RADIUS 및 TACACS+ 인증을 사용하여 9800 WLC 로비 앰배서더 구성

목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 배경 정보 구성 네트워<u>크 다이어그램</u> RADIUS 인증 ISE 구성 - RADIUS TACACS+ 인증 WLC에서 TACACS+ 구성 ISE 구성 - TACACS+ 다음을 확인합니다. 문제 해결 RADIUS 인증 TACACS+ 인증

소개

이 문서에서는 ISE(Identity Services Engine)를 사용하여 Lobby Ambassador 사용자의 RADIUS 및 TACACS+ 외부 인증을 위한 Catalyst 9800 Wireless LAN Controller를 구성하는 방법에 대해 설명 합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Catalyst Wireless 9800 구성 모델
- AAA, RADIUS 및 TACACS+ 개념

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 9800 Wireless Controller Series(Catalyst 9800-CL)
- Cisco IOS®-XE Gibraltar 16.12.1
- ISE 2.3.0

이 문서의 정보는 특정 랩 환경의 디바이스에서 생성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적 인 영향을 이해해야 합니다.

배경 정보

로비 앰버서더 사용자는 네트워크 관리자가 만듭니다.Lobby Ambassador 사용자는 게스트 사용자 의 사용자 이름, 비밀번호, 설명 및 수명을 생성할 수 있습니다.게스트 사용자를 삭제할 수도 있습니 다.게스트 사용자는 GUI 또는 CLI를 통해 생성할 수 있습니다.

구성

네트워크 다이어그램



ISE

이 예에서는 로비 앰버서더 "로비" 및 "lobbyTac"이 구성됩니다.로비 앰배서더 "로비"는 RADIUS 서 버에 대해 인증되어야 하며 로비 앰배서더 "lobbyTac"은 TACACS+에 대해 인증됩니다.

컨피그레이션은 RADIUS 로비 앰버서더 및 마지막으로 TACACS+ 로비 앰버서더에 대해 먼저 수행 됩니다.RADIUS 및 TACACS+ ISE 컨피그레이션도 공유됩니다.

RADIUS 인증

WLC(Wireless LAN Controller)에서 RADIUS를 구성합니다.

1단계, RADIUS 서버를 선언합니다.WLC에서 ISE RADIUS 서버를 만듭니다.

GUI:

이미지에 표시된 대로 Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add로 이동합니다.

Q Search Menu Items	Configuration * > Security * > AAA							
📻 Dashboard	+ AAA Wizard							
Monitoring >	Servers / Groups AAA Method List AAA Advanced							
Configuration >	+ Add × Delete							
() Administration	RADIUS							
💥 Troubleshooting	TACACS+ Server Groups							
	Name ~ Address ~ Auth Port ~ Acct Port ~							
	[] RadiusLobby 192.168.166.8 1812 1813							
	I I Image: Image Image: Image: Image Image: Image: Image Image: Image: Image Image: Image: Image: Image Image: Image: Image: Image Image: Image: Image: Image: Image Image: Image							

컨피그레이션 창이 열리면 필수 컨피그레이션 매개변수는 RADIUS 서버 이름(ISE/AAA 시스템 이 름과 일치하지 않아도 됨), RADIUS 서버 IP 주소 및 공유 비밀입니다.다른 매개변수는 기본값으로 남겨두거나 원하는 대로 구성할 수 있습니다.

CLI:

Tim-eWLC1(config)#radius server RadiusLobby Tim-eWLC1(config-radius-server)#address ipv4 192.168.166.8 auth-port 1812 acct-port 1813 Tim-eWLC1(config-radius-server)#key 0 Cisco1234 Tim-eWLC1(config)#end 2단계. 서버 그룹에 RADIUS 서버를 추가합니다.서버 그룹을 정의하고 구성된 RADIUS 서버를 추 가합니다.이는 로비 앰버서더 사용자의 인증에 사용되는 RADIUS 서버입니다.WLC에 인증에 사용 할 수 있는 여러 RADIUS 서버가 구성된 경우 모든 Radius 서버를 동일한 서버 그룹에 추가하는 것 이 좋습니다.이렇게 하면 WLC가 서버 그룹의 RADIUS 서버 간에 인증을 로드 밸런싱할 수 있습니 다.

GUI:

이미지에 표시된 대로 Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add로 이동합니다.

Q Search Menu Items	Configuration • > Secu	rity * > AAA			
📻 Dashboard	+ AAA Wizard				
Monitoring >	Servers / Groups	AAA Method List AA	AA Advanced		
Configuration	+ Add × Delete				
(◯) Administration →	RADIUS				
💥 Troubleshooting	TACACS+	Servers Server G	àroups		
		Name	 Server 1 	Server 2	Server 3
	LDAP	GroupRadLobby	RadiusLobby	N/A	N/A
			10 v items per page		1 - 1 of 1 items

그룹에 이름을 지정하기 위해 구성 창이 열리면 구성된 RADIUS 서버를 Available Servers 목록에 서 Assigned Servers 목록으로 이동합니다.

