AireOSコントローラを使用したDNAスペースキ ャプティブポータルの設定例

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 設定 ネットワーク図 設定 WLCをCisco DNA Spaceに接続する DNAスペースでのSSIDの作成 コントローラでのACLの設定 <u>DNAスペース上のRADIUSサーバを使用しないキャプティブポータル</u> <u>DNAスペース上のRADIUSサーバを使用し</u>たキャプティブポータル DNAスペースにポータルを作成する DNAスペースでのキャプティブポータルルールの設定 確認 トラブルシュート

概要

このドキュメントでは、AireOSコントローラでCisco DNAスペースを使用してキャプティブポー タルを設定する方法について説明します。

著者: Cisco TACエンジニア、Andres Silva

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ワイヤレスコントローラへのコマンドラインインターフェイス(CLI)またはグラフィックユー ザインターフェイス(GUI)アクセス
- Cisco DNA Spaces

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

•5520ワイヤレスLANコントローラバージョン8.10.112.0

設定

ネットワーク図



設定

WLCをCisco DNA Spaceに接続する

コントローラは、使用可能なセットアップ(Direct Connect、DNA Spaces Connector経由、また はCMXテザリングを使用)のいずれかを使用して、DNAスペースに接続する必要があります。

この例では、[Direct Connect]オプションが使用されていますが、キャプティブポータルはすべて の設定に対して同じ方法で設定されています。

コントローラをCisco DNA Spacesに接続するには、HTTPS経由でCisco DNA Spacesクラウドに 到達できる必要があります。コントローラをDNAスペースに接続する方法の詳細については、『 DNAスペースダイレクトコネクトの設定例』を参照してください。

DNAスペースでのSSIDの作成

ステップ1: DNA Spacesのダッシュボードで[Captive Portals] をクリックします。



ステップ 2:ページの左上隅にある3行のアイコンをクリックしてキャプティブポータルメニュー を開き、[SSIDs:

⊕ - σ e	0 a http://dwapades.la/conferentializat	- 0 6 1
Cisco DNA Sp	aces	C Serie
🛛 nuu		
IF Capital Participal	ins	ImportConfigure 550
	15/Dw	
A Reports		

ステップ 3 : [Import/Configure SSID] をクリックし、[Wireless Network]タイプとして[CUWN (CMX/WLC)] を選択し、SSID名を入力します。

= Cisco DNA Spaces		C Ser St
Cisco Mentil 550s		Input/Configure 1880
	SSID Configuration You favore asted any Open Model 3004 with Soluti Moder to get stand	

コントローラでのACLの設定

Web認証SSIDであるため、事前認証ACLが必要です。ワイヤレスデバイスがSSIDに接続して IPアドレスを受け取るとすぐに、デバイスのPolicy Manager状態がWebauth_Reqd状態に移行し 、ACLがクライアントセッションに適用されて、デバイスが到達できるリソースが制限されます 。

ステップ 1 : [Security] > [Access Control Lists] > [Access Control Lists] に移動し、[New] をクリ ックして、ワイヤレスクライアント間でDNA空間への通信を許可するルールを次のように設定し ます。IPアドレスを、使用中のアカウントのDNAスペースから与えられたIPアドレスに置き換え ます。

Gene	eral									
Access	a Lint Name	DNASpece	n-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 / 255.255.255.255	0.0.0.0 /	TCP	HTTPS	Any	Any	Any	0	•
1	Permit	0.0.0.0 /	52.55.235.39 / 255.255.255.255	Any	Any	Any	Any	Any	0	
4	Permit	52.55.235.39 / 255.255.255.255	0.0.0.0 /	TCP	HTTPS	Any	Any	Any	0	•

注:ACLで許可されるDNAスペースのIPアドレスを取得するには、「ACL設定」セクションの「**DNAスペースでのSSIDの作成**」セクションのステップ3で作成したSSIDから、 [Configure Manually] オプションをクリックします。

SSIDは、RADIUSサーバを使用するように設定することも、使用せずに設定することもできます 。キャプティブポータルルール設定の[Actions] セクションで[Session Duration]、[Bandwidth Limit]、または[Seamently Provision Internet]が設定されている場合は、SSIDをRADIUSサーバで 設定する必要があります。そうでない場合は、RADIUSサーバを使用する必要はありません。 DNAスペース上のすべての種類のポータルは、両方の構成でサポートされています。

