Ejemplo de Configuración de ACS Version 5.2 y WLC para la Autenticación por WLAN

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Configurar la WLC Configuración de Cisco Secure ACS Verificación Troubleshoot

Introducción

Este documento proporciona un ejemplo de configuración para restringir el acceso por usuario a una LAN inalámbrica (WLAN) basado en el identificador del conjunto de servicios (SSID).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo configurar el controlador de LAN inalámbrica (WLC) y el punto de acceso ligero (LAP) para el funcionamiento básico
- Cómo configurar Cisco Secure Access Control Server (ACS)
- Métodos de seguridad inalámbrica y protocolo ligero de punto de acceso (LWAPP)

Componentes Utilizados

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

- WLC de la serie 5500 de Cisco que ejecuta la versión 7.4.110 del firmware
- LAP de la serie 1142 de Cisco
- Servidor Cisco Secure ACS versión 5.2.0.26.11

Configurar

Para configurar los dispositivos para esta configuración, debe:

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

Configurar la WLC

Complete estos pasos para configurar el WLC para esta configuración:

 Configure el WLC 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: Seleccione Security > RADIUS Authentication desde la GUI del controlador para mostrar la página RADIUS Authentication Servers.

.1 1.1 1.	Sale Contraction Data Indian Data
cisco	MONITOR MUANE CONTROLLER AURELESS SECURITY NOVABENENT CONVANCS HELF EEEDBACK
Security	RADIUS Authentication Servers Apply New
AAA General e RoDUS Bothentication Bothentication Bothentication Bothentication Tacacce Town Invest Net Users MCC Flemmin Disabled Clients Invertings Patience Remotidue Energy distance Energy distance	Cell Staten 10 Type I I Address III Law ASS Ever What III Consigned for CES contineers and requires a key area conclust 8A08.8 server) ROC Delevator Ingener III Network linear Management Server Index Server Address Port (Pher Admis Redus 2. Cell States 13 Type all be specified a very nor non-2004 a superfiledba very.
Priority Order	
► Certificate	
► Access Control Lists	
+ Wireless Protection Pullcles	
Web Auth	
TrustSec SXP	
Advanced	

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 Usuario de red y Administración 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 10.104.208.56.

CISCO MONTOR MULHAR CONTROLLER ALMENTIAL CONTRALLER Contraller <thcontraller< th=""> Contraller <thcon< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th>Sage Configuration Eine Legent Bafreeh</th></thcon<></thcontraller<>							Sage Configuration Eine Legent Bafreeh
Security Apply • AAA	CISCO	MONITOR MUANE (ONTROLLER AJRELESS	SECURITY MaNABEME	T COMMANCE	неця деерько	<
* AAA Server 104 (# Article) General Server 19 Address * REDDIS Server 19 Address Addretication Server 19 Address * TABLOCK+ Server 19 Address IDAP Centre Server Local Mel Bars Server Victoring Server Disabled Clubs Fort Server Hear Loop Notice Server 19 Catales Person Notice Server 19 Catal	Security	RADIUS Authentica	tion Servers > New				< Back Apply
TrustSec SXP + Advanced	AAA General enteril Adductication Adductication Adductication Adductication Adduct Aduct Adduct Aduct Aduct Adduct Adduct Addu	Records Autometrica Server 34 Address Shared Secret Format Shared Secret Controm Shared Secret Kay Wrug Port Nambur Server Secret Server Secret Noteurk Over Management IPDoc	I III IIII-,005 GLCT II CARGYAN M ICL2 Tanhan II Cangyan M ICL2 Tanhan II Cangyan M ICL2 Tanhan II Cangyan M Cangyan M Cang	it brffitt durchment for reg in de	is a bey area conclu	re babell 6 centre)	< Back Apply
	TrestSec SXP Advanced						-

Haga clic en Apply (Aplicar).

2. Complete estos pasos para configurar una WLAN para el Empleado con **Empleado** SSID y la otra WLAN para Contratistas con **Contratista** SSID. 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 Employee y el ID de WLAN es 1. Haga clic en Apply (Aplicar).

