AireOS 컨트롤러를 사용하는 DNA Spaces 종속 포털 컨피그레이션 예

목차

소개 사전 요구 사항 요구 사항 <u>사용되는 구성 요소</u> 구성 네트워크 다이어그램 설정 WLC를 Cisco DNA Spaces에 연결 DNA Spaces에 SSID 생성 컨트롤러의 ACL 컨피그레이션 DNA 공간에 RADIUS 서버가 없는 종속 포털 DNA 공간에 RADIUS 서버가 있는 종속 포털 DNA Spaces에서 포털 생성 DNA 공간에 종속 포털 규칙 구성 다음을 확인합니다. 문제 해결

소개

이 문서에서는 AireOS 컨트롤러와 함께 Cisco DNA Spaces를 사용하여 종속 포털을 구성하는 방법 에 대해 설명합니다.

기고자: Andres Silva Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

• 무선 컨트롤러에 대한 CLI(Command Line Interface) 또는 GUI(Graphic User Interface) 액세스

• Cisco DNA 공간

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

• 5520 Wireless LAN Controller 버전 8.10.112.0

구성

네트워크 다이어그램



설정

WLC를 Cisco DNA Spaces에 연결

사용 가능한 설정 중 하나를 사용하여 DNA Spaces에 컨트롤러를 연결해야 합니다. Direct Connect, DNA Spaces Connector 또는 CMX Tethering을 통해 연결할 수 있습니다.

이 예에서는 종속 포털이 모든 설정에 대해 동일한 방식으로 구성되었지만 직접 연결 옵션이 사용 중입니다.

컨트롤러를 Cisco DNA Spaces에 연결하려면 HTTPS를 통해 Cisco DNA Spaces 클라우드에 연결 할 수 있어야 합니다. 컨트롤러를 DNA Spaces에 연결하는 방법에 대한 자세한 내용은 다음 링크를 참조하십시오. <u>DNA Spaces Direct Connect 컨피그레이션 예</u>

DNA Spaces에 SSID 생성

1단계. DNA Spaces의 **대시보드**에서 Captive Portals(종속 포털)를 클릭합니다.



2단계. 페이지의 왼쪽 상단 모서리에 있는 3개의 회선 아이콘을 클릭하여 종속 포털 메뉴를 열고 SSIDs를 **클릭합니다.**

⊕ + ⊂ e	C A Merchenania (conservation)	
Cisco DNA Space	95	C Surse
0 mm		
IF Capital Portal Rules		ImperiConfigure 550
♥ SSEx	25Cv	
All Reports		
A. Unor Management		

3단계. Import/**Configure SSID(SSID 가져오기/**구성)를 클릭하고 "Wireless Network(무선 네트워크)" 유형으로 CUWN**(CMX/**WLC)을 선택하고 SSID 이름을 입력합니다.

I Cisco DNA Spaces 😁		C 5050
Cisco Menéli 158Da		Ingun/Configure 1800
	SSID Configuration Yes/sect atter ary Cost Mean SICs yet, Select follow to per stand	

컨트롤러의 ACL 컨피그레이션

사전 인증 ACL은 웹 인증 SSID이므로 필요합니다. 무선 디바이스가 SSID에 연결하고 IP 주소를 수 신하는 즉시 디바이스의 정책 관리자 상태가 Webauth_**Reqd 상태**로 이동하고 ACL이 클라이언트 세션에 적용되어 디바이스가 연결할 수 있는 리소스를 제한합니다.

1단계. Security(**보안) > Access Control Lists(액세스 제어 목록) > Access Control Lists(액세스 제 어 목록)로 이동하고 New(새로 만들기)를 클릭한 다음 무선 클라이언트와 DNA Spaces 간의 통신 을 허용하는 규칙을 다음과 같이 구성합니다. IP 주소를 사용 중인 계정의 DNA Spaces에서 제공한 주소로 바꿉니다.**

Gen	eral									
Acces	s List Name	DNASpece	+-ACL							
Dety	Counters	٥								
Seq	Action	Source IP/Hask	Destination IP/Hask	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	34.235.249.212 /	0.0.0.0 /	TCP	HTTPS	Any	Any	Any	0	•
r	Permit	0.0.0.0 /	52.55.235.39 /	Any	Any	Any	Any	Any	0	
4	Permit	\$2.55.235.39 / 255.255.255.255	0.0.0.0 /	TCP	HTTPS	Any	Any	Any	0	•

참고: ACL에서 허용할 DNA Spaces의 IP 주소를 가져오려면 ACL 컨피그레이션 섹션의 3단 계에서 생성한 SSID에서 Configure Manually(수동으로 **구성) 옵션을** 클릭합니다.

