# Ejemplo de Configuración de DNA Spaces Captive Portal con Controlador AireOS

## Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Configurar
Diagrama de la red
Configuraciones
Conecte el WLC a Cisco DNA Spaces
Crear el SSID en espacios de ADN
Configuración de ACL en el controlador
Portal cautivo sin servidor RADIUS en espacios DNA
Portal cautivo con servidor RADIUS en espacios DNA
Crear el portal en espacios de ADN
Configuración de las reglas del portal cautivo en espacios DNA
Verificación
Troubleshoot

## Introducción

Este documento describe cómo configurar portales cautivos usando Cisco DNA Spaces con un controlador AireOS.

Colaboración de Andrés Silva, ingeniero del TAC de Cisco.

#### Prerequisites

#### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso mediante interfaz de línea de comandos (CLI) o interfaz gráfica de usuario (GUI) a los controladores inalámbricos
- Espacios de ADN de Cisco

#### **Componentes Utilizados**

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

• Controlador de LAN inalámbrica 5520, versión 8.10.112.0

## Configurar

Diagrama de la red



y configure las reglas para permitir la comunicación entre los clientes inalámbricos a los Espacios de ADN de la siguiente manera. Reemplace las direcciones IP por las direcciones proporcionadas por DNA Spaces para la cuenta en uso:

Gene	ral									
Access	s List Name	DNASpace	s-ACL							
Deny	Counters	0								
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Deat Port	OSCP	Oirection	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 / 255.255.255.255	0.0.0.0 /	TCP	HTTPS	Any	Any	Arry	0	
1	Permit	0.0.0.0 /	52.55.235.39 / 255.255.255.255	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	ō	

Nota: Para obtener las direcciones IP de los Espacios de ADN que se permitirán en la ACL, haga clic en la opción Configure Manually del SSID creado en el paso 3 de la sección Create the SSID on DNA Spaces bajo la sección de configuración de ACL.

El SSID se puede configurar para utilizar un servidor RADIUS o sin él. Si la duración de la sesión, el límite de ancho de banda o el aprovisionamiento de Internet sin problemas se configuran en la sección Acciones de la configuración de la regla de portal cautivo, el SSID debe configurarse con un servidor RADIUS; de lo contrario, no es necesario utilizar el servidor RADIUS. En ambas configuraciones se admiten todo tipo de portales en espacios DNA.

Portal cautivo sin servidor RADIUS en espacios DNA

Configuración de SSID en el controlador

Paso 1. Vaya a WLAN > WLANs. Cree una nueva WLAN. Configure el nombre del perfil y el SSID. Asegúrese de que el nombre SSID es el mismo que el configurado en el paso 3 de la sección Creación del SSID en Espacios de ADN.

altalta cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MEAAGEMENT	COMMANDS HELP	(TEDBACK	
WLANs	WLANs					
* WLANs WLANs	Correct Filter: No	Ne (Change Filter)	(Clear Filter)		Create New	B 9+
> Advanced	O WLAN ID: Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
	O 1 WLAN	,AND	,AND	Enabled	(WFA2((Auth(PSR))	

Paso 2. Configuración de la seguridad de capa 2. Vaya a la pestaña Security > Layer 2 en la pestaña WLAN configuration y seleccione as None en el menú desplegable Layer 2 Security. Asegúrese de que el filtrado de MAC está desactivado.

uhuhu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > Edit 'AireOS-DNASpaces'
WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security 4 None
	MAC Filtering 2
	OWE Transition Mode
	Fast Transition
	Fast Transition Adaptive
	Over the DS
	Reassociation Timeout 20 Seconds

Paso 3. Configuración de la seguridad de capa 3. Navegue hasta la pestaña Security > Layer 3 en la pestaña de configuración WLAN, configure la política web como el método de seguridad de la capa 3, habilite Passthrough, configure la ACL de preautenticación, habilite Override Global Config como set the Web Auth Type as External, configure la URL de redirección.