DNAスペース上のRADIUSサーバを使用しないキャプティブポータル

コントローラでのSSID設定

ステップ 1 : [WLAN] > [WLANs] に移動します。新規 WLAN を作成してください。プロファイル 名とSSIDを設定します。SSID名が、「DNAスペースでのSSIDの作成」セクションのステップ 3で設定したものと同じであることを確認します。

cisco	HONETON HEAVE O	ONTROLLER WORDLESS	SECURITY HEMAGEMENT	COMMANDS HELP	PEEDBACK				
WLANs	WLANs								
WLANS WLANS	Connent Pillion None	Connect Pittery None (Change Filter) (Change Filter) Create None							
> Advanced	WLAN 2D Type	Profile Name	WLAN SSID	Admin Status	Incarity Policies				
	C L WAN	300	.440	brabled	[MPA2][Auth(P9A]]				

ステップ 2:レイヤ2セキュリティを設定します。WLAN設定タブで**Security > Layer 2**タブに移動 し、Layer 2 Securityのドロップダウンメニューから**None**を選択します。MACフィルタリングが 無効になっていることを確認します。

ululu 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 # None MAC Filtering #
	OWE Transition Mode
	Fast Transition Adaptive
	Reassociation Timeout 20 Seconds

ステップ 3: レイヤ3セキュリティを設定します。[WLAN configuration]タブで[Security] > [Layer 3] タブに移動し、レイヤ3セキュリティ方式として[Web **Policy]を設定し、[Enable]** パススルーを 設定し、事前認証ACLを設定し、[Override Global Config] を[Web Auth Type] に[External] を設定 し、リダイレクトURLを設定します。

cisco	NONETON NEWS CONTROLLER WORKLESS SECURITY PRANOCEMENT COMMANDS HELP REEDENCK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
 WLANs WLANs Advanced 	Centeral Security QeS Pelicy-Mapping Advanced
	Prest/Novegt Conditioner Web Relived Topics/ Page Web Relived On MAC Filter failure/II Web policy done locally on Americaniae
	Presidherstation ACL (PVI DWSipace-ACL) (PV6 Nore) WebAuth Rev (PVI Ad Nore) WebAuth Rev (PVI Ad Nore) Or Cade Scareing Redirect (RL Inter-//wileth-drospoon-Jajob/menetts Emeilinget Seesing Client Enable
	Sloeging Client Auto Authenticate 😰 Enable Overrale Bodali ConfigHI 🚱 Braidle Web Auth type External (Ra-direct to external enrier)

注: リダイレクトURLを取得するには、[Configure Manually] オプションをクリックします 。このオプションは、[SSID configuration]セクションの[Create the SSID on DNA Spaces] セクションのステップ3で作成したSSIDから選択します。

DNAスペース上のRADIUSサーバを使用したキャプティブポータル

注:DNAスペースRADIUSサーバは、コントローラからのPAP認証のみをサポートします。

コントローラでのRADIUSサーバの設定

ステップ 1 : [Security] > [AAA] > [RADIUS] > [Authentication] に移動し、[New] をクリックして RADIUSサーバ情報を入力します。Cisco DNA Spacesは、ユーザ認証のためにRADIUSサーバと して機能し、2つのIPアドレスで応答できます。両方のRADIUSサーバを設定します。



注:プライマリサーバとセカンダリサーバの両方のRADIUS IPアドレスと秘密キーを取得す るには、「**DNAスペースでのSSIDの作成**」セクションのステップ3で作成したSSIDから [Configure Manually] オプションをクリックし、[RADIUS Server Configuration] セクション に移動します。

ステップ 2:アカウンティングRADIUSサーバを設定します。[Security] > [AAA] > [RADIUS] > [Accounting] に移動し、[New] をクリックします。同じ両方のRADIUSサーバを設定します。

cisco	HOACTOR	WLANS C	ONTROLLE	n wyneless	SECURITY	наллаенент	соннилос	HELP	TEDMOX		
Security	RADIUS	Accounting	Servers								
AAA General ADDUS ActionTication Accounting Action Theory	Ant Cal MAC Del AP Exer	ind Station 10 T Instar In Accounting	94 Sy 19	atam MAC Addre ghan 📑 Enable	**						
Palback Dass	Network User	Management	Tunnel Praxy	Server Index	Server Address)	(Ipv4/Ipv6)	_ г	Port	IPSec	Admin Status	1
Downloaded #17				1	34.197.146.105			1813	Oasbled	Enabled	
+ TACACS+ LDAP					34.228.1.95			1813	Orabled	Enabled	•