RADIUS 서버를 사용하거나 사용하지 않도록 SSID를 구성할 수 있습니다. 종속 포털 규칙 컨피그 레이션의 **Actions 섹션**에서 세션 기간, 대역폭 제한 또는 인터넷의 원활한 프로비저닝이 구성된 경 우 SSID를 RADIUS 서버로 구성해야 합니다. 그렇지 않으면 RADIUS 서버를 사용할 필요가 없습니 다. DNA Spaces의 모든 종류의 포털은 두 컨피그레이션에서 모두 지원됩니다.

DNA 공간에 RADIUS 서버가 없는 종속 포털

컨트롤러의 SSID 컨피그레이션

1단계. WLAN(WLAN) > WLANs(WLAN)로 이동합니다. 새 WLAN을 생성합니다. 프로파일 이름 및 SSID를 구성합니다. SSID 이름이 DNA Spaces에 SSID 생성 섹션의 3단계**에 구성된 과 동일한지** 확인합니다.

cisco	HONETON HEATS C	ATROLLER WIRELESS	SECURITY PRIMORPHENT	COMPANDS HELP	REDBACK		
WLANs	WLANs						
WLANs WLANS	Convert Filters None	(Change Filter) (Coar filter)			Craste Nov	8 (64)
+ Advanced	WLAN DD Type	Profile Name	WLAN SEED	Admin Status	Security Policie		
	O & WSAN	300	.440	Brabled	[MN2][AIT(PR	01	

2단계. 레이어 2 보안을 구성합니다. WLAN Configuration(WLAN 컨피그레이션) 탭에서 Security(보 안) > Layer 2(레이어 2) 탭으로 이동하고 Layer 2 Security(레이어 2 보안) 드롭다운 메뉴에서 None(없음)으로 선택합니다. MAC 필터링이 비활성화되어 있는지 확인합니다.

uhuhu 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
	OWE Transition Mode
	Fast Transition Adaptive 🕤
	Reassociation Timeout 20 Seconds

3단계. 레이어 3 보안을 구성합니다. WLAN 컨피그레이션 탭에서 Security(보안) > Layer 3(레이어 3) 탭으로 이동하고, Layer 3 보안 방법으로 Web Policy(웹 정책)를 구성하고, Passthrough(통과)를 활성화하고, 사전 인증 ACL을 구성하고, Override Global Config(전역 컨피그레이션 재정의)를 활성 화하고, Web Auth Type(웹 인증 유형)을 External(외부)로 설정하고, Redirect URL(리디렉션 URL)을 구성합니다.



참고: 리디렉션 URL을 가져오려면 Configure Manually(수동으로 **구성) 옵션**을 클릭합니다. 이 옵션은 SSID 컨피그레이션 섹션에서 **DNA Spaces에 SSID**를 생성합니다.

DNA 공간에 RADIUS 서버가 있는 종속 포털

참고: DNA Spaces RADIUS 서버는 컨트롤러에서 오는 PAP 인증만 지원합니다.

컨트롤러의 RADIUS 서버 컨피그레이션

1단계. Security(보안) > AAA > RADIUS > Authentication(인증)으로 이동하고 New(새로 만들기)를 클릭하고 RADIUS 서버 정보를 입력합니다. Cisco DNA Spaces는 사용자 인증을 위해 RADIUS 서 버 역할을 하며 2개의 IP 주소에서 응답할 수 있습니다. 두 RADIUS 서버를 모두 구성합니다.



참고: 기본 및 보조 서버 모두에 대한 RADIUS IP 주소와 비밀 키를 가져오려면 DNA Spaces에서 SSID 생성 섹션의 3단계에서 생성한 SSID에서 Configure Manually(수동으로 구 성) 옵션을 클릭하고 RADIUS Server Configuration(RADIUS 서버 컨피그레이션) 섹션으로 이 동합니다.