ahaha	
CISCO	BORLIOK NEWS CONTROLLER REPELLES SECURITY REPARTERING COMPANIES HELP (EEDERCK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
* WLANs WLANs	General Security QoS Policy-Mapping Advanced
> Advanced	Lever 3 Security       Web Policy         Captive Network Assistant Bygens       None         Authentication       Authentication         Passathrough       Conditional Web Redirect         Splach Page Web Redirect       Splach Page Web Redirect         Conditional Web Redirect       Splach Page Web Redirect         Conditional Web Redirect       Splach Page Web Redirect         Con MAC Pitter failure <sup>18</sup> Web policy done locally on Apennance         Preacthentication ACL       IPv4       OARSpace=ACL       IPv6       WebAuch Piex IPv8 Acl None       WebAuch Piex IPv8 Acl None

Nota: Para obtener la URL de redirección, haga clic en la opción Configure Manually (Configurar manualmente) del SSID creado en el paso 3 de la sección Create the SSID on DNA Spaces (Crear el SSID en espacios de ADN), en la sección de configuración de SSID.

Nota: El servidor RADIUS de Espacios de ADN sólo soporta la autenticación PAP proveniente del controlador.

Configuración de servidores RADIUS en el controlador

Paso 1. Navegue hasta Seguridad > AAA > RADIUS > Autenticación, haga clic en Nuevo e ingrese la información del servidor RADIUS. Cisco DNA Spaces actúa como servidor RADIUS para la autenticación de usuarios y puede responder en dos direcciones IP. Configure ambos servidores RADIUS:

alialia cisco	BONLOR	WLANG O	ONTROLU	ik wijatuti	IS SECURITY	REAGENENT	COMMANDS	ни	DEEDWACK		
Security	RADIUS	Authentica	tion Ser	vers							
AAA     General     Motilus     Activationiation     Accounting     Authonologies     Reflects     SNS	Auth Ca Use AES MAC De Framed	led Station 10 Key Wrap Imitar MTy	Ne+ 2 0 0 E	P MAC Address Designed for PD typhen 100	SSD B	requires a key eraq	i compliant 6420	US serve	3		
Downloaded AVP + TAGNES+	Natwork User	Management	Tunnel Prony	Server Index	Server Address()	(pv4/1pv6)		Pert	(Place	Admin Status	
LOAP	0	8	0	1.	14.197.146.005			1812	Disabled	Enabled	0
HAC Filtering	8	8	0	2	34.228.1.95			1812	Disabled	Enabled	

Nota: Para obtener la dirección IP de RADIUS y la clave secreta para los servidores primario y secundario, haga clic en la opción Configure Manually del SSID creado en el paso 3 de la sección Create the SSID on DNA Spaces y navegue hasta la sección RADIUS Server Configuration.

Paso 2. Configure el servidor RADIUS de cuentas. Navegue hasta Seguridad > AAA > RADIUS > Contabilización y haga clic en Nuevo. Configure los mismos servidores RADIUS:

ahaha cisco	NONTOR	WLANS	CONTROLL	IA WOALLES	is security	HANAGEHENT	COMMANDS	ны	ELEOPACK		
Security	RADIUS	Accounti	ng Server	8							
• AAA Conerol • RADIUS Authentication Accounting	Acct Call MAC Del AP Even	led Station IS limitar Is Accounting	Type S	ystem MAC Add lyphen Enable	inan 😦						
Falback DVG	Natwork User	Hanapama	Tunnel at Proxy	Server Index	Server Addres	o(lavi/lavi)		Part	1PSec	Admin Status	1
Downloaded AUP	0	0	0	1	34,197,546,109	,		140.3	Disabled	Enabled	
LOAP				4	34,218,1.95			1813	(Headlined	Enabled	

Configuración de SSID en el controlador

💊 Importante: Antes de comenzar con la configuración SSID, asegúrese de que Web Radius

Authentication esté configurado como "PAP" en Controller > General.

Paso 1. Vaya a WLAN > WLANs. Cree una nueva WLAN. Configure el nombre del perfil y el SSID. Asegúrese de que el nombre SSID es el mismo que el configurado en el paso 3 de la sección Creación del SSID en Espacios de ADN.

alialia cisco	MONITOR	W.4%	CONTROLLER	WINDLESS	SECURITY	MANAGEMENT	COMMANDS	10,7	FEDBACK		
WLANs	WLANs										
* WLANs WLANs	Current Filte	n Non	• 0	Change Filter) (	Dear Filter)				[	Create New	B 64
+ Advanced	OWAND	Type	Profile Nat		WLA	N 5510	A.6-	in Status	Security Policies		
	01	WEAK	.AND		.ANO		6 nait	ind .	(WPA20)AutoPSK	N	

