# ACS 5.2 및 WLC로 PEAP 및 EAP-FAST 구성

## 목차

<u>소개</u> 사전 요구 사항 요구 사항 사용되는 구성 요소 표기 규칙 구성 네트워크 다이어그램 가정 컨피그레이션 단계 RADIUS 서버 구성 네트워크 리소스 구성 사용자 구성 정책 요소 정의 액세스 정책 적용 WLC 구성 인증 서버의 세부 정보를 사용하여 WLC 구성 VLAN(Dynamic Interface) 구성 WLAN(SSID) 구성 무선 클라이언트 유틸리티 구성 PEAP-MSCHAPv2(user1) EAP-FAST(사용자2) 다음을 확인합니다. <u>사용자1(PEAP-MSCHAPv2) 확인</u> 사용자2(EAP-FAST) 확인 문제 해결 트러블슈팅 명령 관련 정보

# 소개

이 문서에서는 ACS(Access Control Server) 5.2와 같은 외부 RADIUS 서버를 사용하여 EAP(Extensible Authentication Protocol) 인증을 위해 WLC(Wireless LAN Controller)를 구성하는 방법에 대해 설명합니다.

# 사전 요구 사항

## 요구 사항

이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- WLC 및 LAP(Lightweight Access Point)에 대한 기본 지식 보유
- AAA 서버에 대한 기능적 지식이 있어야 합니다
- 무선 네트워크 및 무선 보안 문제에 대한 철저한 지식 보유

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 7.0.220.0을 실행하는 Cisco 5508 WLC
- Cisco 3502 Series LAP
- Intel 6300-N 드라이버 버전 14.3의 Microsoft Windows 7 기본 신청자
- 버전 5.2를 실행하는 Cisco Secure ACS
- Cisco 3560 Series 스위치

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 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 표기 규칙</u>을 참조하십시오.

## 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 섹션에 사용된 <u>명령에</u> 대한 자세한 내용을 보려면<u>명령</u> 조회<u>도구(</u>등록된 고객만 해당)를 사용하십시오.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



다음은 이 다이어그램에서 사용되는 구성 요소의 컨피그레이션 세부 정보입니다.

- ACS(RADIUS) 서버의 IP 주소는 192.168.150.24입니다.
- WLC의 관리 및 AP 관리자 인터페이스 주소는 192.168.75.44입니다.
- DHCP 서버 주소는 192.168.150.25입니다.
- VLAN 253은 이 컨피그레이션 전체에서 사용됩니다. 두 사용자 모두 동일한 SSID "goa"에 연 결됩니다. 그러나 user1은 PEAP-MSCHAPv2를 사용하여 인증하고 user2는 EAP-FAST를 사 용하여 인증하도록 구성됩니다.
- 사용자는 VLAN 253에서 할당됩니다.
  - · VLAN 253: 192.168.153.x/24. 게이트웨이: 192.168.153.1
  - · VLAN 75: 192.168.75.x/24. 게이트웨이: 192.168.75.1

## 가정

- 스위치는 모든 레이어 3 VLAN에 대해 구성됩니다.
- DHCP 서버에는 DHCP 범위가 할당됩니다.
- 레이어 3 연결은 네트워크의 모든 디바이스 간에 존재합니다.
- LAP가 이미 WLC에 연결되어 있습니다.
- 각 VLAN에는 /24 마스크가 있습니다.
- ACS 5.2에는 자체 서명 인증서가 설치되어 있습니다.

# 컨피그레이션 단계

이 컨피그레이션은 세 개의 상위 레벨 단계로 구분됩니다.

- 1. <u>RADIUS 서버를 구성합니다.</u>
- 2. <u>WLC를 구성합니다.</u>
- 3. <u>무선 클라이언트 유틸리티를 구성합니다.</u>

# RADIUS 서버 구성

RADIUS 서버 컨피그레이션은 4단계로 나뉩니다.

- 1. <u>네트워크 리소스를 구성합니다.</u>
- 2. <u>사용자를 구성합니다.</u>
- 3. 정책 요소를 정의합니다.
- 4. <u>액세스 정책을 적용합니다.</u>

ACS 5.x는 정책 기반 액세스 제어 시스템입니다. 즉, ACS 5.x는 4.x 버전에서 사용된 그룹 기반 모 델 대신 규칙 기반 정책 모델을 사용합니다.

ACS 5.x 규칙 기반 정책 모델은 이전의 그룹 기반 접근 방식에 비해 더 강력하고 유연한 액세스 제 어를 제공합니다.

이전 그룹 기반 모델에서 그룹은 세 가지 유형의 정보를 포함하고 연결하므로 정책을 정의합니다.

- ID 정보 이 정보는 AD 또는 LDAP 그룹의 멤버십 또는 내부 ACS 사용자에 대한 정적 할당을 기반으로 할 수 있습니다.
- 기타 제한 또는 조건 시간 제한, 장치 제한 등
- 권한 VLAN 또는 Cisco IOS<sup>®</sup> 권한 레벨

ACS 5.x 정책 모델은 다음 형식의 규칙을 기반으로 합니다.

• 조건이 충족되면

예를 들어, 그룹 기반 모델에 대해 설명된 정보를 사용합니다.

• ID-condition, restriction-condition, authorization-profile이 있는 경우

따라서 사용자가 네트워크에 액세스할 수 있는 조건은 물론 특정 조건이 충족될 때 허용되는 권한 부여 수준도 제한할 수 있는 유연성을 제공합니다.

네트워크 리소스 구성

이 섹션에서는 RADIUS 서버의 WLC에 대해 AAA 클라이언트를 구성합니다.

