

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

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[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](#)

소개

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

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

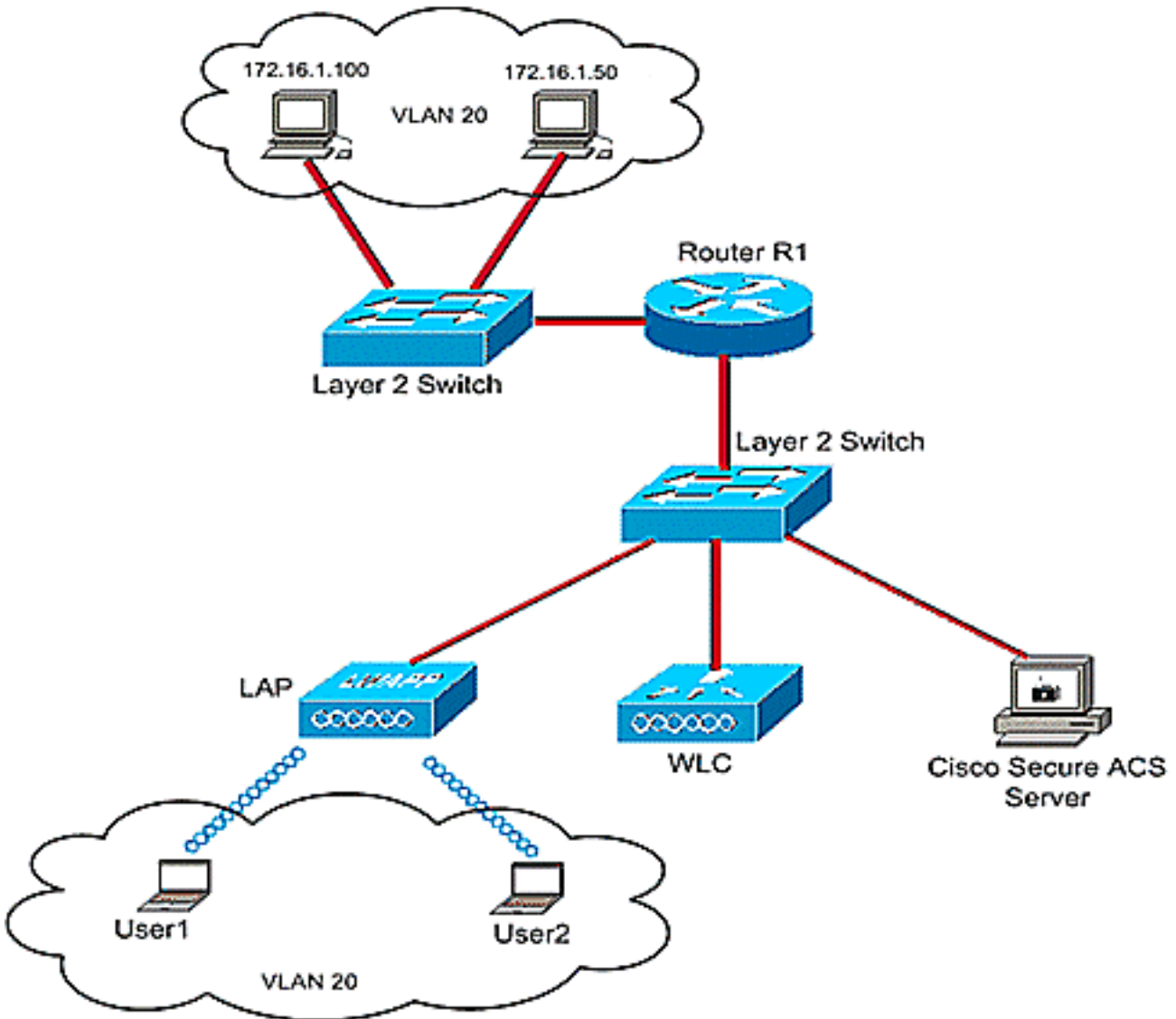
- 무선 클라이언트를 인증하도록 Cisco Secure ACS 서버를 구성하는 방법에 대한 기본 지식
- Cisco Aironet LAP(Lightweight Access Point) 및 Cisco WLC(Wireless LAN Controller) 컨피그레이션에 대한 지식
- Cisco Unified Wireless Security 솔루션에 대한 지식

Cisco Unified Wireless Network Identity Networking에 대한 자세한 내용은 [보안 솔루션 구성 문서의 Configuring Identity Networking](#) 섹션을 참조하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.