Paso 2. Configuración de la seguridad de capa 2. Vaya a la pestaña Security > Layer 2 en la pestaña de configuración WLAN. Configure la Seguridad de Capa 2 como Ninguna. Active el filtrado de Mac.

uluilu 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 1 None
	MAC Filtering 2
	OWE Transition Mode
	Fast Transition Adaptive 😒
	Over the DS Z Reassociation Timeout 20 Seconds

Paso 3. Configuración de la seguridad de capa 3. Vaya a la pestaña Security > Layer 3 en la pestaña de configuración WLAN, configure Web Policy como el método de seguridad de la Capa 3, Enable On Mac Filter failure, configure la ACL de preautenticación, habilite Override Global Config como set the Web Auth Type as External, configure la URL de redirección.

ahaha cisco	HONITOR BLANS CONTROLLER WIRELESS SECURITY HANAGEMENT COMMANDS HELP SEEDBACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
* WLANs WLANs	General Security QoS Policy-Mapping Advanced
+ Advanced	Layer 2 Layer 3 AAA Servers
	Layer 3 Security Web Policy
	Captive Network Assistant Bypass None
	Authentication     Passificitude
	Conditional Web Redirect
	O On MAC Filter failure <sup>18</sup>
	Presubentication ACL (Pref. D'AdSpectra-AC). 3 (Pref. None 3) WebAuth Flex (PVI Ad. None 3) WebAuth Flex (PVI Ad. None 3)
	Redirect URL https://splash.dnaspaces.le/p2/mexeaut1
	Siveping Chant 🔄 Brable
	Steeping Client Auto Authenticate 📫 Enable
	Overnee Gotted Canfight  Drable Web Auth type Driemar(Re-direct to external server)

Paso 4. Configuración de servidores AAA. Navegue hasta la pestaña Security > AAA Servers en la pestaña de configuración WLAN, habilite Authentication Servers y Accounting Servers y en el menú desplegable elija los dos servidores RADIUS:

alialia cisco	MONITOR W.	ANS CONTROLLE	R WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нер	FEEDMACK
WLANs	WLANs > Edi	it 'AireOS-DNA	Spaces'					
WLANs WLANs	General	Security QoS	Policy-Mag	oping Adv	ranced			
Advanced	Advanced     Layer 2 Layer 3 AAA Servers							
	RADOUS S Apply Cisc	erver Overwrite inter o ISE Default Setting Authentication Se	face Enabled	Accounting Se				
		Enabled		C Enabled		_		
	Server 1	IP:34.197.146.10	5, Port: 1812 🚦	IP:34.197.14	6.105, Port:1813	8		
	Server 2	19:34.228.1.95, P	ort:1812 😫	19:34.228.1.5	95, Port:1813	<b>2</b>		
	Server 3	None	0	None		0		
	Server 4	None	0	None		0		
	Server S	None	0	None		8		
	Server 6	None		None		÷		

Paso 6. Configure el orden de prioridad de autenticación para los usuarios de autenticación Web. Navegue hasta la pestaña Security > AAA Servers en la pestaña de configuración de WLAN y establezca RADIUS como el primero en orden.

alialia cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MAN	MGEHENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'AlreOS-DNASpaces'	
* WLANs	General Security QoS Policy-Mapping Advanced	d
Advanced	RADDUS Authentication Survivability	
	Authentication Survivability	
	LDAP Servers	
	Server 1 None	
	Server 2 None 2	
	Server 3 Nore C	
	Local EAP Authentication Enabled	
	Authentication priority order for web-auth user	
	Not Used	Order Used For Authentication
		RADIUS Up LOCAL
	<	LOAP Down

Paso 7. Vaya a la pestaña Advanced en la pestaña WLAN configuration y habilite Allow AAA Override.

