# Exemplo de Configuração do ACS Versão 5.2 e WLC para Autenticação por WLAN

## Contents

Introduction Prerequisites Requirements Componentes Utilizados Configurar Configurar o WLC Configurar o Cisco Secure ACS Verificar Troubleshoot

## Introduction

Este documento fornece um exemplo de configuração para restringir o acesso por usuário a uma LAN sem fio (WLAN) com base no identificador do conjunto de serviços (SSID).

# Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como configurar o Wireless LAN Controller (WLC) e o Lightweight Access Point (LAP) para operação básica
- Como configurar o Cisco Secure Access Control Server (ACS)
- Lightweight Access Point Protocol (LWAPP) e métodos de segurança sem fio

#### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 5500 Series WLC que executa a versão de firmware 7.4.110
- LAP Cisco 1142 Series
- Cisco Secure ACS Server versão 5.2.0.26.11

# Configurar

Para configurar os dispositivos para esta configuração, você precisa:

1. Configure a WLC para as duas WLANs e o servidor RADIUS.

- 2. Configure o Cisco Secure ACS.
- 3. Configure os clientes sem fio e verifique a configuração.

### **Configurar o WLC**

Conclua estes passos para configurar a WLC para esta configuração:

 Configure a WLC para encaminhar as credenciais do usuário a um servidor RADIUS externo. O servidor RADIUS externo (Cisco Secure ACS, neste caso) valida as credenciais do usuário e fornece acesso aos clientes sem fio. Conclua estes passos: Selecione Security > RADIUS Authentication na GUI do controlador para exibir a página RADIUS Authentication



Clique em **New** para definir os parâmetros do servidor RADIUS. Esses parâmetros incluem o endereço IP do servidor RADIUS, o segredo compartilhado, o número da porta e o status do servidor. As caixas de seleção Network User and Management determinam se a autenticação baseada em RADIUS se aplica a usuários de gerenciamento e rede. Este exemplo usa o Cisco Secure ACS como o servidor RADIUS com endereço IP 10.104.208.56.

սիսիս						Sage Configuration Ding Legent Befreeh
CISCO	MONITOR MUANE CONTROLLS	er wijkeliess geoliikth	Management	COMMANCE HE	U ESENAR	
Security	RADIUS Authentication Serv	rens > New				< 8 ack Apply
* AAA	Server Index (Priority)	1 🗰				1
eneral	Server 37 Address	10104.80555				
Authentication Association	Shared Secret Format	45C3 📼				
Fallback	Shared Secret	*******				
LDAP	Confirm Shared Secret	*******				
Excal Net Deers PAC Differing Disabled Clients	Kuy Wrap	Catigranity FIG area		ing any conclusion	DELE (MYAR)	
liker Logo Rolisses	Pert Bamber	1:12				
Pacement Policiae	Server Status	Teshiari 📼				
E Local EAP	Support for INC 3576	backed w				
Priority Order	Server Timeout	2 example				
Eertificate	Notwork User	Z Chatle				
Access Control Lists	Planagement	🖾 6 nable				
<ul> <li>Wireless Protection</li> <li>Pulicies</li> </ul>	IPileo	📰 inde				
Web Auth						
TrestSec SXP						_
Advanced						

Clique em Apply.

 Conclua estes passos para configurar uma WLAN para o Funcionário com o Funcionário SSID e a outra WLAN para Contratante com o Contratante de SSID. Clique em WLANs na GUI do controlador para criar uma WLAN. A janela WLANs será exibida. Essa janela lista as WLANs configuradas no controlador.Clique em **Novo para configurar uma nova WLAN**.Este exemplo cria uma WLAN chamada Employee (Funcionário) e a ID da WLAN é 1. Clique em Apply

дрргу.						Real Conference Rive Lanual Refusion
cisco	MONITOR MLANE (	ONTROLLER AGRELESS S	geolikity Management	ODWANCS HELF	EEEBACK	adla couldantes. Sud. reflect Dataste
WLANs	WLANs > New			_		< Back Apply
<ul> <li>WLANS WLANS</li> <li>▶ Advanced</li> </ul>	Type Profile Name SSID BJ	et.As a Employee C=ployee 2 a				

Selecione a janela WLAN > Edit e defina os parâmetros específicos da WLAN: Na guia Layer 2 Security, selecione 802.1x. Por padrão, a opção Layer 2 Security é 802.1x. Isso habilita as autenticações 802.1 x/Extensible Authentication Protocol (EAP) para a WLAN.



Na guia servidores AAA, selecione o servidor RADIUS apropriado na lista suspensa em Servidores RADIUS. Os outros parâmetros podem ser modificados com base no requisito da rede WLAN. Clique em Apply.