սիսիս						Ŭ		 Sage Configuration ging	Logout Befreeh
CISCO	MONITOR MILANE	CONTROLLER &	RELESS SECURI	пт маларенелт	ODW/4NDS	HE_F	ESEDBACK		
WLANs	WLANs > New							< Back	Apply
 WLANS WLANS Advanced 	Type Profile Name SSID BD	et Ab Employee Employee 2 e							

Seleccione la ventana **WLAN > Edit** y defina los parámetros específicos de la WLAN: En la pestaña Layer 2 Security , seleccione **802.1x**. De forma predeterminada, la opción de seguridad de capa 2 es 802.1x. Esto habilita las autenticaciones 802.1 x/protocolo de autenticación extensible (EAP) para la WLAN.



En la pestaña de servidores AAA, seleccione el servidor RADIUS apropiado de la lista desplegable en Servidores RADIUS. Los otros parámetros se pueden modificar en función de los requisitos de la red WLAN. Haga clic en Apply (Aplicar).

		Sage Centquister Brig Legislit Betresh
CISCO	Rovillor Kitane Covilsofter Alsetter Section, agaverage Corrance Hete Sectement	
WLANs	WLANs > Edit 'Employee'	< Back Apply
WLANS WLANS	General Security QaS Advanced	
▶ Advanced	Layer 2 Layer 3 AM Servers	
	Select AAA servers below to override use of default servers on this WLAN Realms Servers LDAP Servers	
	A misicana oreana marka Dentret	
	Authentication Servers Assessing Servers Server2 tore	= *
	Mitashan Vitratiat during Yitaya a	
	Strug Z to is a line and	
	Sinar 3 tors a Rose	
	Verset to Terre	
	Server 5 bare w The w	
	Server 6 Bore a Toto a	
	Radius Server Accounting	
	Interim Update 📰	
	Local EAP Authentication	
	<[
	Faceb Medica	
	2 Web Policy menet in used in conditioning with Plant	

Del mismo modo, para crear una WLAN para los contratistas, repita los pasos b a d.

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 (Credenciales) para la autenticación basada en SSID.
- 3. Habilite la autenticación EAP.

Complete estos pasos en Cisco Secure ACS:

- Para definir el controlador como un cliente AAA en el servidor ACS, seleccione Recursos de Red > Dispositivos de Red y Clientes AAA de la GUI ACS. En Network Devices y AAA Clients, haga clic en Create.
- 2. Cuando aparezca la página Configuración de red, defina el nombre del WLC, la dirección IP y el método de autenticación y secreto compartido (RADIUS).

	mar D + O Cattle. E d X Cisco Securit ACS ×	
clisco Secure A clisco EvAl(Days Mill 5) clisco EvAl(Days Mill 5)		acaudmin acalomphile (Primary) Log Cut About Help
Activation Device Orbups Location Device Type Default Network Device Default Network Device Device Device Devic	Name: DOT4 Description: Network Device Groups Location All Locators Location All Locators Device Type All Device Types P Address Single IP Address O IP: 10.100.98.4	Authentication Options • TaCACS+ Snared Secret Single Connect Device Logacy TACACS+ Single Connect Support • RADUS • RADUS • RADUS • RADUS • RADUS • TaCACS+ Single Connect Support • RADUS • RADUS • Shared Secret XXXXXX CoApot: 1720 • Erable KeyWrap Key Encrystion Key

3. Seleccione **Users and Identity Stores > Identity Groups** en la GUI de ACS. Cree los grupos respectivos para Empleado y Contratista y haga clic en **Crear**. En este ejemplo, el grupo

creado se denomina Empleados.

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Status Barban Baradi Bar		
Caller (1997) (1	nin/ D + O Centrici, E C X 6 Cisco Secure A	cs ×		A 🛨 🗉
× Garan Browner WebE: -				
uluilu Cisco Secure A	CS		ecautoin	acatiomphile (Primary) Log Out About Help
CISCO EVAL(Days left: 5)				
» St MyWorkspace	Users and Identity Stones > Harity Groups > Grade			
» (5) Nelwork Resources	General			
- 🗿 Users and identity Stores	Name: Employees			
Hersty Croups	Description:			
 Internal Identity Dipres Users 	Parent All Smith	(felect)		
Hosts	0 = Required fields			
 External Identity Stores 				
Active Directory				
RSA SecuriD Taken Seners				
RADIUS Identity Servers				
Continue Automitation Profile				
Mentily Store Sequences				
PolicyElements				
Access Policies				
 Monitoring and Reports 				
 R System Administration 				
	Submit Carcel			
				and the second se

4. Seleccione Users and Identity Stores > Internal Identity Stores. Haga clic en Crear e ingrese el nombre de usuario. Colóquelos en el grupo correcto, defina su contraseña y haga clic en Enviar.En este ejemplo se crea un usuario denominado empleado1 en el grupo Empleado. Del mismo modo, cree un usuario denominado contratista1 en los contratistas del grupo.

