplo crea una WLAN denominada Admin para el departamento Admin y el ID de WLAN es 1. Haga clic en Apply (Aplicar).



En la ventana **WLAN > Edit**, defina los parámetros específicos de la WLAN:En el menú desplegable Layer 2 Security , seleccione **802.1x**. De forma predeterminada, la opción de seguridad de capa 2 es 802.1x. Esto habilita la autenticación 802.1x/EAP para la WLAN.En Políticas generales, marque la casilla **invalidación AAA**. Cuando se habilita la invalidación de AAA y un cliente tiene parámetros de autenticación de AAA y WLAN del controlador en conflicto, el servidor AAA realiza la autenticación del cliente.Seleccione el servidor RADIUS adecuado en el menú desplegable en Servidores RADIUS. Los otros parámetros se pueden modificar en función de los requisitos de la red WLAN. Haga clic en Apply (Aplicar).



Del mismo modo, para crear una WLAN para el departamento de ventas, repita los pasos b y c. Estas son las capturas de pantalla.



Configuración de Cisco Secure ACS

En el servidor Cisco Secure ACS, debe:

- 1. Configure el WLC como un cliente AAA.
- 2. Cree la base de datos de usuario y defina NAR para la autenticación basada en SSID.
- 3. Habilite la autenticación EAP.

Complete estos pasos en Cisco Secure ACS:

1. Para definir el controlador como un cliente AAA en el servidor ACS, haga clic en **Configuración de Red** desde la GUI ACS. Bajo AAA los clientes hacen clic en **Add Entry**.

CISCO SYSTEMS	Network Configura	ation	
autilities at the second s	Select		
User Setup			
Group Setup	% Q	AAA Clients	3
Shared Profile Components	AAA Client Hostname	AAA Client IP Address	Authenticate Using
Network Configuration		None Defined	
System Configuration		Add Entry Search	
Configuration			
Administration Control	℃	AAA Servers	2
18 External User	AAA Server Name	AAA Server IP Address	AAA Server Type
913 Databases	tsweb-laptop	127.0.0.1	CiscoSecure ACS
Posture Validation		Add Entry Search	
Reports and Activity		💡 Back to Help	
Documentation			

 Cuando aparezca la página Network Configuration (Configuración de red), defina el nombre del WLC, la dirección IP, el secreto compartido y el método de autenticación (RADIUS Cisco Airespace).

- 3. Haga clic en **User Setup** desde la GUI de ACS, ingrese el nombre de usuario y haga clic en **Add/Edit**. En este ejemplo, el usuario es A1.
- 4. Cuando aparezca la página User Setup (Configuración de usuario), defina todos los parámetros específicos del usuario. En este ejemplo se configuran el nombre de usuario, la contraseña y la información de usuario adicional porque necesita estos parámetros para la autenticación LEAP.

CISCO SYSTEMS	User Setup
- مىئالالىسىيالالىس	Edit
User Setup	Henry A1 (New Henry)
Group Setup	User: AI (New User)
Shared Profile Components	Account Disabled
Network Configuration	Supplementary User Info ?
System Configuration	Real Name A1
Interface Configuration	Description Admin Department User
Administration Control	<u>.</u>
Databases	User Setup
ourre onno Validation	Password Authentication:
Network Access	ACS Internal Database
Profiles	CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)
Activity	Password *****
Online Documentation	Confirm ****** Password
	Separate (CHAP/MS-CHAP/ARAP)
	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

- 5. Desplácese por la página User Setup (Configuración de usuario) hasta que vea la sección Network Access Restrictions (Restricciones de acceso a la red). En la interfaz de usuario de DNIS/CLI Access Restriction, seleccione **Permitted Calling/ Point of Access Locations** y defina estos parámetros:**Cliente AAA**: dirección IP WLC (172.16.1.30 en nuestro ejemplo)**Puerto**—***CLI**:***DNIS**:*nombre de usuario
- 6. El atributo DNIS define el SSID al que el usuario puede acceder. El WLC envía el SSID en el atributo DNIS al servidor RADIUS.Si el usuario necesita acceder sólo a la WLAN denominada Admin, ingrese *Admin para el campo DNIS. Esto asegura que el usuario sólo tenga acceso a la WLAN denominada Admin. Haga clic en Enter.Nota: El SSID siempre debe ir precedido de *. Es obligatorio.

