# 무선 LAN 컨트롤러 스플래시 페이지 리디렉션 컨 피그레이션 예

## 목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 표기 규칙 배경 정보 네트워크 설정 구성 1단계. Cisco Secure ACS 서버를 통해 RADIUS 인증을 위한 WLC를 구성합니다. 2단계. Admin and Operations(관리 및 운영) 부서의 WLAN을 구성합니다. 3단계. 스플래시 페이지 리디렉션 기능을 지원하도록 Cisco Secure ACS를 구성합니다. 다음을 확인합니다. 문제 해결 관련 정보

# <u>소개</u>

이 문서에서는 무선 LAN 컨트롤러에서 스플래시 페이지 리디렉션 기능을 구성하는 방법에 대해 설 명합니다.

# <u>사전 요구 사항</u>

### <u>요구 사항</u>

이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- LWAPP 보안 솔루션에 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 5.0을 실행하는 Cisco 4400 Series WLC(Wireless LAN Controller)
- Cisco 1232 Series LAP(Light Weight Access Point)
- 펌웨어 버전 4.1을 실행하는 Cisco Aironet 802.a/b/g Wireless Client Adapter

- 버전 4.1을 실행하는 Cisco Secure ACS 서버
- 서드파티 외부 웹 서버

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.

#### <u>표기 규칙</u>

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

# <u>배경 정보</u>

스플래시 페이지 웹 리디렉션은 Wireless LAN Controller 버전 5.0에서 도입된 기능입니다. 이 기능 을 사용하면 802.1x 인증이 완료된 후 사용자가 특정 웹 페이지로 리디렉션됩니다. 리디렉션은 사 용자가 브라우저를 열거나(기본 홈 페이지로 구성) URL에 액세스하려고 할 때 발생합니다. 웹 페이 지로 리디렉션이 완료되면 사용자는 네트워크에 대한 전체 액세스 권한을 갖게 됩니다.

RADIUS(Remote Authentication Dial-In User Service) 서버에서 리디렉션 페이지를 지정할 수 있습니다. 802.1x 인증에 성공하면 Cisco av 쌍 url-redirect RADIUS 특성을 Wireless LAN Controller로 반환하도록 RADIUS 서버를 구성해야 합니다.

스플래시 페이지 웹 리디렉션 기능은 802.1x 또는 WPA/WPA2 레이어 2 보안을 위해 구성된 WLAN에만 사용할 수 있습니다.

# <u>네트워크 설정</u>

이 예에서는 Cisco 4404 WLC와 Cisco 1232 Series LAP가 레이어 2 스위치를 통해 연결됩니다. 외 부 RADIUS 서버로 작동하는 Cisco Secure ACS 서버도 동일한 스위치에 연결됩니다. 모든 디바이 스가 동일한 서브넷에 있습니다.

LAP는 컨트롤러에 처음 등록됩니다. 두 개의 WLAN을 생성해야 합니다. 하나는 **관리 부서 사용자** 를 위한 것이고 다른 하나는 **운영 부서 사용자를 위한** 것입니다. 두 무선 LAN 모두 WPA2/AES를 사 용합니다(EAP-FAST는 인증에 사용됨). 두 WLAN 모두 스플래시 페이지 리디렉션 기능을 사용하여 사용자를 (외부 웹 서버의) 적절한 홈 페이지 URL로 리디렉션합니다.

이 문서에서는 이 네트워크 설정을 사용합니다.



Cisco Secure ACS server

WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196

Subnet Mask used in this example 255.255.255.224

다음 섹션에서는 이 설정을 위해 디바이스를 구성하는 방법에 대해 설명합니다.

# <u>구성</u>

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.

스플래시 페이지 리디렉션 기능을 사용하도록 디바이스를 구성하려면 다음 단계를 완료하십시오.

- 1. <u>Cisco Secure ACS 서버를 통해 RADIUS 인증을 위한 WLC를 구성합니다.</u>
- 2. 관리 및 운영 부서에 대한 WLAN을 구성합니다.
- 3. <u>스플래시 페이지 리디렉션 기능을 지원하도록 Cisco Secure ACS를 구성합니다.</u>

### <u>1단계. Cisco Secure ACS 서버를 통해 RADIUS 인증을 위한 WLC를 구성합니다.</u>

외부 RADIUS 서버에 사용자 자격 증명을 전달하려면 WLC를 구성해야 합니다.

