ISE-Active Directory 그룹 맵을 기반으로 WLC를 사용하여 동적 VLAN 할당 구성

목차
<u>소개</u>
사전 요구 사항
<u>요구 사항</u>
사용되는 구성 요소
<u>표기규칙</u>
RADIUS 서버와의 동적 VLAN 할당
<u>구성</u>
네트워크 다이어그램
<u>설정</u>
<u>ISE에서 ISE의 사용자를 위한 AD 통합 및 인증 및 권한 부여 정책 구성</u>
<u>SSID 'office_hq'에 대한 WLC 구성dot1x 인증 및 AAA 재정의 지원</u>
<u>다음을 확인합니다.</u>
<u>문제 해결</u> 전 11 11 11 11 11 11 11 11 11 11 11 11 1

소개

이 문서에서는 동적 VLAN 할당 개념에 대해 설명합니다.

사전 요구 사항

이 문서에서는 WLAN(무선 LAN) 클라이언트를 특정 VLAN에 동적으로 할당하기 위해 WLC(무선 LAN 컨트롤러) 및 ISE(Identity Services Engine) 서버를 구성하는 방법에 대해 설명합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WLC(Wireless LAN Controller) 및 LAP(Lightweight Access Point)에 대한 기본 지식
- ISE와 같은 AAA(Authentication, Authorization, and Accounting) 서버의 기능 지식
- 무선 네트워크 및 무선 보안 문제에 대한 철저한 지식
- 동적 VLAN 할당에 대한 기능적 및 구성 가능한 지식
- Microsoft Windows AD 서비스, 도메인 컨트롤러 및 DNS 개념에 대한 기본적인 이해
- CAPWAP(Control And Provisioning of Access Point Protocol)에 대한 기본적인 지식 보유

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 8.8.111.0을 실행하는 Cisco 5520 Series WLC
- Cisco 4800 Series AP
- 기본 Windows 서플리컨트 및 Anyconnect NAM
- Cisco Secure ISE 버전 2.3.0.298
- 도메인 컨트롤러로 구성된 Microsoft Windows 2016 Server
- 버전 15.2(4)E1을 실행하는 Cisco 3560-CX Series Switch

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

RADIUS 서버와의 동적 VLAN 할당

대부분의 WLAN 시스템에서 각 WLAN에는 SSID(Service Set Identifier)와 연결된 모든 클라이언트 또는 컨트롤러 용어의 WLAN에 적용되는 정적 정책이 있습니다. 이 방법은 강력하지만 클라이언트 가 서로 다른 QoS 및 보안 정책을 상속하기 위해 서로 다른 SSID에 연결해야 하므로 한계가 있습니 다.

Cisco WLAN 솔루션은 ID 네트워킹의 지원으로 이러한 제한을 해결합니다. 이렇게 하면 네트워크 에서 단일 SSID를 알릴 수 있지만 특정 사용자가 사용자 자격 증명에 따라 서로 다른 QoS, VLAN 특성 및/또는 보안 정책을 상속할 수 있습니다.

동적 VLAN 할당은 사용자가 제공한 자격 증명을 기반으로 무선 사용자를 특정 VLAN에 배치하는 기능입니다. 특정 VLAN에 사용자를 할당하는 이 작업은 Cisco ISE와 같은 RADIUS 인증 서버에서 처리됩니다. 예를 들어, 무선 호스트가 캠퍼스 네트워크 내에서 이동할 때 동일한 VLAN에 유지되도 록 하기 위해 이 기능을 사용할 수 있습니다.

Cisco ISE 서버는 내부 데이터베이스를 포함하는 여러 가능한 데이터베이스 중 하나에 대해 무선 사용자를 인증합니다. 예를 들면 다음과 같습니다.

- 내부 DB
- 액티브 디렉토리
- 일반 LDAP(Lightweight Directory Access Protocol)

- ODBC(Open Database Connectivity) 호환 관계형 데이터베이스
- Rivest, Shamir, and Adelman(RSA) SecurID 토큰 서버
- RADIUS 호환 토큰 서버

<u>Cisco ISE 인증 프로토콜 및 지원되는 외부 ID 소스</u>는 ISE 내부 및 외부 데이터베이스에서 지원하 는 다양한 인증 프로토콜을 나열합니다.

이 문서에서는 Windows Active Directory 외부 데이터베이스를 사용하는 무선 사용자를 인증하는 데 중점을 둡니다.

인증에 성공한 후 ISE는 Windows 데이터베이스에서 해당 사용자의 그룹 정보를 검색하고 해당 사용자를 해당 권한 부여 프로파일에 연결합니다.

클라이언트가 컨트롤러에 등록된 LAP와의 연결을 시도할 때 LAP는 각 EAP 방법의 도움으로 사용 자의 자격 증명을 WLC에 전달합니다.

WLC는 RADIUS 프로토콜을 사용하여(EAP 캡슐화) ISE에 이러한 자격 증명을 전송하고 ISE는 KERBEROS 프로토콜의 도움으로 검증을 위해 사용자의 자격 증명을 AD에 전달합니다.

AD는 사용자 자격 증명을 검증하고 인증에 성공하면 ISE에 알립니다.

인증이 성공하면 ISE 서버는 특정 IETF(Internet Engineering Task Force) 특성을 WLC에 전달합니 다. 이러한 RADIUS 특성은 무선 클라이언트에 할당해야 하는 VLAN ID를 결정합니다. 클라이언트 의 SSID(WLAN, WLC)는 사용자가 항상 미리 지정된 VLAN ID에 할당되므로 상관없습니다.

VLAN ID 할당에 사용되는 RADIUS 사용자 특성은 다음과 같습니다.