User Setup



- Ulcon

Advanced Settings

Group Setup	Network Access Restrictions (NAR)	3
Shared Profile Components	Define IP-based access restrictions	
Network	Table Defines : Permitted Calling/Point of Access Locations	
Configuration	AAA Client Port Address	
System Configuration		
Interface Configuration		
Administration Control	remove.	
ixternal User	AAA Client All AAA Clients	
ibases	Port	
ion	enter	
cess		
ts and tu	Define CLI/DNIS-based access restrictions	
	Table Defines : Permitted Calling/Point of Access Locations •	
tion	AAA Client Port CLI DNIS	
	remove	
	A CALLER AND THE REPORT OF THE	
	Port *	
	Port ×	
	Port CLI Addmin	

- 7. Haga clic en Submit (Enviar).
- 8. Del mismo modo, cree un usuario para el usuario del departamento de ventas. Estas son las capturas de pantalla.

CISCO SYSTEMS	User Setup
	Edit
User Setup	llcor: S1 (Now llcor)
Setup	USEL SI (New USEL)
Shared Profile Components	Account Disabled
Network Configuration	Supplementary User Info
System Configuration	Real Name S1
Configuration	Description Sales Department User
Administration	
Databases	User Setup
Posture Validation	Password Authentication:
Profiles	ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)
Seports and Activity	Password ******
Documentation	Confirm ***** Password
	Separate (CHAP/MS-CHAP/ARAP)
	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

User Setup

CISCO SYSTEMS

Advanced Settings

User Setup	Network Access Restrictions (NAR)
Group Setup	Per User Defined Network Access Restrictions
Shared Profile	Define IP-based access restrictions
ະພະ Components	Table Defines : Permitted Calling/Point of Access Locations
Network Configuration	AAA Client Port Address
System Configuration	
Configuration	
Administration	AAA Client All AAA Clients
Databases	Port Address
Posture Validation	enter
Network Access Profiles	Define CLI/DNIS-based access restrictions
Reports and Activity	Table Defines : Permitted Calling/Point of Access Locations
ها Online ا	AAA Client Port CLI DNIS
Documentation	
	AAA Client MAILC
	Port *
	CLI ×
	DNIS *Sales
	enter
	Submit Cancel

9. Repita el mismo proceso para agregar más usuarios a la base de datos.Nota: De forma predeterminada, todos los usuarios se agrupan bajo el grupo predeterminado. Si desea asignar usuarios específicos a diferentes grupos, consulte la sección <u>Administración de grupos de usuarios de la Guía del usuario para Cisco Secure ACS para Windows Server 3.2.Nota:</u> Si no ve la sección Restricciones de acceso a la red en la ventana Configuración de usuario, es posible que se deba a que no está habilitada. Para habilitar las Restricciones de Acceso a la Red para los usuarios, elija Interfaces > Opciones Avanzadas de la GUI de ACS, seleccione Restricciones de Acceso a la Red a Nivel de Usuario y haga clic en Enviar. Esto activa el NAR y aparece en la ventana User Setup (Configuración de usuario).



