Catalyst 9800에서 Anchor로 중앙 웹 인증 구성

목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 다른 Catalyst 9800에 고정된 Catalyst 9800 구성 네트워크 다이어그램 두 9800에서 모두 AAA 구성 WLC에서 WLAN 구성 외부 WLC에 정책 프로필 및 정책 태그 생성 앵커 WLC에 정책 프<u>로파일 생성</u> 두 9800s 모두에서 ACL 컨피그레이션 리디렉션 ISE 구성 AireOS WLC에 고정된 Catalyst 9800 구성 Catalyst 9800 외부 컨피그레이션 앵커 AireOS WLC의 AAA 구성 AireOS WLC의 WLAN 구성 AireOS WLC에서 ACL 리디렉션 ISE 구성 AireOS WLC가 외부, Catalyst 9800이 앵커인 경우 구성의 차이점 다음을 확인합니다. 문제 해결 Catalyst 9800 문제 해결 정보 클라이언트 세부 정보 임베디드 패킷 캡처 RadioActive 추적 AireOS 문제 해결 정보 클라이언트 세부 정보 CLI에서 디버깅 참조

소개

이 문서에서는 AireOS 또는 다른 9800 WLC를 통해 목적지를 다루는 다른 WLC(Wireless LAN Controller)를 모빌리티 앵커로 가리키는 Catalyst 9800에서 CWA(Central Web Authentication)를 구성하고 트러블슈팅하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

9800 WLC, AireOS WLC 및 Cisco ISE에 대한 기본적인 이해가 있는 것이 좋습니다. CWA 앵커 컨 피그레이션을 시작하기 전에 이미 두 WLC 간에 모빌리티 터널을 가동한 것으로 가정합니다. 이 컨 피그레이션 예제의 범위를 벗어납니다. 도움이 필요한 경우 "Building <u>Mobility Tunnels on Catalyst</u> 9800 controllers" 문서<u>를 참조하십시오</u>.

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

9800 17.2.1

8.5.164IRCM 이미지

ISE 2.4

다른 Catalyst 9800에 고정된 Catalyst 9800 구성

네트워크 다이어그램



두 9800에서 모두 AAA 구성

앵커와 외부 모두에서 먼저 RADIUS 서버를 추가하고 CoA가 활성화되었는지 확인해야 합니다. 이 작업은 메뉴에서 수행할 수 있습니다.Configuration(구성)>Security(보안)>AAA>Servers/Groups(서버/그룹

)>Servers(서버)> Add(추가) 버튼을 클릭합니다.

Cisco Cata	alyst 9800-L Wireless Controller			Welcome admin Last logn Fri, May 15 2020 16:56:51
Q Search Menu Items	Configuration * > Security * > AAA	ן		
Dashboard	+ AAA Wizard			
Monitoring >	Servers / Groups AAA Method Lis	t AAA Advanced		
Configuration	+ Add × Delete			
Administration	RADIUS	Servers Server Groups		
C Licensing	TACACS+	Name	✓ Address	 Auth Port
K Troubleshooting	LDAP Create AAA Radius Server			×
	Name*	CILIE-Second		
	Name-	CLUS-Server		
	Server Address*	XXXX		
	PAC Key			
	Кеу Туре	Clear Text 🔻		
	Key*			
	Confirm Key*			
	Auth Port	1812		
	Acct Port	1813		
	Server Timeout (seconds)	1-1000		
	Retry Count	0-100		
	Support for CoA	ENABLED		
	D Cancel			Apply to Device

이제 서버 그룹을 생성하고 방금 구성한 서버를 해당 그룹에 배치해야 합니다. 이 작업은 Configuration(구성)>**Security(보** 안)>AAA>Servers/Groups(서버/그룹)>Server Groups(서버 그룹)>+Add(추가)에서 수행합니다.

Cisco Cata	llyst 9800-L Wireless Co	ontroller	
Q Search Menu Items	Configuration * > Security	· > AAA	
📻 Dashboard	+ AAA Wizard		
Monitoring >	Servers / Groups AAA	Method List AAA Advanced	
Configuration	+ Add × Delete		
Administration		Servers Server Groups	
C Licensing	TACACS+		
💥 Troubleshooting			~ Ser
	Create AAA Radius Serve	er Group	×
	Name*	CLUS-Server-Group	
	Group Type	RADIUS	
	MAC-Delimiter	none 🔻	
	MAC-Filtering	none 🔻	
	Dead-Time (mins)	1-1440	
	Available Servers	Assigned Servers	
		CLUS-Server	
	Cancel		Apply to Device

이제 **권한 부여** 방법 목록(CWA에는 인증 방법 목록이 필요하지 않음)을 생성합니다. 여기서 유형은 네트워크이고 그룹 유 형은 그룹입니다. 이전 작업에서 이 메서드 목록에 서버 그룹을 추가합니다.

이 컨피그레이션은 Configuration(컨피그레이션)>Security(보안)>AAA>Servers/AAA Method List(서버/AAA 메서드 목록)>Authorization(권한 부여)>+Add(추가)에서 수행합니다.

Cisco Cataly	st 9800-L Wirele	ss Controller				
Q Search Menu Items	Configuration * > S	ecurity - > AAA				
Dashboard	+ AAA Wizard					
Monitoring >	Servers / Groups	AAA Method List	AAA Advanced			
Configuration	Authentication					
Administration	Authorization		+ Add X Del			
C Licensing		uthorization	Name	≺ Туре	√ G	roup Type
	QUICK SETUP: AAA A	Authorization				~
X Troubleshooting	Method List Name*	CLUS-A	AuthZ-Meth-List			
	Type*	network	·			
	Group Type	group	•			
	Fallback to local					
	Authenticated					
	Available Server Groups		Assigned Server Groups	S		
	radius Idap tacacs+ ISE1	* * *	CLUS-Server-Gro	oup	× ×	
	Cancel				Apply to [Device

(선택 사항) 권한 부여 방법 목록과 동일한 서버 그룹을 사용하여 계정 관리 방법 목록을 생성합니다. 어카운팅 목록은 Configuration(컨피그레이션)>Security(**보안)>AAA>Servers/AAA Method List(서버/AAA 방법 목록)>Accounting(어카운팅)>+Add(추가)에서 생성할 수 있습니다.**

Cisco Cata	alyst 9800-L Wirele	ess Controller				
Q Search Menu Items	Configuration * > S	Security > AAA				
📰 Dashboard	+ AAA Wizard					
Monitoring >	Servers / Groups	AAA Method List	AAA Advanced			
Configuration	Authentication	ſ				
Administration	Authorization	,(Name	V Tune		Group1
C Licensing	Quick Setup: AAA	Accounting	Name	. Type		×
X Troubleshooting	Method List Name*	CLUS-/	Acct-Meth-List			
	Туре*	identity	•			
	Available Server Group	S	Assigned Server Gro	oups		
	radius Idap tacacs+ ISE1		> CLUS-Serve	er-Group	× × ×	
	Cancel				Apply to	Device

WLC에서 WLAN 구성

두 WLC에서 WLAN을 생성하고 구성합니다. WLAN이 두 모두에서 일치해야 합니다. 보안 유형은 mac 필터링이어야 하며 이전 단계의 권한 부여 방법 목록을 적용해야 합니다. 이 컨피그레이션은 Configuration(컨피그레이션)>Tags & Profiles(태그 및 프로파일)>WLANs(WLAN)>+Add(추가)에서 수행됩니다.