X Shere Browser WebEr -	In P + O Cetticu E C X	×	-			0 tr 0
Cisco Secure Al	CS			and min	acaliemplate (Primary)	Log Out About 1440
Constant Resources Constant Resource Constant R	General Name: employee1 Dishe Description: Discription: D	Enables • •	Enable Password Information Password musit Continn 4 - 32 characters Enable Password Confirm Password			
	* [Submit] Cance					

5. Seleccione Elementos de política > Condiciones de red > Filtros de estación final. Haga clic en Crear.



Ingrese un nombre significativo y bajo la pestaña **dirección IP** ingrese la dirección IP del WLC. En este ejemplo, los nombres son Empleado y Contratista.



En la ficha CLI/DNIS, deje CLI como -ANY- e introduzca DNIS como *<SSID>. En este ejemplo, el campo DNIS se introduce como *Empleado, ya que este filtro de estación final se utiliza para restringir el acceso sólo a la WLAN del empleado. El atributo DNIS define el SSID al que el usuario puede acceder. El WLC envía el SSID en el atributo DNIS al servidor RADIUS.Repita los mismos pasos para el filtro de la estación final del contratista.



6. Seleccione Elementos de política > Autorización y permisos > Acceso de red > Perfiles de autorización. Debe haber un perfil predeterminado para Permit Access (Permitir acceso).

X Share Browser WebEr •	m/ SP + Q Centre. 2 d X B Circo Securi AC5 ×		□ □
Cisco Secure Al Cisco Eval(Days left, 5)	CS example 2	aca formplade (Primary)	Log CM About 1980
» ∰ MyWorkspace	Policy Berneria > Authorization and Permissions > Televonk Accessa > Authorization Politics		
> (5) Nelwork Resources	Authorization Profiles	Stowing 1-1 of 1	0 • perpage 50
 B Users and Identity Stores 	Filer. • Nech II: • 00 •		
Over Policy Elements	Name + Description		
 Bassion Conditions Date and Time 	Permit Access		_
Custom • Nations Conditions End Statum Filters Device Filters • Authorization and Permissions • Nations Access Part/Filters • Davise Administration • Named Permission Objects • Conditional Particles • Conditional Particles • Conditional Administration • Recess Particles • Conditional Administration			
	Create Dupicate Edt Delate	H 4 Page	1 0/1 10 10

7. Seleccione Access Policies > Access Services > Service Selection Rules. Haga clic en Personalizar. Agregue cualquier condición adecuada. Este ejemplo utiliza Protocol as Radius como condición coincidente.Haga clic en Crear. Nombre la regla. Seleccione Protocol y seleccione Radius.En Resultados, elija el servicio de acceso adecuado. En este ejemplo, se deja como Acceso de red predeterminado.

Webpage Dialog		×
https://10.104.208.56/acsadmin/	PolicyInputAction.do	😵 Certificate error
Customize Conditions Available: ACS Host Name Compound Condition Device Filter Device IP Address Device Port Filter End Station Filter NDG:Device Type NDG:Location Time And Date UseCase	Selected: Protocol	
OK Cancel		

Cisco Secure ACS webpage Dialog	
Attps://10.104.208.56/acsadmin/PolicyInputAction.do	ificate error
General	
Name: Rule-4 Status: Enabled - O	
The Customize button in the lower right area of the policy rules screen controls which policy of conditions and results are available here for use in policy rules.	icy
Conditions	
Protocol: match - Radius Select	
Results	
Service: Default Network Access 👻	
OK Cancel	Help

8. Seleccione Access Policies > Access Services > Default Network Access > Identity . Elija Selección de resultado único y Origen de identidad como usuarios internos.