이 절차에서는 WLC가 사용자 자격 증명을 RADIUS 서버에 전달할 수 있도록 WLC를 RADIUS 서 버에 AAA 클라이언트로 추가하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

1. ACS GUI에서 Network Resources(네트워크 리소스) > Network Device Groups(네트워크 디바이스 그룹) > Location(위치)으로 이동하여 Create(생성)를 클릭합니다(맨 아래).

cisco Cisco Secure A	CS
+ 🛞 My Workspace	Network Resources > Network Device Groups > Location
🔹 🌗 Network Resources	Network Device Groups
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter: _ Match if:
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name Description     All Locations
Users and Identity Stores	
▹ Spolicy Elements	
Access Policies	
<ul> <li>Monitoring and Reports</li> </ul>	
🕞 😹 System Administration	

2. 필수 필드를 추가하고 Submit(제출)을 클릭합니다.

- Nama		
o Name.	LAB	
Description:	LAB Devices	
o Parent	All Locations	Select
= Required field	elds	

이제 다음 화면을 볼 수 있습니다.

cisco Cisco Secure A	CS
🕨 🥳 My Workspace	Network Resources > Network Device Groups > Location
👻 🦣 Network Resources	Network Device Groups
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter: Match if:
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Image: Name     ▲     Description       Image: The second secon
Busers and Identity Stores     Store	LAB LAB Devices
Policy Elements	
Access Policies	
Monitoring and Reports	
System Administration	

3. Device Type(디바이스 유형) > Create(생성)를 클릭합니다.

cisco Cisco Secure ACS			
🕨 🥵 My Workspace	Network Resources > Network Device Groups > Device Type > Create		
	Device Group - General         Image: State         Image: State	Select	
Users and Identity Stores			
Policy Elements			
Access Policies			
<ul> <li>Monitoring and Reports</li> </ul>			
<ul> <li>System Administration</li> </ul>			

4. Submit(제출)을 클릭합니다. 이제 다음 화면을 볼 수 있습니다.

	cisco Cisco Secure A	CS
	🕨 💮 My Workspace	Network Resources > Network Device Groups > Device Type
	Ip Network Resources	Network Device Groups
	Network Device Groups     Location     Device Type	Filter: ▼ Match if: ▼ Go ▼
	Network Devices and AAA Clients	Name  Description
	Default Network Device External RADIUS Servers	All Device Types All Device Types
	B Users and Identity Stores	5508 Wireless LAN Controller
	Policy Elements	
	Access Policies	
	Monitoring and Reports	
ł	System Administration	

- 5. Network Resources(네트워크 리소스) > Network Devices and AAA Clients(네트워크 디바이 스 및 AAA 클라이언트)로 이동합니다.
- 6. Create(생성)를 클릭하고 여기에 표시된 대로 세부 정보를 입력합니다.

► S MyWorkspace	Network Resources > Net	etwark Devices and AAA Clerks > Create		
Ketwork Resources     Network Device Groups     Location     Device Type     Network Devices and AAACtionts     Default Network Device     External RACIUS Servers	o Name: W. Description W. Network Device Gr Location Device Type	LC-5508 reless LAN Controller resp All Locations:LAB All Device Types:5508	Ssiect	
Busers and Identity Stores     Policy Elements     C. Access Policies     Monitoring and Reports	IP Address © Single IP Address © IP Range(s) 9 IP: 192 168 75 44		Authentication Options   TACAC8+	
<ul> <li>System Administration</li> </ul>			CoAport (170) Enable Key Key Encryption Message Author Key Input Form	Witap Key: enticator Code Key: enti C ABCII © HEXADECIMAL

7. Submit(제출)을 클릭합니다. 이제 다음 화면을 볼 수 있습니다.

etwo	TK Devices				
filler.		<ul> <li>Match It.</li> </ul>	•	G0 🔻	
-	Name 4	IP / Mask	NDG:Location	NDG:Device Type	Description
	WLC-5508	192.168.75.44/32	All Locations:LAB	All Device Types:5508	Wireless LAN Controller

사용자 구성

이 섹션에서는 ACS에서 로컬 사용자를 생성합니다. 두 사용자(user1 및 user2)는 모두 "무선 사용 자"라는 그룹에 할당됩니다.

1. Users and Identity Stores(사용자 및 ID 저장소) > Identity Groups(ID 그룹) > Create(생성)로 이동합니다.

cisco Cisco Secure A	CS
> 😚 My Workspace	Users and identity Stores > Identity Groups > Create
In the sources	Constant of the second s
Overs and identity Stores      Identity Groups      Internal identity Stores      Users      Hosts	General       Image: Market       Description: Wireless Users authenticating over wireless       Image: Operation Parent       All Groups
External Identity Stores     LDAP     Active Directory     RSA SecurID Token Servers     RADIUS Identity Servers     Certificate Authorities     Certificate Authentication Profile     Identity Store Sequences     So Policy Elements	

2. Submit(제출)을 클릭하면 페이지가 다음과 같이 표시됩니다.

cisco Cisco Secure Ad	CS		
🕨 🖓 My Workspace	Users and identity Stores > identity Groups		
<ul> <li>Network Resources</li> <li>Users and Identity Stores</li> <li>Identity Groups</li> <li>Internal Identity Stores</li> <li>Users</li> <li>Hosts</li> <li>External Identity Stores</li> <li>LDAP</li> <li>Active Directory</li> </ul>	Identity Groups		
	Filler: 💌 Match it: 💌 Go 🔝		
	Name      Description      * <u>All Groups</u> Identity Group Root      Wisclass Users authoritization prevaipless		
	Wreless Users Wireless Osers authenticating over wireless		
RSA SecurID Tokan Servers RADIUS Identity Servers Certificate Authorities Certificate Authorities Identity Store Sequences			
Policy Elements			

- 3. 사용자 user1 및 user2를 생성하고 "Wireless Users" 그룹에 할당합니다.
  - a. Users and Identity Stores(사용자 및 ID 저장소) > Identity Groups(ID 그룹) > Users(사 용자) > Create(생성)를 클릭합니다.



b. 마찬가지로 user2를 생성합니다.