Cisco Cata	alyst 9800-L Wireless	Controller			
Q Search Menu Items	Configuration > Tage	s & Profiles * > WLANs			
Dashboard	+ Add × Dele				
(2) Monitoring >	Number of WLANs selected	: 0			
	Status - Name	9	~	ID	~ .
Configuration	Add WLAN				×
	General Security	Advanced	_		
C Licensing	Profile Name*	CLUS-WLAN-Name	Radio Policy	All	•
X Troubleshooting	SSID*	CLUS-SSID	Broadcast SSI	D ENABLED	
	WLAN ID*	2			
	Status	ENABLED			
	Cancel				Apply to Device

Cisco Cata	alyst 9800-L Wireless Controller	
Q Search Menu Items	Configuration * > Tags & Profiles * > WLANs	
Dashboard	+ Add × Delete Enable WLAN Disable WLAN	
Monitoring >	Number of WLANs selected : 0	
	Add WLAN	×
	General Security Advanced	
© Licensing	Layer2 Layer3 AAA	_
X Troubleshooting	Layer 2 Security Mode None Lobby Admin Access	
	OWE Transition Mode Reassociation Timeout 20	
	Cancel	

외부 WLC에 정책 프로필 및 정책 태그 생성

외부 WLC 웹 UI로 이동합니다.

정책 프로필을 생성하려면 Configuration(컨피그레이션)>Tags & Profiles(태그 및 프로파일)>Policy(정책)>+Add(추가)로 이동합니다.

고정할 때는 중앙 스위칭을 사용해야 합니다.

Cisco Catal	yst 9800-L Wireless Con	troller		
Q Search Menu Items	Configuration * > Tags & Pro	ofiles * > Policy		
Dashboard Monitoring	Status V Policy Profile	Name		 Description
Configuration	General Access Policies	QOS and AVC Mobility	Advanced of connectivity for clients associated with	this profile.
C Licensing	Name*	CLUS-Policy-Profile	WLAN Switching Policy	
	Description	Policy Profile for CLUS	Central Switching Central Authentication	ENABLED
	Passive Client Encrypted Traffic Analytics	DISABLED DISABLED	Central DHCP Central Association	ENABLED
	CTS Policy Inline Tagging		Flex NAT/PAT	DISABLED
	SGACL Enforcement Default SGT	2-65519		
	Cancel			Apply to Device

"Advanced(고급)" 탭에서 CWA에 대해 AAA 재정의 및 RADIUS NAC가 필수입니다. 여기에서 어카 운팅 방법 목록을 만들도록 선택한 경우에도 적용할 수 있습니다.

Q Search Menu Items	Configuration > Tags & Pro	files > Policy		
🔜 Dashboard	+ Add × Delete			
(Monitoring >	Status v Policy Profile	Name	~	Description
	Add Policy Profile			×
Configuration >	General Access Policies	QOS and AVC Mobility	Advanced	
Administration	WLAN Timeout		Fabric Profile Search or Select	•
C Licensing	Session Timeout (sec)	1800	mDNS Service Search or Select	•
X Troubleshooting	Idle Timeout (sec)	300	Hotspot Server Search or Select	•
	Idle Threshold (bytes)	0	User Private Network	
	Client Exclusion Timeout (sec)	60	Status	
	Guest LAN Session Timeout		Drop Unicast	
	DHCP		Umbrella	
	IPv4 DHCP Required		Umbrella Not Configured Parameter Map	Clear
	DHCP Server IP Address Show more >>>		Flex DHCP Option ENABLED For DNS	
	AAA Policy		DNS Traffic Redirect IGNORE	
	Allow AAA Override		WLAN Flex Policy	
	NAC State		VLAN Central Switching	
	NAC Type	RADIUS	Split MAC ACL Search or Select	•
	Policy Name	default-aaa-policy x	Air Time Fairness Policies	
	Accounting List	CLUS-Acct-Meth-1	2.4 GHz Policy Search or Select	•

"Mobility(모빌리티)" 탭에서 "앵커 내보내기" 확인란을 선택하지 말고 앵커 목록에 앵커 WLC를 추 가합니다. "Apply to Device"를 클릭해야 합니다. 다시 한 번 말씀드리지만, 두 컨트롤러 사이에 모빌 리티 터널이 이미 설정되어 있다고 가정합니다

Cisco Catalyst 94	300-L Wireless Con	troller			
Q. Search Menu Items Conf	guration * > Tags & Pr	ofiles * > Policy			
🔜 Dashboard	Add X Delete				
🔿 Monitoring 💦 Add P	olicy Profile				×
Configuration	al Access Policies	QOS and AVC	obility Advance	ed	
C Administration Mol	oility Anchors				
Licensing Exp	irt Anchor				
Troubleshooting	c IP Mobility Mobility Anchors will cause t	DISABLED	intenty		
disable	and may result in loss of con	inectivity for some clients.			
Drag	nd Drop/double click/click	on the arrow to add/remov	e Anchors		
Ava	lable (0)	Selected (1)		
And	or IP	Anchor IP	Anc	chor Priority	
		192.1	68.160.18	Primary (1)	- +
	No anchors available				
00	ancel				Apply to Device

AP에서 이 정책 프로필을 사용하려면 정책 태그를 생성하여 사용하려는 AP에 적용해야 합니다.

정책 태그를 생성하려면 Configuration(구성)>Tags & Profiles(태그 및 프로파일)>Tags(태그)?Policy(정책)>+Add(추가)로 이동합니다.

