RADIUS 서버를 사용한 외부 웹 인증

목차

소개 사전 요구 사항 요구 사항 사용되는 구<u>성 요소</u> 네트워크 다이어그램 표기 규칙 외부 웹 인증 WLC 구성 Cisco Secure ACS용 WLC 구성 웹 인증을 위해 WLC에 WLAN 구성 WLC에서 웹 서버 정보 구성 Cisco Secure ACS 구성 Cisco Secure ACS에서 사용자 정보 구성 Cisco Secure ACS에서 WLC 정보 구성 클라이언트 인증 프로세스 클라이언트 컨피그레이션 클라이언트 로그인 프로세스 다음을 확인합니다. ACS 확인 WLC 확인 문제 해결 트러블슈팅 명령 관련 정보

<u>소개</u>

이 문서에서는 외부 RADIUS 서버를 사용하여 외부 웹 인증을 수행하는 방법에 대해 설명합니다.

<u>사전 요구 사항</u>

<u>요구 사항</u>

이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- LAP(Lightweight Access Point) 및 Cisco WLC 구성에 대한 기본 지식
- 외부 웹 서버 설정 및 구성 방법에 대한 지식
- Cisco Secure ACS 구성 방법에 대한 지식

<u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 버전 5.0.148.0을 실행하는 무선 LAN 컨트롤러
- Cisco 1232 Series LAP
- Cisco 802.11a/b/g Wireless Client Adapter 3.6.0.61
- 웹 인증 로그인 페이지를 호스팅하는 외부 웹 서버
- 펌웨어 버전 4.1.1.24를 실행하는 Cisco Secure ACS 버전

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.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



다음은 이 문서에 사용된 IP 주소입니다.

- WLC는 IP 주소 10.77.244.206을 사용합니다.
- LAP가 IP 주소 10.77.244.199를 사용하여 WLC에 등록되었습니다.
- 웹 서버는 IP 주소 10.77.244.210을 사용합니다.
- Cisco ACS 서버는 IP 주소 10.77.244.196을 사용합니다
- 클라이언트가 관리 인터페이스에서 WLAN에 매핑된 IP 주소(10.77.244.208)를 수신합니다.

<u>표기 규칙</u>

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

<u>외부 웹 인증</u>

웹 인증은 인터넷 액세스를 위해 게스트 사용자를 인증하는 데 사용되는 레이어 3 인증 메커니즘입 니다. 이 프로세스를 사용하여 인증된 사용자는 인증 프로세스를 성공적으로 완료할 때까지 인터넷 에 액세스할 수 없습니다. 외부 웹 인증 프로세스에 대한 자세한 내용은 <u>Wireless LAN Controllers</u>를 사용한 <u>외부 웹 인증 구성 예</u>의 <u>외부 웹 인증 프로세스 섹션을 참조하십시오</u>.

이 문서에서는 외부 RADIUS 서버를 사용하여 외부 웹 인증을 수행하는 컨피그레이션 예를 살펴보 겠습니다.

<u>WLC 구성</u>

이 문서에서는 WLC가 이미 구성되어 있고 WLC에 LAP가 등록되어 있다고 가정합니다. 이 문서에 서는 WLC가 기본 작동을 위해 구성되고 LAP가 WLC에 등록되어 있다고 가정합니다. LAP를 사용 한 기본 작업을 위해 WLC를 설정하려는 새 사용자인 경우 WLC(<u>무선 LAN 컨트롤러)에 대한</u> LAP(Lightweight AP) 등록을 참조하십시오. WLC에 등록된 LAP를 보려면 Wireless > All APs로 이 동합니다.

WLC가 기본 작동을 위해 구성되고 하나 이상의 LAP가 등록된 경우 외부 웹 서버를 사용하여 외부 웹 인증을 위한 WLC를 구성할 수 있습니다. 이 예에서는 Cisco Secure ACS 버전 4.1.1.24를 RADIUS 서버로 사용하고 있습니다. 먼저 이 RADIUS 서버에 대해 WLC를 구성한 다음 이 설정에 필요한 Cisco Secure ACS 컨피그레이션을 살펴봅니다.

<u>Cisco Secure ACS용 WLC 구성</u>

WLC에 RADIUS 서버를 추가하려면 다음 단계를 수행합니다.

