Per User ACL with Wireless LAN Controller and Cisco Secure ACS Configuration 예

목차

<u>소</u>개 사전 요구 사항 요구 사항 사용되는 구성 요소 표기규칙 배경 정보 네트워크 다이어그램 구성 무선 LAN 컨트롤러 구성 무선 사용자를 위한 VLAN 생성 Cisco Secure ACS로 인증하도록 WLC 구성 무선 사용자를 위한 새 WLAN 생성 사용자에 대한 ACL 정의 Cisco Secure ACS Server 구성 Cisco Secure ACS에서 무선 LAN 컨트롤러를 AAA 클라이언트로 구성 Cisco Secure ACS에서 사용자 및 사용자 프로필 구성 다음을 확인합니다. 문제 해결 문제 해결 정보 관련 정보

<u>소개</u>

이 문서에서는 WLC에 ACL(Access Control List)을 생성하고 RADIUS 권한 부여에 종속된 사용자에게 적용하는 방법을 예시하여 설명합니다.

<u>사전 요구 사항</u>

<u>요구 사항</u>

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 무선 클라이언트를 인증하도록 Cisco Secure ACS 서버를 구성하는 방법에 대한 기본 지식
- Cisco Aironet LAP(Lightweight Access Point) 및 Cisco WLC(Wireless LAN Controller) 컨피그 레이션에 대한 지식
- Cisco Unified Wireless Security 솔루션에 대한 지식

<u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 5.0.148.0을 실행하는 Cisco 4400 Series Wireless LAN Controller
- Cisco Aironet 1231 Series LAP(Lightweight Access Point)
- 버전 3.6을 실행하는 Cisco Aironet 802.11 a/b/g Cisco Wireless LAN 클라이언트 어댑터
- Cisco Aironet Desktop Utility 버전 3.6
- Cisco Secure ACS Server 버전 4.1
- IOS® 버전 12.4(11)T를 실행하는 Cisco 2800 Series Integrated Services Router
- 버전 12.0(5)WC3b를 실행하는 Cisco Catalyst 2900XL Series Switch

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

<u>표기 규칙</u>

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

<u>배경 정보</u>

사용자별 ACL(Access Control List)은 Cisco ID 네트워킹의 일부입니다.Cisco Wireless LAN Solution은 ID 네트워킹을 지원하며, 이를 통해 네트워크에서 단일 SSID를 광고할 수 있지만, 특정 사용자가 사용자 프로필에 따라 다른 정책을 상속할 수도 있습니다.

사용자별 ACL 기능은 RADIUS 권한 부여를 기반으로 사용자에게 무선 LAN 컨트롤러에 구성된 ACL을 적용하는 기능을 제공합니다.이 작업은 VSA(Airespace-ACL-Name Vendor Specific Attribute)를 사용하여 수행됩니다.

이 속성은 클라이언트에 적용할 ACL 이름을 나타냅니다.RADIUS Access Accept(RADIUS 액세스 수락)에 ACL 특성이 있는 경우 시스템은 인증 후 클라이언트 스테이션에 ACL-Name을 적용합니다 .이는 인터페이스에 할당된 모든 ACL을 재정의합니다.할당된 interface-ACL을 무시하고 새 ACL을 적용합니다.

다음은 ACL-Name Attribute 형식의 요약입니다.필드가 왼쪽에서 오른쪽으로 전송됩니다.

0 1 2 3 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 Length Vendor-Id Type Vendor-Id (cont.) | Vendor type | Vendor length | ACL Name... • Type - 26 for Vendor-Specific • Length - >7 • Vendor-Id - 14179 • Vendor type - 6 • Vendor length - >0 • Value - A string that includes the name of the ACL to use for the client.

The string is case sensitive.

Cisco Unified Wireless Network Identity Networking에 대한 자세한 내용은 <u>보안 솔루션 구성</u> 문서 <u>의 Configuring Identity Networking</u> 섹션을 참조하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.

이 설정에서는 Wireless LAN Controller WLC 및 LAP를 사용하여 부서 A와 부서 B의 사용자에게 무 선 서비스를 제공합니다.모든 무선 사용자는 공통 WLAN(SSID) Office를 사용하여 네트워크에 액세 스하고 VLAN Office-VLAN에 있습니다.



Cisco Secure ACS 서버는 무선 사용자를 인증하는 데 사용됩니다.EAP 인증은 사용자를 인증하는 데 사용됩니다.WLC, LAP 및 Cisco Secure ACS 서버는 레이어 2 스위치와 연결되어 있습니다.

라우터 R1은 표시된 것처럼 유선 측의 서버를 레이어 2 스위치를 통해 연결합니다.라우터 R1은 서 브넷 172.16.0.0/16에서 무선 클라이언트에 IP 주소를 제공하는 DHCP 서버 역할도 합니다.

다음과 같이 디바이스를 구성해야 합니다.

부서 A의 User1은 서버 172.16.1.100에만 액세스할 수 있습니다.

부서 B의 User2는 서버 172.16.1.50에만 액세스할 수 있습니다.

이를 위해 WLC에서 2개의 ACL을 생성해야 합니다.하나는 User1이고 다른 하나는 User2입니다. ACL이 생성되면 Cisco Secure ACS 서버가 무선 사용자의 인증에 성공하면 ACL 이름 특성을 WLC로 반환하도록 구성해야 합니다.그런 다음 WLC는 사용자에게 ACL을 적용하므로 네트워크에 대한 제한은 사용자 프로필에 따라 달라집니다.

참고: 이 문서에서는 사용자 인증에 LEAP 인증을 사용합니다.Cisco LEAP는 사전 공격에 취약합니 다.실시간 네트워크에서 EAP FAST와 같은 더 안전한 인증 방법을 사용해야 합니다.이 문서의 핵심 은 사용자별 ACL 기능을 구성하는 방법을 설명하는 것이므로 LEAP를 사용하여 간편하게 사용할 수 있습니다.

다음 섹션에서는 이 설정에 대한 디바이스를 구성하는 단계별 지침을 제공합니다.

<u>구성</u>

사용자별 ACL 기능을 구성하기 전에 기본 작업을 위해 WLC를 구성하고 LDAP를 WLC에 등록해야 합니다.이 문서에서는 WLC가 기본 작동을 위해 구성되었으며 LAP가 WLC에 등록되었다고 가정합 니다.LAP의 기본 작동을 위해 WLC를 설정하려고 시도하는 새 사용자는 WLC<u>(Wireless LAN</u> <u>Controller)에 대한 LAP(Lightweight AP) 등록을</u> 참조하십시오.