Cisco Cata	alyst 9800-L Wireles	s Controller		
Q Search Menu Items	Configuration * > Tag	gs & Profiles * > Tags		
Dashboard	Policy Site R	F AP		
Monitoring >	+ Add ×			
Configuration	Policy Tag Nar	ne		
	Add Policy Tag			×
	Name*	CLUS-Policy-Tag		
C Licensing	Description	Policy Tag for CLUS		
X Troubleshooting	WLAN-POLICY + Add × Del	′ Maps: 0		
	WLAN Profile	~	Policy Profile	~
	4 4 0 ⊨ ⊨	10 🔻 items per page		No items to display
	Map WLAN and Poli	су		
	WLAN Profile*	CLUS-WLAN-Name	Policy Profile*	CLUS-Policy-Profile
		×	 Image: A start of the start of	
	RLAN-POLICY	Maps: 0		
	Cancel			Apply to Device

여러 AP에 동시에 추가하려면 Configuration(컨피그레이션)>Wireless Setup(무선 설정)>Advanced(고급)>Start Now(지금 시작)로 이동합니다. "Tag APs" 옆의 글머리 기호를 클릭하고 선택한 AP에 태그를 추가합니다.

¢	cisco IZ	isco Catal	yst 9800-L Wire	less Controlle	r							
٩	Search Menu Items		Configuration * >	Wireless Setup *	> Adva	nced						
	Dashboard		Start				+ τ	ag APs				
	Monitoring	>		Tags & Profiles		Nu	mber ected	of APs: 3 I Number of APs:	3			
Z		>	0	WLAN Profile	· · ·			P Name	~ AP Model ~	AP MAC ~	AP ~ Mode	AS
		>	0	Policy Profile	-		Ja	ays2800	AIR-AP2802I- B-K9	002a.10f3.6b60	Local	E
Ô	Licensing		0	Policy Tag 🏼 🥔	-		Ja	ays3800	AIR-AP3802I- B-K9	70b3.1755.0520	Local	E
								P0062.ec20.122	c AIR-CAP2702I- B-K9	cc16.7e6c.3cf0	Local	D
X	Troubleshooting	1	0	AP Join Profile	-		4 4	(1 ⊩	10 🔻 items per			
			0	Flex Profile	-	Та	ig Al	Ps			×	٤
			0	Site Tag 🛛 🧳			Tags					
							Policy	, CLU	JS-Policy-Tag 🔻]		
			0	RF Profile	-		Site	Sea	rch or Select			
			0	RF Tag 🧳			RF	Sea	rch or Select 🔻			
				Apply			Chang	ging AP Tag(s) wi	ill cause associated A	P(s) to reconnect		
			0	Tag APs			D Ca	ancel			to Device]
			Done									

앵커 WLC에 정책 프로파일 생성

앵커 WLC 웹 UI로 이동합니다. 앵커 9800의 Configuration(구성)>Tags & Profiles(태그 및 프로파일)>Tags(태그)>Policy(**정책)>+Add(추가)에서 정책 프로파일을 추가합니다**. 모빌리티 탭 및 어카운팅 목록을 제외하고 이 항목이 외주에 서 만든 정책 프로필과 일치하는지 확인합니다.

여기서 앵커를 추가하지 않고 "앵커 내보내기" 확인란을 선택합니다. 여기에 계정 목록을 추가하지 마십시오. 다시 한 번 말씀드리지만, 두 컨트롤러 사이에 모빌리티 터널이 이미 설정되어 있다고 가정합니다

참고: 정책 태그의 WLAN에 이 프로파일을 연결할 이유는 없습니다. 이렇게 하면 문제가 발생합니다. 이 WLC의 AP에 동 일한 WLAN을 사용하려면 다른 정책 프로파일을 생성합니다.

Cisco Catalyst 9800-L Wireless Con	ontroller		
Q Search Menu Items Configuration * > Tags & P	Profiles > Policy		
Dashboard + Add × Delete			
Add Policy Profile			×
General Access Policies	QOS and AVC Mobi	ility Advanced	
Administration >			
C Licensing			
Static IP Mobility Adding Mobility Anchors will cause disable and may result in loss of co Drag and Drop/double click/click	the enabled WLANs to momental connectivity for some clients.	vrily	
Available (1)	Selected (0)		
Anchor IP	Anchor IP	Anchor Priority	
<u></u> 192.168.160.16	*	Anchors not assigned	
ී Cancel			Apply to Device

두 9800s 모두에서 ACL 컨피그레이션 리디렉션

그런 다음 두 9800에서 리디렉션 ACL 컨피그레이션을 생성해야 합니다. 트래픽에 ACL을 적용하는 앵커 WLC가 될 것이 므로 외부 항목은 중요하지 않습니다. 유일한 요구 사항은 그것이 그곳에 있고 어떤 입구를 가지고 있다는 것입니다. 앵커 의 항목은 포트 8443에서 ISE에 대한 액세스를 "거부"하고 다른 모든 것을 "허용"해야 합니다. 이 ACL은 클라이언트에서 "수신"하는 트래픽에만 적용되므로 반환 트래픽에 대한 규칙이 필요하지 않습니다. DHCP 및 DNS는 ACL의 항목 없이 통 과됩니다.

Cisco Cata	alyst 9800-L Wireless Co	ontroller			Welcome admin
Q Search Menu Items	Configuration > Security	· · · ACL			
Dashboard	+ Add × Delete Add ACL Setup	Associate Interfaces			×
Monitoring >	ACL Name*	CLUS-ACL	ACL Type	IPv4 Extended	
	Rules				
	Sequence*		Action	permit v	
C Licensing	Source Type	any 🔻			
X Troubleshooting	Destination Type	any 🔻			
	Protocol	ahp 🔻			
	Log	0	DSCP	None	
	+ Add × Delete				
	Sequence V Action	Source V Source Vildcard	Destination V IP Wildcard V	Protocol v Port	Destination ~ Port DSCP ~ Log ~
	10 deny	any	192.168.160.99	tcp None	eq 8443 None Disabled
	100 permit	any	any	ip None	None None Disabled
	⊲ ⊲ 1 ⊳ ⊮ [10 🔻 items per page			1 - 2 of 2 items
	Cancel				Apply to Device

ISE 구성

마지막 단계는 CWA용 ISE를 구성하는 것입니다. 여기에는 수많은 옵션이 있지만 이 예에서는 기본 사항을 고수하며 기본 셀프 등록 게스트 포털을 사용합니다.