- IETF 64(터널 유형)—VLAN으로 설정
- IETF 65(터널 미디어 유형)—802로 설정
- IETF 81(터널 비공개 그룹 ID)—VLAN ID로 설정

VLAN ID는 12비트이며 1에서 4094 사이의 값(포함)을 사용합니다. IEEE 802.1X에서 사용하는 RFC2868에 정의된 대로 Tunnel-Private- Group-ID는 문자열 유형이므로 VLAN ID 정수 값은 문자 열로 인코딩됩니다. 이러한 터널 특성이 전송되면 Tag 필드를 입력해야 합니다.

RFC <u>2868</u>, 섹션 3.1에 명시된 바와 같이: Tag 필드는 길이가 1 옥텟이며 동일한 터널을 참조하는 동일한 패킷에서 특성을 그룹화하는 수단을 제공하기 위한 것입니다. 이 필드에 유효한 값은 0x01~0x1F(포함)입니다. 태그 필드가 사용되지 않는 경우 0x00(영)이어야 합니다. 모든 RADIUS <u>특</u> 성에 대한 자세한 내용은 RFC 2868을 참조하십시오.

구성

이 섹션에서는 문서에서 설명된 기능을 구성하는 데 필요한 정보를 제공합니다.

네트워크 다이어그램



설정

다음은 이 다이어그램에서 사용되는 구성 요소의 컨피그레이션 세부 정보입니다.

- ISE(RADIUS) 서버의 IP 주소는 10.48.39.128입니다.
- WLC의 관리 및 AP 관리자 인터페이스 주소는 10.48.71.20입니다.
- DHCP 서버는 LAN 네트워크에 상주하며 각 클라이언트 풀에 대해 구성됩니다. 다이어그램에 는 표시되지 않습니다.
- VLAN1477 및 VLAN1478은 이 컨피그레이션 전체에서 사용됩니다. 마케팅 부서의 사용자는 VLAN1477에, HR 부서 사용자는 RADIUS 서버에 의해 VLAN1478에 배치되도록 구성됩니다 두 사용자가 동일한 SSID에 연결하는 경우 office_hq.

VLAN1477: 192.168.77.0/24. 게이트웨이: 192.168.77.1 VLAN1478: 192.168.78.0/24. 게이트 웨이: 192.168.78.1

• 이 문서에서는 802.1x를 보안 메커니즘으로PEAP-mschapv2사용합니다.



참고: WLAN을 보호하기 위해 EAP-FAST 및 EAP-TLS 인증과 같은 고급 인증 방법을 사용 하는 것이 좋습니다. 이러한 가정은 이 컨피그레이션을 수행하기 전에 수행됩니다.

- LAP가 WLC에 이미 등록되어 있습니다.
- DHCP 서버에는 DHCP 범위가 할당됩니다
- 네트워크의 모든 디바이스 간에 레이어 3 연결이 존재합니다.
- 이 문서에서는 무선 측에 필요한 컨피그레이션에 대해 설명하고 유선 네트워크가 있는 것으로 가정합니다
- 각 사용자 및 그룹이 AD에 구성됨

ISE 대 AD 그룹 매핑을 기반으로 WLC를 사용하여 동적 VLAN 할당을 수행하려면 다음 단계를 수 행해야 합니다.

- 1. ISE에서 ISE의 사용자에 대한 인증 및 권한 부여 정책의 AD 통합 및 컨피그레이션으로의 ISE
- 2. SSID 'office_hq'에 대한 dot1x 인증 및 AAA 재정의를 지원하기 위한 WLC 컨피그레이션.
- 3. 최종 클라이언트 신청자 컨피그레이션입니다.

ISE에서 ISE의 사용자를 위한 AD 통합 및 인증 및 권한 부여 정책 구성

- 1. 관리자 계정을 사용하여 ISE 웹 UI 인터페이스에 로그인합니다.
- 2. 로Administration > Identity management > External Identity Sources > Active directory 이동합니다.

dentity Services Engine Home	Context Visibility Operations	Policy Administration Work Centers	
System ✓ Identity Management Network R	esources	ent pxGrid Service	
Identities Groups External Identity Sources	Identity Source Sequences	ngs	
External Identity Sources	Active Directory		
⟨= • ⊞ • ⁽²⁾ ⁽²⁾	/ Edit 😤 Add 💥 Delete 🏑	Node View 音 Advanced Tools 👻 Scope Mode	
Certificate Authentication Profile	Join Point Name	 Active Directory Domain 	
Active Directory			No data available
LDAP			
COBC COBC			
RADIUS Token			
RSA SecurID			
SAML Id Providers			
Social Login			

3. Add(추가)를 클릭하고 Active Directory Join Point Name(Active Directory 가입 포인트 이름) 설정에서 도메인 이름과 ID 저장소 이름을 입력합니다. 이 예에서 ISE는 도메인에 등록되며 wlaaan.comjoinpoint는 ISE에 로컬로 중요한AD.wlaaan.com이름으로 지정됩니다.

cternal Identity Sources		Connection		
	÷	t Jain Deint Mana		
Certificate Authentication Profile		Join Point Name	AD.wiaaan.com	(1)
Contractive Directory		 Active Directory Domain 	wlaaan.com	(i)
EDAP LDAP			L	
CDBC				
RADIUS Token		Cubmit Cancel		
RSA SecurID		Submit Cancel		
SAML Id Providers				
Social Login				

4. ISE를 AD에 즉시 조인할지_{Submit}묻는 버튼을 누르면 팝업 창이 열립니다. 을_{Yes}누르고 Active Directory 사용자 자격 증명에 관리자 권한을 제공하여 도메인에 새 호스트를 추가합니다.