LAP가 등록되면 다음 단계를 완료하여 이 설정에 대한 디바이스를 구성합니다.

- 1. <u>무선 LAN 컨트롤러를 구성합니다.</u>
- 2. <u>Cisco Secure ACS 서버를 구성합니다.</u>
- 3. <u>컨피그레이션을 확인합니다.</u>

참고: 이 문서에서는 무선 측에 필요한 구성에 대해 설명합니다.이 문서에서는 유선 컨피그레이션 이 제자리에 있다고 가정합니다.

<u>무선 LAN 컨트롤러 구성</u>

무선 LAN 컨트롤러에서 다음을 수행해야 합니다.

- <u>무선 사용자를 위한 VLAN을 생성합니다.</u>
- Cisco Secure ACS로 무선 사용자를 인증하도록 WLC를 구성합니다.
- 무선 사용자를 위한 새 WLAN을 생성합니다.
- <u>무선 사용자에 대한 ACL을 정의합니다.</u>

<u>무선 사용자를 위한 VLAN 생성</u>

무선 사용자를 위한 VLAN을 생성하려면 다음 단계를 완료하십시오.

- 1. WLC GUI로 이동하여 Controller(컨트롤러) > Interfaces(인터페이스)를 선택합니다.Interfaces 창이 나타납니다.이 창에는 컨트롤러에 구성된 인터페이스가 나열됩니다.
- 2. 새 동적 인터페이스를 생성하려면 New(새로 만들기)를 클릭합니다.
- 3. Interfaces(**인터페이스) > New(새**) 창에서 Interface Name(인터페이스 이름) 및 VLAN ID를 입 력합니다.그런 다음 Apply(적용)를 클릭합니다.이 예에서 동적 인터페이스의 이름은 Office-VLAN이고 VLAN ID는 20입니다

ahaha				XXXXXXXXXX						- 0
CISCO	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Saye C COMMANDS	nfiguration	<u>P</u> ing Logout	Refre
ontroller	Interfaces	s > New						< 8 a	ck Appl	y
General	Interface	Name 🛛	fice-VLAN							_
Inventory	VLAN Id	21)							
Internal DHCP Server										
Mobility Management										
Master Controller Mode										
Network Time Protocol										
QoS										

4. Interfaces(**인터페이스) > Edit(편집**) 창에 동적 인터페이스의 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 입력합니다.WLC의 물리적 포트에 할당하고 DHCP 서버의 IP 주소를 입력합니 다.그런 다음 **Apply를** 클릭합니다

cisco		ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Saya C COMMANDS	euniguremon Einig Cogout Be
Controller General Inventory Interfaces Internal DHCP Server Mobility Management Ports Master Controller Mode Network Time Protocol QaS CDP	Interfaces > Edit General Information Interface Name MAC Address Interface Address Interface Address VLAN Identifier IP Address Netmask Gateway Physical Information Port Number Configuration Quarantine DHCP Information Primary DHCP Server Secondary DHCP Server Secondary DHCP Server Secondary DHCP Server ACCESS Control List ACL Name Note: Changing the Interfactory	Office-V 00:0b:0 [20] 172 [255 [172 [172 [172 [172 [172 [172 [172 [172	LAN 5:33:64:a0 :161.25 :255.0.0 :161.75 :161.75]]] LANs to be rectivity for			< Back Apply

이 예에서는 다음 매개변수가 Office-VLAN 인터페이스에 사용됩니다. Office-VLAN IP address: 172.16.1.25 Netmask: 255.255.0.0 Default gateway: 172.16.1.75 (sub-interface on Router R1) Port on WLC: 1 DHCP server: 172.16.1.75

<u>Cisco Secure ACS로 인증하도록 WLC 구성</u>

사용자 자격 증명을 외부 RADIUS 서버(이 경우 Cisco Secure ACS)로 전달하려면 WLC를 구성해 야 합니다. 그런 다음 RADIUS 서버는 사용자 자격 증명을 확인하고 무선 사용자의 인증에 성공하 면 ACL 이름 특성을 WLC에 반환합니다.

RADIUS 서버에 대한 WLC를 구성하려면 다음 단계를 완료합니다.

- 1. RADIUS Authentication Servers 페이지를 표시하려면 컨트롤러 GUI에서 Security and RADIUS Authentication(보안 및 RADIUS 인증)을 선택합니다.그런 다음 New(새로 만들기)를 클릭하여 RADIUS 서버를 정의합니다.
- 2. RADIUS Authentication Servers(RADIUS 인증 서버) > New(새 페이지)페이지에서 RADIUS 서버 매개변수를 정의합니다.이러한 매개변수에는 RADIUS 서버 IP 주소, 공유 암호, 포트 번 호 및 서버 상태가 포함됩니다

cisco		Sage Configuration Eing Logout Bafre OLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Authentication	Servers > New < Back Apply
Security AAA General General Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Local EAP Priority Order Access Control Lists IPSec Certs Wireless Protection Policies	RADIUS Authentication Server Index (Priority) Server IPAddress Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status	Servers > New < Back Apply
 Web Auth CIDS 	Support for RFC 3576 Retransmit Timeout	Enabled 💌
	Network User	Enable
	Management	፼ Enable
	IPSec	🗇 Enable

3. Network **User** and **Management**(네트워크 사용자 및 관리) 확인란은 RADIUS 기반 인증이 관 리 및 네트워크 사용자에 적용되는지 결정합니다.이 예에서는 Cisco Secure ACS를 IP 주소가 10.77.244.196인 RADIUS 서버로 사용합니다. Apply를 **클릭합니다**.

<u>무선 사용자를 위한 새 WLAN 생성</u>

다음으로 무선 사용자가 연결할 수 있는 WLAN을 생성해야 합니다.새 WLAN을 생성하려면 다음 단 계를 완료하십시오.

