# DNA Spaces Captive Portal with AireOS Controller配置示例

# 目錄

簡介 必要條件 需求 <u>採用元件</u> 設定 網路圖表 組態 將WLC連線到Cisco DNA Spaces <u>在DNA空間上建立SSID</u> 控制器上的ACL配置 DNA空間上沒有RADIUS伺服器的強制網路門戶 在DNA空間上具有RADIUS伺服器的強制網路門戶 在DNA Spaces上建立入口 在DNA空間上配置強制網路門戶規則 驗證 疑難排解

# 簡介

本文檔介紹如何使用帶有AireOS控制器的Cisco DNA Spaces配置捕獲型門戶。

作者: Andres Silva Cisco TAC工程師。

# 必要條件

# 需求

思科建議您瞭解以下主題:

- 對無線控制器的命令列介面(CLI)或圖形使用者介面(GUI)訪問
- Cisco DNA Space

# 採用元件

本文中的資訊係根據以下軟體和硬體版本:

•5520無線LAN控制器版本8.10.112.0

# 設定

## 網路圖表



# 組態

## 將WLC連線到Cisco DNA Spaces

控制器需要使用任何可用的設定(直接連線)、通過DNA空間聯結器或使用CMX Tethering連線到 DNA空間。

在本示例中,雖然強制網路門戶的配置方式對所有設定都相同,但直接連線選項仍在使用中。

若要將控制器連線到Cisco DNA Spaces,它必須能夠通過HTTPS訪問Cisco DNA Spaces雲。有關 如何將控制器連線到DNA Spaces的詳細資訊,請參閱以下連結:<u>DNA Spaces Direct Connect配置</u> <u>示例</u>

## 在DNA空間上建立SSID

步驟1.在DNA Spaces的控制面板中按一下Captive Portals:



步驟2.按一下頁面左上角的三行圖示開啟強制網路門戶選單,然後按一下SSID:

8 - 0 e	🖉 🛔 https://dompades.in/conference/cold	- 0 6 8
Cisco DNA Sp	saces	C Sarah
🛛 Parad		
IF Caption Portal Ref	ins	ImpartiCentigues 1500
	350v	
A line Measures		

步驟3.按一下Import/Configure SSID,選擇CUWN(CMX/WLC)作為「Wireless Network」型別,然後輸入SSID名稱:

😑 Clisco DNA Spaces 👄		C 100.00
Clace Merall SSOs	[	InsurVerlau 180
	SSID Configuration Yes/Reset atter any Class Model 300s with Select Mode to get iterned	

控制器上的ACL配置

需要預先驗證ACL,因為這是Web驗證SSID,並且一旦無線裝置連線到SSID並收到IP地址,裝置 的策略管理器狀態將變為**Webauth\_Reqd**狀態,並且ACL將應用到客戶端會話以限制裝置可以訪問 的資源。

步驟1.導覽至Security > Access Control Lists > Access Control Lists,按一下New,然後按如下方 式配置規則以允許無線客戶端與DNA空間之間的通訊。使用所用帳戶的DNA空間提供的IP地址替換 :

Gen	eral										
Acces	a List Name	DNASper	an-ACL								
Dety	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	34.235.248.212 255.355.255.25	s′	TCP	Any	HTTPS	Any	Any	0	•
2	Permit	34.235.248.212	0.0.0.0	/	TCP	HTTPS	Any	Any	Any	0	•
r	Permit	0.0.0.0	52.55.235.39 255.355.255.25	s′	Any	Any	Any	Any	Any	0	•
4	Permit	52.55.235.39 255.255.255.255	0.0.0.0	1	TCP	HTTPS	Any	Any	Any	0	•

## **註**:要獲取ACL中允許的DNA空間的IP地址,請在ACL配置部分下**在DNA空間上建立SSID一 節的步驟3中建立的SSID中按一下Configure Manually**選項。

可以將SSID配置為使用RADIUS伺服器或不使用RADIUS伺服器。如果在Captive Portal Rule配置的 Actions部分中配置了Session Duration、Bandwidth Limit或Inscilly Provision Internet,則需要使用 RADIUS伺服器配置SSID,否則,無需使用RADIUS伺服器。兩種配置都支援DNA Spaces上的各 種入口。