User Setup



- N L Uson

Advanced Settings

red Profile ponents vork figuration tem figuration reface figuration reface figuration reface figuration remove AAA Client All AAA Clients remove AAA Client All AAA Clients remove ture Address reface reface reface reface remove AAA Client All AAA Clients remove AAA Clients remove AAA Client Port Address AAA Client Address reface re	Per Us	er Defined Network Ar	cess Restrict	ions	
work figuration tem figuration reface reface figuration reface reface reface figuration reface refac	Shared Profile Components	Def Definition Action	ine IP-based acces	restrictions	
figuration AAA Client Port Address reface figuration remove Image: Constraint of the con	Vetwork	Table Defines : Pe	mitted Calling/Poi	nt of Access Locations 🖉 💌	
tem figuration ministration ministration troi ernal User abases ernal User abases ture idiation remove AAA Client All AAA Clients Port Address ernter vork Access iles norts and ivity Define CLI/DNIS-based access restrictions Table Defines : Permitted Calling/Point of Access Locations AAA Client Port CLI DNIS	Configuration	AAA Client	Port	Address	
errlace figuration inistration trol ernal User abases ernal User abases ernal User abases iture idiation work Access iles ine umentation ine umentation AAA Client AII AAA Clients Port AII AAA Clients ernter Define CLI/DNIS-based access restrictions Table Defines : Permitted Calling/Point of Access Locations AAA Client Port CLI DNIS	Bystem Configuration				
initistration trol ernal User abases enter AAA Client AII AAA Clients Port Address enter vork Accessive vork accessive Define CLi/DNIS-based access restrictions Ine umentation AAA Client Port CLI DNIS	Interface Configuration				
AAA Client All AAA Clients Port Address enter work Access iles orts and ivity Ine umentation AAA Client Port CLI DNIS	Administration Control	1	temove.		
abases Port Address ine umentation AAA Client Port CLI DNIS	xternal User	AAA Client All AA	A Clients	×	
Address Idation Work Access iles Work access iles Define CLI/DNIS-based access restrictions Table Defines: Permitted Calling/Point of Access Locations AAA Client Port CLI DNIS	tabases	Port			
work Access iles Define CLI/DNIS-based access restrictions Table Defines : Permitted Calling/Point of Access Locations AAA Client Port CLI DNIS	ture idation	Address	enter		
rts and vity Define CLI/DNIS-based access restrictions Table Defines : Permitted Calling/Point of Access Locations AAA Client Port CLI DNIS	rk Access es				
e AAA Client Port CLI DNIS	rts and	Define C	LI/DNIS-based acco	ess restrictions	
nentation AAA Client Port CLI DNIS		Table Defines : Permitte	d Calling/Point of /	Access Locations	•
	ation	AAA Client	Port CLI	DNIS	
			remove.		
remove		AAA Client VYLC			•
AAA Client WLC		Port ×			
AAA Client WLC					
AAA Client WLC		DAUG Čádejo			

10. Para habilitar la autenticación EAP, 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 EAP configuration settings (Parámetros de configuración de EAP), seleccione el método EAP adecuado. Este ejemplo utiliza autenticación LEAP. Haga clic en Enviar cuando haya terminado.

CISCO SYSTEMS	System Configuration	
User Setup Setup Setup	Global Authentication Setup	
Shared Profile Components	EAP Configuration	?
Network Configuration System Configuration Interface Configuration Interface Configuration Interface Configuration Interface Configuration Interface Configuration Interface Configuration Interface Configuration Interface Configuration Interface Configuration Interface Validation Interface Configuration Interface Configuration Interface Configuration Interface Configuration Interface Configuration Interface Configuration Interface Configuration Interface Configuration	PEAP Allow EAP-MSCHAPv2 Allow EAP-GTC Allow Posture Validation Cisco client initial message: PEAP session timeout (minutes): 120 Enable Fast Reconnect: EAP-FAST EAP-FAST EAP-FAST Configuration EAP-TLS Allow EAP-TLS Select one or more of the following options: Certificate SAN comparison Certificate Einary comparison EAP-TLS session timeout (minutes): 120	
	Allow LEAP (For Aironet only)	
	Submit Submit + Restart Cancel	

Configure el cliente inalámbrico y verifique

Use esta sección para confirmar que su configuración funciona correctamente. Intente asociar un cliente inalámbrico con el LAP mediante la autenticación LEAP para verificar si la configuración funciona como se espera.

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 información sobre cómo configurar el 802.11 a/b/g Wireless Client Adapter para la autenticación LEAP.

Nota: Desde la ADU verá que ha configurado dos perfiles de cliente. Uno para los usuarios del departamento de administración con SSID **Admin** y el otro para los usuarios del departamento de ventas con SSID **Sales**. Ambos perfiles están configurados para la autenticación LEAP.

Cisco Aironet Desktop Ut on Options Help	ility - Current Profile: Admin	
urrent Status Profile Managem	ent Diagnostics	
Admin		New
Sales		Modify
		Remove
		Activate
- Details		
Network Type:	Infrastructure	Import
Security Mode:	LEAP	
Network Name 1 (SSID1):	Admin	Export
Network Name 2 (SSID2):	<empty></empty>	Coop
Network Name 3 (SSID3):	<empty></empty>	Judit.
Jointo Salact Profiles		Order Profiles

Cuando se activa el perfil del usuario inalámbrico del departamento de administración, se le solicita al usuario que proporcione el nombre de usuario/contraseña para la autenticación LEAP. Aquí tiene un ejemplo:

Enter Wireless N	etwork Password 🗙
Please enter your LE network	EAP username and password to log on to the wireless
User Name :	A1
Password :	•••••
Log on to :	
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter
Profile Name :	Admin
	OK Cancel

El LAP y luego el WLC transfieren las credenciales del usuario al servidor RADIUS externo (Cisco Secure ACS) para validar las credenciales. El WLC pasa las credenciales incluyendo el atributo DNIS (nombre SSID) al servidor RADIUS para la validación.