- 1. Wireless LAN Controller GUI에서 WLANs를 클릭합니다.이 페이지에는 컨트롤러에 있는 WLAN이 나열됩니다.
- 2. 새 WLAN을 생성하려면 New를 선택합니다.WLAN에 대한 WLAN ID, 프로파일 이름 및 WLAN SSID를 입력하고 Apply(적용)를 **클릭합니다**.이 설정을 위해 WLAN **Office**를 **만듭니다**

🖸 • 😔 • 🗈 🖻 🐔 1.	A 🔶 🙆 🔗 😓 🖾		an she an	No. State	AN CONTRACTOR			🚺 – 8 ×
cisco	MONITOR MLANS		WIRELESS	SECURITY	MANAGEMENT	Sege Co COMMANDS	nfiguration Bing HELP	Logout <u>R</u> efresh
WLANs	WLANs > New						< Back	Apply
VULANS	WLAN ID	1 💌						
AP Groups VLAN	Profile Name	Office						
	WLAN SSID	Office						

3. 새 WLAN을 생성하면 새 WLAN에 대한 WLAN > Edit 페이지가 나타납니다.이 페이지에서는 일반 정책, 보안, QoS 및 고급 매개변수를 포함하는 이 WLAN에 특정한 다양한 매개변수를 정 의할 수 있습니다

cisco	Sage Configuration Bing Logout Bet MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS AP Groups VLAN	WLANs > Edit C Back Apply General Security QoS Advanced Profile Name Office WLAN SSID Office WLAN Status F Enabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface Office-vlan BroadCast SSID
	Foot Notes I CKIP is not supported by IOxx model APs 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 5 Client MFP is not active unless WPA2 is configured

WLAN을 활성화하려면 General(일반) 정책 아래에서 WLAN Status(WLAN 상태)를 선택합니 다.풀다운 메뉴에서 적절한 인터페이스를 선택합니다.이 예에서는 인터페이스 **Office-vlan을** 사용합니다.이 페이지의 다른 매개변수는 WLAN 네트워크의 요구 사항에 따라 수정할 수 있습 니다.

4. **보안 탭을 선택합니다**.Layer 2 보안 풀다운 메뉴(LEAP 인증이므로)에서 **802.1x**를 선택합니다 . 802.1x 매개 변수 아래에서 적절한 WEP 키 크기를 선택합니다

ANS	WI ANS > Edit	k Anoli
	General Security OoS Advanced	w matha
WLANS WLANS AP Groups VLAN	Layer 2 Layer 3 AAA Servers	
	Layer 2 Security 802.1X MAC Filtering 802.1X Parameters	
	802-11 Data Encryption Type Key Size	
	@ WEP 104 bits	
	Foot Notes	
	1 CKIP is not supported by 10xx model APs 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication	
	4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to re 5 Client MFP is not active unless WPA2 is configured	set excluded clieni

5. Security(보안) 탭에서 AAA 서버 하위 탭을 선택합니다.무선 클라이언트를 인증하는 데 사용 되는 AAA 서버를 선택합니다.이 예에서는 ACS 서버 10.77.244.196을 사용하여 무선 클라이 언트를 인증합니다

cisco	Sage Configuration Bing Logout B MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS AP Groups VLAN	WLANs > Edit < Back
	Foet Notes 1 CKUP is not supported by 10xx model APs 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients 5 Client MFP is not active unless WPA2 is configured

6. Advanced 탭을 선택합니다.Allow AAA Override(AAA 재정의 허용)를 선택하여 무선 LAN의 AAA를 통해 사용자 정책 재지정을 구성합니다

cisco	Sage Configuration Eing Logout Befre MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS WLANS AP Groups VLAN	WLANs > Edit < Back
	Foot Notes I CKIP is not supported by 10xx model APs 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 5 Client MPP is not active unless WPA2 is configured

AAA 재정의가 활성화되고 클라이언트에 충돌하는 AAA 및 Cisco Wireless LAN Controller 무 선 LAN 인증 매개변수가 있는 경우 AAA 서버에서 클라이언트 인증을 수행합니다.이 인증의 일부로서 운영 체제는 클라이언트를 기본 Cisco 무선 LAN 솔루션 무선 LAN VLAN에서 AAA 서버에서 반환하고 Cisco Wireless LAN 컨트롤러 인터페이스 컨피그레이션에 미리 정의된 VLAN으로 이동하며, 이는 MAC 필터링, 802.1X 및/또는 WPA 작업에 대해 구성된 경우에만 발생합니다.모든 경우 운영 체제는 Cisco Wireless LAN 컨트롤러 인터페이스 컨피그레이션에 서 미리 정의된 경우 AAA 서버에서 제공하는 QoS, DSCP, 802.1p 우선순위 태그 값 및 ACL도 사용합니다.

7. 네트워크의 요구 사항에 따라 다른 매개변수를 선택합니다. Apply를 클릭합니다.

<u>사용자에 대한 ACL 정의</u>

이 설정에 대해 두 개의 ACL을 생성해야 합니다.

• ACL1:User1에 대한 액세스를 172.16.1.100 서버에만 제공

• ACL2:User2에 대한 액세스를 172.16.1.50 서버에만 제공하려면

WLC에서 ACL을 구성하려면 다음 단계를 완료합니다.

- 1. WLC GUI에서 Security(보안) > Access Control Lists(액세스 제어 목록)를 선택합니다.Access Control Lists 페이지가 나타납니다.이 페이지에는 WLC에 구성된 ACL이 나열됩니다.또한 ACL을 수정하거나 제거할 수 있습니다.새 ACL을 생성하려면 New를 클릭합니다.
- 2. 이 페이지에서는 새 ACL을 생성할 수 있습니다.ACL의 이름을 입력하고 Apply를 **클릭합니다** .ACL이 생성되면 **Edit**(편집)를 클릭하여 ACL에 대한 규칙을 생성합니다.
- 3. User1은 서버 172.16.1.100에만 액세스할 수 있어야 하며 다른 모든 디바이스에 대한 액세스 가 거부되어야 합니다.이를 위해 이러한 규칙을 정의해야 합니다.무선 LAN 컨트롤러에서

