# Exemplo de configuração do portal cativo do DNA Spaces com controlador AireOS

# Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Configurar Diagrama de Rede Configurações Conectar a WLC aos Cisco DNA Spaces Criar o SSID em espaços do DNA Configuração da ACL no controlador Portal cativo sem servidor RADIUS em espaços do DNA Portal cativo com servidor RADIUS em espacos do DNA Criar o portal no DNA Spaces Configurar as regras do portal cativo em espaços do DNA Verificar Troubleshoot

# Introduction

Este documento descreve como configurar portais cativos usando o Cisco DNA Spaces com um controlador AireOS.

Contribuição de Andres Silva, engenheiro do Cisco TAC.

# Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso à interface de linha de comando (CLI) ou à interface gráfica de usuário (GUI) dos controladores sem fio
- Cisco DNA Spaces

## **Componentes Utilizados**

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

Controladora 5520 Wireless LAN versão 8.10.112.0

# Configurar

## Diagrama de Rede



## Configurações

### Conectar a WLC aos Cisco DNA Spaces

O controlador precisa ser conectado ao DNA Spaces usando qualquer uma das configurações disponíveis, Direct Connect, via DNA Spaces Connector ou usando Tethering CMX.

Neste exemplo, a opção Direct Connect está em uso, embora os portais cativos sejam configurados da mesma forma para todas as configurações.

Para conectar o controlador ao Cisco DNA Spaces, ele deve conseguir acessar a nuvem do Cisco DNA Spaces por HTTPS. Para obter mais informações sobre como conectar o controlador ao DNA Spaces, consulte este link: <u>Exemplo de configuração de conexão direta do DNA Spaces</u>

#### Criar o SSID em espaços do DNA

Etapa 1. Clique em Portais cativos no painel do DNA Spaces:



Etapa 2. Abra o menu do portal cativo clicando no ícone de três linhas no canto superior esquerdo da página e clique em **SSIDs:** 

	C A March Angeleter A Conference and and	- 0 6 1
Cisco DNA S	paces	C 10000
D Permit		
IF Capital Particle	ules	ImpartConfigure 1550
	550a	
A Reports	*	
A the Measure		

Etapa 3. Clique em **Import/Configure SSID**, selecione **CUWN (CMX/WLC)** como o tipo de "Wireless Network" e insira o nome do SSID:

Cisco DNA Spaces 😁		C 5439
Cisos Meseli (SIOs		Insperi/Configure (880)
	SSID Configuration Youtware actual any Cost Move 1904 yet. Solid Jobs to get actual	

#### Configuração da ACL no controlador

Uma ACL de pré-autenticação é necessária, pois é um SSID de autenticação da Web e assim que o dispositivo sem fio se conecta ao SSID e recebe um endereço IP, o estado do gerenciador de políticas do dispositivo passa para o estado **Webauth\_Reqd** e a ACL é aplicada à sessão do cliente para restringir os recursos que o dispositivo pode acessar.

Etapa 1. Navegue até **Segurança > Listas de controle de acesso > Listas de controle de acesso,** clique em **Novo** e configure as regras para permitir a comunicação entre os clientes sem fio para o DNA Spaces da seguinte maneira. Substitua os endereços IP pelos fornecidos pelos espaços do DNA para a conta em uso:

	ral									
CE 8 81	List Name	DNASpec	m-ACL							
Deny Counters		٥								
Seq	Action	Source IP/Hask	Destination IP/Mask	Protocol	Source Port	Deat Port	OSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 /	34.235.248.212 /	TCP	Any	HTTPS	Any	Any	0	
2	Permit	34.235.248.212 /	0.0.0.0 /	TCP	HTTPS	Any	Any	Any	0	
ı	Permit	0.0.0.0 /	52.55.235.39 /	Any	Any	Any	Any	Any	0	
a.	Permit	52.55.235.39 / 255.255.255.255	0.0.0.0	TCP	HTTPS	Any	Any	Any	0	

**Observação**: para obter os endereços IP dos espaços do DNA a serem permitidos na ACL, clique na opção **Configurar manualmente** do SSID criado na etapa 3 da seção **Criar o SSID nos espaços do DNA** na seção de configuração da ACL.