Conception of the concept	Concernance Concernan	and the second se		All hope that had a mount that	the second se		
X Image Resoure WebEr 11.11.1. CISCO_SOLIZE ACS 01.01.1. CISCO_EVAL(Days Mit 5) • 43. My/Notroppice Access Service > Default Network Access > Meetly • Image Resoure WebEr • Single result selection < California Users	* Wein Trever Webs • * Jung Teacher Webs • * Jung Teacher Webs • * State Teacher Webs • * Advance Barrise Teacher • * State Teacher * * State Teacher * * Ober Webster * * Ober Webster * * State Teacher * * State Teacher * * State Teacher * * Montander States * * Montander States * * Montander States * * States States * States States * Montander States * * Ober Webster * * States States	(-) (-) (-) (-) (-) (-) (-) (-) (-) (-)	min/ D + O Centre. E d × 6 Circo Secure AC	5 ×			6 2 8
• Iliniti: Cisco Socure ACS water: actemptide (Perror) Lip D4 Abort Her • Millionization • Millionization * Single result selection Benetic • O behaltNewson • Millionization • Millionization • Millionization • O behaltNewson • Millionization • Millionization • O behaltNewson • Millionization • Millionization • Millionization • Millionization • Millionization	I.I.I.I. Cisco Secure ACS water:	X Gara Erranzer WebEc -					
Image:	• @ My/Abriagace Access Radium > Access Raview > Default Hear ah Access > Hearty • @ Default Associations • @ Single result selection • @ Default Name • @ Single result selection • @ Default Name • @ Monitoring and Raports • @ Default Name • @ Default Name • @ Default Name • @ Monitoring and Raports • @ Spetern Administration • @ Default Name • @ Spetern Administration • @ Default Name • @ Spetern Administration • @ Default Name	cisco Secure A	CS		scadnin	acalomplais (Primary)	Log Cul About Help
Supple result selection Advanced Options Supple result selection Supple result selection Advanced Options Supple result selection Supp	Source and Beetty Steres Beetty Source Beetty Source Beetty Source Beetty Source Access Dorate Beetty Source Access Dorate Beetty Source Advected Optore Advected Optore Advected Optore Advected Optore Advected Optore Advected Optore Beetty Network Access Beetty Advected Optore Beetty Network Access Beetty Advected Optore Beetty Network Access Beetty Be	» ∰ MyWorkspace	Access Policies > Access Services > Default Network Acce	ns > Berthy			
Identi and Identify States Identify States Image: Contract States Image: Contract States	Subern and Identity Stores Meetity Source Image Examples Advected Options	» (5) Nelwork Resources	· Single result selection · Rule based result sel	lection			
 Procy Elements Access Fracts Access Fracts Access Fracts Debut Device Amm Users Debut Device Amm Users Debut Device Amm Users Access Tracts Access	 Que Parcy Blamants Access Dentites Bernie Selection Rules O Default Device Admin Bernie Selection Rules O Default Network Access Tables, Authorization Register Administration Selection Rules Selection Rules Selection Rules Selection Rules Selection Rules 	B Users and Identity Stores	Identity Source: Internal Upers	Select.			
 Access Braies Cocess Device Sectors Nales O Debut Optice Amm Users and Reports O Debut Network Access Intern Achoration Monitaring and Reports Statem Administration 	Access Protects Access Protects Beckton Rules Obdutt Device Admin Homity Anthonototon O Debutt Network Access Transp Anthonototon System Administration Seve Changes Decart Changes	» Qv PolicyElements	Advanced Options				
	ten sustan	K. Access Polices Access Denices Benice Selector Rules Oblight Device Amm Benity Athorization Arthorization Arthorization Ministring and Reports Bystem Administration	San Change Distant Change				

Seleccione Access Policies > Access Services > Default Network Access >

Authorization. Haga clic en **Personalizar** y agregue las condiciones Personalizadas. En este ejemplo se utiliza Identity Group, NDG:Device Type y End Station Filter en ese orden.



Haga clic en **Crear**. Asigne un nombre a la regla y elija el grupo de identidad adecuado en Todos los grupos. En este ejemplo es Empleado.