ISE에서 권한 부여 프로파일, 인증 정책 및 권한 부여 프로파일을 사용하는 권한 부여 정책을 가진 정책 집합을 생성하고, 네트워크 디바이스로 ISE에 9800(foreign)을 추가하고, 네트워크에 로그인 할 사용자 이름 및 비밀번호를 생성해야 합니다.

권한 부여 프로파일을 생성하려면 Policy(정책)>Policy Elements(정책 요소)>Authorization(권한 부 여)>Results(결과)>Authorization Profiles(권한 부여 프로파일)>로 이동한 다음 Add(추가)를 클릭합 니다. 반환된 액세스 유형이 "access_accept"인지 확인한 다음 다시 전송할 AVP(attribute-value 쌍)를 설정합니다. CWA의 경우 리디렉션 ACL 및 리디렉션 URL은 필수 사항이지만 VLAN ID 및 세션 시간 초과 등의 항목을 다시 전송할 수도 있습니다. ACL 이름은 외래 및 앵커 9800에서 리디렉션 ACL의 이름과 일치해야 합니다.

$\epsilon \rightarrow C$ A Not secure 19	2.168.160.99/admin/#policy/policy_elements/policy_elements_permissions/policy_elements_permissions_authorization/policy_element
dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Cl	ient Provisioning Policy Elements
Dictionaries Conditions Result	
Authentication Authorization Authorization Profiles Downloadable ACLs Profiling Posture Client Provisioning	Authorization Profiles > test Authorization Profile * Name CLUS-AuthZ-Profile-ISE Description * Access Type ACCESS_ACCEPT Network Device Profile Genvice Template Track Movement () Passive Identity Tracking ()
	✓ Common Tasks ✓ Voice Domain Permission ✓ Web Redirection (CWA, MDM, NSP, CPP) () Centralized Web Auth ▼ ACL CLUS-ACL Value Self-Registered Guest Portal (c▼

그런 다음 CWA를 통과하는 클라이언트에 방금 생성한 권한 부여 프로파일을 적용하는 방법을 구 성해야 합니다. 이를 위해, 한 가지 방법은 MAB를 사용할 때 인증을 우회하는 정책 세트를 만들고, 호출된 스테이션 ID에서 전송된 SSID를 사용할 때 권한 부여 프로파일을 적용하는 것입니다. 다시 한 번 말하지만, 이것을 성취하는 방법에는 많은 것들이 있습니다. 그래서 좀 더 구체적이거나 더 안 전한 어떤 것이 필요하다면, 그렇게 하세요. 이것이 바로 가장 간단한 방법입니다.

정책 집합을 생성하려면 Policy(정책)>Policy Sets(정책 집합)로 이동하여 화면 왼쪽에 있는 + 버튼 을 누릅니다. 새 정책 세트의 이름을 지정하고 MAB에 대해 "Process Host Lookup(프로세스 호스트 조회)"을 허용하는 허용된 프로토콜 목록 또는 "기본 네트워크 액세스"로 설정되어 있는지 확인합니 다(허용되는 프로토콜 목록을 확인하려면 정책>정책 요소>결과>인증>허용되는 프로토콜)로 이동 합니다. 이제 생성한 새 정책 세트의 중간에 + 기호를 누릅니다.

-dtude Identity Services Engine Home + Context Visibility + Operations	Policy Administration Work Centers	License Warning 🔺	_9, ∎	0 0
Policy Sets Profiling Posture Client Provisioning + Policy Elements		Click here to do visibility setup Do not	show this again.	×
Policy Sets		ResetAll Hitcounts	Reset	Save
+ Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence	Hits Action	s View
Search				
O <u>CLUS CWA</u> Policy-Set	+	Default Network Access * * +	0	>
Default Default policy set		Default Network Access * * +	• •	>
			Reset	Save

MAB가 ISE에서 사용될 때마다 이 정책 집합에서 실행됩니다. 나중에 사용 중인 WLAN에 따라 다른 결과를 적용할 수 있도록 발신된 스테이션 ID에서 일치하는 권한 부여 정책을 만들 수 있습니다. 이 프로세스는 매칭할 수 있는 많은 것들을 통해 매우 사용자 지정이 가능합니다.

Conditions Studio		
Library	Editor	
mab ♥ ⊑ □ ▲ ⊕ 및 ⊑ 홈 ◙ ∄ 만 1 ♥ ₺ ኞ	Wireless_MAB Set to 'Is not'	<i>(</i>)
Wired_MAB ()		
Wireless_MAB ()	+ New AND OR	

정책 집합 내에서 정책을 생성합니다. 인증 정책은 MAB에서 다시 일치할 수 있지만 "내부 엔드포인 트"를 사용하도록 ID 저장소를 변경해야 하며 인증 실패 및 사용자를 찾을 수 없는 경우 계속 옵션을 변경해야 합니다.

Polcy Sets Profiling Posture Client Provisioning + Polcy Elements	Click here to do visibility setup Do not show this again.
Policy Sets → CLUS-CWA-Policy-Set	ResetAll Hitcounts Reset Save
Status Policy Set Name Description Conditions	Allowed Protocols / Server Sequence Hits
Search	
CLUS-CWA-Polop-Set	Default Network Access ** 🕈 0
◆ Authentication Policy (2)	
Status Rule Name Conditions	Use Hits Actions
CLUS MAR Condition Wreless_MAR	Internal Endpoints ◆ Options If Auth Tall CONTINUE • • If User not found CONTINUE • • If Process fall DROP • •
© Default	Al_User_UD_Stores ● ◆ Options 0
Authorization Policy - Local Exceptions	
Authorization Policy - Global Exceptions	
Authorization Policy (1)	

인증 정책이 설정되면 권한 부여 정책에서 두 개의 규칙을 생성해야 합니다. 이 정책은 ACL과 같이 읽므로 주문에 사후 인증 규칙이 맨 위에 있고 맨 아래에 사전 인증 규칙이 있어야 합니다. 사후 인 증 규칙은 이미 게스트 플로우를 통과한 사용자와 일치합니다. 이것은 그들이 이미 로그인했다면 그 규칙을 무시하고 거기서 멈춘다는 것을 말하는 것입니다. 로그인하지 않은 경우 목록 아래로 계 속 이동하여 사전 인증 규칙을 입력하여 리디렉션을 가져옵니다.권한 부여 정책 규칙을 SSID로 끝 나는 호출된 스테이션 ID와 일치시켜 그렇게 구성된 WLAN에 대해서만 적중시키는 것이 좋습니다.