Connection Whitelisted	Domains Passiv	eID Groups	Attributes	Advanced Settings	
* Join Point Name AD.wa * Active Directory Domain wlaas	aaan.com				
야글 Join 약글 Leave 👤 Test User 音	Diagnostic Tool 🛛 😵 Refree	sh Table			
ISE Node	▲ ISE Node Role	Status	Domain Controller	Site	
rmanchur-ise.wlaaan.com	STANDALONE	A Not Joined			
	Join Domain Please specify the creder • AD U	ntials required to Join ISE ser Name () Administratu * Password	node(s) to the Active Di	rectory Domain.	×

5. 이 시점 이후에는 ISE가 AD에 성공적으로 등록되어야 합니다.

ternal Identity Sources	Connection Whitelisted Don	nains Passiv	eID Groups	Attributes Advanced	Settings		
Certificate Authentication Profile Active Directory LDAP	Join Point Name AD.wlaaan.com wlaaan.com wlaaan.com						
BADIUS Token	👷 Join 👷 Leave 👤 Test User 💼 Dia	gnostic Tool 🛛 🛞 Refres	sh Table				
RSA SecurID	ISE Node	ISE Node Role	Status	Domain Controller	Site		
SAML Id Providers	rmanchur-ise.wlaaan.com	STANDALONE	Operational	WIN-CFA29CSRIL9.wlaaan.com	Default-First-Site-Name		

등록 프로세스에 문제가 있는 경우 를 사용하여 AD 연결_{Diagnostic Tool} 에 필요한 테스트를 실행 할 수 있습니다.

6. 각 권한 부여 프로파일을 할당하기 위해 사용 되는 활성 디렉토리의 그룹을 검색 해야 합니다.

로 이동한Administration > Identity management > External Identity Sources > Active directory >

> Groups

다음 을 클릭하고Add 선택합니다Select Groups from Active Directory.

► System Identity Management ► Network Re	sources	
Identities Groups External Identity Sources	Identity Source Sequences	
External Identity Sources	Connection Whitelisted Domains PassiveID Groups Attributes	Advanced Settings
	/ Edit - XDelete Group Update SID Values	
Certificate Authentication Profile	Nam Select Groups From Directory	
AD.wlaaan.com	Add Group	No data available
EDAP LDAP		
CDBC		
RADIUS Token		
RSA SecurID		
SAML Id Providers		
Social Login		

7. 특정 그룹을 검색하기 위해 필터를 지정하거나 AD에서 모든 그룹을 검색할 수 있는 새 팝업 창이 열립니다.

AD 그룹 목록에서 해당 그룹을 선택하고 키를oK누릅니다.

Sele	ect Direct	ory Groups	rv.				×
1113	Densio		· y.		1		
	Domain	wlaaan.com		*			_
1	Name Filter	*	SID Filter	*	Type Filter GLOBAL		*
		Retrieve Groups 13 Groups Retrie	ved.	1			
	Name			Group SID		Group Type	
	wlaaan.co	m/Users/Cloneable Domain Controll	ers	S-1-5-21-2222429329-410808516	4-3220345271-522	GLOBAL	
	wlaaan.co	m/Users/DnsUpdateProxy		S-1-5-21-2222429329-410808516	4-3220345271-1102	GLOBAL	
	wlaaan.co	m/Users/Domain Admins		S-1-5-21-2222429329-410808516	4-3220345271-512	GLOBAL	
	wlaaan.co	m/Users/Domain Computers		S-1-5-21-2222429329-410808516	4-3220345271-515	GLOBAL	
	wlaaan.co	m/Users/Domain Controllers		S-1-5-21-2222429329-410808516	4-3220345271-516	GLOBAL	
	wlaaan.co	m/Users/Domain Guests		S-1-5-21-2222429329-410808516	4-3220345271-514	GLOBAL	
	wlaaan.co	m/Users/Domain Users		S-1-5-21-2222429329-410808516	4-3220345271-513	GLOBAL	
	wlaaan.co	m/Users/Group Policy Creator Owne	ers	S-1-5-21-2222429329-410808516	4-3220345271-520	GLOBAL	
✓	wlaaan.co	m/Users/HR		S-1-5-21-2222429329-410808516	4-3220345271-1105	GLOBAL	
	wlaaan.co	m/Users/Key Admins		S-1-5-21-2222429329-410808516	4-3220345271-526	GLOBAL	
✓	wlaaan.co	m/Users/Marketing		S-1-5-21-2222429329-410808516	4-3220345271-1104	GLOBAL	
	wlaaan.co	m/Users/Protected Users		S-1-5-21-2222429329-410808516	4-3220345271-525	GLOBAL	
	wlaaan.co	m/Users/Read-only Domain Controll	ers	S-1-5-21-2222429329-410808516	4-3220345271-521	GLOBAL	



8. 각 그룹이 ISE에 추가되고 저장될 수 있습니다. 을 누릅니다_{Save}.

	C	Connecti	on		Whiteliste	d Domains	Passiv	eID	Groups		Attributes	Advanced Se	ttings	
1	Edit	م حک	dd -	X Del	ete Group	Update SID	Values							
	Luit	^	uu +	N De	ete Group	opusic bib	Vulues		SID					
	INA	ame						•	50					
	W	aaan.co	m/Use	ers/HR					S-1-5-21-222	242932	29-4108085164	4-3220345271-1105		
	wi	aaan.co	m/Use	ers/Mar	keting				S-1-5-21-222	242932	29-4108085164	1-3220345271-1104		
Sa	ive	Rese	t											

9. ISE 네트워크 디바이스 목록에 WLC 추가 - 로 이동하고Administration > Network Resources > Network Devices키를Add누릅니다. WLC와 ISE 간에 WLC 관리 IP 주소 및 RADIUS 공유 암호를 제공하여 완전한 컨피그레이션

을 수행합니다.