コントローラでのSSID設定

重要:SSID設定を開始する前に、[Controller] > [General]で[Web Radius Authentication] が [PAP]に設定されていることを確認してください。

ステップ 1 : [WLAN] > [WLANs] に移動します。新規 WLAN を作成してください。プロファイル 名とSSIDを設定します。SSID名が、「**DNAスペースでのSSIDの作成**」セクションのステップ 3で設定したものと同じであることを確認します。

cisco	HONETOR	WLANG C	CATROLLER WO	IEUESS SECURT	Y PRIVACEMENT	COMMANDS	10,7	REDBACK			
WLANs	WLANs										
* WLANs WLANS	Correct Pills	None	(Charg	n Film) (Dear Film)					Cranta Non	8	64
> Advanced	O WLAN D	Type	Profile Name		LAN SED	Adm	in Status	Security Polici			
	0 L	WSAN	.AND		AD-	5140	lei	[8962]]649(P	() ()		

ステップ 2:レイヤ2セキュリティを設定します。[WLAN configuration]タブで[Security] > [Layer 2] タブに移動します。レイヤ2セキュリティを[None] に設定します。MAC フィルタリングの有効 化.

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
	MAC Filtering 2
	OWE Transition Mode
	Fast Transition
	Fast Transition Adaptive 🗘
	Over the DS
	Reassociation Timeout 20 Seconds

ステップ 3:レイヤ3セキュリティを設定します。[WLAN configuration]タブで[Security] > [Layer 3] タブに移動し、レイヤ3セキュリティ方式として[Web **Policy]を設定し、[Enable]** [On Mac Filter failure]を設定し、事前認証ACLを設定し、[Override Global Config] を[Web Auth Type] に [External]を設定し、リダイレクトURLを設定します。



ステップ 4:AAAサーバを設定します。WLAN設定タブの[Security] > [AAA Servers] タブに移動し 、[Authentication Servers] と[Accounting Servers] を有効にして、ドロップダウンメニューから 2つのRADIUSサーバを選択します。

cisco	HONITOR MU	INS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нυ	EEEDBACK
WLANs	WLANs > Edit	AireOS-DNAS	paces'					
* WLANS	General	ecurity QoS	Policy-Map	ping Adv	vanced			
Advanced	Layer 2	Layer 3 AAA S	ervers					
	RADIUS Serv RADIUS Se Apply Close	ers rver Ovenerite interfat ISE Default Settings	ce Enabled Enabled					
		Authentication Serv	ers /	Accounting 54	rvers			
	Server 1	IP:34.197.146.105	Port: 5852 📴	IP:34.197.14	6.105, Port:1813	8		
	Server 2	IP:34.228.1.95, Pert	:1812 🖯	IP:34.228.1.9	6, Pert 1813	8		
	Server 3	None	0	None		0		
	Server 4	None	0	None		0		
	Server 5	None	0	None				
	Server 6	None	8	None		0		

手順 6 : **Web認証ユーザの認証の優先順位**を設定します。WLAN設定タブで[Security] > [AAA Servers] タブに移動し、RADIUSを順に最初に設定します。

ANs	WLANs > E	dit 'Aire	OS-DNAS	paces'					
VLANs	General	Security	Qo5	Policy-Mapp	ing Ad	vanced			
HLANS	RADOUS A	uthanticati	en Survivabi	SRy .					
arances.	Authorit	kation Surv	vability	0					
	LDAP Serv	-							
	Server	None	•						
	Server 3	2 None							
	Server 3	1 Note	0						
	Local EAP	Authentics	tion						
	Local E	P Authentic	tion Cinel	_					
	Authenti	cation pri	ority orde	r for web-aut	h user				
		Not Use	4			Order L	ised For Auther	tication	
					>		RADOUS		Up