O SSID pode ser configurado para usar um servidor RADIUS ou sem ele. Se a Duração da sessão, o Limite de largura de banda ou o Provisionamento contínuo da Internet estiverem configurados na seção **Ações** da configuração Regra de portal cativo, o SSID precisará ser configurado com um Servidor RADIUS; caso contrário, não haverá necessidade de usar o Servidor RADIUS. Há suporte para todos os tipos de portais nos espaços do DNA em ambas as configurações.

#### Portal cativo sem servidor RADIUS em espaços do DNA

Configuração de SSID no controlador

Etapa 1. Navegue até WLAN > WLANs. Crie uma nova WLAN. Configure o Nome do perfil e o SSID. Certifique-se de que o nome do SSID seja o mesmo que o configurado na etapa 3 da seção Criar o SSID em espaços do DNA.

cisco	HONETON	HLANG C	ONTROLLER WIRELESS	SECURITY HEMAGEMENT	COMMANDS HELP	PEEDBACK	
WLANs	WLANs						
WLANS WLANS	Correct Filter	n Nore	(Change Filter)	Cour filter)		Crante New	
> Advanced	O WLAN SD	Type	Profile Name	WLAN SEED	Admin Status	Security Policies	
	01	WSAN	3446	.440	Brabled	[MPR2][Auth(P9K]]	

Etapa 2. Configure a segurança da camada 2. Navegue até a guia **Security > Layer 2** na guia Configuration da WLAN e selecione as **None** no menu suspenso Layer 2 Security. Certifique-se de que a filtragem MAC esteja desativada.

ululu cisco	MONITOR WEANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > Edit 'AireOS-DNASpaces'
VLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security f
	MAC Filtering R
	OWE Transition Mode
	Fast Transition
	Fast Transition Adaptive 😳
	Reassociation Timeout 20 Seconds

Etapa 3. Configure a segurança da camada 3. Navegue até a guia Security > Layer 3 na guia de configuração da WLAN, configure Web **Policy como o método de segurança da Camada 3**, **Enable Passthrough, configure a ACL de pré-autenticação, enable** Override Global Config como o Web Auth Type como External, **configure a URL de redirecionamento.** 

WLANs     WLANs > Edit 'AireOS-DNASpaces'       * WLANs     Security QS Policy-Mapping Advanced       > Advanced     Loser 3 Security Ret Price       > Advanced     Captive National Research	alialia cisco	NONITOR NERVE CONTROLLER WORELESS SECURITY HANAGEMENT COMMANDS HELP FEEDBACK
WLANs     W	WLANs	WLANs > Edit 'AireOS-DNASpaces'
Advanced     Law 3 Security     Net Pairs     Capture Nativer's Assistant Spaces     Capture Nativer's Assistant Spaces     Advanced     Capture Nativer's     Advanced     Capture Nativer's     Conditioner Web Rativer's     Presentmetricetors     Conditioner Web Rativer's     Engel     Conditioner Web Rativer's     Engel     Conditioner Web Rativer's     Engel     Conditioner Web Rativer's     Conditioner     Conditioner Rativer's     Conditioner Rati	* WLANs WLANs	General Security QoS Policy-Mapping Advanced
Skeeping Cleant Auto Automaticals (2) Enable Overrate Blobal Control (2) Brades	> Advanced	Later 3 Resulty       Note Price         Captive Nutwork Assistant Types       Note 2         Authoritation       Image Nuth Redirect         CasedSource Web Redirect       State 1 Results         Table Price Nuth Redirect       On MAC Piter RedureN         PresenterScatson ACL       Image Nuth Results         On MAC Piter RedureN       PresenterScatson ACL         PresenterScatson ACL       Image Nuth Results         Or SMAC Piter RedureN       PresenterScatson ACL         PresenterScatson ACL       Image Nuth Results         Or SMAC Piter RedureN       PresenterScatson ACL         PresenterScatson ACL       Image Nuth Results         Or SMAC Piter RedureN       PresenterScatson ACL         PresenterScatson ACL       Image Nuth Results         Or SMAC Piter RedureN       PresenterScatson ACL         PresenterScatson ACL       Image Nuth Results         Email Input       Seeging Client         Seeging Client       Emails         Seeging Client       Emails         Overniee Robard Coding <sup>20</sup> Truster

**Observação**: para obter o URL de redirecionamento, clique na opção **Configurar manualmente**, no SSID criado na etapa 3 da seção **Criar o SSID em espaços do DNA,** na seção de configuração do SSID.