2단계. 어카운팅 RADIUS 서버를 구성합니다. **Security(보안) > AAA > RADIUS > Accounting(어카 운팅)**으로 이동하고 **New(새로 만들기)**를 클릭합니다. 두 RADIUS 서버를 동일하게 구성합니다.

cisco	HOVELON	WLANS (;ormou	DA WOADLESS	S SECURITY M	INAGEMENT	соннилоз	HELP	TEDBACK		
Security	RADIUS	Accountin	g Serven	5							
AAA General ADUIS Actiontication Accounting Action lines	Aut Cal MAC De AP Even	ind Station ID 1 Imitar In Accounting	Na+ 3	yatawi MAC Addri yghan Enable							
Pailback	Network User	Managaman	Tunnel Praxy	Server Index	Server Address(1)	pv4/3pv6)		Port	1PSec	Admin Status	1
Downloaded #17				1	34.197.146.105			1813	Otabled	Enabled	
TRCACS+ LOAP				2	34.228.1.95			1813	Oxabled	Drabled	•

컨트롤러의 SSID 컨피그레이션

중요: SSID 컨피그레이션으로 시작하기 전에 Controller(컨트롤러) > General(일반)에서 Web Radius Authentication(웹 RADIUS 인증)이 "PAP"로 설정되어 있는지 확인합니다.

1단계. WLAN(WLAN) > WLANs(WLAN)로 이동합니다. 새 WLAN을 생성합니다. 프로파일 이름 및 SSID를 구성합니다. SSID 이름이 DNA Spaces에 SSID 생성 섹션의 3단계에 구성된 과 동일한지 확인합니다.

WLANs WLANs * WLANs Connect Plans WLANs Connect Plans > Advanced MLAN 10 Type * WLAN State Advanced	cisco	HONETON	WLANG (CONTROLLER W	(HOLESS 30	outerry	PRIMACEMENT	COMMANDS	10,7	rttosacx			
WLANs Connect Filters None (CharperFilter) (Date Filter) Advanced WLAN 10 Type Profile Name WLAN 1010 Advanced Installant/Visci	WLANs	WLANs											
Advanced MLAN 10 Type Profile Name WLAN 5510 Advant Status Encertly Policies Type Advant Status Encertly Policies	* WLANs WLANS	Correct Filte	None	(Che	spa. Filter) (Case	(film)					Cranta Non	8	64
I WANT AND AND REALING INVESTIGATION	> Advanced	O WLAN D	Type	Profile Name		WLAN	6600	Adm	in Matus	Security Policies			
C NEW OND DESCRIPTION		0.	WUM	.AND		.AND		Enal	fed.	[MPR2][Autr(PR6]	I		

2단계. 레이어 2 보안을 구성합니다. WLAN 컨피그레이션 탭에서 Security(보안) > Layer 2(레이어 2) 탭으로 이동합니다. 레이어 2 보안을 None으로 구성합니다. Mac 필터링을 활성화합니다.

ululu cisco	MONITOR WLANS O	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT
WLANs	WLANs > Edit 'Aire	OS-DNAS	paces'		
VLANs	General Security	QoS	Policy-Mapp	oing Ad	vanced
Advanced	Layer 2 Layer 3	AAA Se	irvers		
	Layer 2 Security #	Non	e		
	MAC Filtering 2	۵			
	OWE Transition Mod	se 🗆			
	Fast Transition				
	Fast Transition	Adap	stive 🗘		
	Over the DS				
	Reassociation Times	out 20	Seconds		

3단계. 레이어 3 보안을 구성합니다. WLAN 컨피그레이션 탭에서 Security(보안) > Layer 3(레이어 3) 탭으로 이동하고, Layer **3 보안 방법으로 Web Policy(웹 정책)를 구성하고, Enable On Mac** Filter(Mac 필터 실패 시 활성화), preauthentication ACL(사전 인증 ACL)을 구성하고, Override Global Config(전역 컨피그레이션 재정의)를 활성화하고, Web Auth Type(웹 인증 유형)을 External(외부)로 설정하고, Redirect URL(리디렉션 URL)을 구성합니다.



