9800 WLC 및 Aruba ClearPass 구성 - 게스트 액 세스 및 FlexConnect

목차

<u>소</u>개 사전 요구 사항 요구 사항 사용되는 구성 요소 배경 정보 <u>CWA 게스트 엔터프라이즈 구축을 위한 트래픽 흐름</u> 네트워크 다이어그램 구성 게스트 무선 액세스 C9800 매개변수 구성 C9800 - 게스트용 AAA 컨피그레이션 C9800 - 리디렉션 ACL 구성 C9800 - 게스트 WLAN 프로파일 컨피그레이션 C9800 - 게스트 정책 프로필 정의 C9800 - 정책 태그 <u>C9800 - AP 가입 프로필</u> C9800 - Flex 프로필 C9800 - 사이트 태그 C9800 - RF 프로파일 C9800 - AP에 태그 할당 Aruba CPPM 인스턴스 구성 Aruba ClearPass 서버 초기 컨피그레이션 라이센스 신청 서버 호스트 이름 CPPM 웹 서버 인증서(HTTPS) 생성 C9800 WLC를 네트워크 디바이스로 정의 게스트 포털 페이지 및 CoA 타이머 ClearPass - 게스트 CWA 컨피그레이션 ClearPass 끝점 메타데이터 특성: 게스트 인터넷 허용 ClearPass 시행 정책 구성 재인증 ClearPass 게스트 포털 리디렉션 적용 프로파일 컨피그레이션 ClearPass 메타데이터 적용 프로필 컨피그레이션 ClearPass 게스트 인터넷 액세스 적용 정책 컨피그레이션 ClearPass 게스트 사후 AUP 시행 정책 컨피그레이션 ClearPass MAB 인증 서비스 컨피그레이션 ClearPass Webauth 서비스 컨피그레이션 <u>ClearPass</u> - 웹 로그인 확인 - 게스트 CWA 권한 부여 부록

소개

이 문서에서는 Catalyst 9800 WLC(Wireless LAN Controller)와 Aruba ClearPass의 통합을 통해 AP(Access Point) 구축의 Flexconnect 모드에서 CWA(Central Web Authentication)를 활용하는 게 스트 SSID(Wireless Service Set Identifier)를 무선 클라이언트에 제공하는 방법을 설명합니다.

게스트 무선 인증은 게스트 포털에서 AUP(Anonymous Acceptable User Policy) 페이지를 통해 지 원되며, DMZ(secure demilitarized zone) 세그먼트의 Aruba Clearpass에서 호스팅됩니다.

사전 요구 사항

이 설명서에서는 다음 구성 요소가 구성되고 확인되었다고 가정합니다.

- 모든 관련 구성 요소가 NTP(Network Time Protocol)에 동기화되고 올바른 시간이 있는지 확인 됨(인증서 검증에 필요)
- 운영 DNS 서버(게스트 트래픽 흐름, CRL(Certificate Revocation List) 검증에 필요)
- 운영 DHCP 서버
- 선택적 CA(Certificate Authority)(CPPM 호스팅 게스트 포털에 서명하는 데 필요)
- Catalyst 9800 WLC
- Aruba ClearPass Server(플랫폼 라이센스, 액세스 라이센스, 온보드 라이센스 필요)
- Vmware ESXi

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- C9800 구축 및 새로운 구성 모델
- C9800의 Flexconnect 스위칭
- 9800 CWA 인증(https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-serieswireless-controllers/213920-central-web-authentication-cwa-on-cata.html 참조)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 17.3.4c를 실행하는 Cisco Catalyst C9800-L-C
- Cisco Catalyst C9130AX
- Aruba ClearPass, 6-8-0-109592 및 6.8-3 패치
- MS Windows 서버 Active Directory(관리되는 엔드포인트에 대한 자동화된 머신 기반 인증서 발 급을 위해 구성된 GP)DHCP 서버(옵션 43 및 옵션 60)DNS 서버모든 구성 요소를 시간 동기화 하기 위한 NTP 서버CA

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

배경 정보

이 다이어그램은 게스트 사용자가 네트워크에서 허용되기 전에 게스트 Wifi 액세스 교환의 세부 정 보를 전달합니다.

1. 게스트 사용자가 원격 사무실에서 게스트 Wifi와 연결합니다.

2. 초기 RADIUS Access-Request가 C9800에 의해 RADIUS 서버로 프록시됩니다.

3. 서버가 로컬 MAC 엔드포인트 데이터베이스에서 제공된 게스트 MAC 주소를 찾습니다. MAC 주소가 없는 경우 서버는 MAB(MAC Authentication Bypass) 프로필로 응답합니다. 이 RADIUS 응답에는 다음이 포함됩니다.

- URL 리디렉션 ACL(Access Control List)
- URL 리디렉션
- 4. 클라이언트는 IP 주소가 할당된 IP Learn 프로세스를 거칩니다.

5. C9800은 게스트 클라이언트(MAC 주소로 식별됨)를 '웹 인증 보류 중' 상태로 전환합니다.

6. 게스트 WLAN과 연결된 대부분의 최신 디바이스 OS는 일종의 종속 포털 탐지를 수행합니다. 정확한 탐지 메커니즘은 특정 OS 구현에 따라 달라집니다. 클라이언트 OS는 RADIUS Access-Accept 응답의 일부로 제공된 RADIUS 서버가 호스팅하는 게스트 포털 URL로 C9800에 의해 리디 렉션된 페이지가 포함된 팝업(의사 브라우저) 대화 상자를 엽니다.

7. 게스트 사용자는 제시된 팝업 ClearPass의 약관에 동의하고 클라이언트가 인증을 완료했음을 나 타내기 위해 엔드포인트 데이터베이스(DB)의 클라이언트 MAC 주소에 대한 플래그를 설정하며 라 우팅 테이블에 따라 인터페이스를 선택하여 RADIUS CoA(Change of Authorization)를 시작합니다 (ClearPass에 여러 인터페이스가 있는 경우).

8. WLC는 게스트 클라이언트를 '실행' 상태로 전환하며 사용자는 더 이상 리디렉션 없이 인터넷에 액세스할 수 있습니다.

참고: Cisco 9800 Foreign, Anchor Wireless Controller state flow diagram with RADIUS and externally hosted Guest Portal의 경우 이 문서의 부록 섹션을 참조하십시오.

		Guest CWA flow	
CI	ent W		Radius
	[Client Association] [1] Assoc Request [uist Client John		
	[4] Assoc Response	(MAB procedure) [J] Access Request (Session/D-1/LELEG/000000/F/FF76609) [J] Access Request (Session/D-1/LELEG/000000/F/FF76609) [J] Access Request (Session/D-1/LELEG/000000/F/FF766096.portal-1945/780- [MAB complet] [MAB complet]	and
		(IP learn precedure)	
alt	[webauth procedures]		
	10 Laters Get Ministria - Celan Sector - Celan Sect	Controller send HTTP TCP STN ACK and redirects client to Guest Portual URL on CPPR	
		(7) (HTPHTTS session started to Guest Portal Server) (Guest Portal Server sends HTTPHTTPS TCP SYN Ack and displays internal login page) (III Bildedicet to meet social	-
[9	User enters credential and/or clicks on Accept AU	ob. credential HTTP5 pogt (username.password)	
		(11) Validates Cre Mark client as automoticateds	dential
	•	[CoA procedures] [12] CoA Regest (Resultmenticate, Session(D=11111E02000000)#/9876669) [13] CoA Act (Session(D=11111E02000000)#/9876669) [13] CoA Act (Session(D=1111E02000000)#/9876669) [14] Access Request (Session(D=111E102000000)#/9876669) [15] Access Accest (No reflect URL, Session(D=111E102000000)#/9876669) [16] AndrinaLogot Page [16] LandmaLogot Page [16] LandmaLogot Page [16] LendmaLogot Page [16] LandmaLogot Page	
с	ent V	nre	Radius

CWA(Guest Central Web Authentication) 상태 다이어그램

CWA 게스트 엔터프라이즈 구축을 위한 트래픽 흐름

여러 지사를 사용하는 일반적인 엔터프라이즈 구축에서 각 지사는 게스트가 EULA에 동의하면 게 스트 포털을 통해 안전하고 세분화된 액세스를 제공하도록 설정됩니다.

이 컨피그레이션 예에서는 9800 CWA가 네트워크의 보안 DMZ에서 게스트 사용자를 위해 배타적 으로 구축된 별도의 ClearPass 인스턴스에 대한 통합을 통해 게스트 액세스에 사용됩니다.

게스트는 DMZ ClearPass 서버에서 제공하는 웹 동의 팝업 포털에 명시된 약관에 동의해야 합니다. 이 컨피그레이션 예에서는 익명 게스트 액세스 방법(즉, 게스트 포털을 인증하는 데 게스트 사용자 이름/비밀번호가 필요하지 않음)에 중점을 둡니다.

이 구축에 해당하는 트래픽 흐름이 이미지에 표시됩니다.

1. RADIUS - MAB 단계

2. 게스트 클라이언트 URL이 게스트 포털로 리디렉션

3. 게스트 포털에서 EULA의 게스트 승인 후 RADIUS CoA 재인증이 CPPM에서 9800 WLC로 발행 됩니다.

4. 게스트는 인터넷에 액세스할 수 있습니다.



네트워크 다이어그램

참고: 실습 데모에서는 단일/통합 Aruba CPPM 서버 인스턴스를 사용하여 게스트 및 기업 SSID NAS(Network Access Server) 기능을 모두 제공합니다. 모범 사례 구현에서는 독립적인 NAS 인스턴스를 제안합니다.



구성

이 컨피그레이션 예에서는 C9800의 새 컨피그레이션 모델을 활용하여 엔터프라이즈 브랜치에 dot1x Corporate Access 및 CWA 게스트 액세스를 제공하는 데 필요한 프로필 및 태그를 생성합니 다. 결과 컨피그레이션이 이 이미지에 요약되어 있습니다.