이 설정에서는 Wireless LAN Controller WLC 및 LAP를 사용하여 부서 A와 부서 B의 사용자에게 무선 서비스를 제공합니다. 모든 무선 사용자는 공통 WLAN(SSID) Office를 사용하여 네트워크에 액세스하고 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 서브넷 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 취약합니다. 실시간 네트워크에서 EAP FAST와 같은 더 안전한 인증 방법을 사용해야 합니다. 이 문서의 핵심은 사용자별 ACL 기능을 구성하는 방법을 설명하는 것이므로 LEAP를 사용하여 간편하게 사용할 수 있습니다.

다음 섹션에서는 이 설정에 대한 디바이스를 구성하는 단계별 지침을 제공합니다.

구성

사용자별 ACL 기능을 구성하기 전에 기본 작업을 위해 WLC를 구성하고 LDAP를 WLC에 등록해야 합니다. 이 문서에서는 WLC가 기본 작동을 위해 구성되었으며 LAP가 WLC에 등록되었다고 가정합니다. LAP의 기본 작동을 위해 WLC를 설정하려고 시도하는 새 사용자는 WLC([Wireless LAN Controller](#))에 대한 [LAP\(Lightweight AP\) 등록](#)을 참조하십시오.

LAP가 등록되면 다음 단계를 완료하여 이 설정에 대한 디바이스를 구성합니다.

1. [무선 LAN 컨트롤러를 구성합니다.](#)
2. [Cisco Secure ACS 서버를 구성합니다.](#)
3. [컨피그레이션을 확인합니다.](#)

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

무선 LAN 컨트롤러 구성

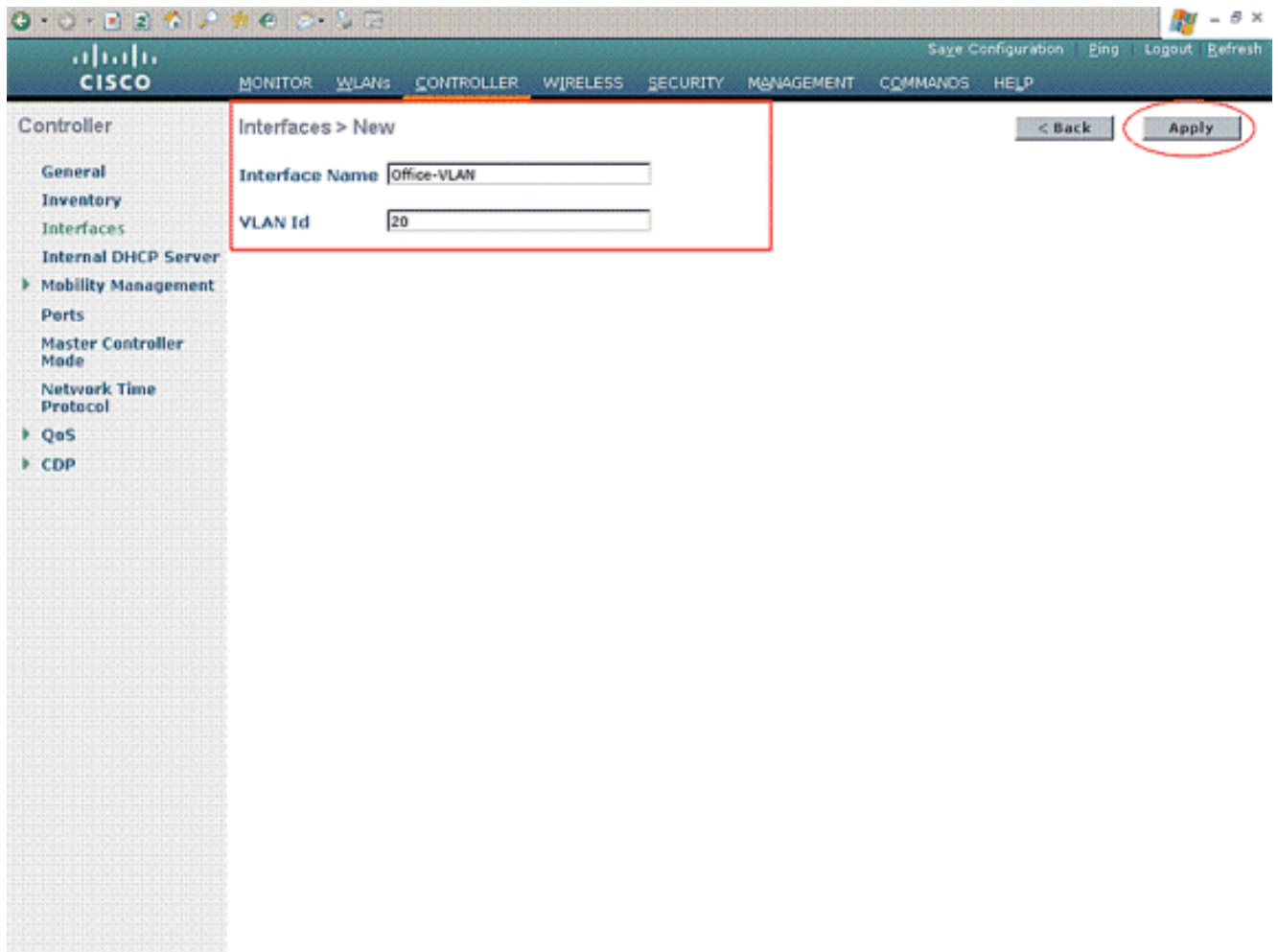
무선 LAN 컨트롤러에서 다음을 수행해야 합니다.