Policy	Sets +	CLUS-CWA-Policy-Set							Reset	All Hitcounts
	Status	Policy Set Name	Descrip	ption	Con	ditions			Allowed	Protocols / Server
Search	h									
	0	CLUS-CWA-Policy-Set				Wireless_MAB			Default	Network Access
> Au	thenticatio	n Policy (2)								
> Au	thorization	Policy - Local Exceptions								
> Au	thorization	Policy - Global Exceptions								
∀ Au	thorization	Policy (4)								
(+ Sea	Status	Rule Name	Cond	titions			Results Profiles	Security Groups		
ſ	ø	Post-CWA	AND	는 Network Acces	s-UseCa Station-I	ISE EQUALS Guest Flow D ENDS_WITH CLUS-SSID	× CLUS-Post-Auth	+	Select from list	• +
	ø	MAB on WLAN	AND	Radius-Called	Station-I	d Ends_with clus-ssid	CLUS-Auth2-Profile-ISE	+	Select from list	• +
	Ø	Flex AuthZ	₽	Radius Called-Station-II	ENDS	WITH FLEX-CWA	× CLUS-Flex_CWA	+	Select from list	- +
	0	Default					× DenyAccess	+	Select from list	- +

이제 정책 집합이 구성되었으므로 ISE가 인증자로 신뢰하도록 하려면 9800(foreign)에 대해 ISE에 알려야 합니다. 이 작업은 Admin(관리)>**Network Resources(네트워크 리소스)**>**Network Device(네 트워크 디바이스)>+에서** 수행할 수 있습니다. 이름을 지정하고 IP 주소(또는 전체 관리 서브넷)를 설정하고 RADIUS를 활성화하고 공유 암호를 설정해야 합니다. ISE의 공유 암호가 9800의 공유 암 호와 일치해야 합니다. 그렇지 않으면 이 프로세스가 실패합니다. 컨피그레이션이 추가된 후 전송 버튼을 눌러 저장합니다.

dentity Services Engine	Home → Con	text Visibility	 Operations 	▶ Policy	- Administration	Work	Centers			
System Identity Management	- Network Resourc	es 🕨 🕨 Device	Portal Management	pxGrid Se	ervices + Feed	Service +	Threat Centric N	AC		
Network Devices Network Device C	Broups Network I	Device Profiles	External RADIUS	Servers R	RADIUS Server Se	equences N	AC Managers	External MDM	Location Services	
Network Devices Default Device Device Security Settings	Network Device Network De	s List > JAysNe vices	* Name CLUS Description	5_Net-Device						
	IP Add	ress 🔻	IP : 192.168.160	.0		/ 2	24			
	* Network Location IPSE Device Typ	* D Soft Device Group on All Location C No De All Device T	Nevice Profile dittic C Model Name ware Version s s S Se Se Se Se Spes S Se	isco 🔹 🕀 • • • • • • • • • • • • • • • • • • •						
	RADI	US Authenticatio	on Settings							
	RAD	IUS UDP Settin	gs Use Seco	Pro Shared S and Shared S	ecret ()		Show)		
	RAD	IUS DTLS Setti	ngs (j)	CoA	Port 1700		Set To	Default		

마지막으로, 클라이언트가 네트워크에 액세스할 수 있어야 하는지 확인하기 위해 로그인 페이지에 입력할 사용자 이름과 비밀번호를 추가해야 합니다. 이 작업은 Admin(관리)>Identity

Management(ID 관리)>Identity(ID)>Users(사용자)>+Add(추가)에서 수행되며 추가한 후 제출을 누 르십시오. ISE의 다른 모든 것과 마찬가지로, 이것은 사용자 지정이 가능하며 로컬에 저장된 사용 자가 아니어도 되지만 다시 말해 가장 쉬운 컨피그레이션입니다.

alialia cisco	Identity Servic	es Engine	Home	Context Visibilit	y ► Opera	ations • Poli	y - Adminis	stration • W	ork Centers	
▶ Sy	/stem 🔽 Identity	/ Management	Network Re	esources 🕨 De	vice Portal Ma	inagement pxG	rid Services	Feed Service	Threat Centric NAC	
▼ Ide	entities Groups	External Identi	ty Sources	Identity Source S	Sequences	 Settings 				
	_	0	Network A	ccess Users List	> New Netwo	ork Access User				
Users			▼ Netv	work Access Us	ser					
Latest	Manual Network 3	Scan Results	* Nam	e CLUS-User						
			Statu	s 🔽 Enabled	•					
			Ema	il						
			T Day	cworde						
			* Pd3	swords						
			Pass	word Type: In	ternal Users					
				Pa	ssword		Re-Enter Pa	ssword		
			* Log	in Password					Generate Password	
			Enab	le Password					Generate Password	1 (i)
			▼ Use	er Information						
			First	Name						
			Last	Name						
			× Acc	count Ontions						
			ACC							
				U						
			Char	ige password on	next login 🗀					
			▼ Acc	ount Disable I	Policy					
				Disable account i	f date exceeds	2020-07-17		(yyyy-mm-o	(bb	
			▼ Hee	ar Groups						
			+ US	a oroups						
			II [Sele	ect an item	(
			Submit	Cancel						

AireOS WLC에 고정된 Catalyst 9800 구성



Catalyst 9800 외부 컨피그레이션

앞서 설명한 것과 동일한 단계를 수행하여 "*Create the policy profile on the anchor WLC(앵커 WLC에서 정책 프로필 생성*)" 섹션을 건너뜁니다.

앵커 AireOS WLC의 AAA 구성

Security(보안)>AAA>RADIUS**>Authentication(인증)>New(새로 만들기)**로 이동하여 WLC에 서버**를 추가합니다**. 서버 IP 주소, 공유 암호 및 CoA 지원을 추가합니다.

ahaha					ut Befresh
cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP	FEEDBACK		A Home
Security	RADIUS Authentication Serve	rs		Apply N	ew
AAA General Calubranication Taiback Dis Dewrloaded AVP TACACS+ LOAP Local R Users Local R Users User Login Ploices AP Policies Passwerd Publices	Auth Called Station ID Type AP 11 Use AES Key Wrap (Dee MAC Delimiter Hype Praned MTU (2000) Network Management Proxy	MC Address (SSID V igned for FIPS customers and requires a key wrap compliant RADIUS server) isn isn Server Server Address(Ipv4/Ipv6) Port IPSec Status	a		
ahaha		WIRELEGE CECURITY MANAGEMENT COMMANDE UELD	Sage Configuration		ut Befresh
cisco	HOMITOK HOMS CONTROLLER	MARLESS SECONTI I NEMAGEMENT COMMUNITY NELF	TEENDAILY		. Home
Security	RADIUS Authentication Serve	rs > New		Back	Apply
AAA General General Activity Accounting Activity Activity Activity Activity Activity Activity Activity Dissription Dissription Dissription Dissription Activity Activi	Server Index (Priority) Server IP Address((prvA/Ipr4)) Shared Secret Format Shared Secret Confirm Shared Secret Apply Cisso ISE Default settings Key Wap Pot Number Server Status Support for CoA Server Timeout Network User Nanagement Retransmit Timeout Tunnel Proxy PAC Provisioning ISSec	I ▼ 192.164.50.99 ▲ ASCII ▼ Image: Complexity of the state	Dus server)		
Wireless Protection Policies Web Auth	PAC Provisioning IPSec	Enable Enable			

AireOS WLC의 WLAN 구성

WLAN을 생성하려면 WLANs>Create New>Go로 이동합니다.