cisco Cisco Secure A	CS
🖌 🥳 My Workspace	Users and Identity Stores > Internal Identity Stores > Users > Create
An Network Resources	Created
🐨 🎬 Users and identity Stores (2002)	© Name: User2 Status: Enabled T @
Identity Groups	Description: EAPFAST user
<ul> <li>Internal Identity Stores</li> <li>Users</li> </ul>	o Identity Group: All Groups: Wireless Users Select
Hosts External identity Stores Certificate Authorities Certificate Authorities Identity Store Sequences	Password Information Password must • Contain 4 - 32 characters
Policy Elements	Password:
Access Policies	Confirm     Password:
Monitoring and Reports	Change password on next login
<ul> <li>R System Administration</li> </ul>	User Information There are no additional identity attributes defined for user records • - Required fields

화면은 다음과 같습니다.

cisco Cisco Secure A		e a laternal identity Star	as > lines	
Network Resources      Users and Identity Stores	Internal Users			
Identity Groups   Internal Identity Stores Users Users Users	Filter:	User Name	Identity Group     All Groups:Wireless Users	Description PEAP:mschapv2 users
External Identity Stores     Certificate Authorities     Certificate Authorities     Identity Store Sequences	Г <del>0</del>	user2	All Groups:Wireless Users	EAPFAST user
S. Policy Elements				

## 정책 요소 정의

Permit Access(액세스 허용)가 설정되어 있는지 확인합니다.

cisco Cisco Secure A	ics
+ 💮 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
Network Resources	Authorization Profiles
+ 🏭 Users and Identity Stores	Either Watch if Go V
👻 🌍 Policy Elements	
► Session Conditions	Name - Description
Authorization and Permissions	Permit Access
Authorization Profiles	
<ul> <li>Device Administration</li> </ul>	
<ul> <li>Named Permission Objects</li> </ul>	
Access Policies	
<ul> <li>Monitoring and Reports</li> </ul>	
System Administration	

## 액세스 정책 적용

이 섹션에서는 사용할 인증 방법과 규칙을 구성하는 방법을 선택하겠습니다. 이전 단계를 기반으로 규칙을 생성합니다.

다음 단계를 완료하십시오.

1. Access Policies(액세스 정책) > Access Services(액세스 서비스) > Default Network Access(기본 네트워크 액세스) > Edit: "Default Network Access(기본 네트워크 액세스)"로 이 동합니다.

cisco Cisco Secure A	CS
+ 💮 My Workspace	Access Policies > Access Services > Default Network Access > Edit "Default Network Access"
Interview Resources	
Users and Identity Stores	General Allowed Protocols
► 🎭 Policy Elements	Name: Default Network Access
👻 🌉 Access Policies	Description: Default Network Access Service
Access Services     Bervice Selection Rules	Service Type : Network Access 🔽
O Default Device Admin	Policy Structure
Default Network Access	✓ Identity
► Ø deleterne	Group Mapping
Monitoring and Reports	Authorization
🕞 🍓 System Administration	

2. 무선 클라이언트에서 인증할 EAP 방법을 선택합니다. 이 예에서는 PEAP- MSCHAPv2 및 EAP-FAST를 사용합니다.

cisco Cisco Secure AC	cis
🕨 🧭 My Workspace	Access Policies > Access Services > Default Network Access > Edit "Default Network Access"
+ 🎲 Network Resources	
Big Users and Identity Stores	General Allowed Protocols
Policy Elements	Process Host Lookup
🖌 🌉 Access Policies	Authentication Protocols
Access Services     Access Services     Service Selection Rules     O Default Device Admin     O Default Network Access	Allow PAP/ASCI      Allow CHAP
Identity Authorization ► Ø deleterne	<ul> <li>M Allow MS-CHAPv1</li> <li>M Allow MS-CHAPv2</li> </ul>
Monitoring and Reports      System Administration	► 🕅 Allow EAP-MD5
· · · · · · · · · · · · · · · · · · ·	Allow EAP-TLS
	Allow LEAP
	Allow PEAP
	Allow EAP-FAST
	Preferred EAP protocol LEAP

• 🐁 Access Policies	► Allow LEAP
Access Services     El Service Selection Rules     @ Default Device Admin     @ Default Network Access     Idently     Authorization     @ deleteme     @ Monitoring and Reports     @ System Administration	<ul> <li>✓ Allow PEAP</li> <li>PEAP Inner Methods</li> <li>✓ Allow EAP-MS-CHAPv2</li> <li>✓ Allow Password Change Retries: 1</li> <li>✓ Allow EAP-GTC</li> <li>✓ Allow Password Change Retries: 1</li> </ul>
	<ul> <li>Now EAP-FAST</li> <li>EAP-FAST Inner Methods</li> <li>Allow EAP-MS-CHAPV2</li> <li>Allow Password Change Retries: 3</li> <li>Allow EAP-GTC</li> <li>Allow TLS-Renegotiation</li> <li>Use PACs DontUse PACs</li> <li>Tunnel PAC Time To Live: 90 Days v</li> <li>Proactive PAC update will occur after 10 % of PAC Time To Live has expired</li> <li>Allow Authenticated in-Band PAC Provisioning</li> <li>Server Returns Access Accept After Authenticsted Provisioning</li> <li>Barver Returns Access Accept After Authenticsted Provisioning</li> <li>Allow Machine Authentication</li> <li>Machine PAC Time To Live: 1 Weeks v</li> <li>Enable Stateless Bession Resume</li> <li>Authorization PAC Time To Live: 1 Hours v</li> </ul>

- 3. Submit(제출)을 클릭합니다.
- 4. 선택한 ID 그룹을 확인합니다. 이 예에서는 ACS에서 생성한 Internal Users를 사용합니다. 변 경 사항을 저장합니다.

Access Policies >	Access Services > Default Network Access > Identity ult selection C Rule based result selection
Identity Source:	Internal Users Select
	- Advanced Options
	If authentication failed Reject 💌
	If user not found Reject 💌
	If process failed Drop 💌
	Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected

5. 권한 부여 프로파일을 확인하려면 Access Policies(액세스 정책) > Access Services(액세스 서

비스) > Default Network Access(기본 네트워크 액세스) > Authorization(권한 부여)으로 이동 합니다.