외부 RADIUS 서버에 대한 WLC를 구성하려면 다음 단계를 완료합니다.

- 1. RADIUS **Authentication** Servers(**RADIUS 인증** 서버) 페이지를 표시하려면 컨트롤러 GUI에서 Security and RADIUS Authentication(보안 및 RADIUS 인증)을 선택합니다.
- 2. RADIUS 서버를 정의하려면 New(새로 만들기)를 클릭합니다.
- 3. RADIUS Authentication Servers(RADIUS 인증 서버) > New(새) 페이지에서 RADIUS 서버 매 개변수를 정의합니다.이러한 매개변수에는 다음이 포함됩니다.RADIUS 서버 IP 주소공유 암 호포트 번호서버 상태

		Sage Configuration   Eing   Logout   Befresh
cisco	MONITOR WLANS CONTRO	LLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Authentication S	ervers > New <back apply<="" th=""></back>
- AAA General	Server Index (Priority)	1 3
<ul> <li>RADIUS Authentication</li> </ul>	Server IPAddress	10.77.244.196
Accounting     TACACS+     LDAP	Shared Secret Format	ASCII
Local Net Users MAC Filtering	Shared Secret	•••••
Disabled Clients User Login Policies AP Policies	Confirm Shared Secret	•••••
Local EAP	Key Wrap	C (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Priority Order	Port Number	1812
Access Control Lists		
<ul> <li>Wireless Protection Policies</li> </ul>	Server Status	Enabled ×
▶ Web Auth	Support for RFC 3576	Enabled ×
Advanced	Server Timeout	2 seconds
	Network User	R Enable
	Management	R Enable
	IPSec	Enable

이 문서에서는 IP 주소가 10.77.244.196인 ACS 서버를 사용합니다.

4. Apply를 **클릭합니다**.

#### <u>2단계. Admin and Operations(관리 및 운영) 부서의 WLAN을 구성합니다.</u>

이 단계에서는 클라이언트가 무선 네트워크에 연결하기 위해 사용할 두 개의 WLAN(관리 부서용 WLAN 및 운영 부서용 WLAN)을 구성합니다.

관리 부서의 WLAN SSID는 Admin 입니다. 운영 부서의 WLAN SSID는 Operations(운영)입니다.

WLAN 및 웹 정책 모두에서 WPA2를 레이어 2 보안 메커니즘으로 활성화하려면 EAP-FAST 인증을 사용합니다. 스플래시 페이지 웹 리디렉션 기능을 레이어 3 보안 방법으로 사용합니다.

WLAN 및 관련 매개변수를 구성하려면 다음 단계를 완료합니다.

- 1. WLANs **페이지**를 표시하려면 컨트롤러의 GUI에서 WLANs를 클릭합니다.이 페이지에는 컨트 롤러에 있는 WLAN이 나열됩니다.
- 2. 새 WLAN을 생성하려면 New(새로 만들기)를 클릭합니다

ahaha						Saye Co	nfiguration Ping	Logout <u>R</u> efresh
CISCO	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > New						< Back	Apply
WLANS	Туре	WLAN						
Advanced	Profile Name	Admin						
	WLAN SSID	Admin						

- 3. WLANs(WLAN) > New(새로 만들기) 페이지에서 WLAN SSID 이름 및 프로파일 이름을 입력 합니다.
- 4. Apply를 클릭합니다.
- 5. 먼저 관리 부서의 WLAN을 생성합니다.새 WLAN을 생성하면 새 WLAN에 대한 WLAN > Edit 페이지가 나타납니다. 이 페이지에서 이 WLAN에 대한 다양한 매개변수를 정의할 수 있습니다 . 여기에는 일반 정책, 보안 정책, QOS 정책 및 고급 매개변수가 포함됩니다.
- 6. General Policies(일반 정책)에서 Status(상태) 확인란을 선택하여 WLAN을 활성화합니다

cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	Sa <u>x</u> e C C <u>O</u> MMANDS	onfiguration Eing HELP	Logout <u>R</u> efr
WLANS WLANS WLANS Advanced	WLANS > General Profile I Type SSID Status Securit Radio P Interfai Broadc	Edit Secur Name y Policies Policy ce ast SSID	rity QoS Admin WLAN Admin IF Enable Splash- (Modificat All admin IF Enable	Advanced ed Page-Web-Ra ions done unde	edirect[WPA2 r security tab	?][Auth(802.1X)] will appear after af	l oplying the chan	< Back	Apply