Portal cativo com servidor RADIUS em espaços do DNA

**Observação**: o servidor RADIUS do DNA Spaces oferece suporte apenas à autenticação PAP proveniente do controlador.

Configuração de servidores RADIUS no controlador

Etapa 1. Navegue para **Security > AAA > RADIUS > Authentication,** clique em **New** e insira as informações do servidor RADIUS. O Cisco DNA Spaces atua como um servidor RADIUS para

autenticação de usuário e pode responder em dois endereços IP. Configure os dois servidores RADIUS:

cisco	HONETON	WEARS .	CONTROLL	IR WORKERS	S SECURITY HAN	AGEMENT	COMMANDS	ни	HEDBACK			
Security	RADIUS	Authentic	ation Ser	vers								
AAA     Consenil     NADOUS     Authentication     Accounting     Auth. Canhead Users     Falbook     ONS	Auth Ca Una Alth MAC Da Pramad	Hed Station 10 1 Kay Wrop Smitar MTU	Tee () () () () () () () () () () () () () (	IP MAC Address Designed for F3P Typhen 300	SSID	5 à kéy ariy	e conștiant Addi	/S serve	1			
Downloaded AVP + TACACE+	Nativork User	Managemer	Tunnel Preny	Server Index	lerver Address(3pv4/1	(###)		Nort 1	(Pfec	Admin \$5	atus	
LEAP				1 1	4.197.146.105			#12	Disabled	Enabled		
Local Net Users				2 1	4.228.1.95			612	Disabled	Enabled		

**Observação**: para obter o endereço IP RADIUS e a chave secreta para servidores primários e secundários, clique na opção **Configurar manualmente** do SSID criado na etapa 3 da seção **Criar o SSID nos espaços do DNA** e navegue até a seção **Configuração do servidor RADIUS**.

Etapa 2. Configure o servidor RADIUS de contabilização. Navegue para **Security > AAA > RADIUS > Accounting** e clique em **New**. Configure os mesmos dois servidores RADIUS:

cisco	HONETOR	WLANS .		ta wyatu	ESS SECURITY	MANAGEMENT	сонников	нер	TEDMAX		
Security	RADIUS	Accountin	g Server	8							
• AAA General • RADIUS Authentication Accounting	Ant Cal MAC De AP Even	ied Station ID Imiter Is Accounting	han is in o	yatam MAC A lyphan Enable	ditress 📑						
Paliback Druš	Network User	Managaman	Tunnel Praxy	Server Index	Server Addre	es(Ipv4/1pv6)	F	Port	1Plies	Admin Status	1
Downloaded #177				1	34.197.146.10	5		1813	Cisabled	Enabled	
TRCACS+ LOAP				2	34.228.1.95			1813	Oashied	Enabled	•

Configuração de SSID no controlador

**Importante**: antes de iniciar com a configuração SSID, certifique-se de que a **Web Radius Authentication** esteja definida como "PAP" em Controller > General.

Etapa 1. Navegue até WLAN > WLANs. Crie uma nova WLAN. Configure o Nome do perfil e o SSID. Certifique-se de que o nome do SSID seja o mesmo que o configurado na etapa 3 da seção Criar o SSID em espaços do DNA.

uluilu cisco	HONETON	ILANS C	ONTROLLER	WINDLESS	SECURITY	NANACEMENT	COMMANDS	157	REDBACK		
WLANs	WLANs										
WLANA WLANA	Correct Filter	Carrent Pillers None (Charge Film) (Dear Film)									8 94
> Advanced	O WLAN 20	Type	Profile Nam		WLA	N SSID		in Status	Security Polici		
	01	WUM	.440		JAND	•	5rel	led.	[8992][649-(99	(i)	

Etapa 2. Configure a segurança da camada 2. Navegue até a guia **Security > Layer 2** na guia de configuração da WLAN. Configure a segurança de camada 2 como **None**. Ative A Filtragem Mac.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > Edit 'AireOS-DNASpaces'
VLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security 4 None C MAC Filtering 2 C
	OWE Transition Mode
	Fast Transition     Adaptive       Over the DS     Image: Comparison of the second se