네트워크에 대한 사용자 액세스를 허용할 조건 및 인증 후 전달 할 인증 프로파일 (특성) 하에 서 사용자 정의 할 수 있습니다. 이 세분화는 ACS 5.x에서만 사용할 수 있습니다. 이 예에서는 Location, Device Type, Protocol, Identity Group, EAP Authentication Method를 선택했습니다 (예:



- 6. OK(확인)를 클릭하고 Save Changes(변경 사항 저장)를 클릭합니다.
- 7. 다음 단계는 규칙을 생성하는 것입니다. 정의된 규칙이 없는 경우 클라이언트는 조건 없이 액 세스가 허용됩니다.

Create(생성) > Rule-1을 클릭합니다. 이 규칙은 "무선 사용자" 그룹의 사용자를 위한 것입니 다.

Access Policies > Access Services > Det	ault Network Access > Authorization					
Standard Policy Exception Policy						
Network Access Aethorization Pc	lines.					
Filter: Status	Cisco Secure ACS - Mosilla Firefox				×	
E	192160150.24 https://192168.	150.24/acsadmin/Policy	InputAction.do		合	
) Status Hame NE			-			
No data to display	General					
	Name: Rule-1	Status: Enabled	- 0			
	Conditions	ution in the lower rig and results are avail	ht area of the policy rules screen con able here for use in policy rules.	ntrois which		
	MDG:Location:	in	All Locations LAB	Select		
	P NDG Device Type:	in	All Device Types:5508	Select		
	Protocol:	match	• Radus	Select		
	M Identity Group:	j in	Groups Wireless Users	Select		
	Cancel	-ANY-	You may select multiple authorization pro defined in multiple profiles will use the vi profile defined.	files. Attributes	rst Help	
Create I. Duplicate I. Edit	Delete				Customize	HtCount

8. 변경 사항을 저장합니다. 화면은 다음과 같습니다.

CONTRACTOR OF	ACCESS NO	thorization Policy					
iter. St	atus	- Mate	ch it. Equals 💽 Enat	led - Ci	ear Filter Go 🔻		
Status	Name	NDG:Location	NDG Device Type	Condition Protocol	identity Group	Esp Authentication Method	Results Authorization Profil
	Rule-1	in All Locations:LAB	In All Device Types 5508	match Radius	in All Groups:Wireless Users	-ANY-	Permit Access
Detaut	_	The rules defined or r	no enabled role matches.				Permit Access

조건과 일치하지 않는 사용자를 거부하도록 하려면 기본 규칙을 편집하여 "액세스 거부"라고 말합니다.

9. 이제 서비스 선택 규칙을 정의하겠습니다. 수신 요청에 적용할 서비스를 결정하는 단순 또는

규칙 기반 정책을 구성하려면 이 페이지를 사용합니다. 이 예에서는 규칙 기반 정책이 사용됩니다.

Acc	ess Pr	gle re:	Access	Senices > tion @ F	Service Selection Rules Rule based result selection								
8	Service Selection Policy												
F	Filter: Status 💌 Match it Equals 💌 Enabled 💌 Clear Filter 🛛 Go 🔝												
			Status	Name	Conditions Protocol		Results Service	Hit Count					
	1		۲	Rule-1	match Radius		Default Network Access	0					
	2		8	Rule-2	match Tacacs		Default Device Admin	0					

# WLC 구성

이 컨피그레이션에는 다음 단계가 필요합니다.

- 1. <u>인증 서버의 세부 정보를 사용하여 WLC를 구성합니다.</u>
- 2. <u>VLAN(Dynamic Interface)을 구성합니다.</u>
- 3. <u>WLAN(SSID)을 구성합니다.</u>

인증 서버의 세부 정보를 사용하여 WLC 구성

클라이언트를 인증하기 위해 RADIUS 서버와 통신할 수 있도록 WLC를 구성하고 다른 트랜잭션에 도 구성해야 합니다.

다음 단계를 완료하십시오.

- 1. 컨트롤러 GUI에서 Security(보안)를 클릭합니다.
- 2. RADIUS 서버의 IP 주소 및 RADIUS 서버와 WLC 간에 사용되는 공유 암호 키를 입력합니다.

이 공유 암호 키는 RADIUS 서버에 구성된 것과 동일해야 합니다.

cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Security	RADIUS Authenti	cation Server	s > New					
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Falback</li> <li>TACACS+</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> </ul>	Server Index (Priorit Server IP Address Shared Secret Form Shared Secret Confirm Shared Sec Key Wrap Port Number	ty) st ret	1 • 192.168.150.2 ASCII • ••••• (Designed for 1812	FIPS custom	ers and requires a	key wrap compl	iant RAD	IUS server)
Local EAP	Support for RFC 357	6	Enabled -					
Priority Order	Server Timeout		Z second	a				
Certificate	Network User		🗷 Enable					
Access Control Lists	Management		🗵 Enable					
Wireless Protection     Policies	IPSec		Enable					
Web Auth								
Advanced								

VLAN(Dynamic Interface) 구성

이 절차에서는 WLC에서 동적 인터페이스를 구성하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

1. 동적 인터페이스는 컨트롤러 GUI의 Controller(컨트롤러) > Interfaces(인터페이스) 창에서 구 성합니다.

cisco		WLANs		WIRELESS	SECURITY	MANAGEMENT
CISCO Controller General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server	MONITOR Interfaces Interface VLAN Id	WLANS > New Name [	CONTROLLER vlan253 253	WIRELESS		MANAGEMENT
<ul> <li>Mobility Management</li> <li>Ports</li> <li>NTP</li> <li>CDP</li> <li>Advanced</li> </ul>						

2. 적용을 클릭합니다.