- 7. Security(보안) 탭을 클릭한 다음 Layer 2(레이어 2) 탭을 클릭합니다.
- 8. Layer 2 Security 드롭다운 목록에서 WPA+WPA2를 선택합니다.이 단계에서는 WLAN에 대한 WPA 인증을 활성화합니다.
- 9. WPA+WPA2 Parameters(WPA+WPA2 매개변수)에서 **WPA2 Policy** and AES Encryption(**WPA2 정책** 및 **AES 암호화) 확인란**을 선택합니다

- alala		age Configuration Pin	g Logout Befre
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMA	NDS HELP	_
WLANS WLANS MLANS Advanced	WLANs > Edit         General       Security       QoS       Advanced         Layer 2       Layer 3       AAA Servers         Layer 2       Layer 3       AAA Servers         MAC Filtering       Image: Compare the security       Image: Compare the security         WPA+WPA2 Parameters       Image: Compare the security       Image: Compare the security         WPA2 Policy       Image: Compare the security       Image: Compare the security         WPA2 Policy       Image: Compare the security       Image: Compare the security         WPA2 Encryption       Image: Compare the security       Image: Compare the security         Auth Key Mgmt       B02.1X       Image: Compare the security	< Back	Apply

- 10. Auth Key Mgmt 드롭다운 목록에서 **802.1x**를 선택합니다. 이 옵션은 WLAN에 대해 802.1x/EAP 인증 및 AES 암호화를 사용하는 WPA2를 활성화합니다.
- 11. Layer **3 Security(레이어 3 보안) 탭**을 클릭합니다.
- 12. Web Policy(웹 정책) 상자를 선택한 다음 Splash Page Web Redirect(스플래시 페이지 웹 리 디렉션) 라디오 버튼을 클릭합니다.이 옵션은 스플래시 페이지 웹 리디렉션 기능을 활성화합 니다

CISCO     MONITOR     WLANS     CONTROLLER     WIRELESS     SECURITY     MANAGEMENT     COMMANDS     HELP       WLANS     WLANS > Edit     < Back     Apply       WLANS     General     Security     QoS     Advanced       WLANS     Layer 2     Layer 3     AAA Servers			Save Configuration   Bing   Logout   Be
WLANs     WLANs > Edit     < Back	CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT	COMMANDS HELP
Advanced  Layer 3 Security None  Web Policy 4  Authentication  Passthrough  Conditional Web Redirect  Splash Page Web Redirect  Preauthentication  ACL  None	WLANS WLANS Advanced	General       Security       QoS       Advanced         Layer 2       Layer 3       AAA Servers         Layer 3       Security       None         Image: Web Policy #       Image: Web Policy #         Image: Web Policy #       Im	< Back Apply

13. AAA Servers(AAA 서버) 탭을 클릭합니다.

.

14. Authentication Servers(인증 서버)의 Server 1(서버 1) 드롭다운 목록에서 적절한 서버 IP 주 소를 선택합니다

	Sa <u>v</u> e Configuration   <u>P</u> ing   Logou	t i <u>R</u> ef
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANs	WLANs > Edit Ap	ply
* WLANS	General Security QoS Advanced	
WLANs	Layer 2 Layer 3 AAA Servers	
▶ Advanced		
	Select ARA servers below to override use of default servers on this WLAN	
	Radius Servers LDAP Servers	
	Authentication Servers Accounting Servers Server 1 None	
	Enabled Server 2 None -	
	Server 3 None ×	
	Server None  None  None	
	Server None · None ·	
	Local EAP Authentication	
	Local EAP Authentication Enabled	
	Authentication priority order for	
	web-auth user	
	٠ •	

이 예에서는 10.77.244.196이 RADIUS 서버로 사용됩니다.