- [무선 사용자를 위한 VLAN을 생성합니다.](#)
- [Cisco Secure ACS로 무선 사용자를 인증하도록 WLC를 구성합니다.](#)
- [무선 사용자를 위한 새 WLAN을 생성합니다.](#)
- [무선 사용자에 대한 ACL을 정의합니다.](#)

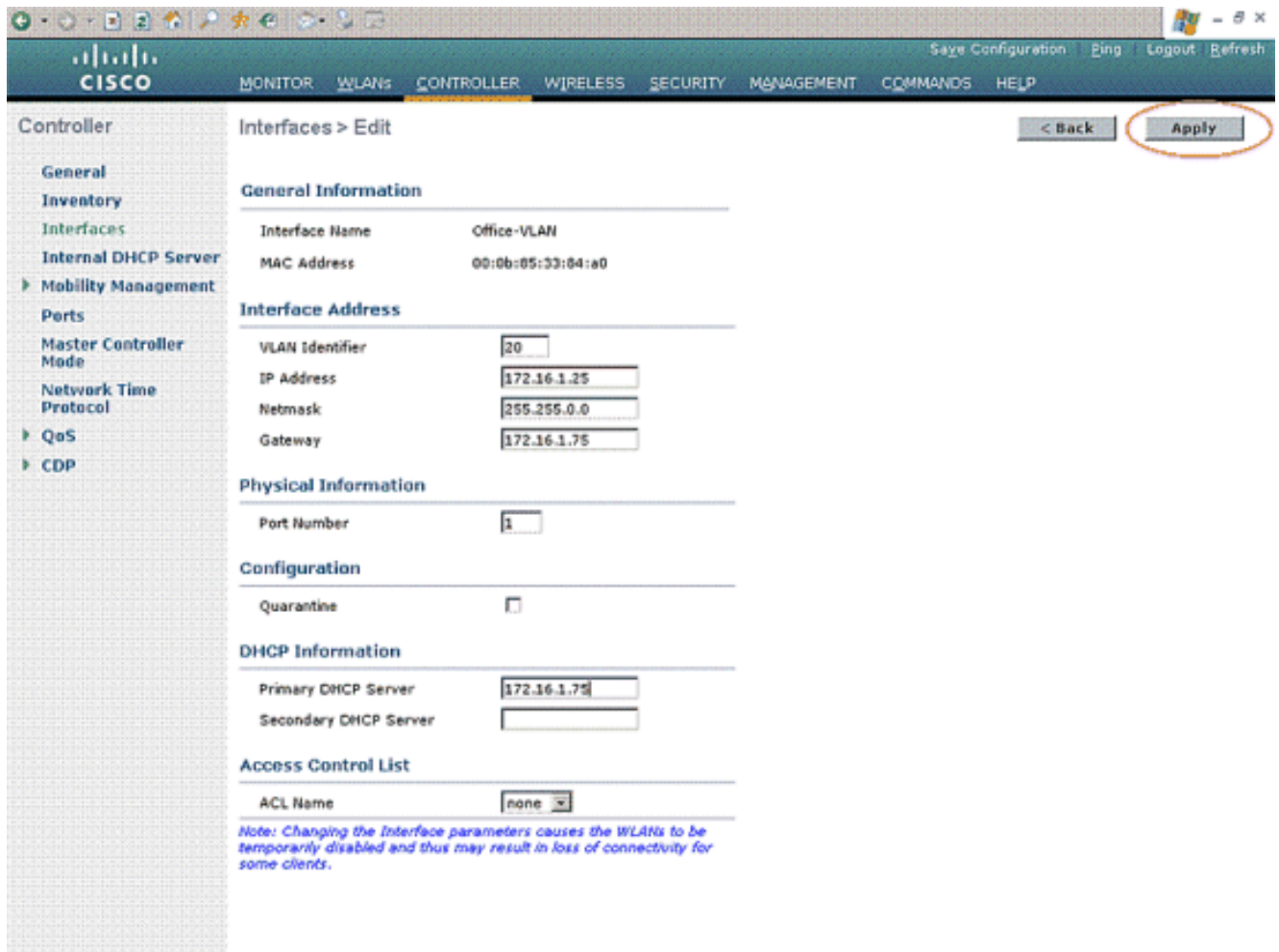
무선 사용자를 위한 VLAN 생성

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 입력합니다. 그런 다음 Apply(적용)를 클릭합니다. 이 예에서 동적 인터페이스의 이름은 Office-VLAN이고 VLAN ID는 20입니다.