	Policy Tag: PT_CAN01	WLAN Profile: WP_Guest SSID: Guest Layer 2: Security None Layer 2: MAC Filtering Enabled Authz List: AAA_Authz-CPPM	Policy Profile: PP_Guest Central Switching: Disabled Central Auth: Enabled Central DHCP: Disabled Vlan: guest (21) AAA Policy: Allow AAA Override Enabled AAA Policy: NAC State Enabled AAA Policy: NAC Type RADIUS AAA Policy Accounting List: Guest_Accounting
AP MAC: X000CX000CX000X	Site Tag: ST_CAN01 Enable Local Site: Off		AP Join Profile: MyApProfile NTP Server: 10.0.10.4 Flex Profile: FP_CAN01 Native Vlan 2 Policy ACL: CAPTIVE_PORTAL_REDIRECT, ACL CWA: Enabled VLAN: 21 (Guest)
			5GHz Band RF: Typical_Client_Density_rf_5gh
	RF Tag: Branch_RF		2GHz Band RF: Typical_Client_Density_rf_2gh

게스트 무선 액세스 C9800 매개변수 구성

C9800 - 게스트용 AAA 컨피그레이션

참고: Cisco 버그 ID <u>CSCvh03827에</u> 대해, 메커니즘이 ClearPass RADIUS 교환을 위해 WLC의 SessionID 지속성을 사용하므로 정의된 AAA(Authentication, Authorization, and Accounting) 서버가 로드 밸런싱되지 않는지 확인합니다.

1단계. 9800 WLC 컨피그레이션에 Aruba ClearPass DMZ 서버를 추가하고 인증 방법 목록을 생성 합니다. Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > RADIUS > Servers(서버) > +Add(추가)로 이동하고 RADIUS 서버 정보를 입력합니다.

Create AAA Radius Server		*
Name*	СРРМ	
Server Address*	10.85.54.98	
PAC Key		
Кеу Туре	Clear Text 🔹	
Key* (i)		
Confirm Key*		
Auth Port	1812	
Acct Port	1813	
Server Timeout (seconds)	5	
Retry Count	3	
Support for CoA	ENABLED	
Cancel		Apply to Device

2단계. 게스트에 대한 AAA 서버 그룹을 정의하고 1단계에서 구성한 서버를 이 서버 그룹에 할당합 니다. Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > RADIUS > Groups(그룹) > +Add(추가)로 이동합니다.

Create AAA Radius Serve	r Group	>
Name*	AAA_Radius_CPPM	
Group Type	RADIUS	
MAC-Delimiter	none	
MAC-Filtering	none 🔹	
Dead-Time (mins)	5	
Source Interface VLAN ID	1	
Available Servers	Assigned Servers	
	> CPPM <	
Cancel	Apply to Device	

3단계. 게스트 액세스를 위한 권한 부여 방법 목록을 정의하고 2단계에서 생성한 서버 그룹을 매핑 합니다. Configuration > Security > AAA > AAA Method List > Authorization > +Add로 이동합니다. Type Network(네트워크 유형)를 선택한 다음 2단계에서 구성한 AAA Server Group(AAA 서버 그룹)을 선택합니다.

Quick Setup: AAA Authoriza	ation	×
Method List Name*	AAA_Authz_CPPM	
Type*	network 🔹	
Group Type	group 🔹	
Fallback to local		
Authenticated		
Available Server Groups	Assigned Server Groups	
radius Idap tacacs+	AAA_Radius_CPPM <	
Cancel		Apply to Device

4단계. 게스트 액세스를 위한 계정 관리 방법 목록을 생성하고 2단계에서 생성한 서버 그룹을 매핑 합니다. Configuration > Security > AAA > AAA Method List > Accounting > +Add로 이동합니다. 드 롭다운 메뉴에서 Type Identity(유형 ID)를 선택한 다음 2단계에서 구성한 AAA Server Group(AAA 서버 그룹)을 선택합니다.

Quick Setup: AAA Accounting	ng		×
Method List Name* Type*	AAA_Accounting_CPPN	A (i)	
Available Server Groups	Assigned S	erver Groups	
radius Idap tacacs+	> AA <	A_Radius_CPPM	
Cancel			Apply to Device

리디렉션 ACL은 게스트 포털로 리디렉션해야 하는 트래픽과 리디렉션 없이 통과해야 하는 트래픽 을 정의합니다. 여기서 ACL 거부는 우회 리디렉션 또는 통과(pass through)를 의미하며 permit은 포 털로의 리디렉션을 의미합니다. 각 트래픽 클래스에 대해 ACE(Access Control Entries)를 생성하고 인그레스 및 이그레스 트래픽에 모두 일치하는 ACE를 생성할 때 트래픽 방향을 고려해야 합니다.

Configuration(컨피그레이션) > Security(보안) > ACL로 이동하고 CAPTIVE_PORTAL_REDIRECT라는 새 ACL을 정의합니다. 다음 ACE로 ACL을 구성합니다.

- ACE1: 양방향 ICMP(Internet Control Message Protocol) 트래픽이 리디렉션을 우회하도록 허용하며 주로 연결 가능성을 확인하는 데 사용됩니다.
- ACE10, ACE30: DNS 서버 10.0.10.4로 양방향 DNS 트래픽 흐름을 허용하고 포털로 리디렉션 하지 않습니다. 게스트 플로우를 트리거하려면 DNS 조회 및 응답에 대한 가로채기가 필요합니 다.
- ACE70, ACE80, ACE110, ACE120: 사용자가 포털과 함께 표시되도록 게스트 종속 포털에 대 한 HTTP 및 HTTPS 액세스를 허용합니다.
- ACE150: 모든 HTTP 트래픽(UDP 포트 80)이 리디렉션됩니다.

Sequence 🗸	Action ~	Source v IP	Source v Wildcard	Destination ~ IP	Destination ~ Wildcard	Protocol 🖂	Source v Port	Destination v Port
1	deny	any		a)ey		icmp		
10	deny	any		10.0.10.4		udp		eq domain
30	deny	10.0.10.4		any		udp	eq domain	
70	deny	any		10.85.54.98		tcp		eq 443
80	deny	10.85.54.98		any		tcp	eq 443	
110	deny	any		10.85.54.98		tcp		eq www
120	deny	10.85.54.98		any		tcp	eq www	
150	permit	any		any		tcp		eq www

C9800 - 게스트 WLAN 프로파일 컨피그레이션

1단계. Configuration(구성) > Tags & Profiles(태그 및 프로필) > Wireless(무선) > +Add(추가)로 이 **동합니다**. 게스트 클라이언트가 연결하는 SSID 'Guest'의 브로드캐스트와 함께 새 SSID 프로필 WP_Guest를 생성합니다.

Add	WLAN				×
Ge	eneral Security	Advanced			
	Profile Name*	WP_Guest	Radio Policy	All	
	SSID*	Guest	Broadcast SSID		
	WLAN ID*	3			
	Status				

Cancel	Apply to Device

동일한 Add WLAN(WLAN 추가) 대화 상자에서 Security(보안) > Layer 2(레이어 2) 탭으로 이동합 니다.

- 레이어 2 보안 모드: 없음

- MAC 필터링: 사용

- 권한 부여 목록: 드롭다운 메뉴의 AAA_Authz_CPPM(3단계에서 AAA 컨피그레이션의 일부로 구성)

А	dd WLAN					×
	General	Security	Advanced			
	Layer2	Layer3	AAA			
	Layer 2 Sec MAC Filterin OWE Transi	urity Mode ng tion Mode		None 🔹	Lobby Admin Access Fast Transition Over the DS Reassociation Timeout	Adaptive Enab 🔹
	Transition M Authorizatio	lode WLAN n List*	ID*	1-4096		
	Cancel]				Apply to Device

C9800 - 게스트 정책 프로필 정의

C9800 WLC GUI에서 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정 책) > +Add(추가)로 이동합니다.

이름: PP_게스트

상태: 사용

- 중앙 스위칭: 비활성화됨
- 중앙 인증: 사용
- 중앙 DHCP: 비활성화됨

중앙 연결: 비활성화됨



Cancel

Apply to Device

Add Policy Pr	rofile						×
		ng in enabled state wil	I result in loss o	of conr	nectivity for clients associated with t	his profile.	
General A	access Policies	QOS and AVC	Mobility	Ad	vanced		
Name*		PP_Guest			WLAN Switching Policy		
Description	I.	Profile for Branch	Guest		Central Switching	DISABLED	
Status		DISABLED			Central Authentication		
Passive Clie	ent	DISABLED			Central DHCP	DISABLED	
Encrypted 7	Traffic Analytics	DISABLED			Central Association	DISABLED	
CTS Polic	:y				Flex NAT/PAT	DISABLED	
Inline Taggi	ing						
SGACL Enfo	orcement						
Default SG	Г	2-65519					
Cancel						Apply to Devi	ice

동일한 Add Policy **Profile(정책 프로필 추가**) 대화 상자에서 Access **Policies(액세스 정책) 탭**으로 이동합니다.

- RADIUS 프로파일링: 사용

- VLAN/VLAN 그룹: 210(즉, VLAN 210은 각 브랜치 위치의 게스트 로컬 VLAN)

참고: Flex용 게스트 VLAN은 VLAN/VLAN 그룹 유형 VLAN 번호의 VLAN에 있는 9800 WLC에서 정의하지 않아도 됩니다.

알려진 결함: Cisco 버그 ID <u>CSCvn48234</u>는 동일한 Flex 게스트 VLAN이 WLC 및 Flex 프로필에 정 의된 경우 SSID가 브로드캐스트되지 않습니다.

A Configur	ng in enabled state will result in loss of connect	ctivity for clients associated with this profile.
neral Access Policies	QOS and AVC Mobility Adva	nced
RADIUS Profiling		WLAN ACL
TTP TLV Caching		IPv4 ACL Search or Select
HCP TLV Caching		IPv6 ACL Search or Select 🗸
VLAN Local Profiling		URL Filters
lobal State of Device lassification	(i)	Pre Auth Search or Select 🔹
ocal Subscriber Policy Name	Search or Select 🚽	Post Auth Search or Select 🗸
'LAN		
LAN/VLAN Group	210	
/ulticast VLAN	Enter Multicast VLAN	



동일한 Add Policy Profile(정책 프로필 추가) 대화 상자에서 Advanced(고급) 탭으로 이동합니다.