		Sage Centquisten Eing Legisut Betresh
cisco	MONILOR MITANE CONLIGNER AGAETERE RECTALLA AGAYORARIA COMPANICE HE'R REEDRACK	
WLANs	WLANs > Edit 'Employee'	< Back Apply
WLANS WLANS	General Security QoS Advanced	
▶ Advanced	Layer 2 Layer 3 AMA Servers	
	Select AAA servers below to override use of default servers on this WLAN	Î.
	Radius Servers UDIP Servers	
	since the constant interval (constant) and the c	
	Autoritation Servers Accounting Servers SErver2 Lova In	-
	A cont 1 121.0.04.20.70, for all 2 The m	
	Street 2 to a last to a	
	Spran 1 tors Trees	
	1 The second sec	
	Server 5 tane w Tree w	
	Server 5 tone in Tuni in	
	Radius Server Accounting	
	Interim Update	
	Lacal EAP Authentication	-
	x	· · ·
	Post Notes	
	2 Wee Proof sector to use in control with the sector of the proof of the manufactor. And a tradem that is an analysis of the manufactor. And an invariant the sector of	

Da mesma forma, para criar uma WLAN para os Contratante, repita as etapas de b a d.

## Configurar o Cisco Secure ACS

No servidor Cisco Secure ACS você precisa:

- 1. Configure a WLC como um cliente AAA.
- 2. Crie o banco de dados de usuários (Credenciais) para autenticação baseada em SSID.
- 3. Ative a autenticação EAP.

Conclua estes passos no Cisco Secure ACS:

- Para definir o controlador como um cliente AAA no servidor ACS, selecione Network Resources > Network Devices and AAA Clients na GUI do ACS. Em Dispositivos de rede e Clientes AAA, clique em Criar.
- 2. Quando a página Network Configuration for exibida, defina o nome da WLC, do endereço IP e do RADIUS (segredo compartilhado e método de autenticação).

	ACCURATE AND A DESCRIPTION OF A DESCRIPR	and the second se	in the second second
🗲 💮 🧭 International Statement	nn/ D = O Cettic E G X G Circo Secure ACS ×	and the second se	n 🖈 9
🗶 🍚 Shara Erowoar - WebEc 📼			
cisco Cisco Secure A	CS	acautoin acalomphic (Nin	ery) Log Clut About Help
» ∰ MyWorkspace	Network Resources > Network Devices and AAA Clamb > Create		
Action References     Instruct References     Instruct Device Groups     Location     Device Type     Moneys Devices and AAACSent     Device Type     Device Type     Device Theory Device     Instruct RADUE States     Inst	Name: DOT4     Descriptor:     Extract Device Goage     Location All_Locations     Device Type All Device Types     Single IP Address     Single IP Address     Single IP Address     IF T0.100.98.4	Authentication Options • TACACS+ binared Secret binared Secret binared Secret binared Secret • R4DUS • Shared Secret CoAppt: 1770 Erable KeyWrap Nary Encrysten Key	
	Submit Carce		

3. Selecione Users and Identity Stores > Identity Groups na GUI do ACS. Crie os respectivos Grupos para Funcionário e Contratante e clique em Criar. Neste exemplo, o grupo criado é chamado de Funcionários.

C Imper/200.384.200.56/scrade	nin/ D + O Contric., E C X 6 Class Secure Ad	cs ×		A 🛨 🗉
× 🖨 Shara Browner, WebEc +				
altata Cisco Secure A	CS		acautoin	acatemptete (Primary) Log Out About Help
CISCO EVAL(Days left 5)				
<ul> <li>St MyWorkspace</li> </ul>	Users and Identity Stones > Mentity Groups > Greate			
+ (5) Network Resources	General			
<ul> <li>B Users and Identity Stores</li> </ul>	<ul> <li>Name: Employees</li> </ul>			
Mersh Croupe	Description:			
<ul> <li>Internal identity Dures</li> </ul>	a Parent All Concert	[ Boject ]		
Hosts	All droups	( all but		
<ul> <li>External Identity Stores</li> </ul>	- Registed telas			
LDAP				
Active Directory BSA Security Taken Senara				
RADIUS Identity Servers				
Certificate Authorities				
Certificate Authentication Profile				
- C. Brite Strength				
· C. Arrass Datains				
D Marine and Departs				
<ul> <li>I stortbring and Reports</li> </ul>				
<ul> <li>Age Bystem Administration</li> </ul>				
	Submit Carcel			

4. Selecione Usuários e Repositórios de identidades > Repositórios internos de identidades. Clique em Criar e digite o nome de usuário. Coloque-os no grupo correto, defina sua senha e clique em Enviar.Neste exemplo, um usuário chamado funcionário1 no grupo Funcionário é criado. Da mesma forma, crie um usuário chamado contratante1 sob os contratados do grupo.