#### 15. Apply를 클릭합니다.

16. 운영 부서에 대한 WLAN을 생성하려면 2~15단계를 반복합니다.WLANs(WLAN) 페이지에는 생성한 두 개의 WLAN이 나열됩니다

				Sa <u>v</u> e C	onfiguration Ping I	.ogout   <u>R</u> efresh
cisco	MONITOR WLANS CONTROL	LER WIRELES	S SECURITY MANAGEN	IENT C <u>O</u> MMANDS	HELP	_
WLANs	WLANs				1	New
VLANs WLANs	Profile Name	Туре у	VLAN SSID	Admin Status	Security Policies	
Advanced	Admin	WLAN A	dmin	Enabled	[WPA2][Auth(802.1X)]	, Splash-Page
	Operations	WLAN 0	perations	Enabled	[WPA2][Auth(802.1X)]	, Splash-Pagi

보안 정책에는 스플래시 페이지 리디렉션이 포함됩니다.

#### <u>3단계. 스플래시 페이지 리디렉션 기능을 지원하도록 Cisco Secure ACS를 구성합니</u> <u>다.</u>

다음 단계는 이 기능에 대해 RADIUS 서버를 구성하는 것입니다. RADIUS 서버는 클라이언트 자격 증명을 확인 하기 위해 EAP-FAST 인증을 수행 해야 하고 성공 적 인 인증 시 사용자를 Cisco av 쌍 *url-redirect RADIUS 특성*에 지정 된 URL에 (외부 웹 서버의*) 리 디렉션* 해야 합니다.

#### EAP-FAST 인증을 위해 Cisco Secure ACS 구성

**참고:** 이 문서에서는 Wireless LAN Controller가 Cisco Secure ACS에 AAA 클라이언트로 추가된다 고 가정합니다. RADIUS 서버에서 EAP-FAST 인증을 구성하려면 다음 단계를 완료하십시오.

1. RADIUS 서버 GUI에서 **System** Configuration(시스템 컨피그레이션)을 클릭한 다음 System Configuration(시스템 컨피그레이션) 페이지에서 **Global Authentication Setup(전역 인증 설정** )을 선택합니다



2. EAP-FAST 설정 페이지로 이동하려면 **Global** Authentication(전역 인증) 설정 페이지에서 EAP-FAST Configuration(EAP-FAST 구성)을 클릭합니다

Configuration	EAP Configuration  EAP Configuration  EAP Allow EAP-MSCHAPv2 Allow EAP-GTC Allow Posture Validation Allow EAP-TLS Relect one or more of the following options:  E Certificate SAN comparison E Certificate Binary comparison E		Use this page to specify settings for various authentication protocols. EAP Configuration PSAP EAP-FASY EAP-FASY EAP-FASY EAP-FASY EAP-FASY EAP-FASY EAP-FASY EAP-FASY EAP-FASY EAP-FASY EAP-FASY EAP-FASS EAP-FAS	
User Setup Setup Setup Setup Setup SupredProfile Components Suprem Configuration Configuration Configuration Configuration Configuration Configuration Configuration	EAP Configuration	▲ Help	Use this page to specify settings for various authentication protocols. CAP Confidentialion ELAP: CAN ELAP: TASY ELAP: TAS	
Setup     S	Allow EAP-MSCHAPv2 Allow EAP-GTC Allow Posture Validation Allow EAP-TLS Elect one or more of the following options: Electrificate SAN comparison Electrificate Binary comparison Electrificate Binary comparison	:	Use this page to specify settings for various authentication protocols. EAP: Configuration EAP: EAP: TAS EAP: T	and
Dangoversion     Configuration     Surtem     Configuration	Allow Posture Validation Allow EAP-TLS Refect one or more of the following options: E Certificate SAN comparison E Certificate CN comparison E Certificate Binary comparison ADUTI S cersion timesed (minutes):		PEAP EAP-EASY EASY EASY EASY EASY EASY EASY EASY	-
Administration Control	Certificate Swi comparison     E Certificate CN comparison     E Certificate Binary comparison			-
Databases	AP-125 Session timeout (minutes): [220		EAP Configuration EAP is a flexible request/response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of	
retwork Access volies E	EAP session timeout (minutes): 120 inable Fast Reconnect: R		andtear protect such as GOV, 002,14 of KADIUS and Supports multiple "authentication" types. [ <u>deck to Tep]</u> PEAP	
Activity Online Documentation	AP-FAST AP-FAST Configuration		PEAP is the outer layer protocol for the secure tunnel.	
E (	AP-TLS Allow EAP-TLS ielect one or more of the following options: E Certificate SAN comparison		News row is a contractive state automotion protocol. FEM automotion can occur with a for you have completed the required stops so the ACS Centificate Setup page. Allows EAP-MSEMAPv2 — Use to enable EAP-MSCHAPv2 within MS PEAP authentic usion. Enable this protocol for any repository that supports MS- CHAPv2, such as Microsoft AD, and the ACS Internal Database.	
	Submit Submit + Restart Cancel	•	,	ŕ

3. RADIUS 서버에서 EAP-FAST를 **활성화 하려면 EAP-FAST** 설정 페이지에서 EAP-FAST 허용 확인 란을 선택 합니다

.