dentity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers
System Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC
Network Devices Network Device G	roups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
0	
Network Devices	Network Devices List > New Network Device
Default Device	• Name 142 / 15270
Device Security Settings	Description
	IP Address • IP: 10.48.71.20 / 32
	O IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected
	* Device Profile dtt Cisco 💌 🕀
	Model Name
	Software Version
	* Network Device Group
	Location LAB O Set To Default
	IPSEC Is IPSEC Device O Set. To Default
	Device Type WLC-lab O Set. To Default.
	✓ RADIUS Authentication Settings
	RADIUS UDP Settings
	Protocol RADIUS
	Shared Secret
	CoA Port 1700 Set To Default
	RADIUS DTLS Settings (i)

- 10. 이제 ISE를 AD에 가입하고 WLC를 디바이스 목록에 추가한 후 사용자에 대한 인증 및 권한 부여 정책의 컨피그레이션을 시작할 수 있습니다.
 - Marketing에서 VLAN1477로 그리고 HR 그룹에서 VLAN1478로 사용자를 할당하기 위 해 권한 부여 프로파일을 생성합니다.
 새 프로파일을 생성하려면Policy > Policy Elements > Results > Authorization > Authorization profiles로Add이 동하여 버튼을 클릭합니다.

dentity Services Engine	Home	Operations Policy	Administration	Work Centers	
Policy Sets Profiling Posture Clier	nt Provisioning - Policy Elements				
Dictionaries + Conditions - Results					
0					
Authentication	Standard Authorization I	Profiles			
- Authorization	For Policy Export go to Administ	tration > System > Backup &	Restore > Policy Export	Page	
	/ Edit + Add C Duplicate	e 🗙 Delete			
Authorization Profiles	□ Name		Profile	•	Description
Downloadable ACLs	Blackhole_Wireless_Acces	55	atta Cisco ⊕		Default profile used to blacklist wireless det
Profiling	Cisco_IP_Phones		📸 Cisco 🕀		Default profile used for Cisco Phones.
Posture	Cisco_Temporal_Onboard		誌 Cisco 🕀		Onboard the device with Cisco temporal ag
	Cisco_WebAuth		諯 Cisco 🕀		Default Profile used to redirect users to the
Client Provisioning	NSP_Onboard		🚓 Cisco 🕀		Onboard the device with Native Supplicant
	Non_Cisco_IP_Phones		諯 Cisco 🕀		Default Profile used for Non Cisco Phones.
	DenyAccess				Default Profile with access type as Access-
	PermitAccess				Default Profile with access type as Access-

• 각 그룹에 대한 VLAN 정보가 포함된 권한 부여 프로파일 컨피그레이션을 완료합니다. 예는 그룹 컨피그레이션 설정을_{Marketing}보여줍니다.

Dictionaries Conditions TR	lesuits
Authentiestics	Authorization Profiles > New Authorization Profile
Authentication	Authorization Profile
Authorization	*Name Marketing
Authorization Profiles	Description Marketing
Downloadable ACLs	Access Type Access ACCEPT *
Profiling	Network Device Profile
Posture	Service Template
Client Provisioning	Track Movement 🔲 🕧
	Passive Identity Tracking 📄 🕡
	▼ Common Tasks
	DACL Name ACL (Filter-ID)
	Security Group
	✓ VLAN Tag ID 1 Edit Tag ID/Name 1477
	✓ Advanced Attributes Settings
	📲 Select an item 💿 = 💽 🔿 — 🕂
	Access Type = ACCESS_ACCEPT Tunnel-Private-Group-ID = 1:1477 Tunnel-Type = 1:13 Tunnel-Medium-Type = 1:6
	Submit Cancel

다른 그룹에 대해서도 유사한 컨피그레이션을 수행해야 하며 각 VLAN 태그 특성을 구성해야 합니다.

 권한 부여 프로파일을 구성한 후 무선 사용자에 대한 인증 정책을 정의할 수 있습니다. 이 작업은 정책 집합을 구성하거나Custom수정하여 수행할 수Default있습니다. 이 예에서는 Default 정책 집합이 수정됩니다. 로Policy > Policy Sets > Default이동합니다. 인증 유형의dot1x경 우 기본적으로 ISE는 현재 기본 설정에서도 작동하지만 AD는 의 ID 소스 목록의 일부이 므로All_User_ID_StoresAll_User_ID_Stores이 예에서 해당 LAB 컨트롤러에 대해 더 구체적인 규칙 WLC_lab을 사용하며 AD를 유일한 인증 소스로 사용합니다.

Policy Sets Pro	filing Posture Client Pr	ovisioning + Pol	icy Elements		Click here to do wireless setup and visibility setup Do r	not show this	again.			
olicy Sets +	Default					Reset	Save			
Status	Policy Set Name	Descrip	tion	Conditions	Allowed Protocols / Server	Sequence	Hits			
Search										
0	Default	Default p	olicy set		Default Network Access	** +	•			
 Authenticatio 	n Policy (4)									
+ Status	Rule Name	Condi	tions		Use	Hits	Actions			
Search										
0					OP	Wired_W		Internal Endpoints × ×		~
	W48	ÜR	Wireless		> Options	v	v			
		_aob AND	Wireless_602.1X	AD wlasan com						
/ 0	WLC_lab		E DEVICE	Device Type EQUALS AE Device Types#WLC-lab	2 Online	0	۰			
			E DEVICE	Son EQUALS AILocations#LAB	* Options					
0	Durity	00	Wired_8		Al_User_ID_Stores × *		•			
	DELIX	UR	Wireless	3X	> Options	Ŭ	•			
0	Defect			Al_User_I0_Stores × *						
Ű					> Options	Ĩ	Ť			
> Authorization	Policy - Local Exception	5								
> Authorization	Policy - Global Exceptio	ns								
> Authorization	Policy (12)									

• 이제 그룹 멤버십을 기반으로 개별 권한 부여 프로파일을 할당하는 사용자에 대한 권한 부여 정책을 생성해야 합니다. 해당 요건을Authorization policy달성하기 위해 섹션으로 이동 하여 정책을 생성합니다.