- 1. WLC GUI에서 **SECURITY**(보안) 메뉴를 클릭합니다.
- 2. AAA 메뉴 아래에서 Radius > Authentication 하위 메뉴로 이동합니다.
- 3. New(**새로** 만들기)를 클릭하고 RADIUS 서버의 IP 주소를 입력합니다. 이 예에서 서버의 IP 주 소는 *10.77.244.196입니다*.
- 4. WLC에 공유 암호를 입력합니다. 공유 암호는 WLC에서 동일하게 구성해야 합니다.
- 5. Shared Secret Format(**공유** 암호 형식)에 대해 ASCII 또는 16진수를 선택합니다. WLC에서 동 일한 형식을 선택해야 합니다.
- 6. **1812**는 RADIUS 인증에 사용되는 포트 번호입니다.
- 7. Server Status(서버 상태) 옵션이 Enabled(활성화됨)로 설정되어 있는지 확인합니다.
- 8. 네트워크 사용자를 인증하려면 Network User Enable 상자를 선택합니다.
- 9. Apply를 클릭합니다

uluili. cisco	MONITOR WLANS CONTR	ROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Authentication	Servers > New
▼ AAA General ▼ RADIUS	Server Index (Priority)	2 10 77 244 196
Authentication Accounting Fallback FACACS+	Shared Secret Format	ASCII 💌
LDAP Local Net Users	Shared Secret	
MAC Filtering Disabled Clients User Login Policies AP Policies	Confirm Shared Secret	•••••
▶ Local EAP	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
 Priority Order Access Control Lists 	Port Number	1812
Wireless Protection Policies	Server Status	Enabled 💙
▶ Web Auth	Support for RFC 3576	Enabled 💙
Advanced	Server Timeout	2 seconds
	Network User	Enable
	Management	Enable
	IPSec	Enable

<u>웹 인증을 위해 WLC에 WLAN 구성</u>

다음 단계는 WLC에서 웹 인증을 위해 WLAN을 구성하는 것입니다. WLC에서 WLAN을 구성하려면 다음 단계를 수행합니다.

- 1. 컨트롤러 GUI에서 WLANs 메뉴를 클릭하고 New(새로 만들기)를 선택합니다.
- 2. Type(유형)에 WLAN을 선택합니다.

.

3. 원하는 프로파일 이름 및 WLAN SSID를 입력하고 Apply를 **클릭합니다.참고:** WLAN SSID는 대/소문자를 구분합니다

cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT
WLANs	WLANs > New				
VLANS	Туре	WLAN	~		
Advanced	Profile Name	WLAN1			
	WLAN SSID	WLAN1			

4. **General(일반) 탭**에서 Status(상태) 및 Broadcast SSID(브로드캐스트 **SSID**)에 대해 Enabled(활성화됨) 옵션이 선택되어 있는지 확인합니다.**WLAN 구성**

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs	WLANs > Edit
 ₩LANS WLANS Advanced 	General Security QoS Advanced Profile Name WLANI Type WLAN SSID WLANI Status Imabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All
	Interface management ¥ Broadcast SSID È Enabled Foot Notes 2 CKIP is not supported by 10xx model APs 2 Web Policy cannot be used in combination with IPsec 3 H-REAP Load Switching is not supported with IPsec, CRANITE authentication 4 When cleant exclusion is enabled, a Timout Value of zero means infinity (swill require administrative override to reset excluded clients) 5 Unet ARE is not active unless Widel is not supported with IPsec.

- 5. WLAN에 대한 인터페이스를 선택합니다. 일반적으로 고유한 VLAN에 구성된 인터페이스는 클라이언트가 해당 VLAN의 IP 주소를 수신하도록 WLAN에 매핑됩니다. 이 예에서는 인터페 이스에 *관리*를 사용합니다.
- 6. **보안** 탭을 선택합니다.
- 7. Layer 2 메뉴 아래에서 Layer 2 Security에 대해 None을 선택합니다.
- 8. Layer 3 메뉴 아래에서 None for Layer 3 Security를 선택합니다. Web Policy(웹 정책) 확인란 을 선택하고 Authentication(인증)을 선택합니다

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS MLANS Advanced	WLANs > Edit General Security Qo5 Advanced Layer 3 AAA Servers Layer 3 Security None Image: Security Image: Security Image: Security Image: Security