Tim-eWLC1(config)#aaa group server radius GroupRadLobby Tim-eWLC1(config-sg-radius)#server name RadiusLobby Tim-eWLC1(config-sg-radius)#end

3단계. 인증 방법 목록을 생성합니다.Authentication Method List(인증 방법 목록)는 찾고 있는 인증 유형을 정의하며, 정의한 서버 그룹에 동일한 유형을 연결합니다.인증이 WLC에서 로컬로 수행되는 지 아니면 RADIUS 서버 외부에서 수행되는지 알 수 있습니다.

GUI:

이미지에 표시된 대로 Configuration > Security > AAA > AAA Method List > Authentication > + Add로 이동합니다.

Q Search Menu Items	Configuration • > Se	Configuration * > Security * > AAA						
🔜 Dashboard	+ AAA Wizard							
	Servers / Groups	AAA Method List AAA Advanced						
	Authentication							
() Administration	Authorization	+ Add × Delete						
💥 Troubleshooting	Accounting	Name v Type v Group v Group1 v Group2 v Group3 v Group4 v						
		AuthenLobby login local GroupRadLob N/A N/A						

컨피그레이션 창이 열리면 이름을 입력하고 유형 옵션을 Login(로그인)으로 선택하고 이전에 생성 한 서버 그룹을 할당합니다.

그룹 유형을 로컬으로 지정합니다.

GUI:

그룹 유형을 '로컬'로 선택하면 WLC는 먼저 사용자가 로컬 데이터베이스에 있는지 확인한 다음 로 컬 데이터베이스에서 로비 앰버서더 사용자를 찾을 수 없는 경우에만 서버 그룹으로 대체합니다.

CLI:

Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod local group GroupRadLobby Tim-eWLC1(config)#end

참고:버그 CSCvs87163<u>에</u> 유의하십시오. 로컬 를 먼저 사용하는 경우17.3에서 수정되었습니 다.

그룹 유형 그룹

GUI:

'그룹 유형'을 '그룹'으로 선택하고 로컬 옵션으로 대체하지 않는 경우 WLC는 서버 그룹에 대해서만 사용자를 확인하며 로컬 데이터베이스를 체크 인하지 않습니다.

CLI:

Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod group GroupRadLobby Tim-eWLC1(config)#end

Group Type as a group 및 fallback to local 옵션이 선택되어 있습니다.

GUI:

'그룹 유형'을 '그룹'으로 선택하고 로컬 옵션으로 대체 옵션을 선택한 경우 WLC는 서버 그룹에 대해 사용자를 확인하고 RADIUS 서버가 응답에서 시간 초과된 경우에만 로컬 데이터베이스를 쿼리합니 다.서버가 응답하면 WLC는 로컬 인증을 트리거하지 않습니다.

CLI:

Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod group GroupRadLobby local Tim-eWLC1(config)#end

4단계. 권한 부여 방법 목록을 생성합니다.Authorization Method List(권한 부여 방법 목록)는 로비 앰버서더에 필요한 권한 부여 유형을 정의합니다. 이 경우에는 'exec'이 됩니다. 또한 정의된 동일한 서버 그룹에 연결됩니다.또한 인증을 WLC에서 로컬로 수행할지 아니면 RADIUS 서버에 대해 외부 에서 수행할지를 선택할 수 있습니다.

GUI:

이미지에 표시된 대로 Configuration > Security > AAA > AAA Method List > Authorization > + Add로 이동합니다.

Q Search Menu Items	Configuration * > Secu	rity * > AAA						
📻 Dashboard	+ AAA Wizard							
Monitoring >	Servers / Groups	AAA Method List	AAA Advan	ced				
🔾 Configuration 🔹 🔸	Authentication							
() Administration ›	Authorization	+ Add \times D						
💥 Troubleshooting	Accounting	Name 🗸	Туре 🗠	Group ~ Type	Group1 ×	Group2 V	Group3 ×	Group4 ×
		AuthozLobby	exec	local	GroupRadLob	N/A	N/A	N/A

이름을 제공하기 위해 구성 창이 열리면 유형 옵션을 'exec'으로 선택하고 이전에 생성한 서버 그룹 을 할당합니다.

Group Type(그룹 유형)은 Authentication Method List(인증 방법 목록) 섹션에서 설명한 것과 동일 한 방식으로 적용됩니다.

CLI:

그룹 유형을 로컬으로 지정합니다.

Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod local group GroupRadLobby Tim-eWLC1(config)#end

그룹 유형 그룹

Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby

Tim-eWLC1(config)#end Group Type as group 및 fallback to local 옵션이 선택되어 있습니다.

Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby local Tim-eWLC1(config)#end

5단계, 방법을 지정합니다.방법이 구성되면 회선 VTY(SSH/텔넷) 또는 HTTP(GUI)와 같은 게스트 사용자를 생성하기 위해 WLC에 로그인하는 옵션에 할당되어야 합니다.

