Configurar o ponto de acesso leve como um solicitante 802.1x

Introduction

Este documento descreve como configurar um Lightweight Access Point (LAP) como um suplicante 802.1x para se autenticar no servidor Identity Services Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controlador de LAN sem fio (WLC) e LAP
- 802.1x em switches Cisco
- ISE
- EAP (Extensible Authentication Protocol) Autenticação flexível via Secure Tunneling (FAST)

Componentes Utilizados

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

- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- ISE 2.0

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.

Informações de Apoio

Nessa configuração, o ponto de acesso (AP) atua como o suplicante 802.1x e é autenticado pelo switch em relação ao ISE que usa EAP-FAST com provisionamento de PAC (Protected Access Credentials) anônimo. Quando a porta é configurada para autenticação 802.1x, o switch não permite que nenhum tráfego diferente do 802.1x passe pela porta até que o dispositivo conectado à porta se autentique com êxito. Um AP pode ser autenticado antes de ingressar em uma WLC ou depois de ingressar em uma WLC, caso em que você configura 802.1x no switch depois que o LAP ingressa na WLC.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento usa estes endereços IP:

- O endereço IP do switch é 10.48.39.141
- O endereço IP do servidor ISE é 10.48.39.161
- O endereço IP da WLC é 10.48.39.142

Configurar o LAP

Nesta seção, você recebe as informações para configurar o LAP como um suplicante 802.1x.

 Se o AP já estiver associado à WLC, vá para a guia Wireless e clique no AP, vá para o campo Credenciais e, no cabeçalho Credenciais do 802.1x, marque a caixa de seleção Sobrepor credenciais globais para definir o nome de usuário e a senha 802.1x para este AP.

cisco	MONITOR	<u>W</u> LANs <u>(</u>	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MM/
Wireless	All APs > I	Details fo	r Aks_desk	_3502			
 Access Points All APs Radios 	General	Creden	tials Inte	erfaces	High Availabil	ity Inventory	/ Fle
802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration	Login Cred	entials e Global cre	dentials				
Advanced Mesh	802.1x Sup	oplicant Cre	edentials				
▶ ATF	Over-rid	e Glo <mark>b</mark> al cre	dentials				
RF Profiles	Userna	ame	ritmahaj				
FlexConnect Groups	Passw	ord					
FlexConnect ACLs FlexConnect VLAN Templates	Confin	m Password	•••••				
OFAD ACLE							

Você também pode definir um nome de usuário e uma senha comuns para todos os APs que estão associados à WLC com o menu Configuração

gl	0	b	а	I.	
					1

CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	
Wirolocc	CDP State			۲		to	3600)		120
HILCICSS	Ethernet Interface	# CDP S	State			A	P Primed	Join Timeout(120 -	0
Access Points	0	4				43	3200 seco	onds)	U
All APs	1					B	ack-up Pr	imary Controller IP	
	2	<u>ح</u>				A	adress(1p	v4/1pv6)	-
802.11b/g/n	3					Ba	ack-up Pr	imary Controller name	
Dual-Band Radios	4 Radio Slot#	CDP S	state			Ba	ack-up Se ddress(Ip	condary Controller IP v4/Ipv6)	C
Global Configuration	0	1				B	ack-up Se	condary Controller	_
Advanced	1					na	ame	contraity controller	
Mesh	2	1							
ATF						TCP	MSS		
RF Profiles	Login Credentials	•	1			Gle 13	63, IPv6:	Adjust MSS (IPv4: 536 1220 - 1331)	- 0
FlexConnect Groups FlexConnect ACLs FlexConnect VLAN	Username Password					AP F Para	a trans	mit Config 5	
remplates	Enable Password		-			AI	P Retrans	mit Count	5
OEAP ACLs	002 ty Cumplican	t Condontials				AI	P Retrans	mit Interval	3
Network Lists	802.1x Supplican	it credentials							
802.11a/n/ac	802.1x Authenticati	ion				OEA	P Confi	g Parameters	
802.11b/g/n	Username					Di	sable Loo	al Access	
Media Stream	Password					NC En	OTE: abling t	his feature could viol	ate s
Application Visibility And Control	Confirm Password					co	thin you mpliance	e with all regulations	e ma ; befo