그러면 이 동적 인터페이스의 Edit(수정) 창(여기서는 VLAN 253)으로 이동합니다.

3. 이 동적 인터페이스의 IP 주소 및 기본 게이트웨이를 입력합니다.

	MONITOR WLANS C	ONTROLLER	WIRELESS	<u>s</u> ecurity	MANAGEMENT
Controller	Interfaces > Edit				
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP CDP Advanced	Configuration Guest Lan Quarantine Quarantine Quarantine Information	vlan253 00;24;97	7:09:03:cf		-
	The interface is attached Enable Dynamic AP	d to a LAG.			
	Management Interface Address				
	VLAN Identifier	253			
	IP Address	192.168.153	.81		
	Netmask	255.255.255	i.0		
	Gateway	192.168.153	1.1		
	DHCP Information				
	Primary DHCP Server Secondary DHCP Serve	r	2.168.150.25		
	Access Control List				
	ACL Name	n.	ne 🖃		
	Note: Changing the Interfa temporarily disabled and to some clients.	ica paramatara hus may result	causes the Wi in loss of conn	Alls to be ectivity for	

4. 적용을 클릭합니다.

5. 구성된 인터페이스는 다음과 같습니다.

cisco	MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT		IDS HELP	FEEDBACK	
Controller	Interfaces	1								
General Inventory	Interface	Name	1	/LAN Identifier	IP Addres	s Interfa	се Туре С	Dynamic AP I	Management	
Interfaces	manageme	nt	;	75	192.168.75	.44 Static	E	Enabled		
Interface Groups	service-por	<u>t</u>	,		0.0.0.0	Static	1	Vot Supported		
Multicast	virtual		1	WA.	1.1.1.1	Static	,	vot Supported		
Network Routes	vlan253		:	253	192.168.15	3.81 Dynamic	. [	Disabled		
Internal DHCP Server										
Mobility Management										
Ports										
NTP										
CDP										
Advanced										

## WLAN(SSID) 구성

이 절차에서는 WLC에서 WLAN을 구성하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

- 1. 컨트롤러 GUI에서 WLANs(WLAN) > Create New(새로 만들기)로 이동하여 새 WLAN을 생성 합니다. New WLANs(새 WLAN) 창이 표시됩니다.
- 2. WLAN ID 및 WLAN SSID 정보를 입력합니다.

어떤 이름이든 WLAN SSID로 입력할 수 있습니다. 이 예에서는 goa를 WLAN SSID로 사용합니다.

uluulu cisco		<u>W</u> LANs		W]RELE5S	SECURITY	MANAGEMENT	COMMANDS
WLANS	WLANs >	New					
<ul> <li>WLANS</li> <li>Advanced</li> </ul>	Type Profile Na SSID ID	9776	WLAA goo goo 1				

3. Apply(적용)를 클릭하여 WLAN 경로의 Edit(편집) 창으로 이동합니다.

cisco			WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
WLANs	WLANs > Edit 'ge	ba'					
WLANS WLANS	General Secur	ity QoS	Advanced				
<ul> <li>Advanced</li> <li>AP Groups</li> </ul>	Profile Name Type SSID Status Security Policies Radio Policy Interface/Interfac Group(G) Multicast Man Feat Broadcast SSID	goa WLAN goa [WPA2]] (Modificati [All ture ☐ Enable P Enable	ed Auth(802.1X ons done under U	+ CCKM)] r security tab (	will appear after ap	oplying the chang	yes.)

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY
WLANs	WLANs > Edit 'goa'
WLANS WLANS	General Security QoS Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Løyer 2 Security VPA+WPA2 -
	WPA+WPA2 Parameters
	WPA Policy
	WPA2 Policy R WPA2 Encryption RAES TRIP
	Auth Key Mgmt 802.1X+CCKN .

WLANs > Edit 'goa'		
General Security QoS	Advanced	
Layer 2 Layer 3 AAA Ser	vers	
Select AAA servers below to over	ide use of default servers on this WLAN	
Radius Servers		LDAP Servers
Radius Server Overwrite interface	Enabled	Server 1 None •
	Authentication Servers Accounting Servers	Server 2 None 💌
	Enabled Enabled	Server 3 None 💌
Server 1	IP:192.168.150.24, Port:1812 V None V	
Server 2	None v None v	
Server 3	None × None ×	
Local EAP Authentication		
Local EAP Authentication Enabl	ed	
Authentication priority order for	0r	
web-auth user		
Not Used	Order Used For Authentication	
•		

### WLANs > Edit 'goa'

Advanced	
Allow AAA Override Enabled	DHCP
Coverage Hole Detection P Enabled	DHCP Server Override
Enable Bession Timeout	
Aironet IE Renabled	DHCP Addr. Assignment 🏼 Required
Diagnostic Channel TEnabled	Management Frame Protection (MFP)
IPv6 Enable 2	MED Client Protection # Disabled
Override Interface ACL None -	
P2P Blocking Action Disabled -	DTIM Period (in beacon intervals)
Client Exclusion 2 Canabled	802.11a/n (1 - 255) 1
Maximum Allowed	802.11b/g/n (1 - 255) 1
Chente -	NAC
Static IP Tunneling 😰 🗆 Enabled	NAC State None -
Channel Scanning Defer	Load Balancing and Band Select
Scan Defer Priority 0 1 2 3 4 5 6 7	Client Load Balancing
	Client Band Select 4
Scan Defer Time(msecs) 100	Parcelus Client

# 무선 클라이언트 유틸리티 구성

PEAP-MSCHAPv2(user1)

테스트 클라이언트에서는 14.3 드라이버 버전을 실행하는 Intel 6300-N 카드와 함께 Windows 7 기 본 신청자를 사용하고 있습니다. 공급업체의 최신 드라이버를 사용하여 테스트하는 것이 좋습니다.

WZC(Windows Zero Config)에서 프로필을 생성하려면 다음 단계를 완료하십시오.