9. AAA servers(AAA 서버) 메뉴에서 Authentication Server(인증 서버)에 대해 이 WLC에 구성된 RADIUS 서버를 선택합니다. 기타 메뉴는 기본값으로 유지되어야 합니다

li.ili. cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMAN	DS HELP		
WLANS WLANS WLANS Advanced	WLANs > Edit General Security QoS Advanced Layer 2 Layer 3 AAA Servers Select AAA servers below to override use of default servers on this WLAN Radius Servers	LDAP Server	75	
	Authentication Servers Accounting Servers Accounting Servers Inabled Server 1 None Server 2 Server 3 None Local EAP Authentication	Server 1 Server 2 Server 3	None v None v	
	Local EAP Authentication Enabled Authentication priority order for web-auth user			
	Foot Notes S CKIP is not supported by 10xx model APs When other to be used in combination with IPsec When client exclusion is enabled, a Timeout Value of zero means infinity (will require administra S Client MPF is not active unless WHAZ is configured S Client MPF is not active unless WHAZ is configured	tive override to reset e	xoluded clients)	

WLC에서 웹 서버 정보 구성

.

웹 인증 페이지를 호스팅하는 웹 서버를 WLC에 구성해야 합니다. 다음 단계를 수행하여 웹 서버를 구성합니다.

1. 보안 탭을 클릭합니다. Web Auth(웹 인증) > Web Login Page(웹 로그인 페이지)로 이동합니

다.

.

- 2. 웹 인증 유형을 외부로 설정합니다.
- 3. Web Server IP Address(웹 서버 IP 주소) 필드에 웹 인증 페이지를 호스팅하는 서버의 IP 주소 를 입력하고 Add Web Server(웹 서버 추가)를 클릭합니다. 이 예에서 IP 주소는 *10.77.244.196이며*, 외부 웹 서버 아래에 표시됩니다.
- 4. URL 필드에 웹 인증 페이지의 URL(이 예에서는 *http://10.77.244.196/login.html*)을 입력합니 다

cisco		WLANs		WIRELESS	SECURITY	MANAGEMENT
Security	Web Logi	in Page				
 ▼ AAA General ▼ RADIUS Authentication Accounting Fallback 	Web Auth URL http://	enticatio /10.77.244 Web Serve	n Type 196/login.html	External (Redirect to ext	ternal server) 🔽
TACACS+ LDAP Local Net Users	10.77.244.3	196	Re	move		
MAC Filtering Disabled Clients User Login Policies AP Policies	Web Serv	er IP Add	Iress	Add Web Ser) ver	
▶ Local EAP						
Priority Order						
Access Control Lists						
Wireless Protection Policies						
 Web Auth Web Login Page Certificate 						
Advanced						

<u>Cisco Secure ACS 구성</u>

이 문서에서는 Cisco Secure ACS Server가 이미 시스템에 설치되어 실행 중인 것으로 가정합니다. Cisco Secure ACS 설정 방법에 대한 자세한 내용은 <u>Cisco Secure ACS 4.2 컨피그레이션 가이드를</u> <u>참조하십시오</u>.

Cisco Secure ACS에서 사용자 정보 구성

Cisco Secure ACS에서 사용자를 구성하려면 다음 단계를 수행합니다.

 Cisco Secure ACS GUI에서 User Setup(사용자 설정)을 선택하고 사용자 이름을 입력한 다음 Add/Edit(추가/수정)를 클릭합니다. 이 예에서 사용자는 *user1입니다*

CISCO SYSTEMS	User Setup	
	Select	
User Setup		
Group Setup	User: user1	
Shared Profile Components	Find Add/Edit	
Network Configuration	List users beginning with letter/number:	
System Configuration	<u>A B C D E F G H I J K L M</u> <u>N O P Q R S T U V U X Y Z</u>	
Interface Configuration	0123456789	
Administration Control	List all users	
External User Databases	Remove Dynamic Users	
Research Posture Validation		
Network Access Profiles	Back to Help	
Reports and Activity		
Online Documentation		

2. 기본적으로 PAP는 클라이언트 인증에 사용됩니다. 사용자의 비밀번호는 User Setup(사용자 설정) > Password Authentication(비밀번호 인증) > Cisco Secure PAP에 입력됩니다. 비밀번 호 인증을 위해 ACS 내부 데이터베이스를 선택해야 합니다