<u>ACL을 구성하는</u> 방법에 대한 자세한 내용은 Wireless LAN Controller 컨피그레이션 예제의 ACL을 참조하십시오

cisco	MON	TOR W	LANS CONTR	OLLE	R WIRELESS	SEC	URITY M		Saya C COMMANDS	onfiguration HELP	n <u>P</u> ing I	.ogout <u>R</u> efre
Security	Acc	ess Cor	trol Lists > E	dit					< B	ack	Add Nev	v Rule
▼ AAA General ▼ RADIUS	Gene	eral s List Nam	ve User1				-					
Accounting	Seq	Action	Source IP/M	ask	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	
LDAP Local Net Users MAC Eltering	1	Permit	172.16.0.0	/	172.16.1.100	/	Any	Any	Any	Any	Inbound	
Disabled Clients User Login Policies AP Policies	2	Permit	172.16.1.100 255.255.255.25	55	172.16.0.0 255.255.0.0	′	Any	Any	Αογ	Any	Outbound	۵
Local EAP	L											
Priority Order												
 Access Control Lists Access Control Lists CPU Access Control Lists 												
> IPSec Certs												
Wireless Protection Policies												
> Web Auth												
> CIDS												
						_						

4. 마찬가지로 User2에 대한 ACL을 생성해야 합니다. 이 경우 User2는 서버 172.16.1.50에만 액 세스할 수 있습니다.이는 User2에 필요한 ACL입니다

cisco	MONI	tor w	ilans co	ONTROLL	ER WIRELESS	SECURIT	Y Mé	NAGEMENT	Saye Co COMMANDS	nfiguration HELP	Eing (Logout <u>R</u>	
Security	Acce	ss Con	trol Lists	> Edit					< 84	ick	Add Nev	v Rule	
-	Gene	iral											
General RADIUS Authentication	Access List Name User2												
Accounting + TACACS+	Seq	Action	Source I	P/Mask	Destination IP/Mask	Prof	tocol	Source Port	Dest Port	DSCP	Direction		
LDAP Local Net Users MAC Filtering	Т	Permit	172.16.0.	0 /	172.16.1.50	/ Any	,	Any	Αογ	Any	Inbound	۰	
Disabled Clients User Login Policies AP Policies	2	Permit	172.16.1.	50 / 55.255	172.16.0.0 255.255.0.0	/ Any	,	Any	Any	Any	Outbound	٠	
Local EAP													
Priority Order	L												
Access Control Lists Access Centrol Lists CPU Access Control Lists													
IPSec Certs													
Wireless Protection Policies													
Web Auth													
CIDS													

이제 이 설정에 대해 무선 LAN 컨트롤러를 구성했습니다.다음 단계는 Cisco Secure Access Control 서버를 구성하여 무선 클라이언트를 인증하고 인증 성공 시 ACL Name 특성을 WLC에 반환하는 것입니다.

<u>Cisco Secure ACS Server 구성</u>

Cisco Secure ACS에서 무선 클라이언트를 인증하려면 다음 단계를 완료해야 합니다.

- <u>Cisco Secure ACS에서 Wireless LAN Controller를 AAA 클라이언트로 구성합니다.</u>
- <u>Cisco Secure ACS에서 사용자 및 사용자 프로필을 구성합니다.</u>

<u>Cisco Secure ACS에서 무선 LAN 컨트롤러를 AAA 클라이언트로 구성</u>

Cisco Secure ACS에서 Wireless LAN Controller를 AAA 클라이언트로 구성하려면 다음 단계를 완료하십시오.

1. Network **Configuration > Add AAA client를 클릭합니다**.Add **AAA client** 페이지가 나타납니다 .이 페이지에서 WLC 시스템 이름, 관리 인터페이스 IP 주소, 공유 암호 및 Authenticate Using **RADIUS Airespace를 정의합니다**.예를 들면 다음과 같습니다

Cisco Statens	Network Configuration	2
all board board	Edit	Help
User Satup Setup Setup Satup Satup Components Components Components Seglere Configuration	Add AAA Client Hostname wlc AAA Client IP Address 10.77.244.210 x Shared Secret Cisco	AAA Client Histname AAA Client Histname AAA Client IP Address Shared Secret Network Device Group Rathus Key Wran Authenticate Using Sindle Cannet TACACS - AAA Client Log Undate/Watchdeg Packets from this AAA Client Log RADIUS Tunneling Packets from this AAA Client Replace RADIUS Fort info with Username from this AAA Client Match Fromed IP-Address with over IP
Admikistration Control Databases Pestare Pestare Pestare Prefiler Reports and Activity	RADIUS Key Wrap Key Encryption Key Message Authenticator Code Key Key Input Format C ASCII Authenticate Using RADIUS (Cisco Airespace)	AAA Client Hestname AAA Client Hestname The AAA Client Hostname is the name assigned to the AAA client. [Rack to Top]
Documentation	Single Connect TACACS+ AAA Client (Record stop in accounting on failure) Log Update/Watchdog Packets from this AAA Client Log RADIUS Tunneling Packets from this AAA Client Replace RADIUS Port info with Usemame from this AAA Client	AAA Client IP Address The AAA Client IP Address is the IP address assigned to the AAA client. If you want to designate more than one AAA client with a single AAA client entry in ACS, you can
	Match Framed-IP-Address with user IP address for accounting packets from this AAA Client Submit Submit + Apply Cancel	specify the IP address for each AAA chart to be represented by this AAA chart to the represented separate each IP address, press Enter. You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every

참고: Cisco Secure ACS에 구성된 공유 암호는 RADIUS **Authentication Servers(RADIUS 인 중 서버) > New(새로 만들기)** 아래에서 WLC에 구성된 공유 암호와 일치해야 합니다.

2. Submit **+Apply를 클릭합니다**.

Cisco Secure ACS에서 사용자 및 사용자 프로필 구성

Cisco Secure ACS에서 사용자를 구성하려면 다음 단계를 완료하십시오.

1. ACS GUI에서 User Setup(사용자 설정)을 선택하고 사용자 이름을 입력한 다음 Add/Edit(추가 /수정)를 클릭합니다.이 예에서는 사용자가 User1입니다

Cisco Systems	User Setup	×
-dbdb-	Select	Help
User Setop Setop <	User: User: Find Add/Edit List users beginning with letter/number: A & & & & & & & & & & & & & & & & & & &	<list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><table-row></table-row></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item>

2. **사용자 설정** 페이지가 나타나면 해당 사용자에 대한 모든 매개변수를 정의합니다.이 예에서는 EAP 인증을 위해 이러한 매개변수만 필요하므로 사용자 이름, 비밀번호, 보조 사용자 정보 및 RADIUS 특성이 구성됩니다