Etapa 3. Configure a segurança da camada 3. Navegue para a guia Security > Layer 3 na guia de configuração da WLAN, configure Web **Policy como o método de segurança da Camada 3**, **Enable On Mac Filter failure, configure a ACL de pré-autenticação, enable Override Global Config** como definido o Web Auth Type como External, **configure o Redirect URL.** 

cisco	MONILLON RETWO CONLINER MARTERS RECTWILL MENVARIMENT COMMANDE HET LEEDENCK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
<ul> <li>WLANs NUMB</li> <li>Advanced</li> </ul>	General Security QoS Policy-Mapping Advanced Layer 2 Layer 3 AAA Servers Layer 3 Security Test Policy Captus National Australiant Bypass Piece C Authoritication
	Conditional Web Redirect Splach Page Web Redirect O on MAC Filter Talkure <sup>37</sup> Presudventication ACL D'V4 DSAdgenese ACL B 3Pv6 Pane B WebAuth Files 3PV4 Ad Rene B WebAuth Files 3PV6 Ad Pane B Redirect UR5, https://wpitch.dnespeces.kr/p2/mcreated5 Desping Clant B Enable Simpling Clant Auto Automiscate B Enable
	Override Global Config <sup>104</sup> C Enable Web Auth hype External (Re-direct to external server)

Etapa 4. Configure os servidores AAA. Navegue até a guia **Security > AAA Servers** na guia de configuração da WLAN, habilite **Authentication Servers** e **Accounting Servers** e, no menu suspenso, escolha os dois servidores RADIUS:

cisco	HONITOR MLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEBAA	×
WLANs	WLANs > Edit 'AireOS-DNASpaces'	
WLANS	General Security QoS Policy-Mapping Advanced	
+ Advanced	Layer 2 Layer 3 AAA Servers	
	RADIUS Servers RADIUS Server Overante Interface Enabled Apply Cisco 19E Default Settings Enabled Authentication Servers Accounting Servers	
	C Enabled C Enabled	
	Server 1 IP:34.197.146.105, Port:1812 DP:34.197.146.105, Port:1813	
	Server 2 19:34.228.1.95, Port:1812 🚦 19:34.228.1.95, Port:1813 🔒	
	Server 3 None O None O	
	Server 4 None 📴 None 📴	
	Server 5 None 0	
	Server 6 None 0	

Etapa 6. Configure a **ordem de prioridade de autenticação para usuários de autenticação da Web**. Navegue até a guia **Security > AAA Servers** na guia de configuração da WLAN e defina RADIUS como o primeiro na ordem.

alialia cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
WLANs	General Security QoS Policy-Mapping Advanced
Advanced	RADOUS Authentication Survivability
	Asthentikation Survivability LDAP Servers
	Server 1 None
	Server 3 None 0
	Local EAP Authentication
	Local EAP Authentication Canabled
	Authentication priority order for web-auth user
	Not Used For Authentication
	<ul> <li>RADUS Up</li> <li>UOCAL</li> <li>UDAP</li> <li>Down</li> </ul>

Passo 7. Navegue até a guia **Advanced** na guia de configuração da WLAN e habilite **Allow AAA Override.** 

alialia cisco	MONITOR MUNIC CONTROLLER WIRELESS SECURITY MANAGEMENT	COMMANDS HELP (TEDBACK		
WLANs	WLANs > Edit 'AireOS-ONASpaces'			
* WLANs MLANs	General Security QoS Policy-Happing Advanced			
> Advanced	Allow AAA Overvide G Enabled	DWCP		
	Coverage Hole Detection 😨 Enabled	DHCP Server Override		
	Enable Session Timeaut (2000 Session Timeaut (secc)	DRCP Addr. Assignment C Required		
	Aronet III Crabled	Management Frame Protection (MPP)		
	Diagnostic Diarnal II Entelled Override Interface IIC, 3Put None II SPut None II Layer? Act None II	MIP Clerc Postection f Optional		
	URL ACL None B 727 Blocking Action Doubled B Claret Declarizer 2 (Crashed 190	802.134/w (1 - 255) 1 902.135/g/w (1 - 255) 1		
	Havinum Allowed Clents	NAC State None		
	Static IP Turneling M Evabled Wi-Fi Direct Pulicy Deadled	Client Load Balancing Client Band Salest		