•

arstens	User Setup			
ser etup	Edit	User: use	r1 (New User)	
ared Profile		C Acc	ount Disabled	
work figuration		Supplemen	tary User Info	?
tem figuration erface figuration	Real Name Description	User1		
ninistration trol		lise	Setun	
ure dation	Password Aut	hentication:	ACS Intern	al Database 💽
ts and ty	CiscoSec	ure PAP (Also used f sword	or CHAP/MS-CHAP/ARA field	P, if the Separate 1 is not checked.)
e	Confirm Pas	sword		
incados.	🗆 Separate ((CHAP/MS-CHAP/AR	AP)	
	Pas	sword	5	
	Confirm Pas	sword		
	When a token CHAP passwor especially use	server is used for a d for a token card u ful when token cach	uthentication, supplying ser allows CHAP auther ing is enabled.	a separate ntication. This is
		Group to which	the user is assigned:	

- 3. 사용자에게 해당 사용자가 속한 그룹을 할당해야 합니다. 기본 그룹을 선택합니다.
- 4. Submit(제출)**을 클릭합니다**.

<u>Cisco Secure ACS에서 WLC 정보 구성</u>

Cisco Secure ACS에서 WLC 정보를 구성하려면 다음 단계를 수행합니다.

- 1. ACS GUI에서 Network Configuration(**네트워크 컨피그레이션) 탭**을 클릭하고 Add Entry(항목 **추가)를 클릭합니다**.
- 2. Add AAA client(AAA 클라이언트 추가) 화면이 나타납니다.
- 3. 클라이언트의 이름을 입력합니다. 이 예에서는 WLC를 사용합니다.
- 4. 클라이언트의 IP 주소를 입력합니다. WLC의 IP 주소는 10.77.244.206입니다.
- 5. 공유 암호 키와 키 형식을 입력합니다. 이는 WLC의 **Security**(보안) 메뉴에 있는 항목과 일치해 야 합니다.
- 6. WLC**에서** 동일해야 하는 키 입력 형식에 대해 ASCII를 선택합니다.
- 7. WLC**와 RADIUS** 서버 간에 사용되는 프로토콜을 설정하려면 Authenticate Using(사용 인증)에 RADIUS**(Cisco Airespace)**를 선택합니다.
- 8. Submit(제출) + Apply(적용)를 클릭합니다

ât -		
	Add AAA Client	
AAA Client Hostname	WLC	
AAA Client IP Address	10.77.244.206	
Shared Secret	abc123	
RADIUS Key Wrap		
Key Encryption Key		
Message Authenticator Code K	ley	
Key Input Format		
Authenticate Using	RADIUS (Cisco Airespace)	
Single Connect TACACS+ A	AAA Client (Record stop in accounting on failure)	
Log Update/Watchdog Paci	kets from this AAA Client	
Log RADIUS Tunneling Pack	ets from this AAA Client	
Replace RADIUS Port info w	vith Username from this AAA Client	
Match Framed-IP-Address	with user IP address for accounting packets from this AAA Client	
	Submit Submit + Apply Cancel	
	Plack to Help	

<u>클라이언트 인증 프로세스</u>

<u>클라이언트 컨피그레이션</u>

이 예에서는 Cisco Aironet Desktop Utility를 사용하여 웹 인증을 수행합니다. Aironet Desktop Utility를 구성하려면 다음 단계를 수행합니다.

- 1. 시작 > Cisco Aironet > Aironet Desktop Utility에서 Aironet Desktop Utility를 엽니다.
- 2. Profile Management(프로필 관리) 탭을 클릭합니다

Cisco Aironet Desktop Utility - Current Profile: Default ion Options Help	?
urrent Status Profile Management Diagnostics	
Default	<u>N</u> ew
	Modify
	Remove
	Activate
Details	
Network Type:	Import
Security Mode:	
Network Name 1 (SSID1):	<u>Export</u>
Network Name 2 (SSID2):	Scan
Network Name 3 (SSID3):	Jeana
Auto Select Profiles	Order Profiles

3. Default(기본) **프로파일**을 선택하고 Modify(수정)**를 클릭합니다.General(일반) 탭**을 클릭합니 다.프로파일 이름을 구성합니다. 이 예에서는 *Default*가 사용됩니다.Network Names(네트워크 이름)에서 SSID를 구성합니다. 이 예에서는 *WLAN1*이 사용됩니다

rofile Management		?
General Security Advanc	ced	
Profile Settings		
Profile Name:	Default	
Client Name:	Client1	
Network Names		
SSID1:	WLAN1	
SSID2:		
SSID3:		
L		
		ancel
		anoor