手順7:WLAN設定タブのAdvancedタブに移動し、Allow AAA Overrideを有効にします。

alialia cisco	HONETON MIANI CONTROLLER WIRELESS SECURITY	MANAGEMENT COMMANGS HELP (EEDBACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'	
* WLANs WLANs	General Security QuS Policy-Happing Adv	anced
> Advanced	Allow AAA Overvide 🛛 Enabled	DWCP
	Coverage Hole Detection 👩 Enabled	DRCP Server Override
	Enable Session Timesut 28000 Session Timeout (secc)	DISCP Addr. Ansignment 🕓 Required
	Aronet III Crubbed	Management Frame Protection (MFP)
	Diagnostik Channel 48 Enabled	
	Override Interface ACI. 3Pv4 None 3P	vé None 🚦 MYP Clerk Protection 1 lightenie 🖬
	Layar2 Ad Bone	OTIM Partied (in beacen intervale)
	URLAD. Bone	#02.11a/n (1 - 255) 1
	F2F Blocking Action Disabled	802.115h/p/n (1 - 258) 1
	Clarif Exclusion 2 GEnabled Store (Store)	MAC
	Maximum Allowed Clients	NAC State None
	Static IP Turneling #4 Crusted	Load Betencing and Band Select
	Wi-Fi Direct Clients Policy Disabled	Client Load Balancing
	Marine Married Classic	Crevel Band Batel

DNAスペースにポータルを作成する

ステップ1: DNA Spacesのダッシュボードで[Captive Portals] をクリックします。



ステップ 2:[Create New] をクリックし、ポータル名を入力して、ポータルを使用できる場所を 選択します。

0.0	C & https://www.acar.lo/				
Cisco DNA	Spaces Captive Portals				
		O	2 Autoritoriae	8 Data Dagture	4 User Aproximation
PORTACIA AireOS	AAC				
i te	ble this portal for all locations				
Loc	ation Herarchy			Selecte	ed Locations
	MEX-EAST-1			MU0-1	description of M
	9506-1-CMX				
	S506-2-Connector				
	S520-1-DirectConnect			2	
	S 9800L-DirectConnect				
			Sev. + r	Next 0	

ステップ 3:認証タイプを選択し、ポータルホームページにデータの取り込みとユーザ契約を表示するかどうか、およびユーザがメッセージを受信することを許可するかどうかを選択します。 [Next] をクリックします。

	0			×
Paral Hermiter	Automation Street	Own-Gaptern	the Approximity	
		_		
Cost Cost				
Colt				
Value name submit that and is access the mome.				
Display Authentication and User Agreements on portal home page				
Allow users to Dpt in to receive message				
	500	Day Next 1		

ステップ 4:データキャプチャ要素を構成します。ユーザからデータをキャプチャする場合は、 [Enable Data Capture] ボックスをオンにし、[Add Field Element] をクリックして目的のフィール ドを追加します。[Next] をクリックします。

	0		-0		×
	Paral Internation	Automisation	Data Cagrant	tion Agreeteens	
El trater Data Capiture Form Fields				+ Add Field Store of	
A Latitude					

544	6 Per	Next 1

ステップ 5 : [Enable Terms & Conditions] にチェックマークを入れ、[Save & Configure Portal] を クリックします。

Proceeding data and the state and and and and the state of the state and the state of the state	
na anton anve pa conspecte que terma a constitue antimista por paramente.	
Instein Weins & Canditions	
Card P (1940 V) with Art	Q# 1 English
0.2.0.2.1.1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.	
8 2 8 5 4 ¥ 5 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
ten - ten - ten - ten - A- B- H -	
10 P. Torres of Unit, Last-united Statement (2, 2013)	
These W-A forms & Candidore Of the the MAT formal spatter with the 100kdS OF URL govern your use at the MAT service.	
Insulption of the Insulae	
The Sentra provides provide services in the Internat whice the previous. We do not us an entirely practical, prosticular, prosticular for accident of trace after some the Sentre or expr or probabilitation for Sentre to answer that areas couply with these SENT for the setting of tracement the sign of the set on the Sentre of the Sentre o	the any adhoted torited over any makeled beneralised, headed

手順 6:必要に応じてポータルを編集し、[Save] をクリックします。

NA, 19708 - Senet a sector to configure. In Brand Name Websame Message Nation		ACITAL PRIVACE
Brand Name Website Unsage Veloc	EVAL MAR	PORTAL PRIVATE
Welcarie Message Nation	INVACIANA I	
Netros		 wome Screen
	Overlapited any tampachic or graphic hash that iterative user brand	Cisco Systema
Email Authentication	fine Orly D Lease	
Venalitip	Shed have	Walkome to 50ceatiliard
 Values 	Crear Summa	SIGN-UP FOR WIR
D Peebeck		Conglide the form bolter to connect to internet
€ ND		English
e Gernan		
· Collisional		
Prones & Oflers		
· Martinette		