프로파일 이름, WLAN ID 및 SSID를 구성한 다음 "Apply(적용)"를 누릅니다.



WLAN 컨피그레이션으로 이동해야 합니다. ISE를 AVP에 전송하도록 구성하지 않으려는 경우 "General(일반)" 탭에서 클라이언트가 사용할 인터페이스를 추가할 수 있습니다. 다음으로 Security>Layer2 탭으로 이동하여 9800에서 사용한 "Layer 2 Security" 컨피그레이션을 확인하고 "MAC Filtering"을 활성화합니다.



이제 **Security>AAA Servers** 탭으로 이동하고 ISE 서버를 "Authentication Servers"로 설정합니다. "Accounting Servers"에 대해 아무것도 설정하지 **마십시오**. 어카운팅에 대해 "Enable(활성화)" 상자 의 선택을 취소합니다.

ahaha		Sage Configuration Ping	Logout Befres
cisco	Honitor <u>Wlang</u> Controller Wireless security hanagement commands help eeedback		🔒 Home
WLANs	WLANs > Edit 'CLUS-WLAN-Name'	< Back	Apply
VILANS	General Security QoS Policy-Mapping Advanced		
Advanced	Layer 2 Layer 3 AAA Servers		<u>^</u>
	Select AAA servers below to override use of default servers on this WLAN HADUIS Server RADUIS Servers RADUIS Servers RADUIS Servers RADUIS Server & Counting Servers RADUIS Server & Ince Server 1 Pr192.368.366.96, Port.182.2 None Server & Ince Server 4 Ince Server 4 Ince Server 4 Ince None None None None None None None Non		

WLAN 컨피그레이션에 있는 동안 "Advanced(고급)" 탭으로 이동하여 "Allow AAA Override(AAA 재 정의 허용)"를 활성화하고 "NAC State(NAC 상태)"를 "ISE NAC"로 변경합니다.

- alada				Sage Configuration Eing	Logout Befresh
cisco	MONITOR WLANS CONTROLLER W	IRELESS SECURITY MANAGEMENT COMMANDS	HELP FEEDBACK		🔒 Home
WLANs	WLANs > Edit 'CLUS-WLAN-Nam	ne"		< Back	Αρρίγ
VLANS	General Security QoS Po	licy-Mapping Advanced			
Advanced	Allow AAA Override Coverage Nole Detection Enable Session Timeout Aironet IE Diagnostic Channel III Override Interface ACL Lawez AL	Crabled Crabled Transol (secs) Crabled Crabled Crabled Ithv6 [Inne v IIvv6 [Inne v] Ithv6 [Inne v]	DHCP DHCP Server DHCP Addic Assignment CAP Split Tunnel Enabled		Î
	URL ACL P2 Biloding Action Client Evolusion ² Nacimum Allowed Clients ⁴ Static IP Tunneling ⁴⁴ Woh Direct Clients Piloy Maximum Allowed Clients Piloy Maximum Allowed Clients Park Padio Cliear HetSpot Configuration	None w Deabled B0 Timesut Value (secs) 0 Enabled Deabled 200 Deabled	Nanagement Frame Protection (HFP) NFP Client Protection # Optional V DTIM Period (in beacon intervals) 802.11a/n (1 - 255) [NAC State [155 NAC V Kad Datancing and Band Select		

마지막 것은 스스로 고정시키는 것입니다. 이렇게 하려면 WLANs 페이지로 돌아가 WLAN>모빌리 티 앵커 오른쪽의 파란색 상자 위에 마우스를 놓습니다. "Switch IP Address (Anchor)"를 로컬로 설 정하고 "Mobility Anchor Create(모빌리티 앵커 생성)" 버튼을 누릅니다. 그러면 우선순위 0이 고정 된 로컬에 표시됩니다.

տիտիտ cisco		MONITOR	WLAN	s <u>C</u> ONTF	Roller Wireles	s <u>s</u> ecurity	MANAGEMENT	C <u>o</u> mmands	HELP	<u>F</u> EEDBACK			
WLANs		WLANs											
VLANs		Current Filt	ler:	None	[Change F	ilter] [Clear Filte	r)				Create New	♥ Go	1
Advanced				e	Profile Name		WLAN SS	ID		Admin Status	Security Policies		
			WLA	AN	CLUS-WLAN-Name		CLUS-SSI)		Enabled	MAC Filtering		
													Mobility Anchors 802.110 Foreign Maps Service Advertisements Hotspot 2.0
WLANs	Mobility /	Anchors											< Back
VLANS WLANS	WLAN SSI	D CLUS-SSID											
Advanced	Switch IP	Address (Anchor)								Data Path	Control Path	Priority	
	local									up	up	0	
	Mobility J	Anchor Create											
	Switch IF	Address (Anch	lor)	192.168.160.	18 🗸								
	Priority I			3~									
	Foot Note	5											

AireOS WLC에서 ACL 리디렉션

이는 AireOS WLC에 필요한 최종 컨피그레이션입니다. 리디렉션 ACL을 생성하려면 Security>Access Control Lists>Access Control Lists>New로 이동합니다. ACL 이름을 입력하고 (AVP에서 전송된 것과 일치해야 함) "Apply(적용)"를 누릅니다.

ahaha		onfiguration Eng Logout Befresh
cisco	Monitor ylanis controller wijreless security management commands help eeedback	🔒 Home
Security	Access Control Lists > New	< Back Apply
General RADIUS	Access Control List Name CLUS-ACL	
Authentication Accounting Fallback DNS Downloaded AVP	ACLType BPv4 OIPv6	
TACACS+		