참고: SSID는 대/소문자를 구분하며 WLC에 구성된 WLAN과 일치해야 합니다.**보안** 탭을 클릭 합니다.웹 **인증**을 위한 보안으로 없음을 선택합니다

Profile Management		? 🔀
General Security Advanced		
Set Security Options		
○ WPA/WPA2/CCKM WPA/WPA2/CCKM EAP Type:	x LEAP 👻	
○ WPA/WPA2 Passphrase		
O 802.1x 802.1x EAP Type:	K LEAP	
O Pre-Shared Key (Static WEP)		
None		
Configure	Mixed Cells	
Group Policy Delay: 0 1 sec		
	ОК	Cancel

Advanced(고급) 탭을 클릭합니다.Wireless Mode 메뉴에서 무선 클라이언트가 LAP와 통신하 는 빈도를 선택합니다.Transmit Power Level(전송 전력 레벨) 아래에서 WLC에 구성된 전력을 선택합니다.절전 모드의 기본값은 그대로 둡니다.Network Type(네트워크 유형)으로 Infrastructure(인프라)를 선택합니다.802.11b Preamble(802.11b 프리앰블)을 Short & Long(짧은 및 긴)으로 설정하여 호환성을 개선합니다.OK(확인)를 클릭합니다

Transmit Power Lev	vel	Power Save Mode:	CAM (Constantly Av	wake Mode) 🛛 👻						
802.11b/g:	100 mW	Network Type:	Infrastructure	~						
802.11a:	40 mW	802.11b Preamble:	Short & Long	O Long Only						
Wireless Mode		Wireless Mode When Starting	Wireless Mode When Starting Ad Hoc Network							
🗹 5 GHz 54 Mbp	\$									
2.4 GHz 54 Mbps		◯ 5 GHz 54 Mbps								
🗹 2.4 GHz 11 MI	ops	O 2.4 GHz 11 Mbps								
		2.4 GHz 54 Mbps	Channe	l Auto						
		802.11 Authentication Mode								
		O Auto 00	pen C) Shared						

4. 클라이언트 소프트웨어에 프로파일이 구성되면 클라이언트가 성공적으로 연결되고 관리 인터 페이스에 대해 구성된 VLAN 풀에서 IP 주소를 수신합니다.

클라이언트 로그인 프로세스

- 이 섹션에서는 클라이언트 로그인이 수행되는 방법에 대해 설명합니다.
 - 1. 브라우저 창을 열고 URL 또는 IP 주소를 입력합니다. 그러면 클라이언트에 웹 인증 페이지가 나타납니다. 컨트롤러가 3.0 이전의 릴리스를 실행 중인 경우 사용자는 https://1.1.1.1/login.html을 *입력하여* 웹 인증 페이지를 불러와야 합니다. 보안 알림 창이 표시 됩니다.
 - 2. 계속하려면 Yes(예)를 클릭합니다.
 - 3. Login(로그인) 창이 나타나면 RADIUS 서버에 구성된 사용자 이름 및 비밀번호를 입력합니다. 로그인에 성공하면 브라우저 창 두 개가 표시됩니다. 더 큰 창은 성공적인 로그인을 나타내며, 이 창에서 인터넷을 찾아볼 수 있습니다. 게스트 네트워크 사용이 완료되면 더 작은 창을 사용

	Web Authentication
	Login Successful I
	You can now use all regular network services over the wireless network.
	Please retain this small logout window in order to logoff when done. Note that you can always use the following URL to retrieve this page: https://1.1.1.10ocout.html Logout
하여 로그아웃합니다.	

<u>다음을 확인합니다.</u>

성공적인 웹 인증을 위해서는 디바이스가 적절한 방식으로 구성되어 있는지 확인해야 합니다. 이 섹션에서는 프로세스에서 사용되는 디바이스를 확인하는 방법에 대해 설명합니다.