DNAスペースでのキャプティブポータルルールの設定

ステップ1:キャプティブポータルメニューを開き、[Captive Portal Rules] をクリックします。

€ → C &	Attps://dnaspaces.io/captiveportal/in/es/captive-portal	
Cisco DNA Space	s	
Portal		
E Captive Portal Rules		Created
ି \$510s		Feb 24, 2020
ය. Reports	>	⊖ 8:02 PM

ステップ 2:+ [Create New Rule]をクリックします。ルール名を入力し、以前に設定したSSIDを 選択し、このポータルルールを使用できる場所を選択します。

Onarta Captive Portal Rule NULLIVIUS, And D Distiguent	
one say or an of the options that apply to your rule below	
	TURNARY
When a user is on WHI - and connected to Anecto-SWOpeon -	NUL MAR Web/Derlagense
UDCATHONG - Where do you want the rule to fina?	NAME
	When user to an MPI and summaries to AreO TRAdyscen
At any of the totswing locations	LODATIONE.
+ Add Loodore	For all insuline under
	1010-1 OwnerConners
Hit-Omelanne x	withol
	10HDAII
the by tendence the providence of the including or maturing investors by maturing.	
	HC10H
	Draw Capitor Purel

ステップ3:キャプティブポータルのアクションを選択します。この場合、ルールがヒットすると、ポータルが表示されます。[Save & Publish] をクリックします。

085	
 Shoe Caption Partal Chapter a Partal to be disposed to Users when they connect to the with. 	SCHEDULE
Amidd-DRAdpaces -	ACTON
Section Duration	Partal AreOS ORAGences
Deraked h Lines	
Seamleasty Provide Internet Directly provide internet without allowing any sufficients	
Desy Internet Dep area has according the internet	
Tage these users as Descent - Insurant Descents and in closer has	
1 Ant fee	
Tregger API	
s Public dore	

確認

SSIDに接続されているクライアントのステータスを確認するには、[Monitor] > [Clients] に移動し、MACアドレスをクリックして[Policy Manager State]を探します。

	MONITOR MLANI	CONTROLLER	WPELESS	SECORITY	HANAGEMENT	COMMANDS	HELP	EEDIMCK	
	Clients > Detail								< Back
	Max Number of Recor	ds 10 * 68	ear AVC Stats	1					
1	General AVC S	tatistics							
						AP radio alot	1.24	1	
	Client Type	Repular				WLAN Profile		AireOS-OMASpaces	
	Client Tunnel Type	Simple IP				WLAN SSID		AireOS-ONASpeces	
	User Name					Status		Associated	
	Webauth User Name	None				Association 1	10	1	
	Port Number	1				802.11 Auth	entication	Open System	
	Interface	management				Reason Code		1	
	VLAN ID	20				Status Code		0	
	Quarantine VLAN 10	0				CF Pollable		Not Implemented	
	CCX Version	Not Supported	_			CF Pull Regu	est	Not Implemented	
	EDE Version	Not Supported				Short Pream	ble	Not Implemented	
	Mobility Role	Latel				PBCC		Not Implemented	
	Hobility Peer IP	NA				Chernel Api	ity	Not Implemented	
	Address	1.0				Timeout		0	
	Fally Hander		_			WEP State		WEP Disable	
	Crate	80,89				and and a			

トラブルシュート

クライアントの関連付けと認証プロセスを確認するためにテストを行う前に、コントローラで次 のコマンドを有効にできます。

(5520-Andressi) >debug client

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

次に、RADIUSサーバを使用せずにSSIDに接続しているときに、関連付け/認証プロセス中に各フ ェーズを識別する試みが成功したときの出力を示します。

802.11アソシエーション/認証:

*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およびレイヤ3認証:

*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- strl 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 レイヤ3認証に成功し、クライアントをRUN状態に移行します。 *emWeb: Apr 09 21:49:57.633: Connection created for MAC:34:e1:2d:23:a6:68 *emWeb: Apr 09 21:49:57.634:

*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)

ewaURLHook: Entering:url=/login.html, virtIp = 192.0.2.1, ssl_connection=0, secureweb=1

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。