cisco	MONITOR MLANN CONTROLLER WORELESS SECURITY MUNAGEMENT	COMMANOS HELP PERDIAOK
WLANs	WLANs > Edit 'AlreGS-DNASpaces'	
* WLANs WLANS	General Security QoS Policy-Happing Advanced	
> Advanced	Allow AAA Override  Coverage Mele Detection Coverage Mele Detection Coverage Mele Detection Coverage Mele Detection Anover II Coverage Meleo Coverage Covera	DHCP Server Override DHCP Adds: Ansignment Required Management Protection (NPP) HTP Clant Protection # Optional DTIH Parled (in leases intervals) H02.114(n (1 - 210)
	Maximum Alexand Clients a Static IP Tunneling Al Constraint Work Direct Clients Policy Direction	Load Balancing and Band Select     Clerit Load Balancing     Clerit Select

Crear el portal en espacios de ADN

Paso 1. Haga clic en Portales cautivos en el panel de Espacios de ADN:

ACT - Leverage Digitization toolkits to Act on Insights.					
Captive Portals	0 Engagements	÷			
Onboard and acquire visitors at your prope	es Deliver contextual multi-channel notifications				
ACTIVE CAPTIVE PORTALS	ACTIVE ENGAGEMENTS				

Cisco DNA Spaces

-

Paso 2. Haga clic en Create New, ingrese el nombre del portal y seleccione las ubicaciones que pueden utilizar el portal:

		0			
		Portal Information	Authentication	Data Capture	User Agreement
20	ISA, NAME				
	im05-DNASpaces				
1.000					
0	Enable this portal for all locations				
0	Enable this portal for all locations				
	Enable this portal for all locations Location Hierarchy			Select	ed Locations
	Enable this portal for all locations Location Hierarchy MEX-EAST-1			Select	d Locations
	Enable this portal for all locations Location Hierarchy MEX-EAST-1 © SS08-1-CMX			Select	Inclosed X
	Enable this portal for all locations Location Hierarchy MEX-EAST-1			Select	d Locations Gractionect X
	Enable this portal for all locations Location Hierarchy MEX-EAST-1 S508-1-CMX S508-2-Connector S520-1-DirectConnect			Select	d Locations GracCorrect X

Paso 3. Seleccione el tipo de autenticación, elija si desea mostrar la captura de datos y los acuerdos de usuario en la página principal del portal y si los usuarios pueden participar para recibir un mensaje. Haga clic en Next (Siguiente):

O-		a lastese	e . Ger Aperteris	×
MUCT NE ALTERNATION FOR		1		
Value read's some her end is acres he rained.		1		
Allow users to Opt in to receive message				
	5m +1	No. 1		

Paso 4. Configurar elementos de captura de datos. Si desea capturar datos de los usuarios, marque la casilla Enable Data Capture y haga clic en +Add Field Element para agregar los campos deseados. Haga clic en Next (Siguiente):

	0	o	-0	(i)	×
	Partal information	Automication	Bata Captore	Ger Agnometic	
Entern Cata Capture Rom Fields				+ App If and Clamare	
A   first Name					
A   Latitude					



Paso 5. Marque la opción Enable Terms & Conditions y haga clic en Save & Configure Portal:

	Partie Montadore	- O	Deter Capitore		Х
This section allows you to enable and configure from Control & Contineer Torres & Control Michael	e & Conditions and Privacy policy (	Summers.			Qr i lingian
0 0 0 0 0 × 0 0 0 0 + - 0 2 0 0 × 0 0 0 0 + - 0 1 0 0 × 0 × 15 0 0 0 0 - 0 0 × 1 + + + + + + + + + + + + + + + + + +	9.5.8 9.8.8.8.8 1.5.0.2.0		0.0 4		
M.P. Terms of Use, Last against September 27, 20 December 20, 20 December 2	1). mai tagether with the TERMS OF (10) Internet within the pointies. We do not with these With Terms and in the to	E geneers your une of the 185.45 se C en an ordinary genetice, proved	rulas. Nely munitor the autodates of those of	eter une the Dentite or exercise any selfect	d control over any Material Tanandited, Nadad
an process society are section in a final that wants are	(	tan etan	Seve & Centigure Pertet		

Paso 6. Edite el portal según sea necesario, haga clic en Guardar:



Configuración de las reglas del portal cautivo en espacios DNA

Paso 1. Abra el menú del portal cautivo y haga clic en Reglas del portal cautivo:



Paso 2. Haga clic en + Crear nueva regla. Introduzca el nombre de la regla, elija el SSID configurado anteriormente y seleccione las ubicaciones para las que esta regla de portal está

#### disponible:

Create Captive Portal Rule     Another Rend -	
When a user is on WFI	Building T
LOCATIONS - Where do you want the rule to live?	Anoth Origination Since When sam is or NWI and converted in AreOd-
Act any of the following locations  Act any of the following locations  Act any of the following locations	USERTONS Are all tecations under 19520 1: Otració comect
Halt-1-OmenConvent X	ADDA
Filter by Metadata     Aview Merganitisation positility including or excluding locations by metalogs	ACTON

Paso 3. Elija la acción del portal cautivo. En este caso, cuando se alcanza la regla, se muestra el portal. Haga clic en Guardar y publicar.