- AAA 재정의 허용: 사용

- NAC 상태: 사용

- NAC 유형: RADIUS

- 회계 목록: AAA_Accounting_CPPM(AAA 컨피그레이션의 일부로 4단계에서 정의됨)

Add Policy Profile

▲ Config	uring in enabled state wil	I result in loss	of connectivity for clients associated with this profile.
General Access Policies	QOS and AVC	Mobility	Advanced
WLAN Timeout			Fabric Profile Search or Select
Session Timeout (sec)	1800		mDNS Service Search or Select
Idle Timeout (sec)	300		Hotspot Server Search or Select 🔻
Idle Threshold (bytes)	0		User Defined (Private) Network
Client Exclusion Timeout (sec)	60		Status
Guest LAN Session Timeout			Drop Unicast
DHCP	_		Umbrella
IPv4 DHCP Required DHCP Server IP Address			Umbrella Parameter Map
how 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	× v	Air Time Fairness Policies
Accounting List	AAA_Accounting_(• • ×	2.4 GHz Policy Search or Select

참고: C9800 WLC에서 RADIUS CoA 메시지를 수락하려면 'NAC(Network Admission Control) State - Enable'이 필요합니다.

C9800 - 정책 태그

C9800 GUI에서 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Tags(태그) > Policy(정책) > +Add(추가)로 이동합니다.

-이름: PT_CAN01

-설명: CAN01 지사 사이트용 정책 태그

동일한 대화 상자에서 Add Policy Tag(정책 태그 추가)의 WLAN-POLICY MAPS(WLAN-POLICY 맵)에서 +Add(추가)를 클릭하고 이전에 생성한 WLAN 프로필을 Policy Profile(정책 프로필)에 매핑합

×

니다.

- WLAN 프로파일: WP_게스트

- 정책 프로필: PP_게스트

Add Policy Tag			×
Name*	PT_CAN01		
Description	Policy Tag for CAN01		
WLAN-POLICY + Add × Dele	Maps: 0		
WLAN Profile		V Policy Profile	v.
⊲ ⊲ 0 ⊳ ⊳	10 🔹 items per page		No items to display
Map WLAN and Pol	icy		
WLAN Profile*	WP_Guest	Policy Profile*	PP_Guest
RLAN-POLICY	Maps: 0		
Cancel			Apply to Device

C9800 - AP 가입 프로필

C9800 WLC GUI에서 Configuration(컨피그레이션) > Tags & Profiles(**태그 및 프로필) > AP** Join(AP 조인) > +Add(추가)로 이동합니다.

-이름: 브랜치_AP_프로파일

- NTP 서버: 10.0.10.4(실습 토폴로지 다이어그램 참조). 브랜치의 AP가 동기화를 위해 사용하는 NTP 서버입니다.

Add AP Jo	oin Profile								×
General	Client	CAPWAP	AP	Management	Sec	urity	ICap	QoS	
Name*		Branch	_AP_Prof	île		Office	Extend A	P Configuratio	n
Descrip	otion	Branch	AP Join	Profile		Local	Access	~	
LED Sta	ate	\checkmark				Link Er	ncryption		
LAG M	ode					Rogue	Detection		
NTP Se	erver	10.0.1	0.4						
GAS AI	P Rate Limit								
Apphos	st								
Cancel									Apply to Device

C9800 - Flex 프로필

프로파일과 태그는 모듈식이며 여러 사이트에 재사용할 수 있습니다.

FlexConnect 구축의 경우 모든 브랜치 사이트에서 동일한 VLAN ID가 사용되는 경우 동일한 Flex 프로파일을 다시 사용할 수 있습니다.

1단계. C9800 WLC GUI에서 Configuration(컨피그레이션) > Tags & Profiles(**태그 및 프로필) >** Flex > +Add(추가)로 이동합니다.

-이름: FP_분기

- 네이티브 VLAN ID: 10(AP 관리 인터페이스를 사용하려는 기본이 아닌 네이티브 VLAN이 있는 경 우에만 필요)

Add Flex Profile				×
General Local Authentica	ation Policy ACL VLAN	N Umbrella		
Name*	FP_Branch	Fallback Radio Shut		
Description	Branch Flex Profile	Flex Resilient		
Native VLAN ID	10	ARP Caching		
HTTP Proxy Port	0	Efficient Image Upgrade		
HTTP-Proxy IP Address	0.0.0.0	OfficeExtend AP		
CTS Policy		Join Minimum Latency		
Inline Tagging		IP Overlap		
SGACL Enforcement		mDNS Flex Profile	Search or Select	
CTS Profile Name	default-sxp-profile x			
Cancel				Apply to Device

동일한 Add Flex Profile(Flex 프로필 추가) 대화 상자에서 Policy ACL(정책 ACL) 탭으로 이동하여 +Add(추가)를 클릭합니다.

- ACL 이름: CAPTIVE_PORTAL_REDIRECT
- 중앙 웹 인증: 사용

Flexconnect 구축에서는 리디렉션이 C9800이 아닌 AP에서 발생하므로 각 관리되는 AP가 리디렉 션 ACL을 로컬로 다운로드해야 합니다.

Add Flex Pr	rofile			×
General	Local Authentication	Policy ACL VLAN Umbrella		
+ Add	× Delete			
ACL Name	e 🗸	Central Web Auth v Filter	ACL Name* CAPTIVE_PORTAL_F	
	0 ▶ ► 10 ¥ ite	ms per page No items to display	Central Web Auth	
			Pre Auth URL Filter Search or Select	
			Save Cancel	
Cancel]			Apply to Device

동일한 Add **Flex Profile(Flex 프로필 추가**) 대화 상자에서 VLAN **탭**으로 이동하여 **+Add**(추가)를 클 릭합니다(랩 토폴로지 다이어그램 참조).

- VLAN 이름: 게스트

- VLAN ID: 210

Add Flex Profile	×
General Local Authentication Policy ACL VLAN Umbrella	
+ Add × Delete	
VLAN Name v ID v ACL Name v	
ULAN Name* guest	
I I ► I I ► II • Items per page VLAN Id* 210	
1 - 1 of 1 items ACL Name Select ACL	
✓ Save つ Cancel	
	_
"Cancel	evice

C9800 - 사이트 태그

9800 WLC GUI에서 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Tags(태그) > Site(사이트) > Add(추가)로 이동합니다.

참고: 설명된 대로 2개의 무선 SSID를 지원해야 하는 각 원격 사이트에 대해 고유한 사이트 태 그를 생성합니다.

지리적 위치, 사이트 태그 및 Flex Profile 컨피그레이션 간에는 1-1 매핑이 있습니다.

Flex Connect 사이트에는 연결된 Flex Connect 프로파일이 있어야 합니다. 각 Flex Connect 사이트에 대해 최대 100개의 액세스 포인트를 가질 수 있습니다.

-이름: ST_CAN01

- AP 가입 프로필: 브랜치_AP_프로파일

- Flex 프로필: FP_분기

- 로컬 사이트 사용: 비활성화됨

Add Site Tag		×
Name*	ST_CAN01	
Description	Site Tag for Branch CA	
AP Join Profile	Branch_AP_Profile	
Flex Profile	FP_Branch	
Fabric Control Plane Name	•	
Enable Local Site		
Cancel		Apply to Device

C9800 - RF 프로파일

9800 WLC GUI에서 Configuration(컨피그레이션) > Tags & Profiles(**태그 및 프로파일) > Tags(태그**) > RF > Add(추가)로 이동합니다.

-이름: 지사 RF

- 5GHz 대역 RF(Radio Frequency) 프로파일: Typical_Client_Density_5gh(시스템 정의 옵션)

- 2.4GHz 대역 RF 프로파일: Typical_Client_Density_2gh(시스템 정의 옵션)

Add RF Tag		×
Name*	Branch_RF	
Description	Typical Branch RF	
5 GHz Band RF Profile	Client_Density_rf_5gh	
2.4 GHz Band RF Profile	Typical_Client_Densi	
Cancel		Apply to Device

C9800 - AP에 태그 할당

정의된 태그를 구축의 개별 AP에 할당하는 데 사용할 수 있는 두 가지 옵션이 있습니다.

- AP Name(AP 이름) 필드의 패턴과 일치하는 regex 규칙을 활용하는 AP 이름 기반 할당 (Configure(구성) > Tags & Profiles(태그 및 프로필) > Tags(태그) > AP > Filter(필터))

- AP 이더넷 MAC 주소 기반 할당(Configure(구성) > Tags & Profiles(태그 및 프로파일) > Tags(태 그) > AP > Static(고정))

DNA Center를 사용하는 프로덕션 구축에서는 DNAC 및 AP PNP 워크플로를 사용하거나 수동 AP당 할당을 방지하기 위해 9800에서 사용 가능한 정적 대량 CSV(Comma-Separated Values) 업 로드 방법을 사용하는 것이 좋습니다. Configure(**구성) > Tags & Profiles(태그 및 프로필) > Tags(태 그) > AP > Static(정적) > Add**(추가)로 이동합니다(**Upload File(파일 업로드**) 옵션 참고).

- AP MAC 주소: <AP_ETHERNET_MAC>

- 정책 태그 이름: PT_CAN01

- 사이트 태그 이름: ST_CAN01

- RF 태그 이름: 지사 RF

참고: Cisco IOS®-XE 17.3.4c부터 컨트롤러당 최대 1,000개의 regex 규칙이 적용됩니다. 구 축의 사이트 수가 이 수를 초과하면 MAC당 고정 할당을 활용해야 합니다.

Associate Tags to	AP	
AP MAC Address*	aaaa.bbbb.cccc	
Policy Tag Name	PT_CAN01	•
Site Tag Name	ST_CAN01	•
RF Tag Name	Branch_RF	•
Cancel		

참고: 또는 AP 이름 regex 기반 태그 할당 방법을 활용하려면 Configure(구성) > Tags & Profiles(태그 및 프로필) > Tags(태그) > AP > Filter(필터) > Add(추가)로 이동합니다.