X Shere Browner WebEr -	m/ P × Q Control ≥ C X		-		∟ <b>□</b> ≙ ☆ 0
cisco Secure Al cisco eval(Days left 5)	CS			aadmin acalumplate (Prinary	1 Log Out About Help
	General       Name:       employee1       Description:       • Identity Group: All Groups Employee       Password Inst:       • Contain 4 - 32 characters       • Contain 4 - 32 characters       • Contain 4 - 32 characters       • Contain 4 - and characters       • Contain 5 - and characters       • Contain 6 - and characters       • Change password on ned login       User Information       There are no additional identity attributes defined for user record       • Engined tedo	s	Enable Password Information Password must • Contain 4 - 32 characters Enable Password : Confirm Password :		
	e   Submit   Carce				

5. Selecione Elementos de política > Condições de rede > Filtros de estação final. Clique em Criar.



Insira um nome significativo e, na guia **IP address**, insira o endereço IP da WLC. Neste exemplo, os nomes são Funcionário e Contratante.



Na guia CLI/DNIS, deixe CLI como -ANY- e insira DNIS como \*<SSID>. Neste exemplo, o campo DNIS é inserido como \*Funcionário, pois esse filtro de estação final é usado para restringir o acesso somente à WLAN do Funcionário. O atributo DNIS define o SSID que o usuário pode acessar. A WLC envia o SSID no atributo DNIS para o servidor RADIUS.Repita as mesmas etapas para o filtro da estação final do Contratante.



6. Selecione Elementos de política > Autorização e permissões > Acesso à rede > Perfis de autorização. Deve haver um perfil padrão para permitir acesso.

X Shere Browner WebEr •	n/ D × Q Centricu B C X Secure ACS ×		<u>-</u> ⊡ - A ☆ 6
CISCO CISCO Secure Al CISCO EVAL(Days left, 5)	CS	enaderin nentemplaie (Primary)	Log Out About Help
» G MyWorkspace	Policy Bernets > Authorization and Permissions > Table ork Access > Authorization Profiles		
<ul> <li>(5) Network Resources</li> </ul>	Authorization Profiles	Stawing 1-1 of 1	0 • perpage 00
Users and identity Stores	Filter. • Netch # Clo •		
<ul> <li>So Policy Elements</li> <li>Exercise Coordinate</li> </ul>	Name A Description		
Date and Time	Permit Access		
Custom * NationS Canditiane End Statum Pitans Device Pitans * Authorization and Permissions * NationS Access Device Patrifians * Device Access Patrifians * Device Access Patrifians * Candition Calculate * Candition Patrific Patrice * Candition Patrific Patrific * Candition Patri			
	Create Duplicate Edit Delate	H R Page	1 of 1 10 10

7. Selecione Access Policies > Access Services > Service Selection Rules. Clique em Personalizar. Adicione qualquer condição adequada. Este exemplo usa o protocolo como RADIUS como a condição correspondente.Clique em Criar. Nomeie a regra. Selecione Protocolo e selecione Raio.Em Results, escolha o Access Service apropriado. Neste exemplo, ele é deixado como Acesso à Rede Padrão.

Webpage Dialog		×
(interstation) (inter	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. Selecione Access Policies > Access Services > Default Network Access > Identity. Escolha Seleção de resultado único e Origem de identidade como usuários internos.

🗲 🛞 🥝 https://20.284.208.56/scrade	nin/ D + O Centric. E C X 6 Cisco Secure ACI	5 ×			6 2 8
🗶 🍘 Shara Browser WebEc 🔹					
altala Cisco Secure A	CS		acadeir	acatiomplatic (Primary)	Log Out About 1940
CISCO EVAL(Days left 5)					
» 🚱 MyWorkspace	Access Policies > Access Services > Default Network Acces	n > Harthy			
* (5) Nelwork Resources	· Single result selection · Rule based result selection	ection			
Users and identity Stores	Identity Source: Internal Usero	Belect.			
> Q> PolicyElements	Advanced Options				
- 🕵 Access Policies					
<ul> <li>Access Dervices</li> <li>Service Selection Rules</li> </ul>					
<ul> <li>O Default/Device Admin</li> </ul>					
Autorization					
* O Default Network Access					
Autorization					
Monitoring and Reports					
» 🦂 System Administration					
	sive changes Liscard changes				

#### Selecione Access Policies > Access Services > Default Network Access >

**Authorization.** Clique em **Personalizar** e adicione as condições Personalizadas. Este exemplo usa Grupo de identidade, NDG:Tipo de dispositivo e Filtro de estação final nessa ordem.