4단계. AAA 서버를 구성합니다. WLAN Configuration(WLAN 컨피그레이션) 탭에서 Security(보안) > AAA Servers(AAA 서버) 탭으로 이동하여 Authentication Servers and Accounting Servers(인증 서버 및 어카운팅 서버)를 활성화하고 드롭다운 메뉴에서 두 개의 RADIUS 서버를 선택합니다.

cisco	HONITOR MLANS CO	WTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS	ния	ELEDBACK
WLANs	WLANs > Edit 'Aire	OS-DNASpaces'				
* WLANs WLANS	General Security	QoS Policy-Map	oping Advanced			
Advanced	Layer 2 Layer 3	AAA Servers				
	RADIUS Servers RADIUS Server Over Apply Close 35E Defe	write interface Conabled sult Settings Conabled	Accounting Servers			
	C Enable	ed	C Enabled	_		
	Server 1 IP:34.2	97.146.105, Port: 1912	IP:34.197.146.105, Port:1813			
	Server 2 IP:34.2	28.1.95, Port:1812	IP:34.228.1.95, Part:1813			
	Server 3 None	0	None			
	Server 4 None	2	None			
	Server 5 None		None	0		
	Server 6 None	8	None	•		

6단계. **웹 인증** 사용자에 **대한 인증 우선 순위 순서를 구성합니다**. WLAN Configuration(WLAN 컨피 그레이션) **탭**에서 **Security(보안) > AAA Servers(AAA 서버)** 탭으로 이동하고 RADIUS를 순서대로 첫 번째로 설정합니다.

alialia cisco	HONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
WLANs WLANs	General Security QoS Policy-Mapping Advanced
Advanced	Authentication Survivability Authentication Survivability
	Server 1 None 0
	Server 3 None 0
	Local EAP Authentication Enabled
	Authentication priority order for web-auth user
	Not Used Order Used For Authentication
	K LOCAL Down

7단계. WLAN Configuration(WLAN 컨피그레이션) **탭**에서 Advanced(고급) 탭으로 이동하고 Allow AAA Override(AAA 재정의 허용)를 활성화합니다.

cisco	HORITOR HUAN CONTROLLER WIRELESS SECURITY NO	SANGEMENT COMMANDS HELP PERDANCK
VLANs	WLANs > Edit 'AireOS-DNASpaces'	
WLANs MLANs	General Security QoS Policy-Mapping Advance	ced
Advanced	Allow AAA Override 🔹 Enabled	04629
	Coverage Hole Detection 🚺 Enabled	DRCP Server Override
	Enable Session Timeout (Seco) Session Timeout (Seco) Aircent 31 Catabled	DISCP Addr. Ansignment Required Nanagament Frame Protection (MPP)
	Diagnetic Diarval 4 Chabled Override Interface ACL 3Pv4 None	None
	URL ACL None B URL ACL None B P29 Blocking Atlian Disabled B Claret Declarism 2 Chronical 180	803.11a/n (1 - 255) 1 803.13b/gre (1 - 255) 1
	Timeout Value (secs) Havinum Allowed Clients	NAC State None Load Balancing and Band Select
	Static (P Turineting M Enabled Wi-Fi Direct Clents Policy Deadled	Olient Load Balancing Olient Band Salest

1단계. DNA Spaces의 **대시보드**에서 Captive Portals(종속 포털)를 클릭합니다.

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

2단계. Create **New(새로 만들기)**를 클릭하고 포털 이름을 입력한 다음 포털을 사용할 수 있는 위치 를 선택합니다.

	0			
	Poral Information	Authentication	Date Cepture	User Agreement
PORTALIMANE				
AireOS-ONASpaces				
Enable this portal for all location			Calanti	d output
Location Herarchy	es		Selecte	d Locations
Cruble this postal for all location Location-Herarchy MEX-EAST-1			Selectron (Marco - 1	d Locations
Cruble this postal for all location Location Herarchy MEX-EAST-1 C 0 9508-1-CMX	•		Selection (MADO 1	d Locations
	••		Selectric (100-1	dilocations desclored X
	es r rect			dilocations descillament 14

3단계. 인증 유형을 선택하고, 포털 홈 페이지에 데이터 캡처 및 사용자 계약을 표시할지 여부 및 사 용자가 메시지 수신을 옵트인할 수 있는지 여부를 선택합니다. 다음을 **클릭합니다**.