-이름: BR_CAN01

- AP 이름 regex: BR-CAN01-.(7)(이 규칙은 조직 내에서 채택된 AP 이름 규칙에 일치합니다. 이 예 에서 태그는 'BR_CAN01-' 뒤에 7개의 문자가 포함된 AP 이름 필드가 있는 AP에 할당됩니다.)

-우선순위: 1

- 정책 태그 이름: PT_CAN01(정의된 대로)
- 사이트 태그 이름: ST_CAN01
- RF 태그 이름: 지사 RF

Associate Tags to AP

A Rule "BR-CAN01"	has this priority	Assigning it to the	e current rule will sy	wap the priorites.
-------------------	-------------------	---------------------	------------------------	--------------------

Rule Name*	BR_CAN01	Policy Tag Name	PT_CAN01	×v
AP name regex*	BR-CAN01{7}	Site Tag Name	ST_CAN01	× v
Active	YES	RF Tag Name	Branch_RF	×v
Priority*	1			
' Cancel				Apply to Devi

Aruba CPPM 인스턴스 구성

Aruba CPPM 컨피그레이션을 기반으로 한 프로덕션/모범 사례에 대해서는 현지 HPE Aruba SE 리 소스에 문의하십시오.

Aruba ClearPass 서버 초기 컨피그레이션

Aruba ClearPass는 다음 리소스를 할당하는 ESXi <> 서버에서 OVF(Open Virtualization Format) 템플릿을 사용하여 구축됩니다.

- 예약된 가상 CPU 2개
- 6GB RAM
- 80GB 디스크(시스템 전원을 켜기 전에 초기 VM 구축 후 수동으로 추가해야 함)

라이센스 신청

다음을 통해 플랫폼 라이센스를 적용합니다. 관리 > 서버 관리자 > 라이센스. 플랫폼, 액세스 및 온 보드 라이센스를 추가합니다.

서버 호스트 이름

Administration(관리) > Server Manager(서버 관리자) > Server Configuration(서버 컨피그레이션)으로 이동하고 새로 프로비저닝된 CPPM 서버를 선택합니다.

- 호스트 이름: cppm
- FQDN: cppm.example.com
- 관리 포트 IP 주소 지정 및 DNS 확인

Administration » Server Manager » Server Configuration - cppm

Server Configuration - cppm (10.85.54.98)

System	Services Control	Service	Parameters	System Monitoring	Network	FIPS			
Hostname:			cppm						
FQDN:			cppm.example	.com					
Policy Mana	iger Zone:		default	~				Manage F	
Enable Perfe	ormance Monitoring	Display:	Enable this	server for performance	e monitoring	display			
Insight Sett	ting:		🗹 Enable Insi	ght 🔽 En	able as Insigh	nt Master	Current Master:cppm(10.85.54.98)		
Enable Ingr	ess Events Processir	ng:	🗌 Enable Ing	ress Events processing	on this serve	er			
Master Serv	ver in Zone:		Primary maste	er v					
Span Port:			None	~					
				IPv	4	_	IPv6	Action	
		IP Add	ress	10.8	5.54.98				
Manageme	ent Port	Subnet	Subnet Mask		255.255.224	•		Configure	
		Default	Gateway	10.8	5.54.97				
		IP Addr	ress			_			
Data/Exte	rnal Port	Subnet	Mask					Configure	
D		Default	Gateway						
		Primary	Y	10.8	5.54.122				
DNS Sattin	26	Second	lary					Configure	
Dito Settin	195	Tertiary	/					oomgure	
		DNS Ca	aching	Disa	bled				

CPPM 웹 서버 인증서(HTTPS) 생성

이 인증서는 ClearPass Guest Portal 페이지가 HTTPS를 통해 브랜치의 게스트 Wifi에 연결하는 게 스트 클라이언트에 제공될 때 사용됩니다. 1단계. CA pub chain 인증서를 업로드합니다.

Administration > Certificates > Trust List > Add로 이동합니다.

- 사용법: 기타 사용

View Certificate Details		8		
Subject DN:				
Issuer DN:				
Issue Date/Time:	Dec 23, 2020 16:55:10 EST			
Expiry Date/Time:	Dec 24, 2025 17:05:10 EST			
Validity Status:	Valid			
Signature Algorithm:	SHA256WithRSAEncryption			
Public Key Format:	X.509			
Serial Number:	86452691282006080280068723651711271611			
Enabled:	true			
Usage:	🗹 EAP 🗹 RadSec 🗹 Database 🔽 Others			
	Update Disable Export Close			

2단계. 인증서 서명 요청을 생성합니다.

Administration > Certificates > Certificate Store > Server Certificates > Usage로 이동합니다. HTTPS 서버 인증서

- Create Certificate Signing Request(인증서 서명 요청 생성) 클릭

- 공용 이름: CPPM

- 조직: cppm.example.com

SAN 필드를 채워야 합니다(SAN에는 공통 이름이 있어야 하며 필요에 따라 IP 및 기타 FQDN도 있 어야 함). 형식은 DNS입니다. **<fqdn1>,DNS:<fqdn2>,IP<ip1>**.

Create Certificate Signing Request

Common Name (CN):	cppm
Organization (O):	Cisco
Organizational Unit (OU):	Engineering
Location (L):	Toronto
State (ST):	ON
Country (C):	CA
Subject Alternate Name (SAN):	DNS:cppm.example.com
Private Key Password:	••••••
Verify Private Key Password:	•••••
Private Key Type:	2048-bit RSA ~
Digest Algorithm:	SHA-512 ~
	Submit

3단계. 선택한 CA에서 새로 생성된 CPPM HTTPS 서비스 CSR에 서명합니다.

4단계. Certificate Template(인증서 템플릿) > Web Server(웹 서버) > Import Certificate(인증서 가 져오기)로 이동합니다.

- 인증서 유형: 서버 인증서

- 사용법: HTTP 서버 인증서

- 인증서 파일: CA 서명 CPPM HTTPS 서비스 인증서 찾아보기 및 선택

Import Certificate		8
Certificate Type:	Server Certificate	
Server:	cppm v	
Usage:	HTTPS Server Certificate	
Upload Method:	Upload Certificate and Use Saved Private	e Key 🗸
Certificate File:	Browse No file selected.	
		Import Cancel

C9800 WLC를 네트워크 디바이스로 정의

Configuration(컨피그레이션) > Network(네트워크) > Devices(디바이스) > Add(추가)로 이동합니다.

8

-이름: WLC_9800_지사

- IP 또는 서브넷 주소: 10.85.54.99(랩 토폴로지 다이어그램 참조)
- RADIUS 공유 Cisco: <WLC RADIUS 암호>
- 공급업체 이름: Cisco
- RADIUS 동적 권한 부여 활성화: 1700

Add Device					
Device SNMP Read Settings SN	MP Write Settings CLI Settin	ngs OnCon	nect Enforcem	ent Attributes	:
Name:	WLC_9800_Branch	1			
IP or Subnet Address:	10.85.54.99	e.g., 192.16	58.1.10 or 192	2.168.1.1/24 or 19	92.168.1.1-20)
Description:	Cisco 9800 WLC for Branch	Guest <u>Wifi</u>			
RADIUS Shared Secret:	•••••		Verify: .		
TACACS+ Shared Secret:]	Verify:		
Vendor Name:	Cisco				
Enable RADIUS Dynamic Authorization:	Port: 1700				
Enable RadSec:		-			
Enable RadSec:					

Add Cancel

게스트 포털 페이지 및 CoA 타이머

구성 전체에서 올바른 타이머 값을 설정하는 것은 매우 중요합니다. 타이머가 조정되지 않은 경우 클라이언트가 'Run State'에 있지 않은 상태에서 순환 웹 포털 리디렉션으로 실행될 수 있습니다. 다음에 유의할 타이머:

• 포털 웹 로그인 타이머: 이 타이머는 상태 전환을 CPPM 서비스에 알리고, 엔드포인트 사용자 지정 특성 'Allow-Guest-Internet' 값을 등록하고, CPPM에서 WLC로의 CoA 프로세스를 트리거 하기 위해 게스트 포털 페이지에 대한 액세스를 허용하기 전에 리디렉션 페이지를 지연시킵니 다. Guest > Configuration > Pages > Web Logins로 이동합니다.

- 게스트 포털 이름 선택: Lab Anonymous Guest Registration(이 게스트 포털 페이지 컨피그레 이션은 다음과 같이 자세히 표시됨)

- Edit를 클릭합니다.
- 로그인 지연: 6초

* Login Delay: 6 The time in seconds to delay while displaying the login message.

• ClearPass CoA 지연 타이머: 따라서 ClearPass에서 WLC로의 CoA 메시지 생성이 지연됩니다. 이는 CPPM이 WLC에서 CoA 승인(ACK)이 반환되기 전에 내부적으로 클라이언트 엔드포인트 의 상태를 성공적으로 전환하기 위해 필요합니다. 랩 테스트에서는 WLC의 밀리초 미만의 응답 시간을 보여 주며, CPPM이 엔드포인트 특성 업데이트를 완료하지 않은 경우 WLC의 새 RADIUS 세션이 인증되지 않은 MAB 서비스 시행 정책과 일치하며 클라이언트에 다시 리디렉 션 페이지가 제공됩니다. CPPM > Administration(관리) > Server Manager(서버 관리자) > Server Configuration(서버 컨피그레이션)으로 이동하고 CPPM Server(CPPM 서버) > Service Parameters(서비스 매개변수)를 선택합니다.

- RADIUS 동적 권한 부여(DM/CoA) 지연 - 6초로 설정

aruba	ClearPass Policy Manager					
Dashboard O	Administration » Server Manager » Server Configuration - cppm					
Monitoring O	Server Configuration - cppm (10.85.54.98)					
🗞 Configuration 🔹 💿	5 () ()					
J Administration 📀						
- J ClearPass Portal	System Services Control Service Parameters System Monitoring Network FIPS					
- Derver Manager	Select Service: Async network services					
- Ja Log Configuration	Parameter Name	Parameter Value				
Local Shared Folders Local Shared Folders Local Shared Folders Device Insight Device Insight	Ingress Event Batch Processing Interval Command Control	30 seconds				
- A External Accounts	RADIUS Dynamic Authorization (DM/CoA) Delay	6 seconds				
🖃 😓 Certificates	Enable SNMP Bounce Action	FALSE ~				
- 🌽 Certificate Store	Post Auth					
- Prust List	Number of request processing threads	20 threads				
	Lazy handler polling frequency	5 minutes				
Agents and Software Lindates	Eager handler polling frequency	30 seconds				
a Support	Connection Timeout	10 seconds				
	Palo Alto User Identification Timeout	45 minutes				

ClearPass - 게스트 CWA 컨피그레이션

ClearPass측 CWA 컨피그레이션은 (3) 서비스 포인트/단계로 구성됩니다.