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



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

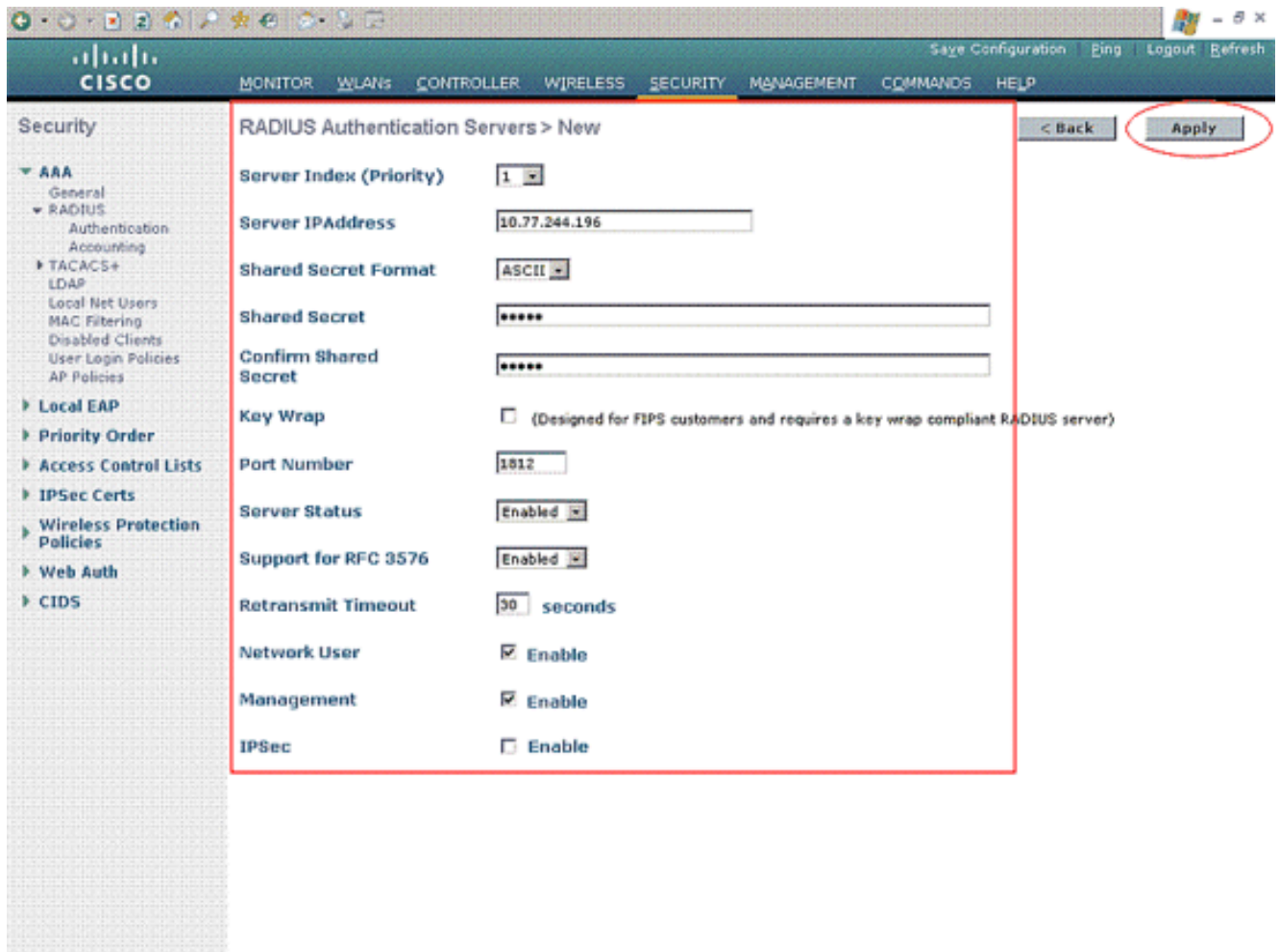
DHCP server: 172.16.1.75

[Cisco Secure ACS로 인증하도록 WLC 구성](#)

사용자 자격 증명을 외부 RADIUS 서버(이 경우 Cisco Secure ACS)로 전달하려면 WLC를 구성해야 합니다. 그런 다음 RADIUS 서버는 사용자 자격 증명을 확인하고 무선 사용자의 인증에 성공하면 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 번호 및 서버 상태가 포함됩니다