Policy Sets Profiling Po	sture Client Provisioning	 Policy Ele 	ementa		Click here to do w	reless setup and visibility setup Do n	ot show this	again. ×
Policy Sets + Default							Reset	Savo
Status Policy S	et Name	Description	Conditions			Allowed Protocols / Server S	Sequence	Hits
Search								
Ø Default		Default policy s	eet.			Default Network Access	×7 +	0
> Authentication Policy (1)							
Authorization Policy - L	ocal Exceptions							
> Authorization Policy - C	lobal Exceptions							
✓ Authorization Policy (1-	I)							
• Status Rule N	ame	Conditions		Results Profiles	Security	y Groups	Hits	Actions
Search								
🖌 🎯 Wroles	Marketing	AND E	Wreless_Access AD wlasan.com ExternalGroups EQUALS wlasan.com/Users/Markering	Marketing	+ Select f	from fact 🔹 🕈	۰	۰
II 🖌 🎯 Wreies	UR	AND E	Winitess, Access AD wilasan.com ExternalGroups ECI/ALS wilasan.com/Users/HR	INR	+ Select	from list 🔹 💌	0	۰

SSID 'office_hq'에 대한 dot1x 인증 및 AAA 재정의를 지원하는 WLC 구성

1. ISE를 WLC에서 RADIUS 인증 서버로 구성합니다. 웹 UIsecurity > AAA > RADIUS > Authentication 인터 페이스의 섹션으로 이동하여 ISE IP 주소 및 공유 암호 정보를 제공합니다.

cisco		<u>N</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	
Security	RADIUS Au	thentic	ation Server	s > New						
Security AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Advanced EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella Advanced	RADIUS Au Server Index Server IP Ad Shared Secre Confirm Shared Apply Cisco J Apply Cisco J Key Wrap Port Number Server Statu Support for C Server Timee Network Use Management Tunnel Proxy PAC Provision IPSec Cisco ACA	Ithentic (Priority) Idress(Ipv et Format et ISE Defau ACA Defau ACA Defau ACA Defau r ISE CoA out er t t Retransmy y ming	A/Ipv6) t t it settings ult settings	s > New 2 ¢ 10.48.39.128 ASCII ¢ (Designed 1812 Enabled ¢ Enabled ¢ S seconds C Enable S econds Enable Enable Enable	for FIPS custon	ners and requires a	a key wrap comp	liant RADI	(US server)	

2. WLC의 섹션office_hq아래에wLANsSSID를 구성합니다. 이 예에서는 및 AAA 재정의를 WPA2/AES+dot1x사용하여 SSID를 구성합니다. 인터페이스Dummy는 RADIUS를 통해 적절한 VLAN이 할당되므로 WLAN에 대해 선택됩니다. 이 더미 인터페이스는 WLC에서 생성하고 IP 주소를 지정해야 하지만, IP 주소가 유효하지 않아도 되며, VLAN이 배치된 VLAN을 업링크 스 위치에서 생성할 수 없으므로 VLAN이 할당되지 않을 경우 클라이언트가 아무 곳으로도 이동 할 수 없습니다.

	<u>W</u> LANs <u>C</u> O	NTROLLER W	IRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK				
WLANs												
Current Filter	None	[]	Change Filte	r] [Clear Filter	1				6	Create New	\$	Go
U WLAN ID	Туре	Profile Name			WLAN SSID		A	dmin Status	Security Policies			
	WLAN	test			test		Er	nabled	[WPA2][Auth(802.1X)	1		
□ <u>2</u>	WLAN	AndroidAP			AndroidAP		Er	nabled	[WPA2][Auth(PSK)]			
253	WLAN	BTER-BTwifi-pu	ublic		BTwifi-public		Er	nabled	[WPA2][Auth(PSK)]			
	MONITOR Y WLANS Current Filter WLAN ID 1 2 2 253	MONITOR WLANS CO WLANS Current Filter: None WLAN ID Type 1 WLAN 2 WLAN 252 WLAN	MONITOR WLANS CONTROLLER W WLANS Current Filter: None [3] WLAN ID Type Profile Name 1 WLAN test 2 WLAN test 2 WLAN AndroidAP 253 WLAN BTER-BTwift-pi	MONITOR WLANS CONTROLLER WIRELESS WLANS Current Filter: None [Change Filte WLAN ID Type Profile Name 1 WLAN test 2 WLAN test 2 WLAN AndroidAP 253 WLAN BTER-BTwift-public	MONITOR WLANS QONTROLLER WIRELESS SECURITY WLANS Current Filter: None [Change Filter] [Clear Filter] WLAN ID Type Profile Name [International content of the second content of the s	MONITOR WLANS QONTROLLER WIRELESS SECURITY MANAGEMENT WLANS Current Filter: None [Change Filter] [Clear Filter] WLAN ID Type Profile Name WLAN SSID 1 WLAN test test 2 WLAN AndroidAP AndroidAP 253 WLAN BTER-BTwift-public BTwift-public	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS WLANS Current Filter: None [Change Filter] [Clear Filter] Vertex Vertex WLAN ID Type Profile Name WLAN SSID Vertex 1 1 WLAN test test test 2 WLAN AndroidAP AndroidAP 253 WLAN BTER-BTwiff-public BTwiff-public	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS Current Filter: None [Change Filter] [Clear Filter] Image: Security of the	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK WLANS	MONITOR WLANS QONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK WLANS Current Filter: None [Change Filter] [Clear Filter] Current Filter: Current Filter: Monton of the security Policies WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies 1 WLAN test test Enabled [WPA2][Auth(802.1X)] 2 WLAN AndroidAP Enabled [WPA2][Auth(PSK)] 253 WLAN BTER-BTwift-public BTwift-public Enabled [WPA2][Auth(PSK)]	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK WLANS	MONITOR WLANS QONTROLLER WIRELESS SECURITY MANAGEMENT CQMMANDS HELP FEEDBACK WLANS Current Filter: None [Change Filter] [Clear Filter] Create New Create New