DNA空間上沒有RADIUS伺服器的強制網路門戶

#### 控制器上的SSID配置

步驟1.導覽至WLAN > WLANs。建立一個新的 WLAN。配置配置檔名稱和SSID。確保SSID名稱與 在DNA空間中建立SSID 一節的步驟3中配置的名稱相同。

uludu. cisco	HONETON HEAVE O	ONTROLLER WIRELESS	SECURITY PRIMORPHENT	COMMANDS HELP	TELEBACK		
WLANs	WLANs						
WLANE WLANE	Connent Pillion None		Craste Nove	8 94			
> Advanced	WLAN 2D Type	Profile Name	WLAN 6600	Admin Status	Security Policie		
	O L WAN	.440	.AND	Brabled	[MPR2][Autr.(PR	91	

步驟2.配置第2層安全性。導覽至WLAN configuration索引標籤中的**Security > Layer 2**索引標籤,然 後從Layer 2 Security的下拉選單中選擇**None。**確保MAC過濾已禁用。

uludu cisco	MONITOR WEARS 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 # None  MAC Filtering #
	OWE Transition Mode
	Fast Transition Adaptive 😳
	Reassociation Timeout 20 Seconds

步驟3.配置第3層安全性。導覽至WLAN configuration索引標籤中的Security > Layer 3索引標籤,將 Web **Policy設定為**第3層安全方**法,啟用Passthrough,設定預先驗證ACL,啟用Override Global Config**,將Web Auth Type設置為**External,**設定重新導向URL。

cisco	NONITON NEWS CONTROLLIN WORLINS SECURITY HANAGEMENT COMMANDS HELP REDMACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
* WLANs WLANs	General Security QeS Policy-Mapping Advanced
> Advanced	Captron Restarting Captron Restarting Authoritization Conditionally Condition
	Presethentication ACL UPyt Drykipaces ACL 2 UPyt Note 2 WebAuth Res UPyt Ad None 2 WebAuth Res UPyt Ad

**註**:要獲取重定向URL,請點選**Configure Manually**選項,該選項位於SSID配置部分下**在** DNA空間上建立SSID一節的步驟3中建立的SSID。

在DNA空間上具有RADIUS伺服器的強制網路門戶

注意: DNA Spaces RADIUS伺服器僅支援來自控制器的PAP身份驗證。

#### 控制器上的RADIUS伺服器配置

步驟1.導覽至**Security > AAA > RADIUS > Authentication**,按一下**New**,然後輸入RADIUS伺服器 資訊。Cisco DNA Spaces充當RADIUS伺服器以進行使用者身份驗證,它可以在兩個IP地址上做出 響應。配置兩台RADIUS伺服器:

cisco	HONETOR	15.4%	CONTROLL	IR WORKLISS	SECURITY HANAGEMENT	COMMANDS HELP	TEDBACK	
Security	RADIUS	Authentica	ation Ser	vers				
AAA     General     RidduS     Authentication     Accounting     Auth Cached Users     ExtMarks	Auth Call Une AES MAC Dell Framed 1	ed Station 10 Key Wrap miker HTU		P MAC Address 5 Designed for F3PS Typhen	ISID	e canaliant AAbit/S server)		
ONS Downiseded AVP + 106ACS+ LOAP Local Net Users	Network User	Managemen	Tunnel Rreay	Server Index Br	erver Address(Spv4/Spv4) 197.146.05	Pert 1912	Disabled	Admin Status Enabled

註:要獲取主伺服器和輔助伺服器的RADIUS IP地址和金鑰,請按一下在DNA空間上建立 SSID部分步驟3中建立的SSID中的Configure Manually選項,然後導航至RADIUS Server Configuration部分。

步驟2.配置記帳RADIUS伺服器。導覽至**Security > AAA > RADIUS > Accounting**,然後按一下 New。配置相同的RADIUS伺服器:

cisco	MONITOR MLANS CONTROLLER WORELESS SECURITY MANAGEM	HENT COMMANDS HELP (TEEDBACK
Security	RADIUS Accounting Servers	
* AAA Ganaral * RADRUS Authentication Accounting	Ant Called Station ID Type System MAC Address  MAC Delimiter Myphen  AP Events Accounting  Evable	
Pailback DryS	Network Tunnel Server User Managament Proxy Index Server Address(Ipv4/1p	v6) Port IPSec Status
Downloaded #1/P	O 0 1 34.397.346.305	1813 Onabled Evabled
TREACE+ LOAP	O 2 34.228.1.05	1813 Osabled Drabled