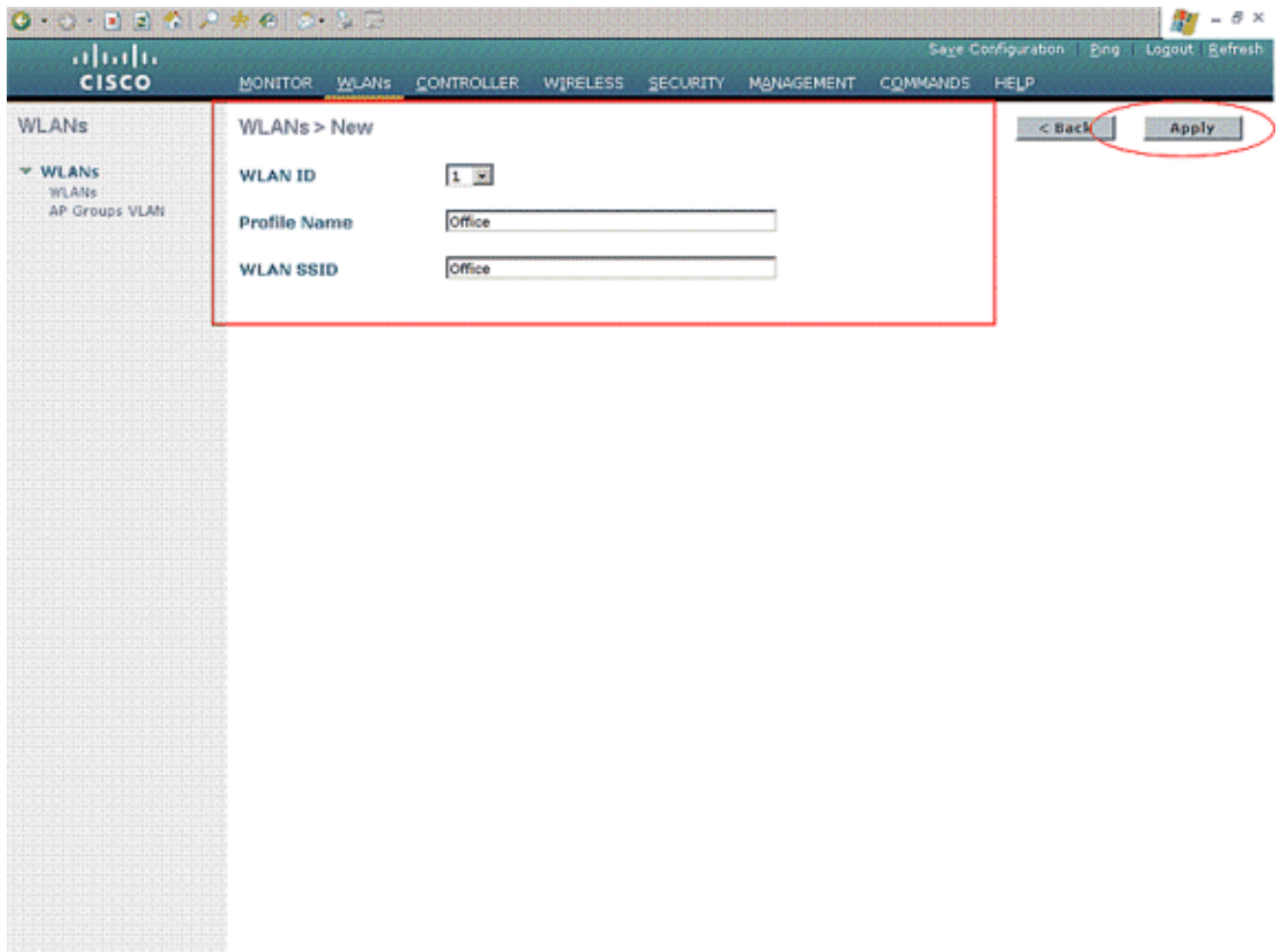


3. Network User and Management(네트워크 사용자 및 관리) 확인란은 RADIUS 기반 인증이 관리 및 네트워크 사용자에 적용되는지 결정합니다. 이 예에서는 Cisco Secure ACS를 IP 주소가 10.77.244.196인 RADIUS 서버로 사용합니다. Apply를 클릭합니다.