이러한 단계는 GUI에서 수행할 수 없으므로 CLI에서 수행해야 합니다.

HTTP/GUI 인증:

Tim-eWLC1(config)#ip http authentication aaa login-authentication AuthenLobbyMethod Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozLobbyMethod

HTTP 컨피그레이션을 변경할 때 HTTP 및 HTTPS 서비스를 다시 시작하는 것이 좋습니다.

6단계, 이 단계는 17.5.1 또는 17.3.3 이전 소프트웨어 버전에서만 필요하며 CSCvu29748이 릴리스 된 후에는 필요하지 않습니다. 구현되었습니다.원격 사용자를 정의합니다.로비 앰버서더의 ISE에 서 생성된 사용자 이름은 WLC에서 원격 사용자 이름으로 정의되어야 합니다.원격 사용자 이름이 WLC에 정의되어 있지 않으면 인증이 올바르게 진행되지만, Lobby Ambassador 권한에만 액세스 하는 대신 WLC에 대한 전체 액세스 권한을 사용자에게 부여합니다.이 컨피그레이션은 CLI를 통해

1단계. ISE에 WLC를 추가합니다. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) > Add(추가)로 이동합니다.WLC를 ISE에 추가해야 합니다 .WLC를 ISE에 추가할 때 RADIUS 인증 설정을 활성화하고 이미지에 표시된 대로 필요한 매개변수

Tim-eWLC1(config)#end

Tim-eWLC1(config) #no ip http server

Tim-eWLC1(config-line)#end

서만 수행할 수 있습니다.

ISE 구성 - RADIUS

를 구성합니다.

CLI:

Tim-eWLC1(config) #no ip http secure-server Tim-eWLC1(config)#ip http server

Tim-eWLC1(config)#ip http secure-server

Tim-eWLC1(config)#end

라인 VTY.

Tim-eWLC1(config)#line vty 0 15

Tim-eWLC1(config-line)#login authentication AuthenLobbyMethod

Tim-eWLC1(config-line)#authorization exec AuthozLobbyMethod

Tim-eWLC1(config) #aaa remote username lobby

dentity Services Engine	Home	tions Policy Administration	Mork Centers		
System Identity Management	Network Resources Device Portal Man	nagement pxGrid Services + Fee	d Service		
▼Network Devices Network Device G	Groups Network Device Profiles External	RADIUS Servers RADIUS Server S	equences NAC Managers Ext	ternal MDM Location Services	
0					
Network Devices	Network Devices				
Default Device					
Device Security Settings	/ Edit Add Lo Duplicate	nport 🔛 Export 👻 😁 Generate PAC	X Delete 🔻		Show
	Name IP/Mask	Profile Name	Location	Туре	Description
	Tim-eWLC1 192.168.166.7	👬 Cisco 🕀	All Locations	All Device Types	9800

구성 창이 열리면 이름, IP ADD, enable RADIUS Authentication Settings(IP 추가, RADIUS 인증 설 정 활성화)를 제공하고 Protocol Radius(프로토콜 반경)에 필요한 공유 암호를 입력합니다.

2단계. ISE에서 로비 앰버서더 사용자를 생성합니다.Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자) > Add(추가)로 이동합니다.

게스트 사용자를 생성하는 로비 앰버서더에 할당된 사용자 이름 및 비밀번호를 ISE에 추가합니다 .관리자가 로비 앰버서더에 할당할 사용자 이름입니다.

dentity Services Engine	Home ► Conte	xt Visibility > Operations	► Policy	on Vork Centers
► System	Network Resources	Device Portal Management	pxGrid Services Fee	d Service
✓Identities Groups External Iden	tity Sources Identity	Source Sequences Settings	;	
(
Users	Network Acces	ss Users		
Latest Manual Network Scan Results	🥖 Edit 🛛 🕂 Add	🔀 Change Status 👻 🔐 Impo	ort 🚯 Export 👻 🗙 Delete	- Duplicate
	Status	Name 🔺	Description	First Name Last Name
	🗌 🛛 Enabled	🧕 lobby		

구성 창이 열리면 로비 앰배서더 사용자의 이름과 암호를 입력합니다.또한 Status(상태)가 Enabled(활성화됨)인지 확인합니다.

3단계. 결과 권한 부여 프로파일을 생성합니다.Policy(**정책) > Policy Elements(정책 요소) >** Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일) > Add(추가)로 이동합니다.이미지에 표시된 대로 WLC 및 Access-Accept로 돌아가려면 결과 권한 부여 프로파 일을 생성합니다.