- 1. 제어판 > 네트워크 및 인터넷 > 무선 네트워크 관리로 이동합니다.
- 2. Add(추가) 탭을 클릭합니다.
- 3. Manually create a network profile을 클릭합니다.

	ally connect to a wireless network	
How do	you want to add a network?	
*	Manually create a network profile This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).	
Ą	Create an ad hoc network This creates a temporary network for sharing files or an Internet connection	
		and

4. WLC에 구성된 대로 세부사항을 추가합니다.

참고: SSID는 대/소문자를 구분합니다.

5. Next(다음)를 클릭합니다.

2-Enterprise			
2-Enterprise			
	•		
	-		
	H	lide characters	
tically			
is not broadcasting			
3	atically is not broadcasting	atically is not broadcasting	Hide characters     dis not broadcasting

6. 설정을 다시 확인하려면 연결 설정 변경을 클릭합니다.

Manually connect to a wireless network		
Successfully added goa		
Change connection settings Open the connection properties so that I can chan	ge the settings.	
	Close	

7. PEAP가 활성화되어 있는지 확인합니다.

goa Wireless Network Pr	operties	23
Connection Security		
	[	
Security type:	WPA2-Enterprise	
Encryption type:	AES 👻	
Choose a network aut	hentication method:	
Microsoft: Protected E	EAP (PEAP) 🔻 Settings	
Remember my cred	lentials for this connection each	
time I'm logged on		
Advanced settings		
	OK	ncel

goa Wireless Network Properties	x
Connection	
Security type: WPA2-Enterprise	
Encryption type: AES -	
Choose a network authentication method: Microsoft: Protected EAP (PEAP)  Settings Remember my credentials for this connector codin time I'm logged on Advanced settings	
OK Cance	

 이 예에서는 서버 인증서의 유효성을 검사하지 않습니다. 이 확인란을 선택했지만 연결할 수 없는 경우 기능을 비활성화하고 다시 테스트해 보십시오.

Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
AAA Certificate Services
C AddTrust External CA Root
Class 3 Public Primary Certification Authority
Class 3 Public Primary Certification Authority
DigiCert Assured ID Root CA
DigiCert High Assurance EV Root CA
DST ROOT CA X3
Do not prompt user to authorize new servers or trusted
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Enable Fast Reconnect
Enforce Network Access Protection
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
UK Cancel

지 않습니다. OK(확인)를 클릭합니다.



10. 사용자 이름과 비밀번호를 구성하려면 Advanced settings를 클릭합니다.

Connection Security	
Security type: WPA2-Enterprise   Encryption type: AES	
Choose a network authentication method: Microsoft: Protected EAP (PEAP) ▼ Settings Remember my credentials for this connection each time I'm logged on	
Advanced settings	
OK Cance	

Advanced settings
802.1X settings 802.11 settings
Specify authentication mode:
User authentication    Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds): 10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK Cancel

mputer to connect to the network le, to download updates).
ie, to download updates).

클라이언트 유틸리티에 연결할 준비가 되었습니다.

EAP-FAST(사용자2)

테스트 클라이언트에서는 14.3 드라이버 버전을 실행하는 Intel 6300-N 카드와 함께 Windows 7 기 본 신청자를 사용하고 있습니다. 공급업체의 최신 드라이버를 사용하여 테스트하는 것이 좋습니다.

WZC에서 프로파일을 생성하려면 다음 단계를 완료하십시오.

1. 제어판 > 네트워크 및 인터넷 > 무선 네트워크 관리로 이동합니다.

2. Add(추가) 탭을 클릭합니다.

3. Manually create a network profile을 클릭합니다.





4. WLC에 구성된 대로 세부사항을 추가합니다.

참고: SSID는 대/소문자를 구분합니다.

5. Next(다음)를 클릭합니다.

Network name:	goa	٦
Security type:	WPA2-Enterprise	
Encryption type:	AES 🔹	
Security Key:	Hide character	s
Start this connect	tion automatically	
Connect even if	the network is not broadcasting	

6. 설정을 다시 확인하려면 연결 설정 변경을 클릭합니다.

Manually connect to a wireless network	
Successfully added goa	
Change connection settings Open the connection properties so that I can change the settings.	
	Close

7. EAP-FAST를 활성화했는지 확인합니다.

참고: 기본적으로 WZC에는 인증 방법으로 EAP-FAST가 없습니다. 타사 공급업체에서 유틸 리티를 다운로드해야 합니다. 이 예에서는 Intel 카드이므로 시스템에 Intel PROSet이 설치되 어 있습니다.

goa Wireless Network Pr	operties	
Connection Security		
Security type: Encryption type:	WPA2-Enterprise   AES	
Choose a network aut Cisco: EAP-FAST Microsoft: Smart Card Microsoft: Protected B Cisco: LEAP Cisco: PEAP Cisco: PEAP Cisco: EAP-FAST Intel: EAP-SIM Intel: EAP-SIM Intel: EAP-AKA Advanced settings	hentication method: I or other certificate AP (PEAP) I n each	
<u>.</u>	ОК Са	ncel

goa Wireless Network Properties	X
Connection	
Security type: WPA2-Enterprise   Encryption type: AES	
Choose a network authentication method: Cisco: EAP-FAST ✓ Settings ✓ Remember my credentials for this connection each time I'm logged on	
Advanced settings	
OK Car	ncel

8. Allow automatic PAC provisioning(자동 PAC 프로비저닝 허용)을 활성화하고 Validate server certificate(서버 인증서 검증)가 선택되지 않았는지 확인합니다.

EAP-FAST Properties
Connection User Credentials Authentication About
Use anonymous outer identity anonymous         Use Protected Access Credentials (PAC)         Allow automatic PAC provisioning         PAC Authority:         None
Validate server certificate
<ul> <li>AAA Certificate Services</li> <li>AddTrust External CA Root</li> <li>Class 3 Public Primary Certification Authority</li> <li>Class 3 Public Primary Certification Authority</li> <li>DigiCert Assured ID Root CA</li> <li>DigiCert High Assurance EV Root CA</li> <li>DST Root CA X3</li> <li>To not prompt user to authorize new servers or trusted certification authorities.</li> </ul>
OK Cancel Help

9. User Credentials(사용자 자격 증명) 탭을 클릭하고 user2의 자격 증명을 입력합니다. 또는 Windows 자격 증명을 사용하여 로그인할 수 있습니다. 그러나 이 예에서는 이를 사용하지 않 습니다.