ACTIONS	AUGUNA
Show Capitive Portal Choose a Portal to be allopored to Them when they connect to the with AneOD-ORAQueers       Decision Duration Bendwidth 1 Junit	SOHDALI ACTON Show Capitur Ponar Ponar JaveOS-OMAlgacos
Estamlistically Providium Internet     Orectly provision internet without showing any authentication	
Overy Internet     Stop uners from accounting the internet	
Tage these users as Children - AssociateDescolateware to these high + Add Tage	
Trigger API	
Seve & Publish Seve	

## Verificación

Para confirmar el estado de un cliente conectado al SSID, navegue hasta Monitor > Clients, haga clic en la dirección MAC y busque Policy Manager State:

HOPELOR	WLANS	CONTROLLER	WIRELESS	SECURITY	HANAGEMENT	COMMANDS	HELP	EEEDBACK	
Clients	> Detail								< Back
Max Num	iber of Record	s to v Ris	tar AVC Stats						
Gener	AVC SI	atistics							
						AP radio sio	t 1d	1	
Cleve	Tune	Render				WLAN Profil		Aire05-DNASpaces	
Client	Tunnel Type	Simple 19				WLAN SSID		Aire05-0NASpaces	
Linev	Name	Section 12				Status		Associated	
Waha	oth Liner Name	None				Association		1	
Port I	turnhar.	1				802.11 Ave	entication	Open System	
Interi	lace.	management				Reason Cod	e	1	
10.44	10	20				Status Code		0	
Ouer	untine VI 4N 1D					CF Pollable		Not Implemented	
central contral	Auraiana	Not Consolat				CF Poll Reg.	ALC: NO	Not Implemented	
and a	territori	Not Consected				Short Pream	ible .	Not Implemented	
Barbarbarbarbarbarbarbarbarbarbarbarbarba	Ro Bola	i scal				PBCC		Not Implemented	
Mobil	ty Peer IP					Channel Api	ity.	Not Implemented	
Addre	166					Timeout		0	
Policy	ey move count Manager		_			WEP State		WEP Disable	
Charles		83,05							

### Troubleshoot

El siguiente comando se puede habilitar en el controlador antes de la prueba para confirmar el proceso de asociación y autenticación del cliente.

<**#root>** (5520-Andressi) >

debug client

(5520-Andressi) >

debug web-auth redirect enable mac

Este es el resultado de un intento exitoso de identificar cada una de las fases durante el proceso de asociación/autenticación mientras se conecta a un SSID sin servidor RADIUS:

Asociación/autenticación 802.11:

\*apfOpenDtlSocket: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Received management frame ASSOCIATION REQUEST \*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 \*apfMsConnTask\_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 CL\_EVENT\_ASSOC\_START (1), reasonCode (1), Resu \*apfMsConnTask\_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Sending assoc-resp with status 0 station:34:e1

#### Autenticación DHCP y de capa 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
*webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68 user_agent = A
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Preparing redirect URL according to configure
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- unable to get the hostName for virtual IP, us
*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://spl
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added switch_url, redirect URL is now https:/
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added ap_mac (Radio ), redirect URL is now ht
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added client_mac , redirect URL is now https:
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Added wlan, redirect URL is now https://splas
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- http_response_msg_body1 is <HTML><HEAD><TITLE
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- added redirect=, URL is now https://splash.dn
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- str1 is now https://splash.dnaspaces.io/p2/me
*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:
*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:
*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
```

Autenticación de capa 3 exitosa, mueva el cliente al 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 t
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_WEB_AUTH_DONE (8), reasonCode (0), Res
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_RUN (9), reasonCode (0), Result (0), R
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 RUN (20) Successfully plumbed mobil
```

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

#### 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).