ClearPass 구성 요소	서비스 유형	목적
1. 정책 관리자	서비스: Mac 인증	사용자 지정 특성 Allow-Guest- Internet = TRUE이면 네트워크 허용합니다. 그렇지 않으면 리더 및 COA를 트리거합니다. 재인
2. 게스트	웹 로그인	익명 로그인 AUP 페이지를 표, 다. Post-auth set custom attribute Allow -Guest-Internet = TRUE.
3. 정책 관리자	서비스: 웹 기반 인증	엔드포인트를 알려진 상태로 일 트 사용자 지정 특성 Allow-Guest- Internet = TRUE 설정 COA: 재인중

ClearPass 끝점 메타데이터 특성: 게스트 인터넷 허용

클라이언트가 'Webauth Pending' 및 'Run' 상태 간에 전환될 때 게스트 엔드포인트 상태를 추적하 려면 Boolean 형식의 메타데이터 특성을 만듭니다.

- wifi에 연결하는 새 게스트의 기본 메타데이터 특성이 Allow-Guest-Internet=false로 설정되어 있습니다. 이 특성에 따라 클라이언트 인증은 MAB 서비스를 통해 이동

- AUP Accept(AUP 수락) 버튼을 클릭하면 게스트 클라이언트의 메타데이터 특성이 Allow-Guest-Internet=true로 업데이트됩니다. True(참)로 설정된 이 특성에 기반한 후속 MAB는 인터넷에 리디 렉션되지 않은 액세스를 허용합니다

ClearPass > Configuration(컨피그레이션) > Endpoints(엔드포인트)로 이동하고 목록에서 엔드포인

트를 선택하고 Attributes(특성) 탭을 클릭한 다음 Allow-Guest-Internet with value false and Save(잘못된 값과 Save)를 추가합니다.

참고: 동일한 엔드포인트를 편집하고 바로 이 특성을 삭제할 수도 있습니다. 이 단계에서는 정 책에서 사용할 수 있는 Endpoints 메타데이터 DB에 필드를 생성합니다.

Edit	t Endpoint				8
E	Endpoint Attributes				
	Attribute		Value		
1.	Allow-Guest-Internet	=	false	Þ	Ť
2.	Click to add				

ClearPass 시행 정책 구성 재인증

클라이언트가 게스트 포털 페이지에서 AUP를 수락 한 직후 게스트 클라이언트에 할당 된 적용 프 로파일을 작성 합니다.

ClearPass > Configuration > Profiles > Add로 이동합니다.

- 템플릿: RADIUS 동적 권한 부여

-이름: Cisco_WLC_Guest_COA

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile Attributes	Summary
Template:	RADIUS Dynamic Authorization
Name:	Cisco_WLC_Guest_COA
Description:	
Туре:	RADIUS_CoA
Action:	Accept O Reject O Drop
Device Group List:	Remove View Details Modify

반경:IETF

호출 스테이션 Id

Radius:Cisco

Cisco-AVPair

Cisco-AVPair

Radius:Cisco

%{Radius:Cisco:Cisco-AVPair:subscriber:audit-sessic 가입자:reauthenticate-type=las type=last

ClearPass 게스트 포털 리디렉션 적용 프로파일 컨피그레이션

'Allow-Guest-Internet'이 '**true**'로 설정된 CPPM 엔드포인트 데이터베이스에서 MAC 주소를 찾을 수 없는 경우 초기 MAB 단계 중에 게스트에 적용되는 시행 프로필을 생성합니다.

그러면 9800 WLC에서 외부 인증을 위해 게스트 클라이언트를 CPPM 게스트 포털로 리디렉션합니 다.

ClearPass > Enforcement > Profiles > Add로 이동합니다.

-이름: Cisco_Portal_Redirect

-유형: RADIUS

-작업: 수락

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary	
Template:		Aruba RADIUS Enforcement	~
Name:		Cisco_Portal_Redirect	
Description:			
Гуре:		RADIUS	
Action:		💿 Accept 🔘 Reject 🔘 Drop	
Device Grou	ıp List:		Remove
			View Details
			Modify
		Select v	

ClearPass 리디렉션 적용 프로파일

동일한 대화 상자의 Attributes(특성) 탭에서 이 이미지에 따라 두 개의 특성을 구성합니다.

Enforcement Profiles - Cisco_Portal_Redirect

-	Summary Profile Attributes				
	Туре	Name		Value	
1.	Radius:Cisco	Cisco-AVPair	-	url-redirect-acl=CAPTIVE_PORTAL_REDIRECT	60
2.	Radius:Cisco	Cisco-AVPair	=	url-redirect=https://cppm.example.com/guest/laccept.php?cmd- login&mac=%{Connection:Client-Mac-Address-Hyphen}&switchip=% {Radius:IETF:NAS-IP-Address}	B

ClearPass 리디렉션 프로파일 특성

url-redirect-acl 특성은 C9800에서 생성된 ACL의 이름인 CAPTIVE-PORTAL-REDIRECT로 설정됩니다.

참고: ACL에 대한 참조만 RADIUS 메시지에 전달되고 ACL 내용은 전달되지 않습니다. 그림 과 같이 9800 WLC에 생성된 ACL의 이름이 이 RADIUS 특성의 값과 정확히 일치해야 합니다.

url-redirect 특성은 여러 매개변수로 구성됩니다.

- 게스트 포털이 호스팅되는 대상 URL, <u>https://cppm.example.com/guest/iaccept.php</u>
- 게스트 클라이언트 MAC, 매크로 %{Connection:Client-Mac-Address-Hyphen}
- 인증 기관 IP(9800 WLC에서 리디렉션 트리거), 매크로 %{Radius:IETF:NAS-IP-Address}
- cmd-login 작업

ClearPass 게스트 웹 로그인 페이지의 URL은 CPPM(**CPPM) > Guest(게스트) > Configuration(컨** 피그레이션) > Pages(페이지) > Web Logins(웹 로그인) > Edit(편집)로 이동할 때 표시됩니다.

이 예에서는 CPPM의 게스트 포털 페이지 이름이 iaccept로 정의됩니다.

참고: 게스트 포털 페이지의 컨피그레이션 단계는 다음과 같습니다.

aruba		(
💱 Guest 🛛 🛛 🛛	Home » Configuration	n » Pages » Web Logins
i ¹ Devices 0	Web Login (La	b Anonynous Guest Regist
📳 Onboard 🔹 📀		
🔦 Configuration 📀	Use this form to make	e changes to the Web Login Lab Anon y
- 🍣 Authentication		
E 🤡 Content Manager	* Name:	Lab Anonynous Guest Registration
– 🚝 Guest Manager	Name.	Enter a name for this web login page.
🗄 🌯 Hotspot Manager	Page Name:	iaccept
🖃 😩 Pages		Enter a page name for this web login.
— 🌆 Fields		The web login will be accessible from /guest/
- 🋅 Forms		
List Views	Description:	
Self-Registrations		Comments or descriptive text about the web I
- 🥵 Web Logins	* Vendor Settings:	Aruba Networks
🔍 Web Pages	tender settingst	Select a predefined group of settings suitable

참고: Cisco 디바이스의 경우 audit_session_id가 일반적으로 사용되지만 다른 벤더에서는 지 원되지 않습니다.

ClearPass 메타데이터 적용 프로필 컨피그레이션

CPPM에서 상태 전환 추적에 사용되는 엔드포인트 메타데이터 특성을 업데이트하도록 시행 프로 필을 구성합니다.

이 프로파일은 엔드포인트 데이터베이스의 게스트 클라이언트 MAC 주소 항목에 적용되며 'Allow-

Guest-Internet' 인수를 'true'로 설정합니다.

ClearPass > Enforcement > Profiles > Add로 이동합니다.

- 템플릿: ClearPass 엔터티 업데이트 적용

-유형: Post_Authentication

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Template:		ClearPass Entity Update Enforcement
Name:		Make-Cisco-Guest-Valid
Descriptior	1:	
Туре:		Post_Authentication
Action:		Accept O Reject O Drop

동일한 대화 상자에서 Attributes **탭을** 선택합니다.

-유형: 엔드포인트

-이름: 게스트 인터넷 허용

참고: 이 이름이 드롭다운 메뉴에 나타나도록 하려면 단계에 설명된 대로 하나 이상의 엔드포 인트에 대해 이 필드를 수동으로 정의해야 합니다.

-가치: 참

Co	onfiguration » Enforcement » Profiles » Add Enforcement Profile									
Er	nforcement Pro	files								
F	Profile Attributes Summary									
	T		Nama	Valua						
	гуре		Name	value						
1.	Endpoint	•	Allow-Guest-Internet	= true	-					

ClearPass 게스트 인터넷 액세스 적용 정책 컨피그레이션

ClearPass > Enforcement > Policies > Add로 이동합니다.

-이름: WLC Cisco 게스트 허용

- 적용 유형: RADIUS

- 기본 프로필: Cisco_Portal_Redirect

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement	Rules	Summary
Name:		WLC Cisco Guest Allow
Description:		
Enforcement Type	e:	● RADIUS → TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application ○ Event
Default Profile:		Cisco_Portal_Redirect View Details Modify

동일한 대화 상자에서 Rules(규칙) 탭으로 이동하고 Add Rule(규칙 추가)을 클릭합니다.