El servidor RADIUS verifica las credenciales del usuario comparando los datos con la base de datos del usuario (y los NAR) y proporciona acceso al cliente inalámbrico siempre que las credenciales del usuario sean válidas.

Tras la autenticación RADIUS correcta, el cliente inalámbrico se asocia con el LAP.

LEAP Authentication Status		? <u>-</u> ×
Card Name: Cisco Aironet 802.1	11a/b/g Wireless Adapter	
Prone Name: Admin	Chabas	
1. Starting LEAP Authentication	Success	
2. Checking Link Status	Success	
3. Renewing IP address	Success	
 Detecting IPX Frame Type 	Success	
5. Finding Domain Controller	Success	
⊏ si	how minimized next time	Cancel

De manera similar, cuando un usuario del departamento de ventas activa el perfil de ventas, el usuario es autenticado por el servidor RADIUS basado en el nombre de usuario/contraseña LEAP y el SSID.

Please enter your Lt network	AP username and password to log on to the wireless
User Name :	S1
Password :	•••••
Log on to :	
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter
Profile Name :	Sales

El informe de autenticación aprobada en el servidor ACS muestra que el cliente ha pasado la autenticación RADIUS (autenticación EAP y autenticación SSID). Aquí tiene un ejemplo:

Reports and Activity

Select															
Passed Aut	thenticat	ions active	.csv	🖹 <u>Refre</u>	sh 🗇	Downl	oad								
Regular Exp	ression				Start D: mm/dd/	ate & ' 'YYYy,	Time hh:mm:ss	End D mm/d	ate & Tir d/yyyy,h	ne h:mm:ss	Rows per I 50	age T			
Apply Filt Filtering is r	ter C	d.													
Date 🗣	Time	Message- Type	User- Name	Group- Name	Caller- ID	NAS- Port	NAS-IP- Address	Access Profile Name	Shared RAC	Downloadable ACL	System- Posture- Token	Application- Posture- Token	Reason	<u>еар</u> Туре	EAP Type Name
10/11/2006	14:48:40	Authen OK	51	Default Group	00-40- 96-AC- E6-57	1	172.16.1.30	(Default)						17	LEAP
10/11/2006	14:47:05	Authen OK	A1	Default Group	00-40- 96-AC- 66-57	1	172.16.1.30	(Default)						17	LEAP

Ahora, si el Usuario de Ventas intenta acceder al SSID **Admin**, el servidor RADIUS niega el acceso del usuario a la WLAN. Aquí tiene un ejemplo:

Card Name: (Cisco Aironet 802.11	a/b/g Wireless Adapter	
Profile N. LEAP	Authentication	×	
Steps	Card Name:	Cisco Aironet 802.11a/b/g Wireless Adapter	
2. Checking	Profile Name:	Admin	
3. Renewing 4. Detecting	Message:	Unable to authenticate wireless user. Make sure you have entered the correct user name and password and try again.	

De esta manera, se puede restringir el acceso a los usuarios en función del SSID. En un entorno empresarial de N, todos los usuarios que pertenecen a un departamento específico pueden agruparse en un único grupo y el acceso a la WLAN se puede proporcionar en función del SSID que utilizan, como se explica en este documento.

Troubleshoot

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.

- debug dot1x aaa enable: habilita la depuración de interacciones AAA 802.1x.
- debug dot1x packet enable: habilita la depuración de todos los paquetes dot1x.

• debug aaa all enable: configura la depuración de todos los mensajes AAA.

También puede utilizar el informe de Autenticación Pasada y el informe Autenticación Fallida en el servidor Cisco Secure ACS para resolver problemas de configuración. Estos informes se encuentran bajo la ventana **Informes y Actividad** en la GUI de ACS.

Información Relacionada

- Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN (WLC)
- Ejemplo de Configuración de la Autenticación Web del Controlador LAN Inalámbrico
- Ejemplo de Configuración de VLANs de Grupo de AP con Controladores de LAN Inalámbrica
- Página de Soporte de Red Inalámbrica
- Soporte Técnico y Documentación Cisco Systems

Acerca de esta traducción

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

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

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