CiscoSecure ACS - N	ticrosoft Internet Explorer	Liel×
Ele Edt Yew Far	vorites Iools Help	Lirks 🍟 🤷
Address http://127.0	0.0.1:1065/	💌 🛃 😡
Croce System	System Configuration	X
User User Setop Setop Setop Setop Setop Setop Setop Setop Setorfier Setorfie	EAP-FAST Configuration  EAP-FAST Settings  EAP-FAST  Active master key TTL  Active master key TTL  Tunnel PAC TTL  Client initial message:  Authority ID Info:  Allow anonymous in-band PAC provisioning  Allow authenticated in-band PAC provisioning  Accept client on authenticated provisioning  Accept client certificate for provisioning  Accept client certificate for provisioning  Allow Machine Authentication  Machine PAC TTL  Allow Stateless session resume  Authorization PAC TTL  Allowed inner methods	Bit Constant Configuration Page     EAP-FAST Configuration Page     Use this page to configure EAP-FAST authentication settings.     EAP-FAST Settings     Check initial measure.     Active ity JD Jafe     Allow antibular setting for the and PAC provisioning     Allow cattering and the set of the band PAC provisioning     Allow EAP-FAST settings     Allow EAP-FAST contains to the APA-FAST authentication settings.     Allow EAP-FAST contains to the EAP-FAST authentication setting a network accurate for the amount of time that a master key is considered and a new master key is generated.     Patiend meater key TR - Enter a value for the amount of time that a master key is considered network and a new master key is generated.     Patiend meater key TR - Enter a value for the amount of time that a master key is considered network and a new master key is generated.     Patiend meater key TR - Enter a value for the amount of time that a master key is considered network and a new master key is generated.     Patiend meater key TR - Enter a value for the amount of time that a master key is considered network and a new master key is generated.     Patiend meater key TR - Enter a value for the amount of time that PACs generated using a network access of time that PACs generated using a network access of time that PACs generated using a network access of time that PACs generated using a network access of time that PACs generated using a network access of time that PACs generated using a network access of time that PACs generated using a network access of time that PACs generated using a network access of time that PACs generated using a network access of time that PACs access of the approximation of the pACs of the pace of
	EAP-GTC     EAP-MSCHAPv2     EAP-TLS     Submit Submit + Restart Cancel	<ul> <li>Tenned PAC TRL - Enter a value for the amount of time that a PAC is used before it expires and must be replaced. If the master key used to generate the Tunnel PAC has not expired, new PAC creation and assignment is automatic. If the master key used to generate the Tunnel PAC expired, automatic. If the master key used to generate the Tunnel PAC expired, automatic and provisioning must be used to provide the end-user client with a new PAC.</li> </ul>
1		👘 Internet
🌯 Start 🔂 🥭	CiscoSecure ACS - Mic	📑 7:58 PM