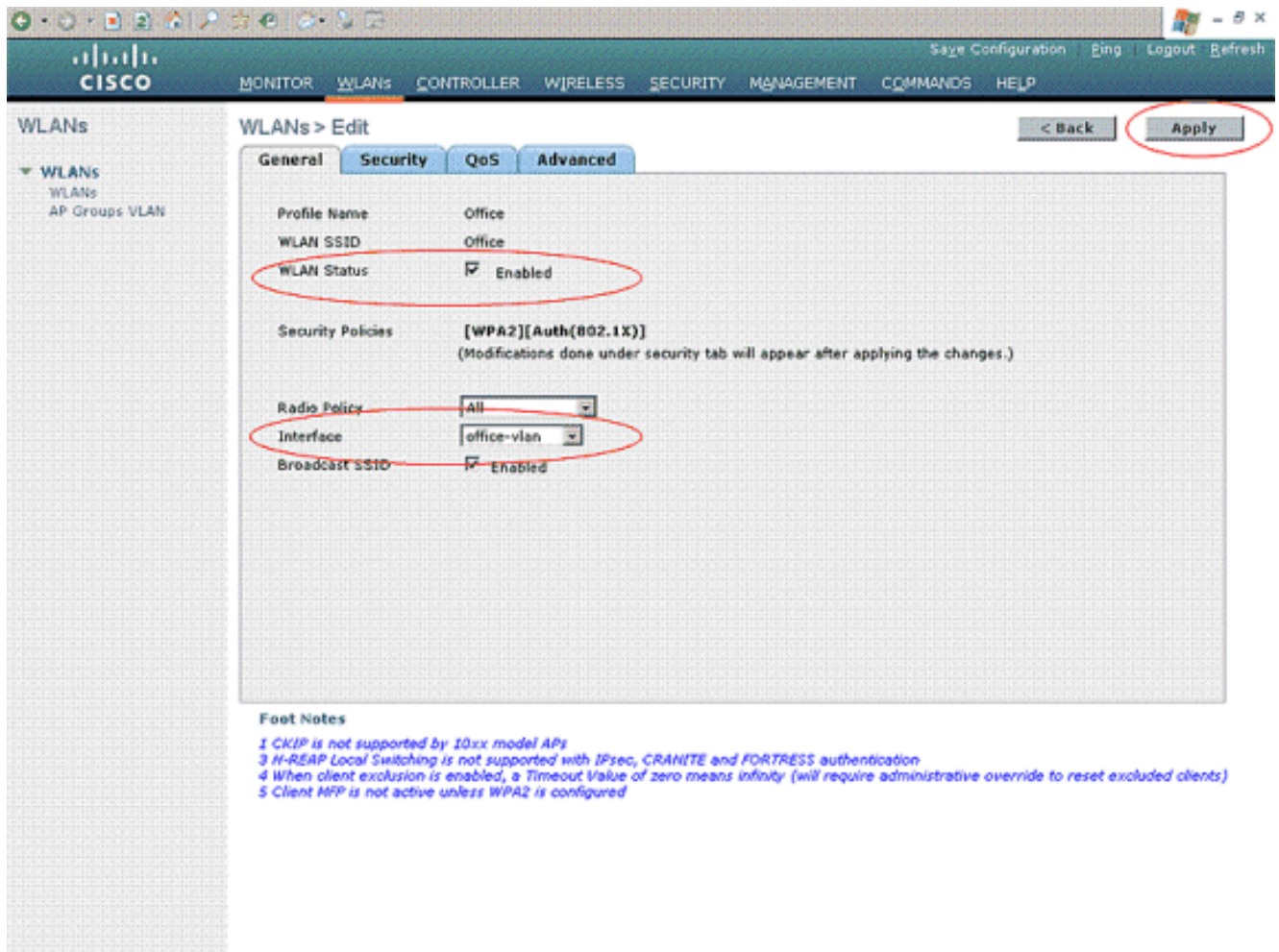
무선 사용자를 위한 새 WLAN 생성

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

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

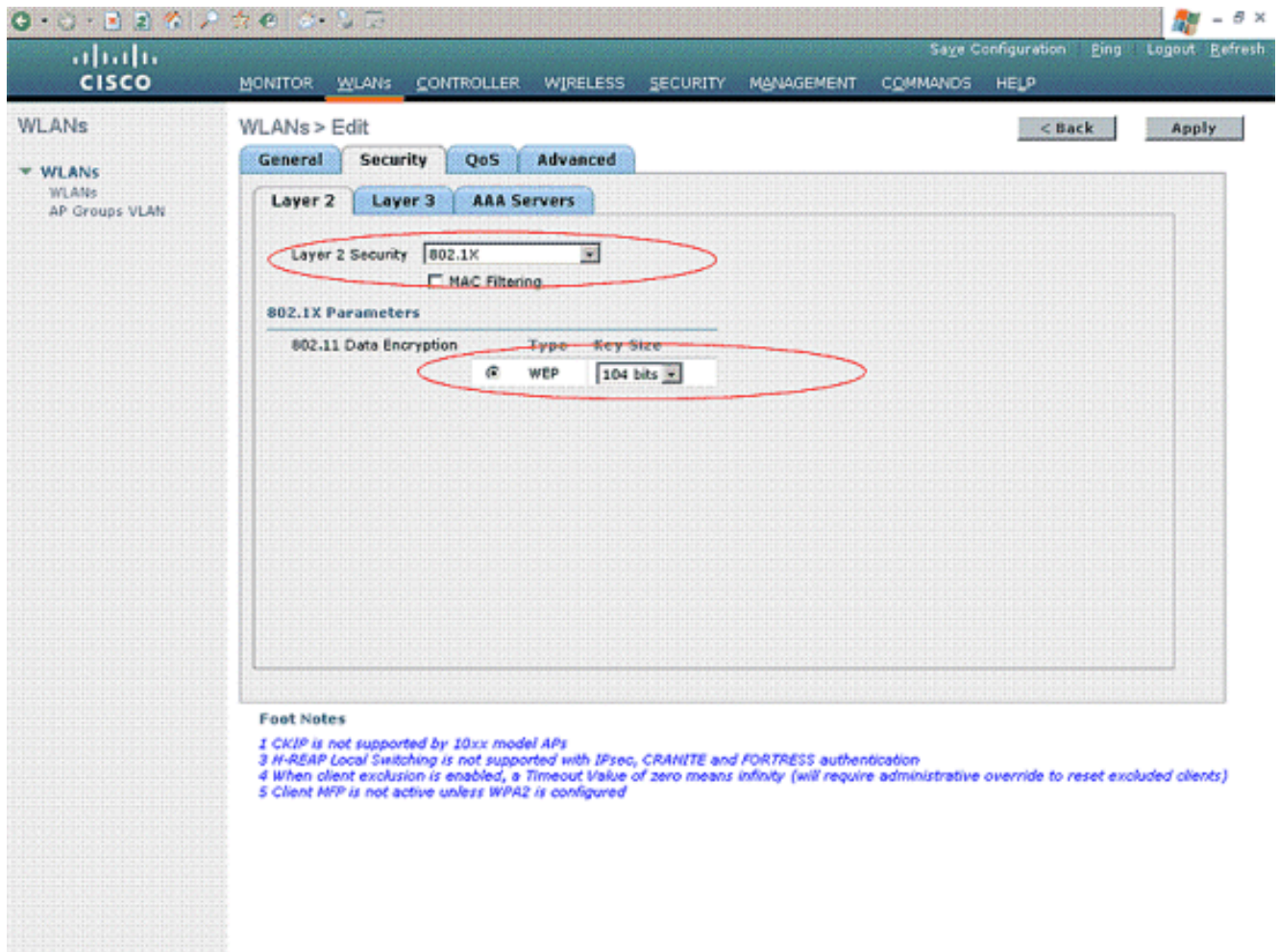


3. 새 WLAN을 생성하면 새 WLAN에 대한 **WLAN > Edit** 페이지가 나타납니다. 이 페이지에서는 일반 정책, 보안, QoS 및 고급 매개변수를 포함하는 이 WLAN에 특정한 다양한 매개변수를 정의할 수 있습니다



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

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.