EAP-FAST Pro	operties	? ×
Connection	User Credentials	Authentication About
© Use © Use © Use © Pro User User Pass Conf	e certificate on this e one-time password Windows username mpt automatically f e saved username a name: word:	computer d e and password for username and password end password ser2
		OK Cancel Help

10. OK(확인)를 클릭합니다.

EAP-FAST Properties	? ×
Connection User Credentials Authentication About	
Select authentication method:	
Any method	Configure
Enable Fast Reconnect	
	Help

이제 클라이언트 유틸리티가 user2를 위해 연결할 준비가 되었습니다.

참고: user2가 인증을 시도할 때 RADIUS 서버는 PAC를 전송합니다. 인증을 완료하려면 PAC를 수 락합니다.



# 다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

OIT(<u>Output Interpreter Tool</u>)(<u>등록된</u> 고객만 해당)는 특정 show 명령을 지원합니다. OIT를 사용하여 show 명령 출력 분석을 볼 수 있습니다.

사용자1(PEAP-MSCHAPv2) 확인

WLC GUI에서 Monitor(모니터) > Clients(클라이언트)로 이동하여 MAC 주소를 선택합니다.

### Clients > Detail

#### **Client Properties**

MAC Address	00:24:d7:ae:f1:98	
IP Address	192,168,153,107	
Client Type	Regular	
User Nerve	user1	
Port Number	13	
Interface	vian253	
VLAN ID	253	
CCX Version	CCXv4	•
E2E Version	E2Ev1	
Mobility Role	Local	
Mobility Peer IP Address	N/A	
Policy Manager State	RLIN	
Management Frame Protection	No	
UpTime (Sec)	12	
Power Save Mode	OFF	
Current TxRateSet		
Data BateSet	6.0,9.0,12.0,15.0,24.0,3	6.0,48.0,54.

### **AP Properties**

AP Address	2c:3f:38:c1:3c:f0
AP Name	3502e
AP Type	802.iian
WLAN Profile	goa
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Pol Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Nat Implemented
Re-authentication timeout	86365
Remaining Re-authentication timeout	0
WEP State	WEP Enable

### Security Information

Security Policy Completed	Yes
Ройсу Туре	REN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Redius NAC State	RUN

### WLC RADIUS 통계:

### <#root>

(Cisco Controller) >

show radius auth statistics

Authentication Servers:
Server Index 1
Server Address 192.168.150.24
Msg Round Trip Time 1 (msec)
First Requests 8
Retry Requests 0
Accept Responses 1
Reject Responses 0
Challenge Responses7
Malformed Msgs 0
Bad Authenticator Msgs0

Pending Requests	0
Timeout Requests	0
Unknowntype Msgs	0
Other Drops	0

ACS 로그:

- 1. 적중 횟수를 보려면 다음 단계를 완료하십시오.
  - a. 인증 후 15분 내에 로그를 확인하는 경우 적중 횟수를 새로 고쳐야 합니다.

SI	ngle re	sult selec	ton 🐏 F	tule based result selection		
Servi	ce Sek	ection Pol	icy			
Filter	: Stat	16 <u>-</u>	Match if:	Equals - Enabled - Clea	r Filtar 🛛 🐨	
		Statue	Name	Conditions Protocol	Results Service	Hit Cou
1			Rule-1	match Radius	Default Network Access	1
2		0	Rule-2	match Tacaca	Default Davice Admin	0

b. 같은 페이지 하단에 Hit Count(적중 횟수) 탭이 있습니다.

letwork /	Access Authorization F	Policy					
Filter: St	tatus	▼ Match if: Equals	<ul> <li>Enabled</li> </ul>	💌 Clear Filter 🛛 Go 💌			
Name	NDG:Location	NDG:Device Type	Conditi Protecol	ions Identity Group	Eap Authentication Method	Results Authorization Profiles	Hit Cour
Rule-1	in All Locations LAB	in All Device Types:5508	match Radius	in All Groups:Wireless Users	-ANY-	Permit Access	1

2. Monitoring and Reports(모니터링 및 보고서)를 클릭하면 New(새) 팝업 창이 나타납니다. Authentications(인증) -Radius -Today(오늘)로 이동합니다. 어떤 서비스 선택 규칙이 적용되 었는지 확인하기 위해 Details를 클릭할 수도 있습니다.

1 1 1											Launch Inter	nactive Waver
Showing Page	1 of 1					6	Colo Page: Ge					
AAA Protocol > RAD	US Auth	enticatio	n									
Authentication Status : Date :	Pass or Fa Jonuary 25	il , 2012 05	40 PM -	January 29	2012 06:10 PM (1	.ast 30 Minutes (Lost Hour	HLoot 12 Hours   Teday   Yes	terday i Last 7 Da	a   Last 30 Dava )			
Generated on January 2	29, 2012 6 1	0.42 PM	EST									
Reited	-Click for	dataila	R-mai	sa over iten	n flor additional info	mation						
Logged At	RADIL	s NAS Failure	Details	Usemane	MAC/IP Address	Access Service	Authentication Method	Natwork Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Instance
Jan 29,12 6:07:37.943	РМ 🖌		0	uper1	00-24-d7-as-f1-98	Default Notesrk Access	PEAP (EAP-MSCHAPv2)	WLC-5508	192.168.75.44			SALL-ACS52