0	0			×
Panal Information	Antonitation	Own Captern	the Agenteen	
BUC 14 A/HEROVA PM		1		
Enal				
More readily solard that anality assess the Homes,		-		
Display Authentication and User Agreements on portal home page				
Allow users to Opt in to worker message				
	500 0	New Dave 2		

4단계. 데이터 캡처 요소를 구성합니다. 사용자로부터 데이터를 캡처하려면 Enable Data Capture(**데이터 캡처 활성화) 상자**를 선택하고 **+Add Field Element(필드 요소 추가)**를 클릭하여 원 하는 필드를 추가합니다. 다음을 **클릭합니다**.

	0		-0	•	×
	Portal Information	Automisation	then Captorn	User Agreements	
E Inste Das Castve Familietés A Fini Name A Last Name				+ Add Paint Doment	:

-	174	and a second second

5단계. Enable **Terms &Conditions(약관 활성화)**를 선택하고 Save **& Configure Portal(포털 저장 및** 구성)을 클릭합니다.

				unite .		d'anticati	893.		Date Capiture	the Appendix		
to ender and a	ontopere	herea & C	orditors a	difference per	ty Danese							
-												
IDADE.												Qr I Drate
0.6.6	6 i e	$\rightarrow \mathbf{Q}$	5.0									
$u^{*} \mid X_{1} \mid Z$	11 H	0.112	X = 0	ca n 🖂	<pre>t</pre>	1.5	9 E	÷ 0 6				
at - Part		5m	1.41	0-1X H								
Lon-petided Sep	number (*	2010										
Canaditions Of the	i De Mi	(here)	option with	to 10 km of	etil geven	-	at the 101-71	antica.				
i des												
pro-with minuless lensing to ensure t	40000 B	the International	d within the s	ranises. No di Toma angle B	nt.e.m	and the second	uction, pros rans: Barriag	etholy neri A' la da sa	te ha activities of the	se vito con tra Senico or over	the any self-only sentral over	r ary material transmitted, healaid
	The end of a set of the set of t	To enable and configure to a first of L_{1} (L_{2} (L_{2} (L_{2}) or quicked Sequence (P -forestime of two pre-trial conceptioned Sequences (P) -forestimes (P (sec) (L_{2} (L_{2}) (The enables and standing we have a LG to the form L of the	The enables and standards have a Libertition of the figure forms Libertition of the figure form L . Conditions of the figure form L is a standard for the figure form L is a standard for the field form of the figure form the figure form the figure formula standards for the figure form the figure	In analytic and survey are been in Conditions and Privacy public in the condition of the	The smaller and configure Thems & Conditions and Privacy policy Distance in the second seco	In stable and surfaces forms is Conditions and Privacy polary Subservers. The field of the stable	In analytic and configure Terms & Conditions and Privacy pulsy Subarranes. In a set of the set of	The smaller and configure from a Condition and Prices, pulsity Dimension. The second	It should not surfager from a Condition and Phase, poly Statements.	It shalls and surfaces from a Conditions and Privacy pathy Statements. It is a statistic and surfaces from a Conditions and Privacy pathy Statements. It is a statistic and surfaces from a state is a state in the statement of	The statistic and surfaces Terms & Conditions and Privacy pathy Statements. The statistic and surfaces Terms & Conditions and Privacy pathy Statements. The statistic density of the statistic de

6단계. 필요에 따라 포털을 수정하고 Save(저장)를 클릭합니다.

autor but but a	Parlam justian /	
NACENOR - Severa sector to configer. 3	ug the lamp constraint methods.	
Brand Name		KONA PRIVIN
Webarto Message	BUAD NAM	< Home Scener
Nation	Origination on tangentic or practic has the method unit loand	Cisco Systems
Email Authentication	the Orly Class	
Venalitip	Shird have	Walkome to Sporatiland
 When 	Clear Summer at	SIGN-UP FOR WIR
D Preduct		Complete the form before to connect to internet
s inp		Profit
 Get App 		
Orthinse Orthinse Orthinse Orth O		(B) # ()
Prones & Oflans		
+ Ref Multim		

DNA 공간에 종속 포털 규칙 구성

1단계. 종속 포털 메뉴를 열고 종속 포털 규칙을 클릭합니다.