Clique em **Criar**. Nomeie a regra e escolha o Grupo de identidade apropriado em Todos os grupos. Neste exemplo, é Funcionário.

P Cisco Secure ACS Webpage Dialog	Cisco Secure ACS Webpage Dalog
🖉 hetpes / 18.514200.16/net a devier Dalay/opublicition da 🛛 📀 Carificate ere	🍘 hetpor/12.214.208. 14/208. 14/200. artisel view Bertanek Device Group Alexian de Prosente Clats, anteren Filmer Marchdon thy Group – Marchdy Group – Marchdon thy Group – Marc
General Name: Rule-2 Datus: Enabled * 0	Retwork Danice Groups Filter:
The Custernize 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  V Al Doc pt  Description  Contractor
Conditions	- Instant
Calendary Group: In Control Calendary	
Carl NDGDevice Type: In Carlos	Carl Annual All Manual State
the bit of the match	🖉 her part 12. 24.244 Were and ministration for all ministration and the second strend stren
Vou may select multiple authorization profiles. Attituite carried in marging profiles will use the values from the first profile defined.	
	(OK) Certer) Teb

Clique no botão de opção **Employee End Stn Filter** ou insira o nome digitado na Etapa 1b na seção "Configure the WLC".

Cisco Secure ACS Webpage Dialog					
	遵 https	://10.104.208.56/acsadmin/N	IARsLPInputAction.do?listType=EndStatio	n	Certificate error
	End Station Filters			Showing 1-2 of 2 50	▼ per page Go
	Filter:	<ul> <li>Match if:</li> </ul>	🗕 🐨		
		Name 🔺	Description		
	0	Contractor End Stn Filter			
	۲	Employee End Stn Filter			
	Crea	te Duplicate Edit	Delete	I Page	1 of 1 🕨 🕅
	OK C	ancel			Help

#### Marque a caixa de seleção Permitir acesso.

Ę	Cisco Secure ACS Webpage Dialog					
	https://10.104.208.56/acsadmin/NetworkAccessLPInputAction.do		💈 Certificate error			
	Authorization Profiles	Showing 1-2 of 2 50	▼ per page GO			
	Filter: 🔹 Match if: 🔹 🐨					
	Name   Description					
	DehyAccess					
	Permit Access		_			
	Create Duplicate Edit Delete	I Page	1 of 1 🕨 🕨			
	OK Cancel		Help			

Repita as mesmas etapas acima para Regras do Contratante também. Verifique se a ação

padrão é **negar acesso**. Depois de concluir a etapa e, suas regras devem se parecer com este

#### exemplo:

A REAL POINT OF THE PARTY NAME						
Caller ( Traper / 100, 18 4 200, 56 / sc rather	n/ D + O Cette. E G X / Cico Seque ACS X					
V Q Share Browner, Webber +						
X Value and the weather of						
ulturlu, Cisco Secure At	S	acautein	acationsphere (Primary)	Log Out About 1Mp		
CISCO EVAL(Days left 5)						
1 H H H H						
> St Wyworksbace	2 My/Norfespace Access Patcles > Access Service > Default Velverk Access > Aethorization					
* (5) Nelwork Resources	Standard Policy Exception Policy					
Users and identity Stores	Network Access Authorization Policy					
» Qv PolicyElements	Dire Gates - Mitch If Causis - Clear Dire Dire					
- 🐍 Access Policies	The owned a match of the contract field a					
* Access Services	Status Name Hasta Conditions	Results	HECOVE			
1 Service Selection Rules	Contractor in all General Contractor in all General Topes (M.C., match Contractor End Str. Ether	Puttorization Profess				
itentiv	Contrator in a dropp contrator in a belice rights will be inder contrator che der met	Pointereness				
Authorization	2 C O Englose in Al Groups Employee in Al Device Types WLC match Employee End Sh Fitter	Pernit Access	,			
<ul> <li>O Default Network Access</li> </ul>						
identy .						
· · · · · · · · · · · · · · · · · · ·						
<ul> <li>System Administration</li> </ul>						
	P Detail I no tales defined or no enabled rule matches.	DenyAccess	8			
	Create Le Duplicate Le Edit Delete A Marein V		Custor	No HoCourt		
	Construction operations in a second s					
	Bave Changes Discard Changes					

Isso conclui a configuração. Depois desta seção, o cliente precisa ser configurado de acordo com o SSID e os parâmetros de segurança para se conectar.

## Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.