#### 控制器上的SSID配置

**重要**資訊:在開始SSID配置之前,請確保Controller > General下的**Web Radius** Authentication設定為「PAP」。

步驟1.導覽至WLAN > WLANs。建立一個新的 WLAN。配置配置檔名稱和SSID。確保SSID名稱與 在DNA空間中建立SSID 一節的步驟3中配置的名稱相同。

cisco	MONETON MLANS O	ONTROLLER WORDLESS	SECURITY PRIMADEMENT	COMMANDS HELP	PEEDBACK				
WLANs	WLANs								
WLANE WLANE	Correct Piller: None	Connect Pillion None (Charge (Eller)							
> Advanced	WLAN 3D Type	Profile Name	WLAN 6600	Admin Status	Security Policies				
	O L WAN	.400	.AND	Brabled	[MPA2][Auth(P9K]]				

步驟2.配置第2層安全性。導覽至WLAN configuration索引標籤中的Security > Layer 2索引標籤。將 第2層安全配置為None。啟用Mac過濾。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > Edit 'AireOS-DNASpaces'
VLANs 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 C
	Over the DS
	Reassociation Timeout 20 Seconds

步驟3.配置第3層安全性。導覽至WLAN configuration索引標籤中的Security > Layer 3索引標籤,將 Web **Policy設定為**第3層安全方**法,Enable On Mac Filter failure,設定預先驗證ACL,啟用 Override Global Config**,將Web Auth Type設定為**External,**設定重新導向URL。

cisco	HONITOR BEAM CONTROLLER WIRELESS SECURITY HUMAGEMENT COMMANDS HELP (REDMACK
WLANs	WLANs > Edit 'AlreOS-DNASpaces'
* WLANs	General Security QoS Policy-Happing Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 3 Security web Pulicy
	Capitue Network Assistant Bypess None
	Authentication     Passifyrough
	Conditional Web Redirect
	C Splach Page Web Redmot
	Presudentization ACL D'vel DAASpaces ACL 2 DVd None 2 WebAuth Flex D'vel Ad None 2 WebAuth Flex D'vel Ad None 2
	Steaping Clant English
	Siesping Cliont Auto-Authenticate 👩 Enable
	Overnite Global Config <sup>24</sup> 2 Endle Web Auth type External (Ba-direct to external server)

alialia cisco	HONITOR WU	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	ния	ELEDBACK
WLANs	WLANs > Edit	AireOS-DNAS	paces'					
* WLANS	General 1	lecurity QoS	Policy-Mapp	aing Adva	nced			
+ Advanced	Layer 2	Layer 3 AAA S	ervers					
	RADIUS Serv RADIUS Se Apply Cox	ers Inver Ovenerite Interfai 15E Default Settings Authentication Serve	en Drabled Drabled	ccounting Serv	ers	-		
	Server 1	IP:34.297.146.105.1	Port:5852	Endored IP:34.197.146.1	105. Port: 1813			
	Server 2	IP:34.228.1.95, Pert	-1812	IP:34.228.1.95	Port:1813			
	Server 3	None	0	None				
	Server 4	None		None		0		
	Server 5	None		None		0		
	Server 6	None	8	None		0		

步驟6.為Web-**auth使用者配置Authentication Priority順序**。導覽至WLAN configuration索引標籤中的Security > AAA Servers索引標籤,然後按順序設定RADIUS。

alialia cisco	MONITOR MUANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
• WLANs WLANs • Advanced	General     Security     QoS     Policy-Mapping     Advanced       RADCUS Authentication Survivability