արտիս									Saye Configuration Bing Logout Befreah
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	G Home
WLANs	WLANs > New								< Back Apply
 ✓ WLANS WLANS > Advanced 	Type Profile Name SSID ID	wLA office affice	n e Jha Jha						

WL	ANs > Edit 'office_hq	
G	eneral Security Q	oS Policy-Mapping Advanced
	Profile Name Type SSID Status	office_hq WLAN office_hq Imabled
	Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
	Radio Policy Interface/Interface Group(G Multicast Vlan Feature	All dummy Enabled
	Broadcast SSID NAS-ID	Enabled none

WLANs > Edit 'office_hq'

General See	curity QoS	Policy-Map	ping Adva	nced			
Layer 2	ayer 3 AAA Se	ervers					
Layer 2 Secur	rity ⁶ WPA+WPA2 MAC Filtering	÷ +)				
Fast Transition							
Fast Transition Over the DS Reassociation Tin	Ada aneout 20 Seconds	ptive 🕈					
Protected Mana	gement Frame						
PMF	Disa	abled \$					
WPA+WPA2 Pa	rameters						
WPA Policy							
WPA2 Policy	V						
WPA2 Encrypt	tion 🗸 🗹 AES	5 TKIP	CCMP256	GCMP128	GCMP256		
OSEN Policy							
Authentication	Key Management	<u>19</u>					
802.1X	🕑 Enable						

WLANs	WLANs > Edit 'office_hq'	
WLANs	General Security QoS Policy-Mapping Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	Select AAA servers below to override use of default servers on this WLAN RADIUS Servers RADIUS Server Overwrite interface Enabled Apply Cisco ISE Default Settings Enabled Authentication Servers Accounting Servers Enabled Parameters Server In: 10.48.39.128, Port:1812 ‡ In: 10.48.39.128, Port:1812 ‡ In: 10.48.39.128, Port:1813 ‡ Server 3 None Server 4 None Server 5 None Server 6 None Server 7 None Server 8 None Server 9 None Server 9 None Server 1 Enabled Server 2 None None ‡ Server 5 None None ‡ Server 6 None Server None ‡ None ‡ None ‡	

neral Security QoS	Policy-Mapping Advanced	
Allow AAA Override	Enabled	DHCP
Coverage Hole Detection	Enabled	DHCP Server Override
Enable Session Timeout 21800 Aironet IE	0 sion Timeout (secs) Zenabled	DHCP Addr. Assignment Required Management Frame Protection (MFP)
Diagnostic Channel As Override Interface ACL	IPv4 None IPv6 None IPv6	MFP Client Protection 4 Optional \$
Layer2 Acl	None \$	DTIM Period (in beacon intervals)
JRL ACL P2P Blocking Action	None \$ Disabled \$	802.11a/n (1 - 255) 1 802.11b/g/n (1 - 255) 1
Maximum Allowed Clients ^g	Cenabled Timeout Value (secs)	NAC State None +
Static IP Tunneling	Enabled	Load Balancing and Band Select
Wi-Fi Direct Clients Policy	Disabled \$	Client Load Balancing
Maximum Allowed Clients Per AP Ra	adio 200	Client Band Select
Clear HotSpot Configuration	Enabled	Passive Client

3. 또한 사용자 VLAN에 대한 WLC에서 동적 인터페이스를 생성해야 합니다. UI 메뉴로_{Controller >} Interfaces이동합니다. WLC는 해당 VLAN에 동적 인터페이스가 있는 경우에만 AAA를 통해 수신 된 VLAN 할당을 승인할 수 있습니다.

ahaha				SECURITY		COMMANIDE		EEEDBACK
CISCO	MONITOR WEAKS	CONTROLLER	WIRELESS	SECORITY	MANAGEMENT	C <u>O</u> MMANDS	nc <u>u</u> r	FEEDBACK
Controller	General Informatio	0.0						
General								
Icons	Interface Name	vlan14	77					
Inventory	MAC Address	00:a3:	8e:e3:5a:1a					
Interfaces Interface Groups	Configuration							
Multicast	Guest Lan							
Network Routes	Quarantine							
Fabric Configuration	Quarantine Vlan Id	0						
Redundancy	NAS-ID	none						
Mobility Management	Physical Informati	on						
Ports	Port Number		1					
▶ NTP	Backup Port		0					
▶ CDP	Active Port		1					
▶ PMIPv6	Enable Dynamic AP M	lanagement						
Tunneling								
▶ IPv6	Interface Address							
▶ mDNS	VLAN Identifier		1477					
Advanced	IP Address		192.168.77.5					
Lawful Interception	Netmask		255.255.255.0					
	Gateway		192.168.77.1					
	IPv6 Address		::					
	Prefix Length		128					
	IPv6 Gateway		::					
	Link Local IPv6 Addre	SS	fe80::2a3:8eff:1	fee3:5a1a/64				
	DHCP Information							
	Primary DHCP Server	· [192.168.77.1					
	Secondary DHCP Serv	ver						
	DHCP Proxy Mode	(Global 🛊					

다음을 확인합니다.

연결을 테스트하려면 Windows 10 기본 신청자 및 Anyconnect NAM을 사용합니다.

EAP-PEAP 인증을 사용 중이고 ISE가 SSC(Self-Signed Certificate)를 사용 중이므로 인증서 경고 에 동의하거나 인증서 검증을 비활성화해야 합니다. 기업 환경에서는 ISE에서 서명되고 신뢰할 수 있는 인증서를 사용하고 최종 사용자 디바이스에 신뢰할 수 있는 CA 목록 아래에 적절한 루트 인증 서가 설치되어 있는지 확인해야 합니다.