Cisco Systems	User Setup	l
-db-db-	Edit	🚔 Help
User Setup	User: UserA (New User)	Account Disabled Beleting a Stername Supplementary User Info Password Avthentication Group to which the user is assigned
Network Configuration System Configuration Interface Configuration	Supplementary User Info Real Name User 1 Description	Callback Clent IP Address Assignment Advanced Settings Mark Sessions Usage Quarter Access Restrictions Man Sessions Usage Quarter Access Restrictions Access Assignment Access Assignment Advanced TACACS+ Settings
Adheartonad Chiefenal User Databases Pestare Validation Validation Validation	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)	TACACS - Enable Dessured TACACS - Enable Dessured TACACS - Outbound Personnel TACACS - Outbound Authorization TACACS - Shell Command Authorization Command Authorization for Network Device Management Applications TACACS + Unknown Services TACACS + Unknown Services
Reports and Activity Dollare Documentation	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password	Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account. [hack to Tan] Deleting a Username
	When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned: 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 tha current user account from the database, click Delete. When asked to confirm your action, click DK. [kack to Top] Supplementary User Info Type the applicable information in any supplemental user information how of the applicable information in any supplemental user information

사용자별 Cisco Airespace RADIUS 특성이 표시될 때까지 아래로 스크롤합니다.Aire**-ACL-**Name을 선택하여 ACS가 WLC에 ACL 이름을 성공적으로 반환하도록 합니다.User1의 경우 WLC에 ACL User1을 생성합니다.ACL 이름을 User1로 입력합니다

0 · 0 · 🖻 🖻	🏠 🔎 😤 🕗 😓 🖪	🦓 – 8 ×
Cisco Sesteus	User Setup	×
ad bard bar	Date exceeds:	Help
User Setup Setup Setup Setup Setup Setup Setup Setup Configuration Seturation Seturation Configuration Seter Configuration	Sep 9 2007 Failed attempts exceed: Failed attempts since last successful login: 0 Reset current failed attempts count on submit Cloce Akrespace RADIUS Attributes (14179/002) Aixe-QeS-Level Bronze (14179/003) Aixe-DSCP 0	Account Disabled Beleting a Busmane Supplementary User Info Busmane Supplementary User Info Calback Calback
S Reports and Activity	[14179404] Aire-802.1P-Tag	
Documentation	[14179005] Aixe-Interface-Name	Account Disabled Status Select the Account Disabled check how to disable this account clear
		the check box to enable the account.
	M [14179/006] Aire-Act-Nume	Iback to Tapl
	User1	Deleting a Username
		The Delete button appears only when you are editing as existing user account, not when you are adding a new user account. To delete the conner user account from the database, click Delete . When asked to confirm your action, click DK .
	P Back to Help	[Back to Top]
		Supplementary User Info
	Submit Cancel	Type the applicable information in any supplemental user information boxes that appear. To add or chance fields, click Interface

3. 동일한 절차를 반복하여 User2를 만듭니다(여기에 표시됨).

G • O • 🖻 🖻 :	🚯 🖻 🕱 🕙 🐼 😼 🖬	$M = \theta \times$
Cisco Systems	User Setup	X
-dlb-dlb-	Select	Help
User Stared Profile Shared Profile </th <th>Select User: User2 Find Add/Edit List users beginning with letter/number: ABCPEFSSIIVYXXII QIIIISSIIVYXXII QIIIISSI List all users Remove Dynamic Users 2 bek to Help</th> <th> Help Person and a factor of these Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rational Rationants Person a factor of the ACS Internal Rational Rationants Person a factor of the ACS Internal Rational Rationants Person ACS and the ACS Internal Rational Rationants Person ACS and the ACS Internal Rational Rationants Person Rationant Rationant Rationants Person Rationant Rationants Person Rationant Rationant Rationants Person Rationants Person Rationants Person Rationant Rationants Person Rationants<!--</th--></th>	Select User: User2 Find Add/Edit List users beginning with letter/number: ABCPEFSSIIVYXXII QIIIISSIIVYXXII QIIIISSI List all users Remove Dynamic Users 2 bek to Help	 Help Person and a factor of these Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rational Rationants Person a factor of the ACS Internal Rational Rationants Person a factor of the ACS Internal Rational Rationants Person ACS and the ACS Internal Rational Rationants Person ACS and the ACS Internal Rational Rationants Person Rationant Rationant Rationants Person Rationant Rationants Person Rationant Rationant Rationants Person Rationants Person Rationants Person Rationant Rationants Person Rationants<!--</th-->
0 · O · E E ·	 A ≠ € ⊗ 5 B 	🕅 - 5 ×
Cisco Systems	User Setup	×
adbad ba	Edit	Help E
User Setup Group Setup Setup Setup Setup Setup Setup Configuration Setup Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration	User: UserA (New User) Account Disabled Supplementary User Info Real Name User2 Description User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS-	Account Disabled Beletima a Distributed Supplementary User Info Supplementary User Info Destroard Authentication Comp to which the user is assigned Calback Client IP Address Assignment Advanced Settings Network Access Restrictions Max Sessions Unage Quetas Network Access Restrictions Max Sessions Disable Aftact Advanced TACACS - Settings TACACS - Inable Password TACACS - Inable Password TACACS - Undersmod Password TACACS - RADIUS Attributes
Reports and Activity Documentation	Password for a token card user allows CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned: Submit Cancel	Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account. [hack to Teo] Deleting a Username The Delete buttos appears only when you are editing as existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When asked to certify your action, click OK. [hack to Teo] Supplementary User Info Type the applicable information in any supplemental user information

😋 • 🗇 🕑 🖻	6 🖉 🖉 🗢 💩 🖬	🥂 – 8 ×
Cisco Systems	User Setup	X
dbdb	Date exceeds:	Help
User Setup Setup Components Configuration Configuration Configuration Configuration	Sep 9 2007 Failed attempts exceed: 5 Failed attempts since last successful login: 0 Reset current failed attempts count on submit	Account Disabled Deletina a Username Supplementary User Info Description of the series assigned Calback Clean UP Advess Assignment Advanced Settings Network Access Restrictions Usar Quetas Max Sessions Usar Quetas Access ThisAble Downlandable ACLS
Administration Centrol	Clisco Alirespace RADIUS Attributes	Advanced TACACS = Settings TACACS = Enable Cantrol TACACS = Enable Researced
Pesternal User Databases Validation Validation Profile:	[14179002] Aire-QoS-Level Bronze [14179003] Aire-DSCP	TACACS - Outloand Password TACACS - Schlound Password TACACS - Schlound Authorization Command Authorization Command Authorization TACACS - Unknown Services TACACS - Unknown Services RADIUS Yeador: Specific Attributes
Reports and Activity	[14179404] Aire-802.1P-Tag	Account Disabled Status
Documentation	[141791005] Aize-Interface-Name	Select the Account Disabled check box to disable this account clear the check box to enable the account.
(₩ [14179006] Aże-Acl.Nate	[hack to Tap]
	jusera	The Delete button appears only when you are editing as emisting user account, not when you are adding a new user account. To delete the current user account from the database, click Delete . When asked to confirm your action, click OK .
	💡 Back to Help	[Rack to Tap]
		Sapplementary User Info
	Submit Cancel	Type the applicable information in any supplemental user information