<u>ACS 확인</u>

1. User **Setup(사용자 설정**)을 클릭한 다음 ACS GUI**에서 List All Users(모든 사용자** 나열)를 클 릭합니다

CISCO SYSTEMS	User Setup
anti Utraanti Utraa-	Select
User Setup	
Setup	User:
Shared Profile Components	Find Add/Edit
Network Configuration	List users beginning with letter/number:
System Configuration	<u>A B C D E F G H I J K L M</u> <u>N O P Q R S T U V W X Y Z</u>
Interface Configuration	
Administration Control	
Databases	Remove Dynamic Users
nnnn Posture Validation	
Network Access Profiles	Back to Help
Reports and Activity	
Documentation	

Status of the User(사용자 상태)가 *Enabled(활성화됨)*이고 Default(기본) 그룹이 사용자에게 매핑되어 있는지 확인합니다

	100
н.	LIST

User	Status	Group	Network Access Profile
user1	Enabled	Default Group (2 users)	(Default)

2. Network Configuration(**네트워크 컨피그레이션**) 탭을 클릭하고 AAA Clients(AAA 클라이언트) 테이블에서 WLC가 AAA 클라이언트로 구성되어 있는지 확인합니다

TOUP	(
Setup	% ₽Q	A	AA Clients					
hared Profile emponents	AAA Client Hostname	AAA Client	AAA Client IP Address Au					
rtwork infiguration	wici	10.77.244.206	77.244.206 RADIUS (Cisco Airespace)					
Apten Sonfiguration		Add Entr	y Search					
efiguration entrol	% Q	AAA Servers						
sternal Uper	AAA Server Name	AAA Ser	AAA Server IP Address					
artabases	TS-Web	10.77.244.196	0.77.244.196 Cit					
Validation Internation Reports and Activity		Add Entr	γ Search bution Table					
ocumentation	Character String		AA Servers	Strip	Account			
	(Default)	TS-Web		No	Local			
		and France	Sort Entron					

<u>WLC 확인</u>

1. WLC GUI에서 **WLANs** 메뉴를 클릭합니다.웹 인증에 사용되는 WLAN이 페이지에 나열되어 있는지 확인합니다.WLAN의 Admin Status(관리자 상태)가 Enabled(활성화됨)*인지 확인합니 다*.WLAN에 대한 보안 정책에서 *웹* 인증*을 표시하는지 확인합니다*

cisco		CONTROLLER WIR	ELESS SECURITY	M&NAGEMENT COMMANDS	5 HELP
WLANS	WLANs Profile Name	Туре	WLAN SSID	Admin Status	Security Policies
Advanced	WLAN1	WLAN	WLAN1	Enabled	Web-Auth

2. WLC GUI에서 SECURITY(보안) 메뉴를 클릭합니다.Cisco Secure ACS(10.77.244.196)가 페 이지에 나열되어 있는지 확인합니다.Network User(네트워크 사용자) 상자가 선택되어 있는지 확인합니다.포트가 *1812*이고 Admin Status(관리 상태)가 Enabled(활성화됨)*인지 확인합니다*

cisco	MONITOR	<u>W</u> LANs <u>C</u> C	ONTROLLE	R WIRELESS S	ECURITY 1	MANAGEMENT C	<u>O</u> MMANDS HE	P
Security	RADIUS	Authenticati	ion Serve	ers				
 ▼ AAA General ▼ RADIUS Authentication Accounting Fallback ▼ TACACS+ LDAP Local Net Users 	Call Stat	ion ID Type [Key Wrap	IP Address	ed for FIPS custome	ers and requir	es a key wrap com	pliant RADIUS serv	ver)
	Network User	Management	Server Index	Server Address	Port	IPSec	Admin St	atus
		V 1 10.77.244.1				Disabled	Enabled	
Disabled Clients								
User Login Policies AP Policies Local EAP								
User Login Policies AP Policies Local EAP Priority Order								
User Login Policies AP Policies Local EAP Priority Order Access Control Lists								
User Login Policies AP Policies Cocal EAP Priority Order Access Control Lists Wireless Protection Policies								
User Login Policies AP Policies Local EAP Priority Order Access Control Lists Wireless Protection Policies Web Auth								

<u>문제 해결</u>

웹 인증이 성공하지 못하는 이유는 여러 가지가 있습니다. WLC<u>(Wireless LAN Controller)에서 웹</u> 인증 문제 해결 문서는</u> 이러한 이유를 자세히 설명합니다.

<u>트러블슈팅 명령</u>

참고: 디버그 명령<u>을</u> 사용하기 <u>전에 디버그</u> 명령에 대한 중요 정보를 참조하십시오.

WLC에 텔넷을 연결하고 다음 명령을 실행하여 인증 문제를 해결합니다.