Identity Services Engine	ome	Policy Administration Work Centers
Policy Sets Profiling Posture Client	Provisioning Policy Elements	
Dictionaries Conditions Results		
G		
Authentication	Standard Authorization Profiles	
- Authorization	For Policy Export go to Administration > Sys	tem > Backup & Restore > Policy Export Page
Authorization Drafiles	/ Edit 🕂 Add 🖓 Duplicate 🗙 Dele	te
Authonization Profiles	Name	Profile
Downloadable ACLS	9800RadiusLobby	diste Cisco 🕀

이미지에 표시된 대로 Access-Accept를 전송하도록 프로파일이 구성되어 있는지 확인합니다.

dentity Services Engine	Home 🕨	Context Visibility	Operations	✓ Policy
Policy Sets Profiling Posture CI	ient Provisionin	g Policy Ele	ements	
Dictionaries Conditions Result	s			
G			op. It. i. i.i.	
Authentication	Authorizatio	n Profiles > 980 ation Profile	ORadiusLobby	
- Authorization		* Name	9800RadiusLobby	
Authorization Profiles		Description		
Downloadable ACLs		* Access Type	ACCESS_ACCEPT	*

Advanced Attributes Settings(고급 특성 설정) 아래에서 특성을 수동으로 추가해야 합니다.사용자 를 Lobby Ambassador로 정의하고 Lobby Ambassador가 필요한 변경을 수행할 수 있도록 권한을 제공하려면 특성이 필요합니다.



Attributes Details

Access Type = ACCESS_ACCEPT cisco-av-pair = user-type=lobby-admin cisco-av-pair = shell:priv-lvl=15

4단계. 인증을 처리하기 위한 정책을 생성합니다.Policy(**정책) > Policy Sets(정책 집합) > Add(추가)로 이동합니다**.정책을 구성하는 조건은 관리자 결정에 따라 달라집니다.네트워크 액세스 사용자 이름 조건 및 기본 네트워크 액세스 프로토콜은 여기에서 사용됩니다.

Authorization Policy(권한 부여 정책)에서 Results Authorization(결과 권한 부여)에 구성된 프로파일 이 선택되었는지 확인해야 합니다. 그러면 필요한 특성을 이미지에 표시된 대로 WLC에 반환할 수 있습니다.

cisco	Identity Se	rvices Engine	Home	Context Visibility	Operations	✓ Policy	Administration	Work Centers		
Policy	Sets Pro	filing Posture	Client Provisio	ning Policy Elem	ents					
Policy	y Sets									
+	Status	Policy Set Nan	10	Description	C	Conditio	ns		Allowed Protocols / Serue	or Sequence
Searc	th	Tonoy Oet Ivan		Description	0	-on altro	110			o oquence
	0								Default Network Assess	
	0	9800LobbyRadiu	S			- 1	Network Access UserNam	e EQUALS lobby	Delault NetWORK Access	** +

컨피그레이션 창이 열리면 권한 부여 정책을 구성합니다.인증 정책은 기본값으로 둘 수 있습니다.

Policy Sets → 9800LobbyRadius									
	Status	Policy Set Name	Description	Conditions		Allowed Protocols / Serve	r Sequence		
Sean	h								
	0	9800LobbyRadius		Network Access-UserName EQUALS lobby		Default Network Access	× • +		
> At	thenticatio	n Policy (1)							
> Au	thorization	Policy - Local Exceptions							
> Au	thorization	Policy - Global Exceptions							
¥ Au	thorization	Policy (2)							
Results									
	Status Rule Name Conditions Profiles Security Groups Hits								
Sea	rch								
	Ø	9800LobbyAutho	Network Access-UserNa	me EQUALS lobby	× 9800RadiusLobby	+ Select from list • +	0		

TACACS+ 인증

WLC에서 TACACS+ 구성

1단계. TACACS+ 서버를 선언합니다.WLC에서 ISE TACACS 서버를 생성합니다.

GUI:

이미지에 표시된 대로 Configuration > Security > AAA > Servers/Groups > TACACS+ > Servers > + Add로 이동합니다.

Q Search Menu Items	Configuration * > Securit	onfiguration * > Security * > AAA							
扇 Dashboard	+ AAA Wizard								
Monitoring >	Servers / Groups A	AA Method List AAA Advanced	d						
🔾 Configuration 🛛 🔸	+ Add × Delete								
() Administration >	RADIUS								
💥 Troubleshooting	TACACS+	Server Groups							
		Name	 Server Address 	~	Port	~			
	LDAP	[TACACSLobby	192.168.166.8		49				
		∉ ∉ 1 ⊨ ⊨ 10 ▼	items per page			1 - 1 of 1 items			

컨피그레이션 창이 열리면 필수 컨피그레이션 매개변수는 TACACS+ 서버 이름(ISE/AAA 시스템 이름과 일치하지 않아도 됨), TACACS 서버 IP 주소 및 공유 암호입니다.다른 매개변수는 기본값으 로 남겨두거나 필요에 따라 구성할 수 있습니다. Tim-eWLC1(config)#tacacs server TACACSLobby Tim-eWLC1(config-server-tacacs)#address ipv4 192.168.166.8 Tim-eWLC1(config-server-tacacs)#key 0 Cisco123 Tim-eWLC1(config-server-tacacs)#end 2단계. 서버 그룹에 TACACS+ 서버를 추가합니다.서버 그룹을 정의하고 구성된 원하는 TACACS+

서버를 추가합니다.인증에 사용되는 TACACS+ 서버가 됩니다.