- 4. 활성/폐기된 마스터 키 TTL(Time-to-Live) 값을 원하는 대로 구성하거나 이 예에 표시된 대로 기본값으로 설정합니다.Authority ID Info(권한 ID 정보) 필드는 이 ACS 서버의 텍스트 ID를 나 타냅니다. 최종 사용자는 이 ACS 서버를 사용하여 인증할 ACS 서버를 결정할 수 있습니다. 이 필드는 반드시 입력해야 합니다.Client initial display message(클라이언트 초기 표시 메시 지) 필드는 EAP-FAST 클라이언트로 인증하는 사용자에게 보낼 메시지를 지정합니다. 최대 길이는 40자입니다. 최종 사용자 클라이언트가 디스플레이를 지원하는 경우에만 사용자에게 초기 메시지가 표시됩니다.
- 5. ACS가 익명 대역 내 PAC 프로비저닝을 수행하도록 하려면 Allow anonymous 대역 내 PAC provisioning(익명 대역 내 PAC 프로비저닝 허용) 확인란을 선택합니다.
- 6. Allowed *inner methods(허용된 내부* 방법) 옵션은 EAP-FAST TLS 터널 내에서 어떤 내부 EAP 방법을 실행할 수 있는지를 결정합니다. 익명 대역 내 프로비저닝의 경우 이전 버전과의 호환성을 위해 EAP-GTC 및 EAP-MS-CHAP를 활성화해야 합니다. Allow anonymous in-band PAC provisioning(익명 대역 내 PAC 프로비저닝 허용)을 선택하는 경우 EAP-MS-CHAP(0단 계) 및 EAP-GTC(2단계)를 선택해야 합니다.
- 7. Submit(제출)**을 클릭합니다.참고:** 익명 대역 내 PAC 프로비저닝 및 인증된 대역 내 프로비저 닝을 사용하여 EAP FAST를 구성하는 방법에 대한 자세한 내용 및 예는 <u>무선 LAN 컨트롤러</u> <u>및 외부 RADIUS 서버 컨피그레이션의 EAP-FAST 인증 예를</u> 참조하십시오.

#### 사용자 데이터베이스를 구성하고 url-redirect RADIUS 특성을 정의합니다

이 예에서는 무선 클라이언트의 사용자 이름 및 비밀번호를 각각 User1 및 User1로 구성합니다.

사용자 데이터베이스를 생성하려면 다음 단계를 완료하십시오.

- 1. 탐색 모음의 ACS GUI에서 **User** Setup(**사용자 설정)**을 **선택합니다**.
- 2. 새 사용자 무선을 만든 다음 Add/Edit를 클릭하여 이 사용자의 Edit 페이지로 이동합니다

For Tour of	Buardie Tone Diefs	Ling
s 👸 http://127	.0.0.1:1065/	
CO STOTEMO	User Setup	
Banatilian.	Select	Help
User Setup Group Setup Shared/Profile Components Network	User: User1 Find Add/Edit	<ul> <li>Shor Setup, and External User Databases</li> <li>Ending, a Specific User in the ACS Internal Database</li> <li>Adding, a User to the ACS Internal Oatabase</li> <li>Listing Usersames that Break with a Particular Character</li> <li>Listing All Usersames in the ACS Internal Oatabase</li> <li>Changing a Usersame in the ACS Internal User Database</li> <li>Ensure Operanic Users</li> </ul>
Configuration  Sprim Configuration  Interface Configuration  Administration  Configuration  Administration  Control  Control  Control  Porture  Porture  Porture  Porture  Reports and  Activity  Dolline  Documentation	List users beginning with letter/number: A R C P K K C B I I V V X I I Q I I Z S S C R 2 List all users Remove Dynamic Users Remove Dynamic Users	<ul> <li>User Setup enables you to configure individual user information, add user and delete users in the database. User Setup and External User Database Before ACS Can authenticate users with an external user database.</li> <li>You must have the database up and running on the external server. For example, if you are using this in card authentication, your taken server in be running and properly configured.</li> <li>You must have configuration overrides Group Setup Configuration.</li> <li>Notes User Setup configuration overrides Group Setup Configuration.</li> <li>Byou rely on the Unknown User Policy in the External User Databases section.</li> <li>Stokases section.</li> <li>External user database modification overrides Group Setup Configuration.</li> <li>Byou rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for years defined estamal user database. User Setup Cantificated once.</li> <li>External user database modification must be done from within the externat user database. User Setup Early External database inded a security, authorization, and accounting purposes. User Setup leaps track of users individual user information user database. User Setup lets you configure individual user information user database.</li> </ul>
		Finding a Specific User in the ACS Internal Database
		To find a user already in the ACS internal database, type the first few let of the username in the <b>liner</b> field, add an asterick (*) as a wildcard, and i <b>Field</b> . From the list of usernames displayed, click the username whose information you want to view or change.

3. 이 예에 표시된 대로 User Setup Edit(사용자 설정 수정) 페이지에서 Real Name(실명) 및 Description(설명)과 Password(비밀번호) 설정을 구성합니다.이 문서에서는 비밀번호 인증에 ACS 내부 데이터베이스를 사용합니다

.