⊖ → ♂ ☆	A https://dnaspaces.io/captiveportal/in/es/captive-portal	
Cisco DNA Space	s	
Dental		
E Captive Portal Rules		Created
ଟି \$\$IDs	DOT .	Feb 24, 2020
a Reports	>	⊖ 8.02 PM

2단계. + Create **New Rule을 클릭합니다**. 규칙 이름을 입력하고 이전에 구성한 SSID를 선택한 다 음 이 포털 규칙이 사용 가능한 위치를 선택합니다.

Charte Captive Portal Rule RELEVANCE And Co-Ballyanne	
ae any or an of the options that apply to your rule below	
	TUMBANY
When a user is or VKH - and connected to AwdD-dNRQpacer -	111 144
	sim01-Ontiperm
DOFDING - When its you want the rule to the?	10.400
	Warn year is an NPT and conserved to film?
At any of the following locations	th Adjuster
to any or the contemporation	LOD/VIDHE
+ Additionations	For all locations under
	10/0-1 (Decidence)
Hitt-t-Smallanmet X	and and a
	ID-RD-M
The by Security The particular and to including an excluding location by rotatings	
	10/10/1

3단계. 종속 포털의 작업을 선택합니다. 이 경우, 규칙이 적중되면 포털이 표시됩니다. 저장 **및 게시** 를 클릭합니다.

X 6	Notesta.
Show Capital Partial Grasse a Partial to depend to Users when they connecting the will.	SCHERALE
AmOS-DRADpaces v	ADDN
Section Duration	Bhia Capite Perfai Pertal : AneOS: ON/Opecas
Bardwidt-Unit	
Searclassig Provider Internet Directly produce internet without shoeing any automitication	
Charty Internet Day serve from accounting the Internet	
Targe these units as Choose - Incontra Choosenate units to choose tap.	
+ And Tege	
Li Trigger Art	

다음을 확인합니다.

SSID에 연결된 클라이언트의 상태를 확인하려면 **Monitor(모니터) > Clients(클라이언트)**로 이동하 고 MAC 주소를 클릭하고 Policy Manager State(정책 관리자 상태)를 찾습니다.

M	ONITOR	MLANI	CONTROLLER	WPELESS	SECORITY	HANAGEMENT	COMMANDS	HELP	EEDBACK	
С	lients > D	etail								< Back
M	tax Number	of Record	Is 10 * Ck	ter AVC Stats	I					
ſ	General	AVC S	tatistics							
l		_					AP radio als	e 1d	1	
	Client Typ	e	Regular				WLAN Profil		AireOS-OMASpaces	
	Client Tur	rel Trpe	Simple IP				WLAN SSID		AireOS-ONASpeces	
	User Nam						Status		Associated	
	Webeuth	User Name	None				Association	10	1	
	Port Num	ber	1				802.11 Aut	hentication	Open System	
	Setevface		management				Reason Cod	e .	1	
	VLAN ID		20				Status Code		0	
	Quarantie	+ VLAN ID	0				CF Pollable		Not Implemented	
	CCX Version		Not Supported				CF Pull Reg	rest.	Not Implemented	
	EDE Versi		Not Supported				Short Pream	able	Not Implemented	
	Mahilles R		Land				PBCC		Not Implemented	
	Mobility P	eer IP	N/A				Chernel Ap	iity.	Not Implemented	
	Address						Timesul		0	
	FORCY MA	INVE COURT		_			WEP State		WEP Disable	
	Oraba		POURS .				and and a			

문제 해결

클라이언트의 연결 및 인증 프로세스를 확인하기 위해 테스트하기 전에 컨트롤러에서 다음 명령을 활성화할 수 있습니다.

(5520-Andressi) >debug client

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

이는 RADIUS 서버가 없는 SSID에 연결하는 동안 연결/인증 프로세스 중에 각 단계를 식별하려고 시도한 성공적인 시도의 출력입니다.

802.11 연결/인증:

*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 capability 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 및 레이어 3 인증:

*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 레이어 3 인증에 성공하면 클라이언트를 RUN 상태로 이동합니다. *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 ACL ACL ID 255, URL AC

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.