2. Se o AP ainda não ingressou em uma WLC, você deve usar o console no LAP para definir as credenciais e usar estes comandos CLI: LAP#debug capwap console cli LAP#capwap ap dot1x username 1. Ative o dot1x no switch globalmente e adicione o servidor ISE ao switch.

```
!
aaa authentication dot1x default group radius
!
dot1x system-auth-control
!
radius server ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
key 7 123A0C0411045D5679
2. Agora, configure a porta do switch AP.
interface GigabitEthernet0/4
```

```
switchport access vlan 231
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Configurar o servidor ISE

1. Adicione o switch como um cliente de Autenticação, Autorização e Auditoria (AAA) no servidor ISE.

• System • Identity Management • Network Resources • Device Portal Management pxGrid Services • Identity Mapping • Network Devices Group Network Device Profile External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM • Network devices Network Devices Ust > akshat_sw Default Device • Name akshat_sw Description • Device Profile @ Clsco • ① • Device Profile @ Clsco • ① • Network Devices Group Location All Locations • Set To Default • Network Device Types • Set To Default • RADIUS Authentication Settings Protocol RADIUS • Shared Secret	cisco	Identity Serv	vices Engine	Home	 Operations 	▶ Policy	▶ Guest A	ccess	✓ Admini	istration	♦ World	k Centers		
Network Device Group vetwork Device Group Network Device Profile Default Device Default Device * Name * Device * Device Profile * Device Type Set To Default Device Type Enable Authentication Settings Protocol RADIUS * Shared Secret * Show	▶ Sy	stem 🕨 Ident	tity Management	✓Network	k Resources	Device Portal	Management	pxGrid	Services	► Feed	Service	Identity Mappin	g	
Network devices Default Device * Name akshat_sw Description * IP Address: 10.48.39.141 / 32 * Device Profile # Cisco * Device Profile # Obvice State * Device Profile # Obvice Profile <td>▼Ne</td> <td>twork Devices</td> <td>Network Device</td> <td>Groups</td> <td>Network Device Pr</td> <td>ofiles Exte</td> <td>ernal RADIUS</td> <td>Servers</td> <td>RADIUS</td> <td>Server Se</td> <td>quences</td> <td>NAC Managers</td> <td>External MDM</td> <td>► L</td>	▼ Ne	twork Devices	Network Device	Groups	Network Device Pr	ofiles Exte	ernal RADIUS	Servers	RADIUS	Server Se	quences	NAC Managers	External MDM	► L
Network devices Default Device * Name_akshat_swl				Netwo	rk Devices List > ak	shat_sw								
Default Device * Name	Networ	rk devices		Netv	vork Devices									
Description	Default	t Device			* N	ame akshat	_sw							
P Address: 10.48.39.141 32 * Device Profile ** Cisco * Model Name v Software Version v Software Version v * Network Device Group Location All Locations Set To Default Device Type All Device Types Set To Default v rADIUS Authentication Settings Frable Authentication Settings Protocol RADIUS * Shared Secret					Descrip	tion								
* Device Profile 🗰 Cisco • 🕀 Model Name • • Software Version • • * Network Device Group Location All Locations • Set To Default Device Type All Device Types • Set To Default • RADIUS Authentication Settings Finable Authentication Settings Protocol RADIUS * Shared Secret • Show					* IP Address: 1	0.48.39.141	/	32						
* Network Device Group Location All Locations Set To Default Device Type All Device Types Set To Default • RADIUS Authentication Settings Enable Authentication Settings Protocol RADIUS * Shared Secret					* Device Pr Model N Software Ver	ofile della Cis ame	co ▼ ⊕							
Location All Locations Set To Default Device Type All Device Types Set To Default Image: Contract of the set of the					Network Device	Group								
Device Type All Device Types Set. To Default Image: Constraint of the set of the					Location All Lo	ocations	S	et To Def	ault					
 RADIUS Authentication Settings Enable Authentication Settings Protocol RADIUS * Shared Secret Show 				ſ	Device Type All D	evice Types	0 s	et To Def	ault					
RADIUS Authentication Settings Enable Authentication Settings Protocol RADIUS * Shared Secret														
Enable Authentication Settings Protocol RADIUS * Shared Secret Show				✓		ntication Sett	ings							
Protocol RADIUS * Shared Secret Show						Ena	ble Authentica	tion Settin	gs					
* Shared Secret Show								Proto	col RAD	IUS				
							* Sł	nared Sec	ret	•••		Show		

dentity Services Engine	Home ► Opera	ations Policy Guest Access		0
System Identity Management	✓ Network Resources	Device Portal Management pxGrid S	Services Feed Service Fidentity Mappin	g
Network Devices Network Device	e Groups Network Dev	vice Profiles External RADIUS Servers	RADIUS Server Sequences NAC Managers	External MDM Locat
	0			
Network devices	Network Devi	ices		
Default Device				
	🖊 Edit 🕂 Add	I Duplicate Duplicate Export -	Generate PAC X Delete	