CiscoSecure ALS - Microsoft Internet Explorer	<u>_[@]×</u>
Ele Edit Yew Fgvorites Icols Help	Linis » 🦧
Agdress a http://127.0.0.1:1065/	💌 🎽 🐼
User Setup	×
Edit	Help
User: User1 (New User)  Group Setup  Group Setup  Account Disabled	Account Disabled     Onisting a Unersons     Supplement Law Uner Info     Economic Anthentication     Group to which the uner is assigned
Components Configuration Supplementary User Info	Calibach     Cleant JP: Address Assignment     Advanced Settlines
Real Name Description Description	Natived Access Restrictions     Man Searches     Searches     Access Destas     Access Disable
Administration Central User Setup	Advanced IACACS - Sattleas     Advanced IACACS - Sattleas     IACACS - Inable Partner     IACACS - Inable Partner     IACACS - Dather Partner
Perform     Password Authentication:     ACS Internal Database     CiscoSecure PAP (Also used for CHAP/MS-	TACACS - Shell Command Antherization     Command Antherization     Command Antherization for Network Device Nanarement Applications     TACACS - Unknown Specific Attributes     RADUS Yeader Specific Attributes
CHAP/ARAP, if the Separate field is not checked.)	Account Disabled Status
Confirm Password	Select the Account Disabled check box to disable this account clear the check box to enable the account.
Separate (CHAP/MS-CHAP/ARAP) Password	[Back to Yes]
Confirm	Defeting a Username
Password Submit Cancel	The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the commut user account from the database, click <b>Delete</b> . When asked to confirm your action, click <b>OK</b> .
2) Done	internet
Start 🔀 🧶 👘 CiscoSecure ACS - Mic	9 7:56 PM

- 4. 페이지를 아래로 스크롤하여 RADIUS 특성을 수정합니다.
- 5. **[009\001] cisco-av-pair 확인란**을 선택합니다.
- 6. 사용자가 리디렉션되는 URL을 지정하려면 [009\001] cisco-av-pair 편집 상자에 다음 Cisco av-pair를 입력합니다.url-redirect=http://10.77.244.196/Admin-

Login.html

Cisco Systems	User Setup	[
addus addus	(useu iur benueass anu benukuun cherus such as routers)	A Help
User Setup	Password	Account Disabled
Group Setup	Password	Onisting a Username     Supplementary User Info     Passward Authonisation
Shared Profile Components	Cisco Airespace RADIUS Attributes	Group to which the user is assigned     Callback
Network Configuration	[14179/005] Aire-Interface-Nume	Clean IP. Address Assignment     Advanced Settings     Network Access Restrictions
System Configuration		Has Session     Usage Ovotas
Configuration		Account Disable     Demoloadable ACLs     Advanced TACACS - Settings
Administration Centrel	Cisco IOS/PIX 6.x RADIUS Attributes	TACACS - Enable Control     TACACS - Enable Passward
Databases	₩ [009\001] cisco-av-pair	InCACS- Outbound Passwerd     TACACS- Shell Command Authorization     Command Authorization     Command Authorization
Validation	url- redirect=http://10.77.244.196/	TACACS - Unknown Services     TETE RADRUS Attributes
Network Access Profiles	xumin-login.ncmi	RADIUS Vendor-Specific Attributes
Reports and Activity		Account Disabled Status
Documentation		Select the Account Disabled check box to disable this account clear the check box to enable the account.
	Back to Help	[Back to Top]
		Deleting a Username
	Submit Delete Cancel	The Delete button appears only when you are editing an existing user

관리 부서 사용자의 홈 페이지입니다.

- 7. Submit(제출)을 클릭합니다.
- 8. User2(운영 부서 사용자)를 추가하려면 이 절차를 반복합니다.
- 9. 데이터베이스에 관리 부서 사용자 및 운영 부서 사용자를 더 추가하려면 1단계부터 6단계까지 반복합니다.**참고:** RADIUS 특성은 Cisco Secure ACS의 사용자 레벨 또는 그룹 레벨에서 구성 할 수 있습니다.

# <u>다음을 확인합니다.</u>

컨피그레이션을 확인하려면 관리 부서 및 운영 부서의 WLAN 클라이언트를 해당 WLAN에 연결합 니다.