4. 원하는 EAP **인증** 방법을 수행하도록 인증 서버가 구성되어 있는지 확인하려면 System Configuration and **Global Authentication Setup**을 클릭합니다.EAP 컨피그레이션 설정에서 적 절한 EAP 방법을 선택합니다.이 예에서는 LEAP 인증을 사용합니다.완료되면 **Submit(제출**)을 클릭합니다

O • O • 🖬 🗐	6 × 3 C & V E	📲 – 9 X
Cisco Systems	System Configuration	Hep A
DA LUser	Allow EAP-MSCHAPv2	
Lig Setup	Allow EAP-GTC	Use this page to specify settings for various authentication protocols.
Graup Setup	Allow Posture Validation	EAP Configuration
Shared Profile Components	C Allow EAP-TLS	• EAP-FIS
2 Network	Select one or more of the following options:	+ LEAP
Configuration	F Certificate SAN comparison	EAP-H05 AD EAD Request Tracest
System Configuration	M Certificate CN comparison	HS-CHAP.Configuration
- University	Fi Certificate Binary comparison	
Configuration	EAP-TLS session timeout (minutes): 120	
Administration Centrel	La construction de la constructi	EAP Configuration
12 External User	Cisco client initial message:	EAP is a flexible request-response protocol for arbitrary surface in a figure state (REC 2204) EAP is learned on two of
913 Databases	PEAP session timeout (minutes): 120	another protocal such as UDP, 802.1x or RADIUS and supports
Pesture Validation	Enable Fast Reconnect:	Back to Teol
Network Access	545 540T	1
	EAP-FAST Configuration	PEAP
Activity	CAP TAGT CONSIGNATION	PEAP is the euter layer protocel for the secure tunnel.
and 1 Online	EAP-TLS	
Documentation	Allow EAP-TLS	Notes IEAP is a certificate-based authentication protocol. IEAP authentication can across only after your base consoluted the required stress
	Select one or more of the following options:	to the ACS Certificate Setup page.
	R Certificate SAN comparison	Allow EAD-MSCHADy2 Use to enable EAD-MSCHADy2 within MS DEAD
	E Certificate CN comparison	authentication. Enable this protocol for any repository that supports MS-
	Fo Certificate Binary comparison	CHAPV2, SUCH as microsoft AU, and the AUS Internal Database.
	EAP-TLS session timeout (minutes): 120	Allow EAP-GTC - Use to enable EAP-GTC within Cisco PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.
-	LEAP	Allow Porture Validation
	Allow LEAP (For Aironet only)	posture validation of Network Admission Control (NAC) clients.
	Submit Submit + Restart Cancel	Allow EAP-TLS - Use to enable the EAP-TLS protocol as an additional inner method for PEAP. The PEAP/EAP-TLS feature strongly laverages the existing

<u>다음을 확인합니다.</u>

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

무선 클라이언트를 LEAP 인증과 함께 Lightweight AP에 연결하여 컨피그레이션이 예상대로 작동 하는지 확인합니다.

참고: 이 문서에서는 클라이언트 프로파일이 LEAP 인증을 위해 구성된 것으로 가정합니다.LEAP <u>인증을</u> 위해 802.11 a/b/g 무선 클라이언트 어댑터를 구성하는 방법에 대한 자세한 내용은 EAP 인 증 사용을 참조하십시오.

무선 클라이언트의 프로파일이 활성화되면 사용자에게 LEAP 인증을 위한 사용자 이름/비밀번호를 입력하라는 메시지가 표시됩니다.이는 User1이 LAP에 대한 인증을 시도할 때 발생합니다.

Enter Wireless Network Password		
Please enter your LE network	AP username and password to log on to the wireless	
User Name :	User1	
Password :	•••••	
Log on to :		
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter	
Profile Name :	Office	
	OK Cancel	

경량 AP와 WLC는 자격 증명을 확인하기 위해 외부 RADIUS 서버(Cisco Secure ACS)에 사용자 자 격 증명을 전달합니다.RADIUS 서버는 데이터를 사용자 데이터베이스와 비교하고, 인증에 성공하 면 사용자에 대해 구성된 ACL 이름을 WLC에 반환합니다.이 경우 ACL User1은 WLC로 반환됩니 다.

Cisco Aironet Desktop Utility - Current Profile:	Office-TSWEB
Action Options Help	
Current Status Profile Management Diagnostics	
CISCO SYSTEMS	
Profile Name: Office-TSWEB	
Link Status: Authenticated	Network Type: Infrastructure
Wireless Mode: 5 GHz 54 Mbps	Current Channel: 64
Server Based Authentication: LEAP	Data Encryption: WEP
IP Address: 172.16.0.14	
Signal Strength:	Excellent
	Advanced