#### Criar o portal no DNA Spaces

Etapa 1. Clique em Portais cativos no painel do DNA Spaces:

ACT - Leverage Digitization toolkits t	o Act on Insights.
Captive Portals	Engagements
Onboard and acquire visitors at your properties	Deliver contextual multi-channel notifications
1	0

Etapa 2. Clique em **Criar novo,** insira o nome do portal e selecione os locais que podem usar o portal:

	0			
	Portal Information	Authentication	Data Dapture	User Agreement
PORTAL NAME				
AirwOS-DNASpaces				
Enable this control for all local	inter .			
the bring of a party of an article				
Location Herarchy			Selecto	d Locations
Location Herarchy MEX-EAST-1			Selecto	d Locations
Location-Herarchy MEX-EAST-1			C Selecter	d Locations Investment X
Location Herarchy MEX-EAST-1 © \$9568-1-CMX © \$9568-2-Connect	tor		Selecter INDO-10	d Locations Sectored X
Location Herarchy MEX-EAST-1 © 9508-1-CMX © 9508-2-Connect © 9520-1-DirectCo	tor privact		Selecter (MAD-1-	d Locations

Etapa 3. Selecione o tipo de autenticação, escolha se deseja exibir a captura de dados e os contratos de usuário na home page do portal e se os usuários têm permissão para optar por receber uma mensagem. Clique em Next:

	0	<u> </u>			>
	Paralistemation	And an address of the second s	Onto Captore	Line Agenetismin	
18407 THE ALTHRADIAN CALIFORN			-		
Enal					
Value names admit that amaking access the internet.			-		
Display Authentication and Unar Agreement	on pertailhere page				
Allow users to Opt in to receive message					
		500	Page 1		

Etapa 4. Configurar elementos de captura de dados. Se você quiser capturar dados dos usuários, marque a caixa **Enable Data Capture** e clique em **+Add Field Element** para adicionar os campos

desejados. Clique em Next:

	Constantion and a second	Attentiation	-O Interiment	4 Inter Agreements	×
E Brutte Data Capture					
A   Ent Name					:
					·
			_		
		544	C Page 1		

Etapa 5. Marque Ativar termos e condições e clique em Salvar e configurar o portal:

	0	-0		<u> </u>	
	Parial Information	Automicatory	Date Capture	the Agreements	
To active alove you to enable and configure for	Hall-Conditions and Preacy pel-	(y Saneera			
Tradae Terriscik Canditons					
UNIC & CENTRON MESSAGE					Qe I Drup
	0.11				
			0.0.0		
8 2 8 9 K F K Z Z Z Z	THE R R R R	Color of Managers	000		
Syles - Format - Fast - B	<ul> <li>(Y, 0) [X ])</li> </ul>				
M P. Terres of Unit. Loss optimist Department (1.3)	×8.				
These Wirl Parts & Canadiana Orline the Mir/13	innel spatier with the 10 MeG OF	USE govern your use of the M-FL or	phice.		
Description of the Decision					
The Register structure are sufficiently as the local	biographic film for exercises. March	at a substant substant substant	and some the second second second	the second se	terior and the second barried beauty
or posted using the Dervice to accurate fail users con	phy with it was the fit is the sampler it	o ine all'ough i contrat the sight	k-ik m.	and the late of the period is described by the period to	COLOR BY CREW HERE CREW
		San ( Free	Save & Configure Portal		

Etapa 6. Edite o portal conforme necessário. Clique em Salvar:

Sealther / Beal / Bailing /	Han annait Pine Nama Jani Nama /	
9854, 19708 - Souri a sector to configera Just	the lamest-reprint methods	
Brand Name		ROTA PRIVIN
Weisarie Message	EVAD NAME	< wome Scoon.
Netwo	Charlanted are tampentic or graphic mark that identifies user formal	Cisco Systems
Email Authentication	Twe Only D Lease	
Ø Venallip	5840 MME	Welcome to Spoulierd
· Vileo	Cisor Summa	Side UP FOR WITH
D Peebenk		Complete the lower before is connect to internet
€ Hep		Tenter
<ul> <li>Get Apps</li> </ul>		
· Cellifered		
Prones & Offers		
· Mat Human		