GUI:

이미지에 표시된 대로 Configuration > Security > AAA > Servers / Groups > TACACS > Server Groups > + Add로 이동합니다.

Q Search Menu Items		Configuration * > Se	curity * > AAA			
🔜 Dashboard		+ AAA Wizard				
Monitoring	>	Servers / Groups	AAA Method List	AAA Advanced		
🔾 Configuration	>	+ Add × Del				
() Administration	>	RADIUS				
💥 Troubleshooting		TACACS+	Servers Serve	er Groups		
		1040	Name	 Server 1 	Server 2	Server 3
		LUAP	GroupTacLobby	TACACSLobby	N/A	N/A
				▶ 10 ▼ items per page		1 - 1 of 1 items

구성 창이 열리면 그룹에 이름을 지정하고 원하는 TACACS+ 서버를 Available Servers(사용 가능한 서버) 목록에서 Assigned Servers(할당된 서버) 목록으로 이동합니다.

CLI:

Tim-eWLC1(config)#aaa group server tacacs+ GroupTacLobby Tim-eWLC1(config-sg-tacacs+)#server name TACACSLobby Tim-eWLC1(config-sg-tacacs+)#end

3단계. 인증 방법 목록을 생성합니다.Authentication Method List(인증 방법 목록)는 필요한 인증 유 형을 정의하며, 구성된 서버 그룹에 동일한 유형을 연결합니다.또한 WLC에서 로컬로 또는 TACACS+ 서버에서 외부에서 인증을 수행할 수 있는지 여부를 선택할 수 있습니다.

GUI:

이미지에 표시된 대로 Configuration > Security > AAA > AAA Method List > Authentication > + Add로 이동합니다.



컨피그레이션 창이 열리면 이름을 입력하고 유형 옵션을 Login(로그인)으로 선택하고 이전에 생성 한 서버 그룹을 할당합니다.

그룹 유형을 로컬으로 지정합니다.

GUI:

그룹 유형을 '로컬'로 선택한 경우 WLC는 먼저 사용자가 로컬 데이터베이스에 있는지 확인하고 로 컬 데이터베이스에서 로비 앰버서더 사용자를 찾을 수 없는 경우에만 서버 그룹으로 대체합니다.

참고:이 버그 CSCvs87163<u>에 대해</u> 유의하십시오.17.3에 고정되어 있습니다

CLI:

Tim-eWLC1(config)#aaa authentication login AutheTacMethod local group GroupTacLobby
Tim-eWLC1(config)#end

그룹 유형 그룹

GUI:

Group Type(그룹 유형)을 group(그룹)으로 선택하고 local(로컬)로 대체하지 않는 경우 WLC는 Server Group(서버 그룹)에 대해서만 사용자를 확인하며 로컬 데이터베이스를 체크 인하지 않습니 다.

CLI:

Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby Tim-eWLC1(config)#end

Group Type as group 및 fallback to local 옵션이 선택되어 있습니다.

GUI:

'그룹 유형'을 '그룹'으로 선택하고 Fallback to local(로컬에 대체) 옵션을 선택한 경우 WLC는 서버 그룹에 대해 사용자를 확인하고 TACACS 서버가 응답에서 시간 초과된 경우에만 로컬 데이터베이 스를 쿼리합니다.서버가 거부를 전송하면 로컬 데이터베이스에 있더라도 사용자가 인증되지 않습 니다.

CLI:

Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby local Tim-eWLC1(config)#end

4단계. 권한 부여 방법 목록을 생성합니다.

Authorization Method List(권한 부여 방법 목록)는 Lobby Ambassador에 필요한 권한 부여 유형을 정의하며 이 경우 exec이 됩니다.구성된 동일한 서버 그룹에도 연결됩니다.또한 인증이 WLC에서 로컬로 수행되는지 아니면 TACACS+ 서버에 대해 외부에서 수행되는지를 선택할 수도 있습니다.

GUI:

이미지에 표시된 대로 Configuration > Security > AAA > AAA Method List > Authorization > + Add로 이동합니다.

Q Search Menu Items	Configuration * > Security * AAA	
🔜 Dashboard	+ AAA Wizard	
Monitoring	Servers / Groups AAA Method List AAA Advanced	
	Authentication	
() Administration	Authorization + Add × Delete	
₩ Troubleshooting	Accounting	
	Name v Type v Type Group1 v Group2 v Group3 v Group4	~
	[] AuthozTacMe exec local GroupTacLob N/A N/A N/A	
	I	~

컨피그레이션 창이 열리면 이름을 입력하고 type 옵션을 exec으로 선택하고 이전에 생성한 서버 그 룹을 할당합니다.

Group Type(그룹 유형)은 Authentication Method List(인증 방법 목록) 부품에 설명된 것과 동일한 방식으로 적용됩니다.