步驟7.導覽至WLAN configuration索引標籤中的Advanced索引標籤,然後啟用Allow AAA Override。

cisco	HONETOR MUNIC CONTROLLER WIRELESS SECURITY NUMBER	DHENT CQHHMHOS HELP (TEDGACK
WLANs	WLANs > Edit 'AireOS-ONASpaces'	
WLANs	General Security Qu5 Policy-Happing Advanced	
Advanced	Allow AAA Override C Enabled	DHCP
	Coverage Hele Detection 🖸 Enabled	DRCP Server Override
	Enable Session Timesut 2000 Session Timesut (secc)	DINCP Adds. Assignment 💿 Required
	Aronet 20 Endoted	Management Frame Protection (MFP)
	Diagnostis Diarnal 44 Endeled Override Interface ACs. 39-4 None 3 39-6 None Layer2 Ad None 3	MIP Cient Protection f Optional      Ottint Parlod (in Season Intervals)
	URL AC), Kone B P2P Blocking Artison Disabled B Claint Exclusion 2 Bitratelad 100	002.114/n (1 - 250) 1 002.1154/s/4 (1 - 250) 1 NAC
	Maximum Allowed Clients	NAC State None  Load Balancing and Band Select
	Static IP Turneling 44 Enabled Wi-Pi Direct Clearies Policy Directived	Client Load Balancing

## 在DNA Spaces上建立入口

步驟1.在DNA Spaces的控制面板中按一下Captive Portals:

ACT - Leverage Digitization toolki	its to Act on Insights.
Captive Portals	Engagements
Onboard and acquire visitors at your properties	Deliver contextual multi-channel notifications

步驟2.按一下Create New	,輸入門戶名稱	,然後選擇可以使用該門戶的	り位置 :
-------------------	---------	---------------	-------

	0			
	Portal Information	Authentication	Data Capture	User Agreement
PORTALINANC				
AirwOG-DNASpaces				
<ul> <li>Enable this portal for all location</li> <li>Location Henanchy</li> </ul>	es		Selector	ed Locations
Enable this portal for all location     Location-Hierarchy     MEX-EAST-1	•		Selecte	di Locations desclarent ix
Cruble this portal for all location Location Hierarchy MEX-EAST-1 C S506-1-CMX			Selectron (MUD) 1	discoursed at
Enable this portal for all location  Location Hierarchy  MEX-EAST-1	••		Selectron (100)	dictions deciliared X
	•== r *+et			discussions

步驟3.選擇身份驗證型別,選擇是否要在門戶首頁上顯示資料捕獲和使用者協定,以及是否允許使 用者選擇接收消息。按一下「Next」:

Paral information	0	a beckenn	4 Intel Agentities in	×
BLIC 14 ARENOVALIVE Enal	Ų	1		
Vature vantile admit the end to access the mome.  Clapter Authentication and User Agreements on pertailform page  Access users to Cpt in to monive message				
	500 (1)	-		

步驟4.配置資料捕獲元素。如果要從使用者捕獲資料,請選中Enable Data Capture框,然後按一下 +Add Field Element以新增所需的欄位。按一下「Next」:

	Conception and the second seco			a land appendix to	×
Ender Data Capture um Fields				+ Add Field Deners	
A   Ent Note					
A Latiture					
		5=	C Prev		

步驟5.選中Enable Terms & Conditions,然後按一下Save & Configure Portal:

	Paral Internation	Automicatory	Date Capture	the Agreements	
and the set is such as a subscript	have a freedom on the second	- Treeses			
actor and your reads of compre	must a conjunct and some ho	of states a			
Ingline The Free & Constitions					
					QF 1 0 0
1 8 <b>0</b> 8 1 X 1 8 8 6 <b>1</b> •	- 9.0 H				
110568222000	11023444	이 아이는 것 같 것 같 것 같 것	0.0 <		
Nes - Parent - Part	5a - 1 A B R R				
III // Terms of Unit. Loss'-patients Sectorebury (7)	2013				
These Well Terms & Canadiana (17 Jan 204 Mel	Viene spater with the 10 Medi-OF	USE growt and use of the MAT is	anica.		
Installation of the Device					
The function concerns only advances are set.	its biored within the speciaes. We do	to a substance station and	task menter ha anteitas el hora	alte ana ita famina a anarita ata adimini m	the second se
out interest between between working working a	and all free \$1.5 here early \$	to be all and I may so he tok	To do no.	and the residence is a second by the one of	

步驟6.根據需要編輯門戶,按一下Save:

Partial - Almobil: CHAMpaces /	nn. Marana Pertan jathan /	Q   g   Spanneton   K <sup>0</sup>   (hpp
PORTAL (SPOR - Since a sector in confige Based Name  Venturine Monage  Venturine Monage  Venturine Mona  Portal Authonization  Portal Munice  Portal Munice  Portal Munice	n: Day, the servery-uncer module.	Action Periodice Concerning Concerning Complete the type for the period Complete the type to be the operand to internet. Internet Complete the type to be the operand to internet. Internet Complete the type to be the operand to internet.
	Core Career	

# 在DNA空間上配置強制網路門戶規則

步驟1.開啟強制網路門戶選單,然後按一下**強制網路門戶規則:** 

⊖ → ♂ ≙	0	https://dnaspaces.io/captiveportal/hules/captive-portal	
Cisco DNA Spaces			
D Portal			
Captive Portal Rules			Created
ି \$\$D\$		201 201	Feb 24, 2020
al Reports			0 8:02 PM

步驟2.按一下「+ Create New Rule」。輸入規則名稱,選擇先前配置的SSID,並選擇此入口規則 可用於的位置:

Onaria Captine Portal Rula Inc. 1 (Are Co. Billionne	
one any or an or the options that apply to your rule Genow	
When a user is on VRPI - and connected to AwdD-DWDpaces -	READING
LOOFDOE - When do you want the rule to fin?	Bredd-Okalipana 16/95 Ritercare is an NP and summaind to BordD-
At any of the following locations + Add(sections)	Involution Incontrol Fare at locations under 1000-1 Owned passes
Mill + General areas A	and and a
The To Matchie	1040Aut
<ul> <li>Factor can be an active that of second or second second second by support</li> </ul>	NC 10H Dese Cauter Henel

步驟3.選擇強制網路門戶的操作。在這種情況下,當規則被命中時,將顯示入口。按一下「Save &

## Publish」。

chows	A1844
Show Capital Partal     Onesia a Partal     Deal and the depayed to Likers when they connect to the with	SCHEMAL
And Divideous	ACTON
	Shine Capitor Parts
Section Duration	Partal AreOS ON/Gauces
Bandwide Laws	
Seamlersig Providen Internet     Directly providen Internet     Directly providen enternet effect deceing any authoritopics	
Deny Internet     Registers free accessing the Internet	
Tage these users as Decese - Associate Decessories users to choose tage.	
* Add Tage	
C Trapper API	
Steel & Picture .	

# 驗證

要確認連線到SSID的客戶端的狀態,請導航到**Monitor > Clients**,按一下MAC地址並查詢Policy Manager State:

MONITOR	MLAN	CONTROLLER	WPELESS	SECURITY	HANAGEHENT	COMMANDS	HELP	EEDBACK	
Clients > Detail									< Back
Max Number of Records 10 * Clear AVC Stats									
General	AVC S	tatistics							
						AP radio als	e 1d	1	
Client 7	ype	Regular				WLAN Profil	e	AireOS-ONASpaces	
Client T	unnel Type	Simple IP				WLAN SSID		AireOS-ONASpeces	
User Na	ine					Status		Associated	
Webeut	h User Name	None				Association	10	1	
Port Nu	mber	1				802.11 Aut	hentication	Open System	
breefer	e	management				Reason Cod	le	1	
VLAN II		20				Status Code		0	
Quarant	tine VLAN ID	0				CF Pollable		Not Implemented	
CCX Ve	noion	Not Supported				CF Poll Reg	vest.	Not Implemented	
E2E Ver	noian	Not Supported				Short Prear	alde	Not Implemented	
Mobility	Role	Local				PBCC		Not Implemented	
Mobility Address	Peer IP	N/A				Channel Ag	iky	Not Implemented	
Hobility	Hove Count	0				Timeput		0	
Peacy H State	tereger	RUN				WEP State		WEP Disable	

# 疑難排解

在測試確認客戶端的關聯和身份驗證過程之前,可以在控制器中啟用以下命令。

(5520-Andressi) >debug client

以下是連線到沒有RADIUS伺服器的SSID時,在關聯/身份驗證過程中成功嘗試識別每個階段的輸出 :

#### 802.11關聯/身份驗證:

\*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

#### DHCP和第3層身份驗證:

\*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=" \*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

#### 第3層身份驗證成功,將客戶端移動到RUN狀態:

\*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

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。