- -유형: 엔드포인트
- -이름: 게스트 인터넷 허용
- 연산자: 같음
- 값 True

- 프로필 이름/추가할 항목 선택: [RADIUS] [액세스 프로필 허용]

Rules	s Editor								8
			Co	onditions					
Mate	h ALL of the followin	a conditions:							_
Matt	Type	ig conditions.	Name	Operator	Value				
1.	Endpoint	*	Allow-Guest-Internet	EOUALS	-	true		B	÷
2.	Click to add							_	
_									
			Enforce	ment Profiles					
Prof	île Names:	[RADIUS] [Allow Acc	ess Profile) Move Up ↑ Move Down ↓ Remove	~					
							Save	Cance	el 🛛

ClearPass 게스트 사후 AUP 시행 정책 컨피그레이션

ClearPass > Enforcement > Policies > Add로 이동합니다.

-이름: Cisco WLC 웹 인증 시행 정책

- 적용 유형: WEBAUTH(SNMP/에이전트/CLI/CoA)

- 기본 프로필: [RADIUS_CoA] Cisco_Reauthenticate_Session

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement	Rules	Summary
Name:		Cisco WLC Webauth Enforcement Policy
Description:		
		11.
Enforcement Typ	e:	○ RADIUS ○ TACACS+
Default Profile:		[RADIUS_CoA] Cisco_Reautl > View Details Modify

동일한 대화 상자에서 Rules > Add로 이동합니다.

- -조건: 인증
- -이름: 상태
- 연산자: 같음
- -가치: 사용자
- 프로필 이름: <각각 추가>:
- [인증 후] [엔드포인트 알 수 있는 업데이트]
- [인증 후] [Make-Cisco-Guest-Valid]
- [RADIUS_CoA] [Cisco_WLC_Guest_COA]

		Conditions		
atch ALL of the follow	ving conditions:			
Туре	Name	Operator	Value	
. Authentication	Status	EQUALS	User	6
Click to add				
		Enforcement Profiles		
rofile Names:	[Post Authentication] [Update Endpoint Known]	Enforcement Profiles		
rofile Names:	[Post Authentication] [Update Endpoint Known] [Post Authentication] Make-Cisco-Guest-Valid [PADUIS_CoAL Gisco WIC Guest COA	Enforcement Profiles		
rofile Names:	[Post Authentication] [Update Endpoint Known] [Post Authentication] Make-Cisco-Guest-Valid [RADIUS_CoA] Cisco_WLC_Guest_COA	Enforcement Profiles Move Up ↑ Move Down ↓		
Profile Names:	[Post Authentication] [Update Endpoint Known] [Post Authentication] Make-Cisco-Guest-Valid [RADIUS_CoA] Cisco_WLC_Guest_COA	Enforcement Profiles Move Up ↑ Move Down J Remove		

참고: 연속 게스트 포털 리디렉션 의사 브라우저 팝업으로 시나리오를 실행하는 경우 CPPM 타이머를 조정해야 하거나 RADIUS CoA 메시지가 CPPM과 9800 WLC 간에 제대로 교환되 지 않음을 나타냅니다. 이러한 사이트를 확인합니다.

- CPPM **> Monitoring > Live Monitoring > Access Tracker로 이동하고 RADIUS** 로그 항목에 RADIUS CoA 세부 정보가 포함되어 있는지 확인합니다.

- **9800 WLC**에서 **Troubleshooting(문제 해결) > Packet Capture(패킷 캡처)**로 이동하고 RADIUS CoA 패킷이 도착할 것으로 예상되는 인터페이스에서 pcap를 활성화하고 CPPM에서 RADIUS CoA 메시지가 수신되는지 확인합니다.

ClearPass MAB 인증 서비스 컨피그레이션

서비스는 AV(특성 값) 쌍 Radius에서 일치합니다. Cisco | CiscoAVPair | cisco-wlan-ssid

- ClearPass > Configuration > Services > Add로 이동합니다.
- **서비스** 탭:
- -이름: 게스트 포털 Mac 인증
- -유형: MAC 인증

```
- 추가 옵션: Authorization(권한 부여), Profile Endpoints(엔드포인트 프로파일)를 선택합니다.
```

- 일치 규칙 추가:
- -유형: RADIUS: Cisco
- -이름: Cisco-AVPair
- 연산자: 같음
- -가치: cisco-wlan-ssid=게스트(구성된 게스트 SSID 이름 일치)

참고: 'Guest'는 9800 WLC에서 브로드캐스트한 게스트 SSID의 이름입니다.

Confi	guration » Services »	Add									
Ser	vices										
Ser	vice Authentication	Authorization	Roles	Enforcement	Profiler	Summary					
Туре:		MAC Authentication	1	v							
Name	:	GuestPortal - Mac A	uth								
Description: MAC-based Authentication Service											
Monit	or Mode:	Enable to monito	or networ	k access without	enforcemen	t					
More	Options:	Authorization	Audit E	nd-hosts 🗹 Prof	ile Endpoint	ts [🛛 Accounti	ng Proxy				
						Servi	ce Rule				
Match	ies 🔘 ANY or 💿 ALI	L of the following co	nditions:								
	Туре		Na	ime			Operator	Value			
1.	Radius:IETF		NA	S-Port-Type			BELONGS_TO	Ethernet (15), Wireless-802	.11 (19)	6	8
2.	Radius:IETF	Service-Type			BELONGS_TO	Login-User (1), Call-Check ((10)	60	÷		
3.	Connection		Cli	ent-Mac-Address			EQUALS	%{Radius:IETF:User-Name	}	6	Ť
4.	Radius:Cisco		Ci	sco-AVPair			EQUALS	cisco-wlan-ssid=Guest		6	÷

동일한 대화 상자에서 Authentication(인증) 탭을 선택합니다.

- 인증 방법: [MAC AUTH] 제거, 추가 [모든 MAC AUTH 허용]
- 인증 소스: [엔드포인트 저장소][로컬 SQL DB], [게스트 사용자 저장소][로컬 SQL DB]

aruba		ClearPass Policy Manager						
Dashboard O	Configuration » Services » Edit - GuestPortal - Mac Auth							
Monitoring O	Services - GuestPortal - Mac Auth							
Configuration 📀	Summary	Service	Authentication	Authorization	Roles	Enforcement	Profiler	
— 🔆 Service Templates & Wizards — 🏠 Services	Authentication	Methods:	[Allow All MAC A	UTH]		Move Up↑]	
Authentication						Move Down J		
- Q Methods						Remove	ĺ	
→ O Identity						View Details	ĺ	
Single Sign-On (SSO)					Ì	Modify	ĺ	
Local Users					`		, ,	
- 🛱 Endpoints			Select to Add	Select to Add				
- 🛱 Static Host Lists	Authentication	Sources:	[Endpoints Repo	sitory] [Local SQL D	B]			
- 🛱 Roles			[Guest User Rep	ository] [Local SQL	DB]	Move Up ↑	J	
- C Role Mappings						Move Down ↓	J	
→ ↑ Posture						Remove	J	
Enforcement					[View Details]	
- St Policies						Modify)	
- I Promes								
- Provices			Select to Add			~		
- the Device Groups	Strip Usernam	e Rules:	Enable to specified and the specified of the specified	cify a comma-se	parated lis	st of rules to strip	o username prefixes or suffixes	
A Deriver Groups								

동일한 대화 상자에서 적용 탭을 **선택합니다**.

- 시행 정책: WLC Cisco 게스트 허용

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary				
Use Cached	Results:	🗌 Use cach	ed Roles and Pos	ture attributes	from prev	vious sessions	5	
Enforcemen	nt Policy:	WLC Cisco	Guest Allow	v	Modify			
						Enforcen	nent Policy De	etails
Description	:	MAB Enfor	cement Redirect					
Default Prot	file:	Cisco_Port	al_Redirect					
Rules Evalu	ation Algorithm:	first-applic	able					
Cond	litions							Enforcement Profiles
1. (En	dpoint:Allow-Gue	est-Internet	EQUALS true)					[Allow Access Profile]

동일한 대화 상자에서 적용 탭을 **선택합니다**.

Configuration » Services » Add

Services

Service	Authentication	Authorization	Roles	Enforceme	nt	Profiler	Summary	
Endpoint Cl	assification:	Select the classifica	ation(s) af	ter which an	actic Rei	on must be	triggered -	
RADIUS Co.	A Action:	Cisco_Reauthentica	te_Sessio	า	~	View Deta	ails Modify	

ClearPass Webauth 서비스 컨피그레이션

ClearPass > Enforcement > Policies > Add로 이동합니다.

-이름: Guest_Portal_Webauth

-유형: 웹 기반 인증

Configuration » Services » Add

Services

Ser	vice	Authentication	Roles	Enforcement	Summary			
Type:			Web-base	d Authentication		~		
Name	9:		Guest					
Descr	ription	:				11.		
Monit	or Moo	de:	Enable to monitor network access without enforcement					
More	Optior	is:	Authorization Posture Compliance					
						S		
Match	nes O	ANY or 🧿 ALL	of the follo	wing conditions:				
	Туре			Na	ame			
1.	Host			Cł	neckType			
2.	Click	to add						

동일한 대화 상자의 Enforcement 탭에서 Enforcement Policy: Cisco WLC Webauth 시행 정책.

Configuratio	Configuration » Services » Add									
Service	5									
Service	Authentication	Roles	Enforcement	Summary						
Use Cached	Results:	Use cach	ned Roles and Pos	sture attribute	s from previo	ous sessions				
Enforcemen	t Policy:	Cisco WLC	Webauth Enforce	ment Policy	✓ Modify	1	Add New Enforcement Poli			
						Enforcement Policy Details	\$			
Description	:									
Default Pro	file:	Cisco_Rea	uthenticate_Sess	sion						
Rules Evalu	ation Algorithm:	first-applic	cable							
Cond	litions						Enforcement Profiles			
1. (Au	thentication:Stat	us EQUALS	S User)				[Update Endpoint Known], Make-Cisco-Guest-Valid, Cisco_Reauthenticate_Session			

ClearPass - 웹 로그인

익명 AUP 게스트 포털 페이지의 경우 비밀번호 필드가 없는 단일 사용자 이름을 사용합니다.

사용되는 사용자 이름에는 다음 필드가 정의되어 있어야 합니다.