CLI:

그룹 유형을 로컬으로 지정합니다.

Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod local group GroupTacLobby Tim-eWLC1(config)#end

그룹 유형 그룹

Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby Tim-eWLC1(config)#end

Group Type as group 및 Fallback to local 옵션이 선택되어 있습니다.

Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby local Tim-eWLC1(config)#end

5단계. 방법을 지정합니다.방법이 구성되면 WLC에 로그인하여 회선 VTY 또는 HTTP(GUI)와 같은 게스트 사용자를 생성하기 위해 옵션에 할당되어야 합니다. 이러한 단계는 GUI에서 수행할 수 없으 므로 CLI에서 수행해야 합니다.

HTTP/GUI 인증:

Tim-eWLC1(config)#ip http authentication aaa login-authentication AutheTacMethod Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozTacMethod Tim-eWLC1(config)#end

HTTP 컨피그레이션을 변경할 때 HTTP 및 HTTPS 서비스를 다시 시작하는 것이 좋습니다.

Tim-eWLC1(config)#no ip http server Tim-eWLC1(config)#no ip http secure-server Tim-eWLC1(config)#ip http server Tim-eWLC1(config)#ip http secure-server Tim-eWLC1(config)#end 라인 VTY:

Tim-eWLC1(config)#line vty 0 15
Tim-eWLC1(config-line)#login authentication AutheTacMethod
Tim-eWLC1(config-line)#authorization exec AuthozTacMethod
Tim-eWLC1(config-line)#end

6단계. 원격 사용자를 정의합니다.로비 앰버서더의 ISE에서 생성된 사용자 이름은 WLC에서 원격 사용자 이름으로 정의되어야 합니다.원격 사용자 이름이 WLC에 정의되어 있지 않으면 인증이 올바 르게 진행되지만, Lobby Ambassador 권한에만 액세스하는 대신 WLC에 대한 전체 액세스 권한을 사용자에게 부여합니다.이 컨피그레이션은 CLI를 통해서만 수행할 수 있습니다.

CLI:

Tim-eWLC1(config)#aaa remote username lobbyTac

ISE 구성 - TACACS+

1단계. 디바이스 관리를 활성화합니다.Administration(관리) > System(시스템) > Deployment(구축))로 이동합니다.더 진행하기 전에 Enable Device Admin Service(디바이스 관리 서비스 활성화)를 선택하고 이미지에 표시된 대로 ISE가 활성화되었는지 확인합니다.

cise	de le	dentity	Services	Engine	Home	Context	Visibility	 Operations 	Polic	y ▼Adr	ministration	Work Cen	ters
•	Syste	m	Identity Ma	inagement	Network F	Resources	Device F	Portal Manager	ment pxGr	id Services	Feed Se	rvice + Thre	at Centric NAC
D	eployr	ment	Licensing	 Certificat 	es 🕨 Log	ging ►N	faintenance	Upgrade	Backup &	Restore	Admin Acces	ss 🕨 Setting	5
<u>ا</u>	Dep	loyme	nt			Deplo	yment Node	s List > timise	23				
	4	• 1	*		<u>نۇن</u>	Edit	Node						
	•	e Depl	oyment			Ge	neral Settings	s Profiling (Configuration				
	2	PAN 🗠	Failover										
						Ho	ostname		timise23				
						FC	2DN		timise23.cl	sco.com			
						N	Address de Type		Identity Ser	o.o rvices Enai	ne (ISE)		
							de type		,				
						R	ole STANDA		Make Pri	mary			
						\checkmark	Administ	tration					
							- Monitorin	10					
							· Monitoria	9					
							Role	e	PRIMA	ARY	, in the second s		
							Oth	er Monitoring N	lode				
						~	 Policy Set 	ervice					
							V V	Enable Session	Services (1)				
								Include N	ode in Node	Group Non	ie		Ð
							✓ E	Enable Profiling	Service 👔				
							<u></u> Е	Enable Threat (Centric NAC	Service 🕖			
							🗆 🕨 E	Enable SXP Se	rvice (i)				
							✓ E	Enable Device	Admin Servic	æ 👔			-

2단계. ISE에 WLC를 추가합니다.Administration(관리) > **Network Resources(네트워크 리소스)** > **Network Devices(네트워크 디바이스) > Add(추가)로 이동합니다**.WLC를 ISE에 추가한 때 TACACS+ Authentication Settings를 활성화하고 이미지에 표시된 대로 필요한 매개변수를 구성합니다.

dentity Services Engine	Home Contex	t Visibility	ations Policy	✓Administration	Work Centers		
System Identity Management		 Device Portal Ma 	nagement pxGrid S	ervices Feed Service	Threat Centric N	AC	
Network Devices Network Device C	Groups Network Dev	rice Profiles Externa	RADIUS Servers	RADIUS Server Sequence	s NAC Managers	External MDM Locati	ion Services
0							
Network Devices	Network Devi	ces					
Default Device		-		-			
Device Security Settings	/ Edit 🕂 Add	Duplicate	mport 💮 Export 👻	Generate PAC X De	lete 🔻		Show
	Name	 IP/Mask 	Profile Name	Location		Туре	Description
	Tim-eWLC1	192.168.166.7	aste Cisco 🕀	All Locati	ons	All Device Types	9800

이름, IP ADD, TACACS+ Authentication Settings(TACACS+ 인증 설정)를 제공하는 컨피그레이션 창이 열리면 필요한 공유 암호를 입력합니다.