	Name	IP/Mask Profile Name	Location	Туре
	GurpWLC1	10.48.39.155/32 🗰 Cisco 🕀	All Locations	All Device Types
	GurpWLC2	10.48.39.156/32 💼 Cisco 🕀	All Locations	All Device Types
	akshat_sw	10.48.39.141/32 \arg Cisco 🕀	All Locations	All Device Types

2. No ISE, configure a política de autenticação e a política de autorização. Nesse caso, a regra de autenticação padrão que é wired dot.1x é usada, mas é possível personalizá-la de acordo com o requisito.

cisco Ident	ity Services Engine Hon	ne		Guest Access	Administration	► Work
Authenticatio	n Authorization Profiling	Posture Client Provi	sioning 🕨 P	olicy Elements		
Authenticat	ion Policy					
Define the Auth For Policy Expo	entication Policy by selecting the ort go to Administration > System >	protocols that ISE shou > Backup & Restore > P	ld use to comr olicy Export P	nunicate with the netw age	vork devices, and the	identity sou
Policy Type () Simple 💿 Rule-Based					
	MAB	: If Wired_MAB C	DR			
Wireless_MA	BAllow Protocols : Default Netwo	ork Access and				
<u> </u>	Default	:use Internal E	Endpoints			
	Dot1X	: If Wired_802.1X	OR			
Wireless_802	.1XAllow Protocols : Default Net	work Access and				
	Default	:use All_User	_ID_Stores			
	Default Rule (If no match)	: Allow Protocols :	Default Netw	ork Access and use :	All User ID Stores	

Certifique-se de que nos protocolos permitidos de Acesso à Rede Padrão, EAP-FAST seja permitido.

dentity Services Engine	Home Operations Policy Guest Access Administration Work Centers	(
Authentication Authorization Profiling	Posture Client Provisioning Policy Elements	
Dictionaries Conditions Results		
 Authentication 	Allow EAP-FAST EAP-FAST Inner Methods	
Allowed Protocols	Allow EAP-MS-CHAPv2	
▶ Authorization	Allow Password Change Retries 3 (Valid Range 0 to 3)	
▶ Profiling	Allow EAP-GTC	
▶ Posture	Allow Password Change Retries 3 (Valid Range 0 to 3)	
► Client Provisioning	 Allow EAP-TLS Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy Use PACs Don't Use PACs Tunnel PAC Time To Live 90 Days Proactive PAC update will occur after 90 % of PAC Time To Live has expired Allow Anonymous In-Band PAC Provisioning Allow Authenticated In-Band PAC Provisioning Server Returns Access Accept After Authenticated Provisioning Accept Client Certificate For Provisioning 	

3. Quanto à política de autorização (Port_AuthZ), nesse caso, as credenciais de AP foram adicionadas a um grupo de usuários (APs). A condição usada foi "Se o usuário pertencer ao AP do grupo e fizer o dot1x com fio, pressione o Perfil de autorização padrão para acessar." Novamente, isso pode ser personalizado de acordo com o requisito.

cisco	Identity	Services Engin	ne Ho	me ⊧O	perations	- Policy	Guest Access	Administration	Work Centers		
Authe	ntication	Authorization	Profiling	Posture	Client Provis	sioning 🕨 F	Policy Elements				
Autho	rization	Policy									
Define t For Poli	he Authori cy Export	zation Policy by c go to Administration	onfiguring ru on > System	les based on > Backup &	identity gro Restore > P	ups and/or ot olicy Export F	her conditions. Drag a Page	nd drop rules to chang	e the order.		
First M	atched Ru	le Applies	*								
▼ Ex	ceptions	(0)									
+	Create a	New Rule									
Star	ndard										
	Status	Rule Name			Condi	ions (identity	groups and other con	ditions)		Permissions	
		Port_AuthZ			APs	ND Wired_8	02.1X			PermitAccess	
cisco la	lentity Ser	vices Engine	Home	 Operations 	▶ Policy	► Guest /	Access - Administra	ition + Work Centers	-	0	Licens
► System	m 🗸 Ider	itity Management	Network R	esources 🕨	Device Porta	I Management	pxGrid Services	Feed Service Identi	ty Mapping		
Identit	ies Grou	ips External Iden	tity Sources	Identity Sour	rce Sequence:	s Settings	i				
Iden	tity Group	5		User Iden	tity Groups > A	Ps					
•			Q	Identit	y Group						
III CALL	100		070	* N	Jame APd						

y Groups	Identity Group						
	D Identity Group						
₩ •	* Name APs						
Endpoint Identity Groups	Description Credentials f	or APs					
	Save Reset Member Users Users					Selected 0 Total 1 🥞	<u>چې</u>
	🕂 Add 👻 🗶 Delete 👻			Show	All		8
	Status	Email	Username	 First 	t Name	Last Name	
	🗌 📴 Enabled		🙎 ritmahaj				

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Quando o 802.1x é ativado na porta do switch, todo o tráfego, exceto o 802.1x, é bloqueado pela porta. O LAP, que se já estiver registrado na WLC, é desassociado. Somente após uma autenticação 802.1x bem-sucedida é permitido que outro tráfego passe. O registro bem-sucedido do LAP para a WLC depois que o 802.1x é ativado no switch indica que a autenticação do LAP é bem-sucedida. Você também pode usar esses métodos para verificar se o LAP foi autenticado.

1. No switch, insira um dos comandos **show** para verificar se a porta foi autenticada ou não. akshat_sw#**show** dot1x interface g0/4