무선 LAN 컨트롤러는 이 ACL을 User1에 적용합니다. 이 Ping 출력은 User1이 서버 172.16.1.100에만 액세스할 수 있지만 다른 장치는 액세스할 수 없음을 나타냅니다.

```
D:\Documents and Settings\Administrator>ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time=3ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 3ms, Average = 1ms
D:\Documents and Settings\Administrator>ping 172.16.1.50
Pinging 172.16.1.50 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

마찬가지로 User2가 WLAN에 액세스를 시도하면 인증에 성공하면 RADIUS 서버는 ACL User2를 WLC로 반환합니다.

Enter Wireless Network Password		
Please enter your LE network	AP username and password to log on to the wireless	
User Name :	User2	
Password :	•••••	
Log on to :		
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter	
Profile Name :	Office	
	OK Cancel	

Authentication Status	?
Card Name: Cisco Aironet 802.1	1a/b/g Wireless Adapter
Profile Name: Office-TSWEB	
Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Skipped because the domain name was not configured

무선 LAN 컨트롤러는 이 ACL을 User2에 적용합니다. 이 Ping 출력은 User2가 서버 172.16.1.50에 만 액세스할 수 있지만 다른 장치는 액세스할 수 없음을 나타냅니다.

D:\Documents and Settings\Administrator>ping 172.16.1.50 Pinging 172.16.1.50 with 32 bytes of data: Reply from 172.16.1.50: bytes=32 time=3ms TTL=255 Reply from 172.16.1.50: bytes=32 time=18ms TTL=255 Reply from 172.16.1.50: bytes=32 time=1ms TTL=255 Reply from 172.16.1.50: bytes=32 time=1ms TTL=255 Ping statistics for 172.16.1.50: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 18ms, Average = 5ms D:\Documents and Settings\Administrator>ping 172.16.1.100 Pinging 172.16.1.100 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 172.16.1.100: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

<u>문제 해결</u>

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

무선 LAN 컨트롤러에서 AAA 인증 문제를 해결하기 위해 이러한 디버그 명령을 사용할 수도 있습니 다 • debug aaa all enable - 모든 AAA 메시지의 디버그를 구성합니다.

• debug dot1x packet enable - 모든 dot1x 패킷의 디버그를 활성화합니다.

• debug client <MAC Address> - 무선 클라이언트 디버깅을 활성화합니다.

다음은 debug aaa all enable 명령의 예입니다.

참고: 출력의 일부 행이 공간 제약으로 인해 두 번째 라인으로 이동되었습니다.

Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104 Thu Aug 16 14:42:54 2007: Callback.....0x85ed228
 Thu Aug 16 14:42:54 2007:
 protocolType.....0x00140001
 proxyState......00:40:96:AF:3E:93-03:01 Thu Aug 16 14:42:54 2007: Thu Aug 16 14:42:54 2007: Packet contains 16 AVPs (not shown) Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Successful transmission of Authentication Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00 Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99 b4 19 27 28 eb 5f 35 9c-4.....'(._5. Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73 65 72 31 1f 13 30 30 2duser1..00-Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46 2d 33 45 2d 39 33 1e 20 40-96-AF-3E-93.. Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35 2d 35 42 2d 46 42 2d 44 00-0B-85-5B-FB-D Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65 2d 54 53 57 45 42 05 06 0:Office-TSWEB.. Thu Aug 16 14:42:54 2007: 00000050: 00 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1awlc. Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00 00 01 06 06 00 00 00 ...7c.... Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d 06 00 00 13 40 06 00 = @ . . Thu Aug 16 14:42:54 2007: 0000080: 00 00 0d 41 06 00 00 00 06 51 04 32 30 4f 27 02 ...A....Q.200'. Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d 87 9d 0b f9 dd e5 39 0d Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96 dc c3 55 ff 7c 51 4e 75 Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56 43 3d 30 2e 31 3b 50 12 ser1..SVC=0.1;P. Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0 c6 2f 5e f5 65 e9 3e 2d ..;5[^].../[^].e.>-Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4 27 e6 d4 0e 1b 8e 5d 19 ...6.1j.'....]. Thu Aug 16 14:42:54 2007: 00000010: 60 lc c2 16 4f 06 03 01 00 04 18 0a 53 56 43 3d Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb 90 ec 48 9b fb d7 ce ca 0.1;P.1...H.... Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09 ;d.... Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=11 Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=11 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Access-Challenge received from RADIUS server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3 Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800 Thu Aug 16 14:42:54 2007: structureSize.....104 Thu Aug 16 14:42:54 2007: resultCode.....255 protocolUsed.....0x0000001 Thu Aug 16 14:42:54 2007: Thu Aug 16 14:42:54 2007: proxyState..... 00:40:96:AF:3E:93-03:01