이제 방금 생성한 ACL의 이름을 클릭합니다. "Add New Rule" 버튼을 클릭합니다. 9800 컨트롤러 와 달리 AireOS WLC에서는 리디렉션되지 않고 ISE에 연결할 수 있는 트래픽에 대한 permit 문을 구성합니다. DHCP 및 DNS는 기본적으로 허용됩니다.

uluilu cisco	MONI	TOR M	LANs		w	IRELESS	SECURIT	Y M	ANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK		Sa <u>v</u> e Con	figuration]	jing Log	out <u>R</u> efresh <mark>A H</mark> ome
Security	Acce	ess Cor	trol Li	ists > Edit											< Back	Add N	ew Rule
AAA General RADIUS	Gene	eral															
Authentication Accounting	Access	s List Nam	e	CLUS-ACL					_								
Fallback DNS	Deny (Counters		5													
Downloaded AVP	Seq	Action	Sou	rce IP/Mask		Destina	tion IP/M	ask	Protocol	Source Por	t	Dest Port	DSCP	Direction	Number of	Hits	
LDAP Local Net Users	т	Permit	0.0.0).0).0	/	192.168	.160.99 .255.255	/	тср	Any		8443	Any	Any	273		
MAC Filtering Disabled Clients User Login Policies	2	Permit	192. 255.	168.160.99 255.255.255	/	0.0.0.0 0.0.0.0		/	тср	8443		Any	Any	Any	566		
AP Policies Password Policies																	
Local EAP																	
Advanced EAP																	
Priority Order																	
Certificate Access Control Lists Access Control Lists CPU Access Control																	

ISE 구성

CWA ISE . .

ISE , , ISE 9800(foreign) , .

Policy()>Policy Elements()>Authorization()>Results()>Authorization Profiles()>+Add() . "access_accept" AVP(attribute-value) . CWA ACL URL VLAN ID . ACL WLC ACL .

C A Not secure | 192.168.160.99/admin/#policy/policy_elements/policy_elements_permissions/policy_elements_permissions_authorization/policy_element

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture C	ient Provisioning Policy Elements
Dictionaries + Conditions - Resul	s
G	
Authentication	Authorization Profile
Authorization	* Name CLUC Auth2 Drofile ICE
Autionzation	
Authorization Profiles	
Downloadable ACLs	Access Type ACCESS_ACCEPT
▶ Profiling	Network Device Profile dista Cisco 💌 🕀
► Posture	Service Template
Client Provisioning	Track Movement
•	Passive Identity Tracking
	▼ Common Tasks
	Voice Domain Permission
	✓ Web Redirection (CWA, MDM, NSP, CPP) ①
	Centralized Web Auth ACL CLUS-ACL Value Self-Registered Guest Portal (c

CWA . , MAB , ID SSID . , . , . . . Policy() >Policy Sets() + . MAB "Process Host Lookup()" " " (>>>>). + .

-shulls Identity Services Engine Home + Context V	Visibility	inistration ► Work Centers License Warming 🔺	۹ ۴	o •
Policy Sets Profiling Posture Client Provisioning + Po	folicy Elements	Click here to do visibility setup Do not sho	ir this again.	×
Policy Sets		ResetAll Hitcounts	Reset	Save
+ Status Policy Set Name Descri	ription Conditions	Allowed Protocols / Server Sequence H	ts Action	s View
Search				
O CLUS-CWA-Policy-Set		+ Default Network Access * * +	٥	>
O Default Default	It policy set	Default Network Access * * *	•	>
			Reset	Save

MAB ISE . WLAN ID .

Conditions Studio		
Library	Editor	
mab ♥ ⊑ □ ▲ ⊕ 및 및 중 ◙ 遵 반 € € €	Wireless_MAB Set to 'Is not'	<i>()</i>
Wired_MAB ()		
Wireless_MAB ()	+ New AND OR	

. MAB "" ID .

Policy Sets Profiling Posture Client Provisioning + Policy Elements		Click here to do visibility setup Do not sho	w this again.	×
Policy Sets → CLUS-CWA-Policy-Set		ResetAll Hitcounts	Reset	Save
Status Policy Set Name Description	Conditions	Allowed Protocols / Serve	er Sequence	e Hits
Search				
CLUS-CWA-Policy-Set	Wireless_MAB	Default Network Access	** +	•
▲ Authentication Policy (2)				
+ Status Rule Name Conditions		Use	Hits	Actions
Vireless_MAB		Internal Endpoints		٥
⊘ Default		All_User_JD_Stores * Options	•	٥
Authorization Policy - Local Exceptions				
> Authorization Policy - Global Exceptions				
Authorization Policy (1)				

. ACL SSID ID WLAN .

Policy Sets → CLUS-CWA-Policy-Set

,

Policy	Sets +	CLUS-CWA-Policy-Set							ResetAll Hitcounts
	Status	Policy Set Name	Descrip	tion	Cond	titions			Allowed Protocols / Server S
Search									
	0	CLUS-CWA-Policy-Set				Wireless_MAB			Default Network Access
> Aut	hentication	n Policy (2)							
> Aut	horization	Policy - Local Exceptions							
> Aut	horization	Policy - Global Exceptions							
∀ Aut	horization	Policy (4)							
٠	Status	Rule Name	Condi	tions			Results Profiles	Security G	Groups
Sear	ch								
	Ø	Post-CWA	AND	Le Network Acces Image: Called - Ca	UseCa	se EQUALS Guest Flow D ENDS_WITH CLUS-SSID	CLUS-Post-Auth +	Select fro	m list 💌 🕇
	Ø	MAB on WLAN	AND	Radius-Called-	tation-II	D ENDS_WITH CLUS-SSID	CLUS-AuthZ-Profile-ISE	Select fro	m list 🔹 🕈
	Ø	Flex AuthZ	₽	Radius Called-Station-ID	ENDS,	WITH FLEX-CWA	CLUS-Flex_CWA	Select fro	m list 🔹 🕇
	0	Default					* DenyAccess	Select fro	m list 🔹 🕇

ISE 9800(foreign) ISE . Admin()>Network Resources()>Network Device()>+. IP() RADIUS . ISE 9800 . . .