Configurar as regras do portal cativo em espaços do DNA

Etapa 1. Abra o menu do portal cativo e clique em Captive Portal Rules:

⊕ → ♂ ≙	A https://dnaspaces.io/captiveportal/hules/captive-portal	
Cisco DNA Spaces		
D Portal		
E Captive Portal Rules		Created
ି \$\$10s	and and a set	Feb 24, 2020
a Reports	>	○ 8.02 PM

Etapa 2. Clique em + Criar nova regra. Insira o nome da regra, escolha o SSID configurado anteriormente e selecione os locais para os quais esta regra de portal está disponível:

see any or an or the options that apply to your rule below	
	Distance of the second s
When a user is on VIPI - and connected to Avect-th/Ripaces -	NUL MAR
	anu01-Oferligeren
(3041040) - When its you want the rule to tes?	50,995
	When your is so fully and contracted to flow?
	INAlyacar
At any of the tonsweng locations	LODATIONE.
+ destination	For all longiture under
( Constant)	1000-1 OwnCommon
Hild-Himsdammer N	and all have a second
	ID-RAAI
Filter by Mintachila	
1.2 Further than your to other your by including of reached by containing.	107104
	Res Castra Repair

Etapa 3. Escolha a ação do portal cativo. Nesse caso, quando a regra é atingida, o portal é mostrado. Clique em **Salvar e publicar.** 

<ul> <li>Show Digitie Partal Chases a Portal to is dispand to Dans when they connecting the will.</li> </ul>	SCHEDULE
AlwCG-DRAGacan	ACTON Non-Contractioner
Inscient Duration	Partal AreOS OPAGasces
two-add-Unit	
Seamleasi Previolen Internet     Descrip produke internet without showing any sufferentiation	
Deep Internet     Stag area-here accessing the Internet	
Tage these users as Descent - Sectors Teamonts - and is clean too	
* And Tage	
1 tager AT	

## Verificar

Para confirmar o status de um cliente conectado ao SSID, navegue para **Monitor > Clients**, clique no endereço MAC e procure Policy Manager State:

Nove	TOR WLANS	CONTROLLER	WPELESS	SECURITY	HANAGEHENT	COMMANDS	HELP	EEDBACK	
Clien	its > Detail								< Back
Max	number of Record	s 10 * Ck	ter AVC Stats	1					
Ger	eral AVC St	atistics							
						AP radio als	e 1d	1	
o	ient Type	Regular				WLAN Profil		AireOS-OMASpaces	
0	ient Tunnel Type	Simple IP				WLAN SSID		AireOS-ONASpeces	
U	ser Name					Status		Associated	
15	iebauth User Name	None				Association	10	1	
Pt	ort Number	1				802.11 Aut	hentication	Open System	
54	terface	management				Reason Cod	e .	1	
V	LAN ID	20				Status Code		0	
0	varantine VLAN ID	0				CF Pollable		Not Implemented	
0	CX Version	Not Supported				CF Pull Reg	Helt.	Not Implemented	
	of Version	Not Supported				Short Pream	able	Not Implemented	
	ability Role	Lacal				PBCC		Not Implemented	
54	obility Peer IP	ALCO.				Chernel Ap	iity.	Not Implemented	
A	ddress	10.0				Timesul		0	
	obliky Move Count	P	_						
6	Incy Manager	RUN				wer state		WEP Disable	

## Troubleshoot

O comando a seguir pode ser ativado no controlador antes do teste para confirmar o processo de associação e autenticação do cliente.

```
(5520-Andressi) >debug client
```

(5520-Andressi) >debug web-auth redirect enable mac

Este é o resultado de uma tentativa bem-sucedida de identificar cada uma das fases durante o processo de associação/autenticação durante a conexão a um SSID sem servidor RADIUS:

#### Associação/autenticação 802.11:

```
*apfOpenDtlSocket: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Received management frame ASSOCIATION
REQUEST on BSSID 70:d3:79:dd:d2:0f destination addr 70:d3:79:dd:d2:0f slotid 1
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Updating the client capabiility as 4
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Processing assoc-req
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 ssid : AireOS-DNASpaces thread:bd271d6280
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 CL_EVENT_ASSOC_START (1), reasonCode
(1), Result (0), Ssid (AireOS-DNASpaces), ApMac (70:d3:79:dd:d2:00), RSSI (-72), SNR (22)
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Sending assoc-resp with status 0
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 on apVapId 1
```

#### Autenticação de DHCP e Camada 3:

\*apfMsConnTask\_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Mobility query, PEM State: DHCP\_REQD
\*webauthRedirect: Apr 09 21:49:51.949: captive-bypass detection enabled, checking for wispr in
HTTP GET, client mac=34:e1:2d:23:a6:68
\*webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68

user\_agent = AnyConnect Agent 4.7.04056 \*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Preparing redirect URL according to configured Web-Auth type \*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- unable to get the hostName for virtual IP, using virtual IP =192.0.2.1 \*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Checking custom-web config for WLAN ID:1 \*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Global status is 0 on WLAN \*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- checking on WLAN web-auth type \*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Web-auth type External, using URL:https://splash.dnaspaces.io/p2/mexeast1 \*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added switch\_url, redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch\_url=https://192.0.2.1/login.html \*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added ap\_mac (Radio ), redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch\_url=https://192.0.2.1/login.html&ap\_mac=70:d3:79: dd:d2:00 \*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added client\_mac , redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch\_url=https://192.0.2.1/login.html&ap\_mac=70:d3:79: dd:d2:00&client\_mac=34:e1:2d:23:a6 \*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Added wlan, redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch\_url=https://192.0.2.1/login.html&ap\_mac=70:d3:79: dd:d2:00&client\_mac=34:e1:2d:23:a6:68&wla \*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- http\_response\_msg\_body1 is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control"</pre> content="no-cache"><META http-equiv="Pragma" content="</pre> \*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- added redirect=, URL is now https://splash.dnaspaces.io/p2/mexeast1?switch\_url=https://192.0.2.1/login.html&ap\_mac=70:d3:79: dd:d2:00&client\_mac=34:e1:2d:23:a6:68&wlan=Ai \*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- str1 is now https://splash.dnaspaces.io/p2/mexeast1?switch\_url=https://192.0.2.1/login.html&ap\_mac=70:d3:79: dd:d2:00&client\_mac=34:e1:2d:23:a6:68&wlan=AireOS-DNASpaces&r \*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Message to be sent is HTTP/1.1 200 OK Location: https://splash.dnaspaces.io/p2/mexeast1?switch\_url=https://192.0.2.1/login.html&ap\_mac=70:d3:79: dd:d2:00&client\_mac=34: \*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- 200 send\_data =HTTP/1.1 200 OK Location: https://splash.dnaspaces.io/p2/mexeast1?switch\_url=https://192.0.2.1/login.html&ap\_mac=70:d3:79: dd:d2:00&client\_mac=34:e1:2d:23 \*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- send data length=688 \*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68-Url:https://splash.dnaspaces.io/p2/mexeast1 \*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- cleaning up after send Autenticação da camada 3 bem-sucedida, mova o cliente para o estado RUN:

\*emWeb: Apr 09 21:49:57.633: Connection created for MAC:34:e1:2d:23:a6:68
\*emWeb: Apr 09 21:49:57.634:
ewaURLHook: Entering:url=/login.html, virtIp = 192.0.2.1, ssl\_connection=0, secureweb=1
\*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 WEBAUTH\_NOL3SEC (14) Change
state to RUN (20) last state WEBAUTH\_NOL3SEC (14)
\*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL\_EVENT\_WEB\_AUTH\_DONE (8), reasonCode
(0), Result (0), ServerIp (), UserName ()
\*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL\_EVENT\_RUN (9), reasonCode (0), Result
(0), Role (1), VLAN/VNID (20), Ipv4Addr (10.10.30.42), Ipv6Present (No)
\*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 RUN (20) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255, URL ACL ID 255, URL ACL
Action 0)

\*emWeb: Apr 09 21:49:57.634: User login successful, presenting login success page to user

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.