```
Dot1x Info for GigabitEthernet0/4
_____
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
akshat_sw#show dot1x interface g0/4 details
Dot1x Info for GigabitEthernet0/4
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
Dot1x Authenticator Client List
_____
EAP Method = FAST
Supplicant = 588d.0997.061d
Session ID = 0A30278D000000A088F1F604
Auth SM State = AUTHENTICATED
Auth BEND SM State = IDLE
```

```
akshat_sw#show authentication sessions
```

Interface MAC Address Method Domain Status Fg Session ID Gi0/4 588d.0997.061d dot1x DATA Auth 0A30278D000000A088F1F604

 No ISE, escolha Operations > Radius Livelogs e verifique se a autenticação foi bemsucedida e se o perfil de autorização correto foi enviado.

cisco Identity S	ervices Engine	Home	✓ Operations	▶ Policy	 Guest Access 	Administration	Work Centers	0	License Warning 👍	۹.
RADIUS Livelog	TACACS Livelog	Reports	Troubleshoot	 Adaptive N 	letwork Control					
Misconfigu	red Supplicants ①		Misconfigured N O	letwork Device	s D	RADIUS Drops 0	(i) Clie	nt Stopped Responding (1) 3		Repeat Cou 0
Show Live Ses	iions 🎲 Add or Rer	move Columr	ns 🔻 🏀 Refresh	🕐 Reset Repe	at Counts		Refresh	1 minute * Show	Latest 100 records	• within
Time	▼ Status All ▼ D	etails Rep	eat Count	ty () Er	ndpoint ID (i)	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Pr	rofiles ()
2017-03-09 10:32	28.956	ò	ritmaha	aj 58	:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ	PermitAccess	a
2017-03-09 10:31:	29.227	ò	ritmaha	aj 58	:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ		a

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

- 1. Insira o comando **ping** para verificar se o servidor ISE está acessível no switch.
- 2. Verifique se o switch está configurado como um cliente AAA no servidor ISE.
- 3. Verifique se o segredo compartilhado é o mesmo entre o switch e o servidor ACS.
- 4. Verifique se o EAP-FAST está ativado no servidor ISE.
- 5. Verifique se as credenciais 802.1x estão configuradas para o LAP e são as mesmas no servidor ISE. **Note**: O nome de usuário e a senha diferenciam maiúsculas e minúsculas.
- 6. Se a autenticação falhar, insira estes comandos no switch: **debug dot1x** e **debug authentication**.