3단계. ISE에서 로비 앰버서더 사용자를 생성합니다.Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자) > Add(추가)로 이동합니다.게스트 사용자를 생성할 로비 앰버서더에 할당된 사용자 이름 및 비밀번호로 ISE에 추가합니다.이미지에 표시된 대 로 관리자가 로비 앰배서더에 할당하는 사용자 이름입니다.

dentity Services Engine	Home	► Operations ► F	Policy Administration	Work Centers						
System Identity Management	Network Resources Devic	e Portal Management	pxGrid Services Feed	Service						
✓Identities Groups External Identit	y Sources Identity Source Sec	quences Settings								
0	0									
Users	Network Access Users									
Latest Manual Network Scan Results										
	/ Edit 🕂 Add 🔢 Chang	ge Status 👻 🎼 Import	Export - XDelete -	Duplicate						
	Status 👻 Name	D	Description	First Name Last Name						
	🗌 🗹 Enabled 👤 lobbyTa	ac								

구성 창이 열리면 로비 앰배서더 사용자의 이름과 암호를 입력합니다.또한 Status(상태)가 Enabled(활성화됨)인지 확인합니다.

4단계. 결과 TACACS+ 프로파일을 생성합니다.이미지에 표시된 대로 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Profiles(TACACS 프로파일)로 이동합니다.이 프로필을 사용하여 사용자를 로비 앰버서더로 배치하 려면 필요한 특성을 WLC에 반환합니다.

dentity Services Engine	Home Cor	ext Visibility	Operations	▶ Policy	Admini	stration	✓ Work Centers
Network Access Guest Access	► TrustSec ► E	OD Profiler	▶ Posture	- Device A	dministration	Passi	velD
► Overview ► Identities User Ident	ity Groups Ext I	Sources Ne	twork Resources	▼Policy	Elements	Device Adr	min Policy Sets
0							
▶ Conditions	TACACS F	rofiles					
Network Conditions	0 Selected						
▼ Results	${old C}$ Refresh	+ Add	Duplicate 💼	Trash -	🖸 Edit		
Allowed Protocols	Nan	Э		г	Гуре De	escription	
TACACS Command Sets	Defa	It Shell Profile		5	Shell De	fault Shell P	Profile
TACACS Profiles	Deny	All Shell Profile		5	Shell De	ny All Shell	Profile
	U WLC	ALL		V	VLC WI	_C ALL	
	U WLC	MONITOR		V	VLC WI	C MONITO	R

컨피그레이션 창이 열리면 프로필에 이름을 제공하고, Default Privileged 15 및 Custom Attribute as Type Mandatory(기본 권한 15 및 사용자 지정 특성 유형 필수)를 구성하고, 이름을 user-type(사용 자 유형) 및 value lobby-admin으로 지정합니다.또한 이미지에 표시된 대로 **공통 작업 유형**을 셸로 선택할 수 있습니다.

Task Attribute View	Raw View		
Common Tasks			
Common Task Type Shell	v		
Default Privilege	15	0	(Select 0 to 15)
Maximum Privileg	e	0	(Select 0 to 15)
Access Control Lis	st	0]
Auto Command		0]
No Escape		0	(Select true or false)
Timeout		0	Minutes (0-9999)
🔲 Idle Time		0	Minutes (0-9999)
Selected ★ Add	dit		
✓ Туре	Name	Value	
	user-type	lobby-admin	

5단계. 정책 세트를 생성합니다.이미지에 표시된 대로 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 세트)로 이동합니다 .정책을 구성하는 조건은 관리자 결정에 따라 달라집니다.이 문서에서는 Network Access-Username 조건 및 Default Device Admin 프로토콜이 사용됩니다.Authorization Policy(권한 부여 정 책)에서 Results Authorization(결과 권한 부여)에 구성된 프로파일이 선택되었는지 확인해야 합니 다. 그러면 필요한 특성을 WLC에 반환할 수 있습니다.

alialia cisco	Identity Se	vices Engine	Home	Context Visibili	ty > Operations	Polic	y 🕨 Adminis	stration	✓ Work Centers				Q	0	• •
► Ne	etwork Access	Guest Access	 TrustSec 	BYOD	Profiler Posture	- Device	Administration	 Pass 	iveID						
+ O1	verview 🕨 Id	entities User Iden	tity Groups	Ext Id Sources	Network Resource	s Po	icy Elements	Device Ad	Imin Policy Sets	Reports	Settings				
							_								
Poli	cy Sets													Reset	Save
+	Status	Policy Set Name		Description		Conditi	ons			Allo	wed Protocols /	Server Sequence	e Hits	Actions	s View
Sea	irch														
	Ø	9800TacacsLobby				Ŧ	Network Access EQUALS lobby	⊡serNam /Tac	e	De	fault Device Admi	n × • +	• •	¢	>