Windows 10 및 기본 신청자와의 연결 테스트:

1. 버튼Network & Internet settings > Wi-Fi > Manage known networks을 눌러 새 네트워크 프로파일을 열고 생성합 니다.Add new network필요한 정보를 입력합니다.

← Settings	
命 Wi-Fi	
Manage known networks	
Add a new network	Add a new network
+	Network name
Search this list \wp	office_hq
Sort by: Preference $ \lor $ Filter by: All $ \lor $	Security type
	WPA2-Enterprise AES V
	EAP method
	Protected EAP (PEAP) V
	Authentication method
	Secured password (EAP-MSCHAP v2)
(m.	Connect automatically
	Connect even if this network is not broadcasting
	Save Cancel

2. ISE의 인증 로그를 확인하고 사용자에 대해 올바른 프로파일이 선택되었는지 확인합니다.

c	Refresh O Reset Repeat Counts	Export To *														,	Filter -	۰۰
	Time	Status	Details	Repeat	Identity		Endpoint ID	Endpoint P	Authenticat	Authorization Policy	Authorizati	IP Address	Network Device	Device Port	Identity Group	Posture St	Server	
×					Bob	×	Endpoint ID	Endpoint Profi	Authentication	Authorization Policy	Authorization I	IP Address	Network Device	Device Port	Identity Group	Posture Statur	Server	
	Feb 15, 2019 02:16:43:300 PM	•	9	3	Bob		F4.8C 50 62 14 68	Unknown	Default >> W	Default >> Wireless_HR	HR						manchur-	ise
	Feb 15, 2019 02:09:56.389 PM		0		800		F4.8C 50.62.14.68	Unknown	Default >> W	Default >> Wireless_HR	HR		WLC5520		Unknown		manchur-	ise

3. WLC에서 클라이언트 항목을 확인하고 올바른 VLAN에 할당되었으며 RUN 상태에 있는지 확 인합니다.

սիսիս														Saya Con	figuration	Eing Logo	t Befresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	PECOKITA	MANAGEMENT	COMMANDS	HEUP	FEEDBACK									. Home
Monitor	Clients															Entries 1	- 1 of 1
Summary	Current Filter No	one	(Change Filter]	(Clear Filter)												
Access Points																	
Cisco CleanAir																	
Statistics	Client MAC Addr	IP Address/Io	w4/Inv6)	_	AP	Name			WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth P	ort Slot Id	Tunnel	Fastiane
+ CDP	f4:8c:50:62:14:6b	192.168.78.36			AP40	077.6D9E.6162			office_hq	office_hq	Bob	802.11ac(5 GHz)	Associated	Yes 1	1	No	No
Rogues																	
Clients																	
Sleeping Clients																	
Multicast																	
Applications																	

4. WLC CLI에서는show client dertails 를 사용하여 클라이언트 상태를 확인할 수 있습니다.

show client detail f4:8c:50:62:14:6b
Client MAC Address..... f4:8c:50:62:14:6b
Client Username Bob
Client Webauth Username N/A

Hostname:	
Device Type:	Intel-Device
AP MAC Address	70:69:5a:51:4e:c0
AP Name	AP4C77.6D9E.6162
AP radio slot Id	1
Client State	Associated
User Authenticated by	RADIUS Server
Client User Group	Bob
Client NAC OOB State	Access
Wireless LAN Id	3
Wireless LAN Network Name (SSID)	office_hq
Wireless LAN Profile Name	office_hq
Hotspot (802.11u)	Not Supported
Connected For	242 secs
BSSID	70:69:5a:51:4e:cd
Channel	36
IP Address	192.168.78.36
Gateway Address	192.168.78.1
Netmask	255.255.255.0
Policy Manager State	RUN
EAP Type	PEAP
Interface	vlan1478
VLAN	1478
Quarantine VLAN	0
Access VLAN	1478

Windows 10 및 Anyconnect NAM과의 연결 테스트:

1. 사용 가능한 SSID 목록 및 해당 EAP 인증 유형(이 예에서는 PEAP) 및 내부 인증 양식에서 SSID를 선택합니다.

		🕥 Cisco An	AnyConnect Secure Mobility Client — 🗆 🗙
		Web Auth	VPN: Use a browser to gain access.
		F	Network: Connected (10.103.150.57) internet
Cisco Ar	yConnect		× curity:
	Enter information	on for the connection.	e key.
Media:		Wi-Fi	
Descrip SSID:	tive Name:	office_hq office_hq	Scan: can not required on current Wi-Fi.
Securit	/:	WPA2 Enterprise AES	<u>~</u>
802.1X	Configuration	PEAP	g Security: not currently protected by Umbrella. missing.
		OK	

2. 사용자 인증을 위한 사용자 이름 및 비밀번호를 제공합니다.

	Sisco AnyConnect Secure Mobility Client − □ ×
Cisco AnyConnect office_hq X Please enter your username and password for the network: office_hq	VPN: Verify your network connection.
Username: Alice Password: ******* Show Password OK Cancel	No Network Connectivity Network: Authenticating office_hq Image: state of the stat
	Web Security: No License Key.
	System Scan: Limited or no connectivity.

3. ISE가 SSC를 클라이언트에 전송하므로 인증서를 신뢰하도록 수동으로 선택해야 합니다(프 로덕션 환경에서는 ISE에 신뢰받는 인증서를 설치하는 것이 매우 권장됨).

Cisco AnyConnect X		
The server certificate for the network 'office_hq' has failed validation. Do you want to trust it? Certificate Name: rmanchur-ise.wlaaan.com@ Issued To: rmanchur-ise.wlaaan.com	VPN: Verify your network connection.	
Issued By: rmanchur-ise.wlaaan.com Expiration Date: 2020-02-13 15:03:40 UTC Trust Do Not Trust	Image: Network: Authenticating office_hq @ utll ∨	
	Web Security: No License Key.	