# 사용자2(EAP-FAST) 확인

## WLC GUI에서 Monitor(모니터) > Clients(클라이언트)로 이동하여 MAC 주소를 선택합니다.

Clients > Detail

Client Properties			AP Properties	
MAC Address	00r24rd7raerf1r98		AP Address	2013fr38rc1r3crf0
IP Address	192.168.153.111		AP Name	3502e
Client Type	Regular		АР Туре	002.11an
User Name	user2		WLAN Profile	goa
Port Number	13		Status	Associated
Interface	vlan253		Association 1D	1
VLAN ID	253		802.11 Authentication	Open System
CCX Version	CCXV4	•	Reason Code	1
E2E Version	E2Ev1		Status Code	0
Mobility Role	Local		CF Pollable	Not Implemented
Mobility Peer IP Address	N/A		CF Poll Request	Not Implemented
Policy Manager State	RUN		Short Preamble	Not Implemented
Management Frame Protection	No		PBCC	Not Implemented
UpTime (Sec)	29		Channel Agility	Not Implemented
Power Save Mode	OFF		Re-authentication timeout	86302
Current TxRateSet	m15 6.0,9.0,12.0,18.0,24	1.0,36.0,48.0,54.	Remaining Re-authentication timeout	0
Data RateSet	0	di la constante de la constante	WEP State	WEP Enable

#### Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
ЕАР Туре	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

### ACS 로그:

1. 적중 횟수를 보려면 다음 단계를 완료하십시오.

a. 인증 후 15분 내에 로그를 확인하는 경우 HIT 수를 새로 고쳐야 합니다.

Servic	e Sek	ection Pol	licy					
Filter:	Stat	us 📼	Match It	Equals 🝷	Enabled -	Clear Filter	Go 🗢	
	E	Status	Name	Protocol	Conditions		Results Service	Hit Cou
1		۲	Rule-1	match Radius			Default Network Access	3
2		0	Rule-2	match Tacaca			Default Device Admin	0

b. 같은 페이지 하단에 Hit Count(적중 횟수) 탭이 있습니다.

COO MUSICIAL COURT	Aolicy					
8	Match if: Equals	<ul> <li>Enabled</li> </ul>	▼ Clear Filter Go 🛡			
DG:Location	NDG:Device Type	Conditi Protocol	ions Identity Group	Eap Authentication Method	Results Authorization Profiles	Hit Cour
All Locations:LAB	in All Device Types:5508	match Radius	in All Groups: Wireless Users	-ANY-	Permit Access	2
	s DG:Location All Locations:LAB	s I Match it: Equals DQ:Location NDG:Device Type All Locations:LAB in All Device Types:5508	s Match it. Equals Enabled Condit DG:Location NDG:Device Type Protocol All Locations:LAB in All Device Types:5508 match Radius	s v Match it: Equals v Enabled v Clear Filter Go v Conditions DG:Location NDG:Device Type Protocol Identity Group All Locations:LAB in All Device Types:5508 match Radius in All Groups: Wireless Users	s Match it: Equals Enstitled Clear Filter Go Conditions DG:Location NDG:Device Type Protocol Identity Group Eap Authentication Method All Locations:LAB in All Device Types:5508 match Radius in All Groups:Wireless Users -ANY-	s Match it: Equals Enabled Clear Filter Go Conditions DG:Location NDG:Device Type Protocol Identity Group Eap Authentication Method Authorization Profiles All Locations:LAB in All Device Types:5508 match Radius in All Groups:Wireless Users -ANV- Permit Access

2. Monitoring and Reports(모니터링 및 보고서)를 클릭하면 New(새) 팝업 창이 나타납니다. Authentications(인증) -Radius -Today(오늘)로 이동합니다. 어떤 서비스 선택 규칙이 적용되 었는지 확인하기 위해 Details를 클릭할 수도 있습니다.

2.5	•											La	unch Interactive	Vewer 5
199144	Showin	g Pege 1	of 1	1	1111	int free	most Lost	Get	io Page: Ge					
AAA Pn	otocol >	RADIU	S Auther	ticatio	•									
Authenti Data :	cation St	atus : Pa Ja	os or Fail 100ry 29, 2	2012 05:	STPM -	January 29, 3	2012 06:23 PM (La	st 30 Ninutes   <u>Last Hour</u>   L	.ast 12 Hours   Today   Yesterday	Last 7 Days   Last	130 Døys (			
Generati	ed on Jar	wary 29, 1	2912 6 23	17 PM E	ST						10000000			
Reica	4							_						
	Logged	An	RACIUS Status	NAS Falure	Details	Usemane	MAC/IP Address	Access Service	Authentication Method	Natwork Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS INS
Jan 29,	12 6:19 3	7.270 FN			14	user2	90-24-d7-ap-f1-98	Default Network Access	EAP-FAST (EAP-MSCHAP42)	WLC-5508	192.168.75.44			SALL-A
Jan 29.	12 6 07 3	7 943 PN	- 1		4	user1	00-24-d7-ae-f1-98	Default Network Access	PEAP (EAP-MSCHAPv2)	WLC-5598	192 168 75 44			SALL-A



이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

## 트러블슈팅 명령

OIT(<u>Output Interpreter Tool</u>)(<u>등록된</u> 고객만 해당)는 특정 show 명령을 지원합니다. OIT를 사용하여 show 명령 출력 분석을 볼 수 있습니다.

참고: debug 명령을 사용하기<u>전에 Debug 명령</u>에 대한 중요 정보를 참조하십시오.

- 1. 문제가 발생하면 WLC에서 다음 명령을 실행합니다.
  - debug client <클라이언트의 mac 추가>
  - debug aaa all enable
  - show client detail <mac addr> 정책 관리자 상태를 확인합니다.
  - show radius auth statistics 실패 사유를 확인합니다.
  - debug disable-all 디버그를 끕니다.
  - clear stats radius auth all WLC에서 radius 통계를 지웁니다.

2. ACS의 로그를 확인하고 실패 이유를 기록합니다.

# 관련 정보

• <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.