구성 창이 열리면 권한 부여 정책을 구성합니다.인증 정책은 이미지에 표시된 대로 기본값으로 둘 수 있습니다. Policy Sets → 9800TacacsLobby

Reset Save

	Status Policy Set Name Description Conditions									e Hits	
Search											
	0	9800TacacsLobby		Network Access-UserName EQUAL	Network Access UserName EQUALS lobbyTac						
> Auth	Authentication Policy (1)										
> Auth	Authorization Policy - Local Exceptions										
> Auth	orization	Policy - Global Exceptions									
∀ Auth	orization	Policy (2)									
						Results					
÷	Status	Rule Name	Conditions			Command Sets	Shell Pro	files	Hits	Actions	
Searc	h										
	ø	9800TacacsAuth	Network Access-UserNam	ne EQUALS lobbyTac		Select from list	+ 9800Tac	acsLobby × v	+ 0	٥	

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

show	run	aaa
show	run	sec remote
show	run	sec http
show	aaa	method-lists authentication
show	aaa	method-lists authorization
show	aaa	servers
show	taca	acs
이는	성공	공적인 인증 후 로비 앰배서더 GUI의 모양입니다.

Q Search Menu Items	+ Add × Delete			
	User Name	V. Description	 Created By 	Ч.
	H 4 0 F H 10 v items	per page		No items to display

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

RADIUS 인증

RADIUS 인증의 경우 다음 디버그를 사용할 수 있습니다.

Tim-eWLC1#debug aaa authentication Tim-eWLC1#debug aaa authorization Tim-eWLC1#debug aaa attr Tim-eWLC1#terminal monitor 디버그에서 올바른 메서드 목록을 선택했는지 확인합니다.또한 필요한 특성은 ISE 서버에서 올바 른 사용자 이름, 사용자 유형 및 권한을 사용하여 반환됩니다.

Tim-eWLC1#undebug all

Feb 5 02:06:48.267: TPLUS: Queuing AAA Authorization request 0 for processing Feb 5 02:06:48.267: TPLUS: Authorization request created for O(lobbyTac) Feb 5 02:06:48.267: TPLUS: Using server 192.168.166.8 Feb 5 02:06:48.279: TPLUS(0000000)/0/7FB7819E2100: Processing the reply packet Feb 5 02:06:48.279: TPLUS: Processed AV priv-lvl=15 Feb 5 02:06:48.279: TPLUS: Processed AV user-type=lobby-admin Feb 5 02:06:48.279: TPLUS: received authorization response for 0: PASS 이전에 RADIUS 및 TACACS+에 대해 언급된 디버그 예에는 성공적인 로그인을 위한 주요 단계가 있습니다.디버그가 더 자세히 표시되고 출력이 더 커집니다.디버그를 비활성화하려면 다음 명령을 사용할 수 있습니다.

권한 부여 단계 예:

Feb 5 02:06:48.245: TPLUS: Queuing AAA Authentication request 0 for processing Feb 5 02:06:48.245: TPLUS: Authentication start packet created for O(lobbyTac) Feb 5 02:06:48.245: TPLUS: Using server 192.168.166.8 Feb 5 02:06:48.250: TPLUS: Received authen response status GET_PASSWORD (8) Feb 5 02:06:48.266: TPLUS(0000000)/0/7FB7819E2100: Processing the reply packet Feb 5 02:06:48.266: TPLUS: Received authen response status PASS (2)

인증 단계 예:

Tim-eWLC1#debug tacacs Tim-eWLC1#terminal monitor 인증이 올바른 사용자 이름 및 ISE IP ADD로 처리되는지 확인합니다.또한 "PASS" 상태를 확인해 야 합니다.동일한 디버깅에서 인증 단계 바로 다음에 권한 부여 프로세스가 표시됩니다.이 권한 부 여 단계에서는 올바른 사용자 이름이 올바른 ISE IP ADD와 함께 사용되도록 합니다.이 단계에서는 WLC를 적절한 권한을 가진 로비 앰버서더 사용자로 표시하는 ISE에 구성된 특성을 볼 수 있습니다

TACACS+ 인증의 경우 이 디버그를 사용할 수 있습니다.

7FBA5500C870 0 00000081 username(450) 5 lobby

TACACS+ 인증

Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(1): 7FBA5500C8B0 0 00000001 user-type(1187) 4 lobby-admin Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(2): 7FBA5500C8F0 0 00000001 priv-lvl(335) 4 15(F) Feb 5 02:35:27.683: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host 192.168.166.104 by user 'lobby' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256'