관리 부서의 사용자가 무선 LAN 관리자에 연결할 때 802.1x 자격 증명(여기서는 EAP-FAST 자격 증명)을 입력하라는 메시지가 표시됩니다. 사용자가 자격 증명을 제공하면 WLC는 해당 자격 증명 을 Cisco Secure ACS 서버에 전달합니다. Cisco Secure ACS 서버는 데이터베이스에 대한 사용자 의 자격 증명을 검증하고, 인증에 성공하면 Wireless LAN Controller에 url-redirect 특성을 반환합니 다. 이 단계에서 인증이 완료됩니다.

😨 Cisco Aironet Desktop Utilit	y - Current Profile: Admin		? 🗙
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
Profile Name:	Admin		
Link Status:	Not Associated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149	
Server Based Authentication:	None	Data Encryption: AES	
IP Address:	10.77.244.221		
Signal Strength		Good	
		Advanced	

사용자가 웹 브라우저를 열면 관리 부서의 홈 페이지 URL로 리디렉션됩니다. (이 URL은 cisco-avpair 특성을 통해 WLC로 반환됩니다.) 리디렉션 후에는 사용자가 네트워크에 대한 전체 액세스 권 한을 갖습니다. 스크린샷은 다음과 같습니다.



운영 부서의 사용자가 WLAN 작업에 연결할 때도 동일한 일련의 이벤트가 발생합니다.

🛜 Cisco Aironet Desktop Utility	y - Current Profile: Operatio	INS	? 🗙
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
utilituutilituu Profile Name:	Operations		
Link Status:	Authenticated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149	
Server Based Authentication:	EAP-FAST	Data Encryption: AES	
IP Address:	10.77.244.221		
Signal Strength:		Good	
		Advanced	



# <u>문제 해결</u>

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

**참고:** debug 명령을 사용하기 전에 Debug 명령에 대한 중요 정보를 참조하십시오.

다음 명령을 사용하여 컨피그레이션의 문제를 해결할 수 있습니다.

• show wlan wlan\_id - 특정 WLAN에 대한 웹 리디렉션 기능의 상태를 표시합니다.예를 들면 다음과 같습니다.

WLAN Identifier	1
Profile Name	Admin
Network Name (SSID)	Admin
Web Based Authentication	Disabled
Web Based Authentication Web-Passthrough	Disabled Disabled
Web Based AuthenticationWeb-PassthroughConditional Web Redirect	Disabled Disabled Disabled

• debug dot1x events enable - 802.1x 패킷 메시지의 디버그를 활성화합니다.예를 들면 다음과 같습니다.

Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to mobile 00:40:96:ac:dd:05 (EAP Id 16)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from

mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from

mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43)

- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for mobile 00:40:96:ac:dd:05
- Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800
   seconds, got from WLAN config.

Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05

```
setting dot1x reauth timeout = 1800
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry
     for station 00:40:96:ac:dd:05 (RSN 2)
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf
     to PMKID cache for station 00:40:96:ac:dd:05
 Fri Feb 29 10:27:16 2008: New PMKID: (16)
 Fri Feb 29 10:27:16 2008:
                              [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
     fb fa 8e 3c
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK
     lifetime can take care of same.
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile
     00:40:96:ac:dd:05 (EAP Id 17)
 Fri Feb 29 10:27:16 2008: Including PMKID in M1 (16)
                              [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
 Fri Feb 29 10:27:16 2008:
     fb fa 8e 3c
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to
     mobile 00:40:96:ac:dd:05
     state INITPMK (message 1), replay counter 00.00.00.00.00.00.00
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while
     in Authenticating state for mobile 00:40:96:ac:dd:05
• debug aaa events enable - 모든 aaa 이벤트의 디버그 출력을 활성화합니다. 예를 들면 다음과
 같습니다.
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
     Authentication Packet (id 103) to 10.77.244.196:1812, proxy state
     00:40:96:ac:dd:05-00:00
 Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11
 Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from
     RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
     Authentication Packet (id 104) to 10.77.244.196:1812, proxy state
     00:40:96:ac:dd:05-00:00
 Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2
 Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from
     RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
     'http://10.77.244.196/Admin-login.html' set
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for
     station 00:40:96:ac:dd:05
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station
     00:40:96:ac:dd:05
```

source: 4, valid bits: 0x0
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfName: '', aclName: '

## <u>관련 정보</u>

- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 5.0
- <u>Wireless LAN Controller 웹 인증 컨피그레이션 예</u>
- Wireless LAN Controller를 사용한 외부 웹 인증 컨피그레이션 예
- <u>무선 지원 페이지</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.