사용자 이름_인증 | 사용자 이름 인증: | 1

사용자에 대한 'username_auth' 필드를 설정하려면 먼저 'edit user'(사용자 수정) 양식에 해당 필드

를 표시해야 합니다. ClearPass > Guest > Configuration > Pages > Forms로 이동하고 create_user form을 선택합니다.

aruba	arPass Guest				
🐏 Guest 🛛 0	Home » Configuration » Pages » Forms				
Customize Forms					
🕞 Onboard 🔹 📀	• Use this list view to customize the forms within the application.				
- 🄧 Authentication	△ Name	Title			
Content Manager	change_expiration Change the expiration time of a single guest account.	Change Expiration			
- Public Files	create_multi Create multiple guest accounts.	Create Multiple Guest Accounts			
- 🛃 Guest Manager 🖅 🌯 Hotspot Manager	Create multiple accounts results page.	Create Multiple Accounts Results			
Pages	Create a single guest account.	Create New Guest Account			
- III List Views	Edit Eields Constant Fields Constant Fields Constant Fields Constant Fields Constant Fields	n Show Usage 🥘 Translations			
Self-Registrations	Create single guest account receipt.	Create New Guest Account Receipt			
- 🚜 Web Logins	🚍 quest edit				

visitor_**name**(행 20)을 선택하고 Insert After(다음**에 삽입)를** 클릭합니다.

Home » Configuration » Pages » Forms

Customize Form Fields (create_user)

Use this list view to modify the fields of the form create_user.

() Q	uick Help		Preview Form			
A Rank	Field	Туре	Label	Description		
1	enabled	dropdown	Account Status:	Select an option for changing the status of this account.		
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.		
13	sponsor_profile_name	text	Sponsor's Profile:	Profile of the person sponsoring this account.		
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.		
20	visitor_name	text	Guest's Name:	Name of the guest.		
E E	dit 🛯 🛅 Edit Base Field	😣 Remove	📤 Insert Before 🗔	Insert After 🔀 Disable Field		

Customize Form Field (new)

Use this form to add a new field to the form create_user.

Form Field Editor						
* Field Name:	ame: Select the field definition to attach to the form.					
Form Display Prope These properties control the	erties user interface displayed for this field.					
Field:	Enable this field When checked, the field will be included as part of the form.					
* Rank:	22 Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.					
* User Interface:	No user interface Revert Re					
Form Validation Pro	the value of this field is checked.					
Field Required:	Field value must be supplied Select this option if the field cannot be omitted or left blank.					
Initial Value:	Revert Control of the form is first displayed.					
* Validator:	IsValidBool The function used to validate the contents of a field.					
Validator Param:	(None) V Optional name of field whose value will be supplied as the argument to a validator.					
Validator Argument:						
Validation Error:	The error message to display if the field's value fails validation and the validator does not return an error message directly.					

이제 AUP 게스트 포털 페이지 뒤에서 사용할 사용자 이름을 생성합니다.

CPPM > Guest > Manage Accounts > Create로 이동합니다.

- 게스트 이름: 게스트와이파이
- 회사 이름: Cisco
- 이메일 주소: guest@example.com
- 사용자 이름 인증: 사용자 이름만 사용하여 게스트 액세스를 허용합니다. 사용
- 계정 활성화: 지금
- 계정 만료: 계정이 만료되지 않음
- 이용 약관: 후원자: 사용

Create Guest Account

New guest account being created by **admin**.

Create New Guest Account				
* Guest's Name:	GuestWiFi Name of the guest.			
* Company Name:	Cisco Company name of the guest.			
* Email Address:	guest@example.com The guest's email address. This will become their username to log into the network.			
Username Authentication:	✓ Allow guest access using their username only Guests will require the login screen setup for username-based authentication as well.			
Account Activation:	Now Select an option for changing the activation time of this account.			
Account Expiration:	Account will not expire Select an option for changing the expiration time of this account.			
* Account Role:	[Guest] ~ Role to assign to this account.			
Password:	281355			
Notes:				
* Terms of Use:	I am the sponsor of this account and accept the terms of use			
Create				

웹 로그인 양식을 만듭니다. CPPM > Guest > Configuration > Web Logins로 이동합니다.

인증 후 섹션의 엔드포인트 특성:

사용자 이름 | 사용자 이름 방문자 이름 | 방문자 이름 cn | 방문자 이름 방문자 전화 | 방문자 전화 email | 이메일 메일 | 이메일 스폰서_이름 | 스폰서 이름 스폰서_이메일 | 스폰서 이메일 **게스트 인터넷 허용 | 참**

aruba		CleanPass Guest
Guest 0		Web Login tidtor
Onloard 0	* Name:	e-more provide the second integrate assessed in the second s
Configuration 0	Page Name:	laceaged Teldar a popper source that they well hopes.
Nuthertication		The and logic will be accessible from "/partit/page_serve.php".
Content Hanager	Description:	
Public Files		Conversion or descriptive test aloud the web logic.
Guest Manager	* Vendor Settings:	Andra Nativorka v
Pages	Inchestante and	Server alcased — Change of authorization (MPC 3514) events carboder V
Tields	Light Method:	Second new the cases relation tight will be handled. Server-initiated lighte require the case's RMC address to be available, usually from the captive portal redirection process.
- Dist Views	Page Redirect Output for spectrum on	cheeders around in the initial redruct.
· Self-Repotrations	Barriello analisi	Do not shock - login will shouts be permitted w
Web Logins	arrant soon.	Beleak the layed of chemising its apply to UVL parameters passed to the anti-legit page. Taxe this splice to detext when URL parameters have taxes modified by the axes, for example their RAC address.
Receipts	Legis Form Delivers for samelying the	induction and motion of the liquin form.
SHS Services		Averyment - De not require a username or password
Transilations	Automotions	Secon the sumain sport many ensurement. Access Cinde requires a single-code Jusemented to be entered.
		Actor is pinite to enough the test of page to attempt to a Lag at actors of pre-testing eccent or reported. Actor is pinite to enough the test page is automotically submitted. Accord calls and pre-test possible the accord to have the lagrange Authentication faild are.
		Cryster a new anonymaus account
	Auto-Generate:	The account will be created without a measure test or expension time, and with the theet rate (15 2). Bitter a value for "Wonymeus beer to use a specific usemane, or leave blank to randomly generate a usemane.
		OverWP1 The manufacture of the conversion addression in the conversion of the conver
	* Anergeneus Geert	The presented will be visible within the HTML. It is reconversible in increase the assumet Density Until in the number of gamla year with its support.
		Enable bypassing the Apple Captive Network Assistant
10-1-1-0-0	Prevent CNA:	The Apple Captive Network Assistant (DM) is the pop-up browser shown when joining a network that has a captive portal. Note that this potent may not work with all vanisors, depending on how the captive portal is inclusionated.
Administration 01	Quation Form:	Provide a custom legin form
		E salesled, you must supply your and HTML legin form in the Header or Foster HTML areas. Councils the datasit labels and ever researces
	Custore Labels:	If selected, you will be able to also labels and error messages for the summit logis form.
	* Pro-Auth Check:	Local — match a local account v
	Pre-Auth Error:	The heal to display if the common and parameter likelog fails. Leave Marik to use the default (Smuld commons or parameter).
	Terms:	Require a Terms and Conditions confirmation Knowled, the user all be found to sense a Terms and Conditions checklary
		a concesso con est anno de actes de actes de canceler a canceler a canceler a
	Terms Lobel:	The form label for the tames checkles. Laws blank to use the default (Twms).
	Teams Teach	
		THE only contribute over Terms and Fandlines
		takes black to use the default () accept the -is herb-* (new, global name-guest, scount, terms, of, use, unly* target+*, black*>terms of use-vin-).
	Terma Layout:	Chipfuly before terms checkbox w Entert the layout for the terms and conditions bot.
	Tenter Party	
	Terris Erteri	The text is display if the terms are not accepted. Leave blank to use the default [In order to lag in, you must accept the terms and conditions.].
	CAPTCHA:	None w
	100 70 10 10	annept and comment
	Lag in Laber	The form state for the log in states. General Ideals to use the default (Log Dr).
	Translations	Skip satematic translation handling Ham Sale and sates have translation wallable under Conferention + Translations + Dass Contractations, Salert His sation in Sace all text as Arbeit.
	Default Destination	
	Options for controlling to	he depthetion clients will redirect to after hepin.
	* Default URL	Enter the default UR, to reduced classs. Places server the content "NTLA" for any external domain.
	Override Destination	Porce default destination for all clients
	Lasis Terre	If university the stand's dedication will be averyidden regardless of its value.
	Options for controlling it	he look and feel of the logic page.
	* Skin:	ClearPass Guest Skin M Occess the skin to use when this web loain page is displayed.
		Asonymous dured WHFI Class
	Title :	The title to display on the well-legin gage. Lakes blank to an the default (page).
		(ma_mulierback)
		Chenal> Clonk culor = 'navy'>
		Conference to Darest WL-FLICAD Card
	weader HTML	Card Card Card salar - "Mark":
		Cofference and Conditionary/No- Cofference you projective the Terms and Conditions in the
		lish below because by obsching the tich hos and aniseting "Denister", you are confirming that you've
		linet. v
		NTNS, kemplate ande skapleyed kelver før legte form. Urson næret (de 2019) som
		Contact a staff member if you are experiencing
		<pre>w/pm(/mma_text)</pre>
	* Lagin Delay:	The loss of sounds in deley while deploying the legis message.
	Advertising Services English advertising contents	ent are then logics parges.
	Advertising	Drable Advertising Services content
	Cloud Identity Optimally present quest	a with various doud identity / social login options.
	Enabled:	Invable lagres with claud identity / social network predentials
	Hulti-Paster Author	Graften
	Providers	No multi-factor authorization v
	Network Login Acce	55
	Carlinsis assess to the la	lip inder
	Planet Server	
	Accord Access	Entry the Westerney and advantation between the second secon
		ther the an exercises and retworks from which topics are permitted.
	Denied Several	
	United Accession	
		In our the or addresses and relevant that are deened topy access. Earch HTTP 404 Net Paurel status v
	* Deny Behaviari	Ericei the request of the system is a request that is not previlted.
	Post-Authentication Actions to perform allow	a summalial pre-subinvisation.
	Health Check	Require a successful Onlined health check
		In process, the substitution is becaused to see a hearth check arise to accussing the advants.
	Update Endpoint:	If selected, the endpoint's attributes will also be updated with other details from the user account.
	Advanced	Contamice ditributes stored with the endpoint
		vision vision vision
	Endpoint Attributes:	Visitor shope Visitor Phase
		List of nemetivalue pairs to pass along.