· debug aaa all enable

Fri	Sep	24	13:59:52	2010:	00:40	:96:	ac:c	1d:(05 \$	Succ	cess	sful	l tı	ransi	miss	sior	ı of	ΕAι	ithe	enti	ίC
atio	on Pa	acke	et (id 1)	to 10	.77.24	4.19	6:18	312,	, pi	roxy	/ st	tate	e 0():40	:96	ac	dd	:05-	-00:	01	
Fri	Sep	24	13:59:52	2010:	00000	000:	01	01	00	73	00	00	00	00	00	00	00	00	00	00	0
0 00).	s																			
Fri	Sep	24	13:59:52	2010:	00000	010:	00	00	00	00	01	07	75	73	65	72	31	02	12	93	С
3 66	5.		user1	f																	
Fri	Sep	24	13:59:52	2010:	00000	030:	75	73	65	72	31										
	us	seri	L																		
Fri	Sep	24	13:59:52	2010:	****E	Inter	pro	oces	ssIn	ıcon	ning	gMes	ssag	ges:	res	spor	ıse	cod	le=2	2	
Fri	Sep	24	13:59:52	2010:	**** <u></u> E	Inter	pro	oces	ssRa	adiu	ısRe	espo	onse	e: r	espo	onse	e co	ode=	=2		
Fri	Sep	24	13:59:52	2010:	00:40	:96:	ac:c	dd:()5 Z	Acce	ess	-Acc	cept	re	ceiv	zed	fro	om F	RADI	US	S
erve	er 10).77	7.244.196	for mo	obile	00:4	0:96	5:ac	c:do	1: 05	5 re	ecei	lve	[d =	0						
Fri	Sep	24	13:59:52	2010:	Autho	riza	tior	nRes	spor	ise:	: 02	x122	2380	lb0							
Fri	Sep	24	13:59:52	2010:		str	ucti	ires	Size	∍	•••		• • •							.89	Э
Fri	Sep	24	13:59:52	2010:		res	ult(Code	€				•••		• • •	•••	•••			.0	
Fri	Sep	24	13:59:52	2010:		pro	toco	olUs	sed				•••		• • •	•••	•••			.02	ĸ0
0000	0001																				
Fri	Sep	24	13:59:52	2010:		pro	xySt	cate	€				•••		• • •	•••	•••			.00):
40:9	96:A0	C:DI	0:05-00:0	0																	
Fri	Sep	24	13:59:52	2010:		Pac	ket	cor	nta	lns	2 2	AVPs	5:								
Fri	Sep	24	13:59:52	2010:			AVI	P[01	L] I	Fran	ned-	-IP-	-Ado	lres	s	•••	•••			•••	
	0x1	Eff	Effff (-1) (4 by	ytes)																
Fri	Sep	24	13:59:52	2010:			AVI	2[02	2] (Clas	ss.		•••		• • •	•••	•••			•••	
• • •	CAC	CS:()/5183/a40	df4ce/ı	lser1	(25]	byte	es)													
Fri	Sep	24	13:59:52	2010:	Authe	entica	atio	on f	Eail	Led	foi	r us	serí	L, S	ervi	ice	Тур	pe:	0		

Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for statio n 00:40:96:ac:dd:05 Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96 :ac:dd:05 source: 48, valid bits: 0x1 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s tation 00:40:96:ac:dd:05 Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c Fri Sep 24 13:59:52 2010: Packet contains 12 AVPs: AVP[01] User-Name..... Fri Sep 24 13:59:52 2010:user1 (5 bytes) Fri Sep 24 13:59:52 2010: AVP[02] Nas-Port.....0x00000002 (2) (4 bytes) Fri Sep 24 13:59:52 2010: AVP[03] Nas-Ip-Address.....0x0a4df4ce (172881102) (4 bytes) AVP[04] Framed-IP-Address..... Fri Sep 24 13:59:52 2010:0x0a4df4c7 (172881095) (4 bytes)

debug aaa detail enable

실패한 인증 시도는 Reports and Activity > Failed Attempts에 있는 메뉴에 나열됩니다.

<u>관련 정보</u>

- Wireless LAN Controller 웹 인증 컨피그레이션 예
- WLC(Wireless LAN Controller)에서 웹 인증 문제 해결
- Wireless LAN Controller를 사용한 외부 웹 인증 컨피그레이션 예
- <u>WLC(Wireless LAN Controller)에서 LDAP를 사용한 웹 인증 컨피그레이션 예</u>
- <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.