4. ISE의 인증 로그를 확인하고 사용자에 대해 올바른 권한 부여 프로파일이 선택되었는지 확인 합니다.

C Refresh O Reset Repeat Court	a Z Export To •																	¥ Filter -	۰۰
Time	Status	Details	Repeat	Identity		Endpoint ID		Endpoint P	Authenticat	Authorization Policy	Authorizati	IP Address		Network Device	Device Port	Identity Group	Posture St	Server	Mdm
×				Alice	×	60	×	Endpoint Prof	Authentication	Authorization Policy	Authorization	IP Address		Network Device	Device Port	Identity Group	Posture Statu	Server	Mdm
Feb 15, 2019 02:51:27.163 PM	٠	<u>o</u>	0	Alice		F4/8C/50/62/14/68		Microsoft-W	Default >>	Default >> Wireless_Marketing	Marketing	192.168.77.32						manchur-ise	
Feb 15, 2019 02:51:24.837 PM	2	à +		Alce	٠	F4:8C:50:62:14:68	٠	Morosoft-W	Default >>	Default >> Wireless_Marketing	Marketing		*	WLC5520		Workstation 💠		manchur-ise 💠	

5. WLC에서 클라이언트 항목을 확인하고 올바른 VLAN에 할당되었으며 RUN 상태에 있는지 확 인합니다.

Clients									Entries 1 - :
Current Filter None	[Change_Filter] [Clear_Filter]								
Client MAC Adds TD Address (Tour (Tours)	40 Norma	WI AN DesClo	W/ AN COTO	Here Name	Protocol	El al luc		Clob Td	Turnel
Client MAC Addr IP Address(Ipv4/Ipv6) [4:8c:50:62:14:6b 192.168.77.32	AP Name AP4C77.6D9E.6162	office_hq	office_hq	Alice	802.11ac(5 GHz)	Associated	Yes 1	1	No
Cliant MAC Addr IP Address(Ipv4/Ipv6) 61:8::50:62:14:69 192.168.77.32	AP Name AP4C77.6D9E.6162	WLAN Profile office_hq	WLAN SSID office_hq	User Name Alice	Protocol 802.11ac(5 GHz)	Status Associated	Auth Por Yes 1	Slot Id	Tunnel No

6. WLC CLI에서는show client dertails

를 사용하여 클라이언트 상태를 확인할 수 있습니다.

Client MAC Address	f4:8c:50:62:14:6b
Client Username	Alice
Client Webauth Username	N/A
Hostname:	
Device Type:	Intel-Device
bettee type:	Incer bevice
AP MAC Address	70:69:5a:51:4e:c0
AP MAC Address	70:69:5a:51:4e:c0 AP4C77.6D9E.6162

Client State	Associated
User Authenticated by	RADIUS Server
Client User Group	Alice
Client NAC OOB State	Access
Wireless LAN Id	3
Wireless LAN Network Name (SSID)	office_hq
Wireless LAN Profile Name	office_hq
Hotspot (802.11u)	Not Supported
Connected For	765 secs
BSSID	70:69:5a:51:4e:cd
Channe1	36
IP Address	192.168.77.32
Gateway Address	192.168.77.1
Netmask	255.255.255.0
Policy Manager State	RUN
Policy Type	WPA2
Authentication Key Management	802.1x
Encryption Cipher	CCMP-128 (AES)
Protected Management Frame	No
Management Frame Protection	No
EAP Type	PEAP
Interface	vlan1477
VLAN	1477

문제 해결

1. WLCtest aaa radius username

password

wlan-id

와 ISE 간의 RADIUS 연결을 테스트하려면 를 사용하고 결과를test aaa show radius표시하려면 를 사용합니다.

test aaa radius username Alice password <removed> wlan-id 2

2
none
Values
Alice
00-00-00-00-00:AndroidAP
00-11-22-33-44-55
0x0000001 (1)

Nas-Ip-Address	10.48.71.20
NAS-Identifier	0x6e6f (28271)
Airespace / WLAN-Identifier	0x0000002 (2)
User-Password	cisco!123
Service-Type	0x0000008 (8)
Framed-MTU	0x00000514 (1300)
Nas-Port-Type	0x0000013 (19)
Cisco / Audit-Session-Id	1447300a000003041d5665c
Acct-Session-Id	5c66d541/00:11:22:33:44:55/743

test radius auth request successfully sent. Execute 'test aaa show radius' for response (Cisco Controller) >test aaa show radius Radius Test Request Wlan-id..... 2 ApGroup Name..... none Radius Test Response Radius Server Retry Status _____ -----1 Success 10.48.39.128 Authentication Response: Result Code: Success Attributes Values _____ _____ User-Name Alice ReauthSession:1447300a000003041d5665c State Class CACS:1447300a000003041d5665c:rmanchur-ise/339603379/59 Tunnel-Type 0x000000d (13) 0x0000006 (6) Tunnel-Medium-Type Tunnel-Group-Id 0x000005c5 (1477)

(Cisco Controller) >

- 2. 무선 클라이언트 연결 문제를 해결하려면_{debug client} 를 사용합니다.
- 3. WLC에서debug aaa all enable인증 및 권한 부여 문제를 트러블슈팅하려면 를 사용합니다.



참고: 디버깅이 수행되는 MAC 주소에_{debug mac addr}따라 출력을 제한하려면 이 명령을 와 함께만 사용하십시오.

4. 인증 실패 및 AD 통신 문제를 파악하려면 ISE 라이브 로그 및 세션 로그를 참조하십시오.

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.