확인 - 게스트 CWA 권한 부여

CPPM에서 Live Monitoring(**라이브 모니터링) > Access Tracker(액세스 추적기)로 이동합니다**.

MAB 서비스를 연결 하고 시작 하는 새 게스트 사용자 입니다.

요약 탭:

Request Details					
Summary Input O	utput RADIUS CoA				
Login Status:	ACCEPT				
Session Identifier:	R0000471a-01-6282a110				
Date and Time:	May 16, 2022 15:08:00 EDT				
End-Host Identifier:	d4-3b-04-7a-64-7b (Computer / Windows / Windows)				
Username:	d43b047a647b				
Access Device IP/Port:	10.85.54.99:73120 (WLC_9800_Branch / Cisco)				
Access Device Name:	wlc01				
System Posture Status:	UNKNOWN (100)				
	Policies Used -				
Service:	Guest SSID - GuestPortal - Mac Auth				
Authentication Method:	MAC-AUTH				
Authentication Source:	None				
Authorization Source:	[Guest User Repository], [Endpoints Repository]				
Roles:	[Employee], [User Authenticated]				
Enforcement Profiles:	Cisco_Portal_Redirect				
I ≤ Showing 8 of 1-8 reco	rds ► ► Change Status Show Configuration Export Show Logs Close				

동일한 대화 상자에서 **입력** 탭으로 이동합니다.

Request Details				
Summary Input	Output RA	ADIUS CoA		
Username:	d43b047a647	b		
End-Host Identifier:	d4-3b-04-7a-6	64-7b (Computer / Windows / Windows)		
Access Device IP/Port:	10.85.54.99:7	73120 (WLC_9800_Branch / Cisco)		
RADIUS Request			0	
Radius:Airespace:Air	espace-Wlan-Id	1 4		
Radius:Cisco:Cisco-A	VPair	audit-session-id=6336550A00006227CE452457		
Radius:Cisco:Cisco-A	VPair	cisco-wlan-ssid=Guest		
Radius:Cisco:Cisco-A	VPair	client-iif-id=1728058392		
Radius:Cisco:Cisco-A	VPair	method=mab		
Radius:Cisco:Cisco-A	VPair	service-type=Call Check		
Radius:Cisco-AVPair vlan-id=21				
Radius:Cisco:Cisco-A	VPair	wlan-profile-name=WP_Guest		
Radius:IETF:Called-S	Station-Id	14-16-9d-df-16-20:Guest		
Radius:IETF:Calling-	Station-Id	d4-3b-04-7a-64-7b		
I ◄ Showing 8 of 1-8 r	records 🕨 📔	Change Status Show Configuration Export Show Logs C	lose	

동일한 대화 상자에서 **출력** 탭으로 이동합니다.

		Request Details					
ut Ou	utput	RADIUS CoA					
Enforcement Profiles: Cisco_Portal_Redirect							
atus: Ul	NKNOWI	N (100)					
Audit Posture Status: UNKNOWN (100)							
RADIUS Response							
Radius:Cisco:Cisco-AVPair url-redirect-acl=CAPTIVE_PORTAL_REDIRECT							
Radius:Cisco:Cisco-AVPair		edirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=d4-3b- a-64-7b&switchip=10.85.54.99					
	ut O es: Ci atus: U us: U co-AVPa co-AVPa	ut Output es: Cisco_Por atus: UNKNOWI us: UNKNOWI co-AVPair url-re co-AVPair url-re 04-7a	ut Output RADIUS CoA es: Cisco_Portal_Redirect atus: UNKNOWN (100) us: UNKNOWN (100)				

۲

참고로, 여기서는 RADIUS 서버 및 외부에서 호스팅되는 게스트 포털과의 Cisco 9800 Foreign,

I ≤ Showing 8 of 1-8 records ► ► Change Status Show Configuration Export Show Logs Close

Anchor 컨트롤러 상호 작용에 대한 상태 흐름 다이어그램을 보여줍니다.

			9800 Foreign-WLC Guest Portal CWA flow				
Client	AP WLC-P	Foreign WLC-	Anchor	рнср р	NS	Radius	Guest Portal(CPPM)
alt [Client Assocication]							1
[1] Assoc #	equest	•					
Guest Client join	_					_	
		[MAB procedure]	Access-Repuest (sessionid=1E1E1E020000003F3F876869)				
					(3) <redirect_url>=<redirect_url>+<?sessio</td><td>ebb</td><td></td></redirect_url></redirect_url>	ebb	
		[4] Access-Accept [[<redirect url="">, <redirect acl="">] <redirec< td=""><td>T URL>: https://<cppm.fpdn.com>/guest/<page.name>.php?session</page.name></cppm.fpdn.com></td><td>nid+1E1E1E021</td><td>0000003F3F8768696portal+194a5780)</td><td>_</td><td></td></redirec<></redirect></redirect>	T URL>: https:// <cppm.fpdn.com>/guest/<page.name>.php?session</page.name></cppm.fpdn.com>	nid+1E1E1E021	0000003F3F8768696portal+194a5780)	_	
(5) Assoc B	esponse			-			
		(6) Export Anchor Request (<redirect url="">, <redirect acl="">, <vlan>)</vlan></redirect></redirect>					
		[7] Export Anchor Response					
		Foreign: Client goes to run state. Traffic is forwarded on Mobility Tunnel (CAPWAP)					
alt (External WebAuth)				-			
		(8) Redirect ACL enforcement for Client <mac_addr></mac_addr>	-				
[Client IP DHCP Process]				—			
			Client goes to DHCP-Required state				
		REDIRECT ACL Ident' statement allows DHCP, DNS, TCPRD to Guest Port					
(9) DHCP Ha	ndshake	(10) DHCP Handshake	[11] DHCP Handshake				
		[12] <ip update=""> MSG: <client.ip></client.ip></ip>		•			
			Client goes to webauth pending state				
King of Cost Rodal Dated				-	L.		
[13] DNS Query www.msftco	nnecttest.com (CAPWAP)	D4L095 Query (CAPWAP)	[15] DNS Query				
[18] DNS Response www.msftconnectte	ISLCOM IS AT IP <x.x.x.x.h (capwap)<="" td=""><td>[17] DNS Response</td><td>[16] DNS Response</td><td></td><td></td><td></td><td></td></x.x.x.x.h>	[17] DNS Response	[16] DNS Response				
(19) TCP SYN IP <x.x.x.d< td=""><td>.80 (msftconnecttest)</td><td>(20) TCP SYN (CAPWAP)</td><td></td><td></td><td></td><td></td><td></td></x.x.x.d<>	.80 (msftconnecttest)	(20) TCP SYN (CAPWAP)					
			Anchor: «REDIRECT_ACL>: redirect enforced				
4 [22] TCP SYN	ACKIACK	[21] TCP SYN-ACK/ACK speefing <x.x.x.x> (WebAuth <global> VIP)</global></x.x.x.x>					
[23] HTTP GET http://www.msftco	nnecttest.com/connecttest.txt	[24] HTTP GET (CAPWAP)					
The second second second	2 PSTRICTER RECEIPTION	LOINUPSKI SAMARI					
Cospidy Psecial Browser							
[27] DNS Query <#	EDIRECT URL>	[28] DNS Query (CAPWAP)	[29] DNS Query	+ +			
(32) DNS Response <redires< td=""><td>T URL> is at P <y.y.y.y></y.y.y.y></td><td>(31) DNS Response (CAPWAP)</td><td>[30] DNS Response</td><td>-</td><td></td><td></td><td></td></redires<>	T URL> is at P <y.y.y.y></y.y.y.y>	(31) DNS Response (CAPWAP)	[30] DNS Response	-			
Client must trust Guest Portal certificati	0						
			Anchor: <redirect_acl>: redirect bypass <y.y.y.y> (Guest Porta</y.y.y.y></redirect_acl>	4			
[33] Guest Portal(CPPM); TCP-SYN/SYN	ACK/ACK :443 (CAPWAP)	[34] TCP-SYN(SYN-ACK/ACK (CAPWAP)	4	_	[35] TCP-SYN/SYN-ACK/ACK	_	•
[36] HTTP GET «REDIRI	CT_URL/sessionid>	[37] HTTP GET (CAPWAP)		-	E381 HTTP GET	-	•
	40000		4				
	TR0 1 200.0F	LATE ATTE POSTAUTTER 1, 200 GK			LAUNTE POSTAUTEL 1 305 OF		
			1		Telefortin Fortentin Forten	(45) Update E	Indpoint DB: <client_mac>:AllowInternetAccess=True</client_mac>
							[46] Captive Portal page refresh delay
	alt	(CoA Reauth)				_	-
					[47] CoA delay	imer	
		4	48] CoA Request (Type= <reauthenticate>, <sessionid>)</sessionid></reauthenticate>			_	
			[49] CoA Ack (<sessionid>)</sessionid>	-		-	
		(MAB)	[50] Access Request (<sessionid>)</sessionid>				
		4	[51] Access Accept (No redirect URL, «sessionid»)				
		[52] Export Anchor Request					
		[53] Export Anchor Response. No [<redirect url="">,<redirect acl="">]</redirect></redirect>					
			Anchor: Client goes to run state				
	_		1541 HTTP GET/HTTP 2000K Landing Page				
			Client goes to RUN state				•
						_	
Client	AP WLC-F	Foreign WLC-	Anchor	DHCP D	NS	Radius	Guest Portal(CPPM)

앵커 WLC를 사용하는 게스트 중앙 웹 인증 상태 다이어그램

관련 정보

- <u>Cisco 9800 구축 모범 사례 가이드</u>
- Catalyst 9800 Wireless Controller 컨피그레이션 모델 이해
- Catalyst 9800 Wireless Controller의 FlexConnect 이해
- <u>기술 지원 및 문서 Cisco Systems</u>

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.