Cisco Secure ACS Webpage Dialog	Cisco Secure ACS Webpage Dialog
🌀 https://10.114.200.56/accedition/Policy/opublician do 📀 Carificate area	🍘 https://10.114.200.W/scraderin: Natwork EnviroGeo.pt. Republician de Poerte AData, externa Filter: Liter ByGroup: Manthylin 🔮 🤇
General Name: Rule-2 Distus: Enabled + 0	Retwork Danice Groups Filter: • Malch if • 💿 🔻
The Custerrize butten in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.	Name Description All Data Building Boot Contractor
Conditions	• Instant
12 Identity Droup: In • Belat	MC VAC
IZ NDQDevce Type: In	
2 End Station Filter, math • Belast	El Constantin ACS Writering Clarke
Fesuits	2 https://11.101.201.00.000 mit.nls/fictured.ls.it.effengel.Phys.olton.it/freetesticities.comestic testilization Type II. Tertificate com Internet in Action Systems
Vou nay exist multiple autoritation profiles. Attitutes autorial in multiple profiles will use the value from the first profile defined.	
	(X) Center (Net

Haga clic en el botón de radio **Employee End Stn Filter** o ingrese el nombre que ingresó en el Paso1b en la sección "Configure the WLC".

Cisco Secure ACS Webpage Dialog							
1	🥖 https:	://10.104.208.56/acsadmin/N	IARsLPInputAction.do?listType=EndStation		🙄 Certificate error		
	End St	ation Filters		Showing 1-2 of 2 50	▼ per page Go		
	Filter:	 Match if: 	🗕 🐨				
		Name 🔺	Description				
	0	Contractor End Stn Filter					
	۲	Employee End Stn Filter					
	Crea	te Duplicate Edit	Delete	Id Page	1 of 1 🕨 🕅		
	OK C				Help		
					THOP		

Marque la casilla de verificación Permitir acceso.

4	Cisco Secure ACS Webpage Dialog				x
	Https://10.104.208.56/acsadmin/NetworkAccessLPInputAction.do		8	Certificate	error
	Authorization Profiles Showin	ng 1-2 of 2	50 🔻	per page	Go
	Fliter: 🔹 Match if: 🔹 🐨				
	🖂 Name 🔺 Description				
	DehyAccess				_
	Permit Access				
1					
		-	-		
	Create Duplicate Edit Delete	Page		of1 🕞	
	OK Cancel			H	qlg

Repita los mismos pasos anteriores para las Reglas del Contratista. Asegúrese de que la

acción predeterminada es **Denegar acceso**. Una vez que haya completado el paso e, las reglas deben verse como en este ejemplo:

of the Post of the State of State								
🗲 🛞 🍊 https://20.204.200.54/actade	n/ D + Q Cette E d X 6 Circo Secure ACS X			6 🕁 🗄				
🗶 🍘 Shara Browser - WebEc 📼								
Juliulu, Cisco Secure Ar		acastein	acationsphile (Primary)	Log Out About 140				
CISCO EVAL(Days left: 5)								
 MyWorkspace 	Access Rokies > Access Services > Default Network Access > Authorization							
+ (3) Network Resources	30 Network Resources Standard Policy Excention Policy							
B Users and Identity Stores	stress Melwerk Anness Authoritation Policy							
» Qv PolicyElements	Elter States . Mitch if Faugh							
 Access Policies 								
 Access Services Single Selection Robert 	Status Name Hently Group NDO Device Ture End Station Filter	Autorizator Prelias	HECOU E					
* O Default/Device Admin	1 Contactor in Al Groups:Contractor in Al Device Types:VLC match Contractor End Stri Filter	Pernit Access	7	_				
identity	2 🗉 🛛 Engloyee in Al Oroups Employee in Al Device Types WLC match Employee End Sth Filter	Permit Access	5					
O Default Network Access								
Identity								
- D Mailtains and Bacada								
· · · · · · · · · · · · · · · · · · ·								
· · · · · · · · · · · · · · · · · · ·								
		_						
	E Detail Fino tales defined ar no enabled rule matches. Dety/scess 8							
	Create * Dupitate * Edt Delete Move to	Custor	nize Hit Count					
	Save Changes Discard Changes							

Esto concluye la configuración. Después de esta sección, el cliente necesita ser configurado en consecuencia con el SSID y los parámetros de seguridad para conectarse.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.