System Identity Management Network Devices Network Device Grou	Network Resources + Device					
Network Devices Network Device Grou		Portal Management pxG	id Services Feed Servi	ce F Threat Centric N	IAC	
	ups Network Device Profiles	External RADIUS Servers	RADIUS Server Sequen	ces NAC Managers	External MDM	Location Services
Network Devices Default Device Device Security Settings	Vetwork Device Profiles Network Devices List > JAysNe Network Devices IP Address * D Soft * Network Device Group Location All Location IPSEC No Device Type All Device T RADIUS Authenticatic RADIUS UDP Settin RADIUS DTLS Setti		ADJUS Server Sequen ADJUS Server Sequen ADJUS Protocol RADIUS ed Secret CoA Port 1700	24	Default	Location Services

. Admin()>Identity Management(ID)>Identity(ID)>Users()>+Add() submit() . ISE ,

.

cisco	Identity Ser	vices Engine	Home	Context Visibility	Operations	Policy	✓ Administra	ation > We	ork Centers	
► Sy	stem 🔽 Iden	tity Management	▶ Network I	Resources • Devi	ce Portal Management	pxGrid S	Services F	eed Service	Threat Centric NAC	
▼ Ide	ntities Grou	ps External Ide	ntity Sources	Identity Source Se	quences F Settings	5				
Cisco ► Sy: ↓ Ide Users Latest	Manual Networ	tity Management ps External Ide k Scan Results	Home Network Networ		Operations Coperations Coperations Coperations Settings New Network Access r r r r coperation cope	Policy pxGrid S User User	Re-Enter Passion	word	ork Centers Threat Centric NAC Generate Pas Generate Pas Generate Pas	sword () sword ()
			v U	ser Groups elect an item nit Cancel	0-					

AireOS WLC가 외부, Catalyst 9800이 앵커인 경우 구성의 차이점

AireOs WLC를 외부 컨트롤러로 지정하려면 컨피그레이션은 두 가지 차이만 있는 이전과 동일합니 다.

- 1. AAA 어카운팅은 앵커에서 수행되지 않으므로 9800에는 어카운팅 방법 목록이 없고 AireOS WLC는 어카운팅이 활성화되고 ISE를 가리키도록 합니다.
- 2. AireOS는 그 자체가 아닌 9800에 고정되어야 합니다. Policy Profile(정책 프로파일)에서 9800에는 앵커가 선택되지 않았지만 "Export Anchor(앵커 내보내기)" 상자가 선택되어 있습니 다.
- 3. AireOS WLC가 클라이언트를 9800으로 내보낼 때 정책 프로파일의 개념이 없으면 WLAN 프 로파일 이름만 보냅니다. 따라서 9800은 AireOS에서 전송된 WLAN 프로파일 이름을 WLAN 프로파일 이름 및 정책 프로파일 이름 모두에 적용합니다. AireOS WLC에서 9800 WLC로 고 정할 경우 두 WLC의 WLAN 프로파일 이름과 9800의 정책 프로파일 이름이 모두 일치해야 한 다는 것입니다.

다음을 확인합니다.

문제 해결은 클라이언트가 중지하는 프로세스의 어느 지점에 따라 다르게 나타납니다. 예를 들어 WLC가 MAB에서 ISE로부터 응답을 받지 못하면 클라이언트는 "Policy Manager State:(정책 관리 자 상태:): "연결 중"을 선택하고 앵커로 내보내지 않습니다. 이 경우 외부 문제 해결만 수행하며 WLC와 ISE 간의 트래픽에 대한 RA 추적 및 패킷 캡처를 수집할 수 있습니다. 또 다른 예는 MAB가 성공적으로 통과되었지만 클라이언트가 리디렉션을 수신하지 못한다는 것입니다. 이 경우 외주가 AVP에서 리디렉션을 수신하여 클라이언트에 적용했는지 확인해야 합니다. 또한 클라이언트가 올

문제 해결

Show mobility summary

• 모빌리티가 외부와 일치하는지 확인

Show acl detailed <acl name>

• ACL

Show WLAN <wlan id>

• WLAN

Show radius summary 참고: RFC3576은 CoA 컨피그레이션입니다.

• AAA

Show wireless mobility summary AireOS WLC의 컨피그레이션을 확인하려면 명령을 실행합니다.

Show IP access-list <ACL name> • 앵커와 함께 모빌리티가 작동되는지 확인

ACL

Show wireless tag policy detailed <policy tag name>

• 정책 태그

Show wireless profile policy detailed <profile name>

• 정책 프로파일

Show wlan id <wlan id>

• WLAN

Show Run | section aaa|radius

• AAA

9800 WLC에서 컨피그레이션을 확인하려면 명령을 실행합니다.

바른 ACL을 사용하여 있는지 확인하려면 앵커를 확인해야 합니다. 이 트러블슈팅 범위는 이 기술 문서의 설계 외부에 있습니다(일반 클라이언트 트러블슈팅 지침에 대한 참조 확인).

9800 WLC의 CWA 문제 해결에 대한 자세한 내용은 Cisco Live! 프레젠테이션 DGTL-TSCENT-404

Catalyst 9800 문제 해결 정보

클라이언트 세부 정보

show wireless client mac-address

여기서는 "Policy Manager State(정책 관리자 상태)", "Session Manager(세션 관리자)>Auth Method(인증 방법)", "Mobility Role(모빌리티 역할)"을 확인해야 합니다.

Monitoring(모니터링)>Clients(클라이언트) 아래의 GUI에서 이 정보를 찾을 수도 있습니다

임베디드 패킷 캡처

CLI에서 명령은 capture <capture name>#monitor을 시작한 다음 옵션이 나타납니다.

GUI에서 Troubleshoot(문제 해결)>Packet Capture(패킷 캡처)>+Add(추가)로 이동합니다.

RadioActive 추적

CLI에서

debug wireless mac/ip

이 명령을 중지하려면 이 명령의 no 형식을 사용합니다. 이 파일은 "ra_trace"라는 bootflash에서 클 라이언트의 MAC 또는 IP 주소와 날짜 및 시간에 기록됩니다.

GUI에서 Troubleshoot(문제 해결)>Radial Trace(방사능 추적)>+Add(추가)로 이동합니다. 클라이언 트의 mac 또는 ip 주소를 추가하고 Apply를 누른 다음 start를 누릅니다. 프로세스를 몇 번 거친 후 추적을 중지하고 로그를 생성한 다음 디바이스에 다운로드합니다.

AireOS 문제 해결 정보

클라이언트 세부 정보

CLI show client details <client mac>에서

GUI Monitor(GUI 모니터)>Clients(클라이언트)에서

CLI에서 디버깅

Debug client

Debug mobility handoff

Debug mobility config



<u>9800 컨트롤러를 사용하여 모빌리티 터널 구축</u>

<u>9800의 무선 디버깅 및 로그 수집</u>