```
Thu Aug 16 14:42:54 2007: Packet contains 3 AVPs (not shown)
```

Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xblab104 Thu Aug 16 14:42:54 2007: Callback......0x85ed228 protocolType.....0x00140001 Thu Aug 16 14:42:54 2007: Thu Aug 16 14:42:54 2007: proxyState..... 00:40:96:AF:3E:93-03:02 Thu Aug 16 14:42:54 2007: Packet contains 16 AVPs (not shown) Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Successful transmission of Authentication Packet (id 2) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00 Thu Aug 16 14:42:54 2007: 00000000: 01 02 00 c0 38 b6 b2 20 ff 5b f2 16 64 df 02 618....[..d..a Thu Aug 16 14:42:54 2007: 00000010: cf f5 93 4b 01 07 75 73 65 72 31 1f 13 30 30 2d ...K..User1..00-Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46 2d 33 45 2d 39 33 1e 20 40-96-AF-3E-93.. Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35 2d 35 42 2d 46 42 2d 44 00-0B-85-5B-FB-D Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65 2d 54 53 57 45 42 05 06 0:Office. Thu Aug 16 14:42:54 2007: 00000050: 00 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1aM....wlc. Thu Aug 16 14:42:54 2007: 0000060: 0c 00 00 37 63 01 06 00 00 01 06 06 00 00 00 ...7c.... Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d 06 00 00 01 13 40 06 00 = @ . . Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00 06 51 04 32 30 4f 17 01 ...A....Q.200.. Thu Aug 16 14:42:54 2007: 00000090: 01 00 15 11 01 00 08 0f 14 05 65 1b 28 61 c9 75e.(a.u Thu Aug 16 14:42:54 2007: 000000a0: 73 65 72 31 18 0a 53 56 43 3d 30 2e 31 3b 50 12 ser1..SVC=0.1;P. Thu Aug 16 14:42:54 2007: 000000b0: 05 ba 6b af fe a4 b0 d1 a2 94 f8 39 80 ca 3c 96 Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8 6c 07 8e fb 58 84 8d f6=].1...X... Thu Aug 16 14:42:54 2007: 00000010: 33 6d 93 21 08 06 ff ff ff ff 4f 27 02 01 00 25 3m.!...8 Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 le 33 b5 4e 69 90 e7 84 25% Thu Aug 16 14:42:54 2007: 00000030: 42 a9 20 ac 84 33 9f 87 ca dc c9 b3 75 73 65 72 B....3....user Thu Aug 16 14:42:54 2007: 00000040: 31 1a 3b 00 00 00 09 01 35 6c 65 61 70 3a 73 65 1.;....5leap:se Thu Aug 16 14:42:54 2007: 00000050: 73 73 69 6f 6e 2d 6b 65 79 3d 29 80 1d 2c 1c 85 ssion-key=).... Thu Aug 16 14:42:54 2007: 00000060: db 1c 29 7e 40 8a b8 93 69 2a 55 d2 e5 46 89 8b ...)~@...i*U...F.. Thu Aug 16 14:42:54 2007: 00000070: 2c 3b 65 49 3e 44 cf 7e 95 29 47 54 1a 1f 00 00 ,;eI>D.~.)GT.... Thu Aug 16 14:42:54 2007: 00000080: 00 09 01 19 61 75 74 68 2d 61 6c 67 6f 2d 74 79auth-algo-ty Thu Aug 16 14:42:54 2007: 00000090: 70 65 3d 65 61 70 2d 6c 65 61 70 1a 0d 00 00 37 pe=eap-leap....7 Thu Aug 16 14:42:54 2007: 000000a0: 63 06 07 55 73 65 72 31 19 14 43 41 43 53 3a 30 c..User1..CACS:0 Thu Aug 16 14:42:54 2007: 000000b0: 2f 39 2f 61 34 64 66 34 64 32 2f 31 50 12 9a 71 /9/a4df4d2/1P..q Thu Aug 16 14:42:54 2007: 000000c0: 09 99 7d 74 89 ad af e5 c8 b1 71 94 97 d1 ..}t....q... Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=2 Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=2 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Access-Accept received from RADIUS server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3

Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800 Thu Aug 16 14:42:54 2007: structureSize......236 Thu Aug 16 14:42:54 2007: resultCode.....0 Thu Aug 16 14:42:54 2007: protocolUsed.....0x0 0000001 Thu Aug 16 14:42:54 2007: proxyState.....00: 40:96:AF:3E:93-03:02 Thu Aug 16 14:42:54 2007: Packet contains 6 AVPs: Thu Aug 16 14:42:54 2007: AVP[01] Framed-IP-Address.....0xffffffff (-1) (4 bytes) Thu Aug 16 14:42:54 2007: AVP[02] EAP-Message.....DATA (37 bytes) Thu Aug 16 14:42:54 2007: AVP[03] Cisco / LEAP-Session-Key...DATA (16 bytes) Thu Aug 16 14:42:54 2007: AVP[04] Airespace / ACL-Name.....User1 (5 bytes) Thu Aug 16 14:42:54 2007: AVP[05] Class.....CACS:0/9/a4df4d2/1 (18 bytes) Thu Aug 16 14:42:54 2007: AVP[06] Message-Authenticator.....DATA (16 bytes) Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Applying new AAA override for station 00:40:96:af:3e:93 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Override values for station 00:40:96:af:3e:93 source: 4, valid bits: 0x400 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName:User1 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Inserting new RADIUS override into chain for station 00:40:96:af:3e:93

show wlan summary 명령의 조합을 사용하여 어떤 WLAN에서 RADIUS 서버 인증을 사용하는지 인 식할 수 있습니다.그런 다음 show client summary 명령을 보고 RADIUS WLAN에서 어떤 MAC 주소 (클라이언트)가 성공적으로 인증되었는지 확인할 수 있습니다.또한 이를 Cisco Secure ACS에서 시 도 또는 실패한 시도 로그와 연계할 수 있습니다.

Cisco에서는 무선 클라이언트를 사용하여 ACL 구성을 테스트하여 올바르게 구성했는지 확인하는 것이 좋습니다.올바르게 작동하지 않을 경우 ACL 웹 페이지에서 ACL을 확인하고 ACL 변경 사항이 컨트롤러의 인터페이스에 적용되었는지 확인합니다.

다음 show 명령을 사용하여 컨피그레이션을 확인할 수도 있습니다.

• show acl summary - 컨트롤러에 구성된 ACL을 표시하려면 show acl summary 명령을 사용합니다.

예를 들면 다음과 같습니다.

(Cisco Controller) >show acl summary

ACL	Name	Applied
Usei	c1	Yes
Usei	2	Yes

• show acl detailed <ACL_Name> - 구성된 ACL에 대한 자세한 정보를 표시합니다.예를 들면 다 음과 같습니다.참고: 출력의 일부 행이 공간 제약으로 인해 두 번째 라인으로 이동되었습니다. Cisco Controller) >show acl detailed User1

co controller) show act detailed us

Source Port Dest Port I Dir IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action __ ___ ____ ----- -----1 In 172.16.0.0/255.255.0.0 172.16.1.100/255.255.255.255 Any 0-65535 0-65535 Any Permit 2 Out 172.16.1.100/255.255.255 172.16.0.0/255.255.0.0 Any 0-65535 0-65535 Any Permit (Cisco Controller) > show acl detailed User2 Source Destination Source Port Dest Port I Dir IP Address/Netmask IP Address/Netmask Range Range DSCP Action Prot __ ___ ____ ---- ----- ----- -----1 Tn 172.16.0.0/255.255.0.0 172.16.1.50/255.255.255.255 0-65535 0-65535 Any Permit Anv 2 Out 172.16.1.50/255.255.255.255 172.16.0.0/255.255.0.0 0-65535 0-65535 Any Permit Anv

• show client detail <MAC Address of the client> - 무선 클라이언트에 대한 자세한 정보를 표시 합니다.

<u>문제 해결 정보</u>

다음 팁을 사용하여 문제를 해결하십시오.

- 컨트롤러에서 RADIUS 서버가 활성 상태이고 대기 또는 비활성화되어 있지 않은지 확인합니다
- 컨트롤러에서 WLAN(SSID)의 드롭다운 메뉴에서 RADIUS 서버를 선택했는지 확인합니다.
- RADIUS 서버가 무선 클라이언트에서 인증 요청을 수신하고 검증하는지 확인합니다.
- 이 작업을 수행하려면 ACS 서버에서 Passed Authentications and Failed Attempts 보고서를 확 인합니다.이러한 보고서는 ACS 서버의 Reports and Activities에서 사용할 수 있습니다.

<u>관련 정보</u>

- <u>무선 LAN 컨트롤러의 ACL:규칙, 제한 사항 및 예</u>
- <u>무선 LAN 컨트롤러 컨피그레이션의 ACL 예</u>
- WLC(Wireless LAN Controller)를 사용하는 MAC 필터 컨피그레이션 예
- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 5.2
- <u>기술 지원 및 문서 Cisco Systems</u>