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

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 Servers	
Authentication Servers	Accounting Servers	Server 1	Server 2
Server 1	IP:10.77.244.196, Port:1812	None	None
Server 2	None	None	None
Server 3	None	None	None

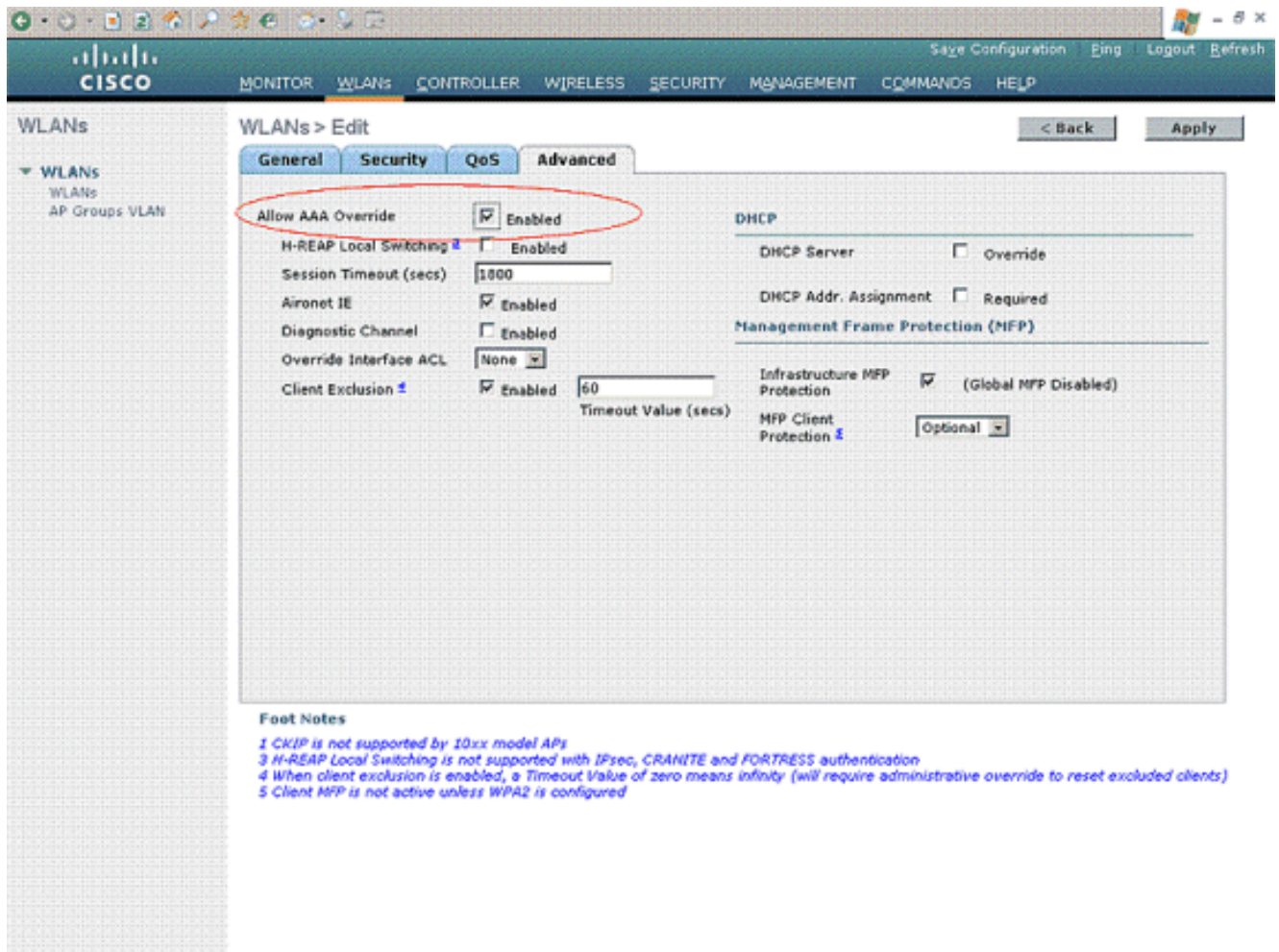
Local EAP Authentication

Local EAP Authentication enabled

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 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



AAA 재정의가 활성화되고 클라이언트에 충돌하는 AAA 및 Cisco Wireless LAN Controller 무선 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 컨피그레이션에서 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.

사용자에 대한 ACL 정의

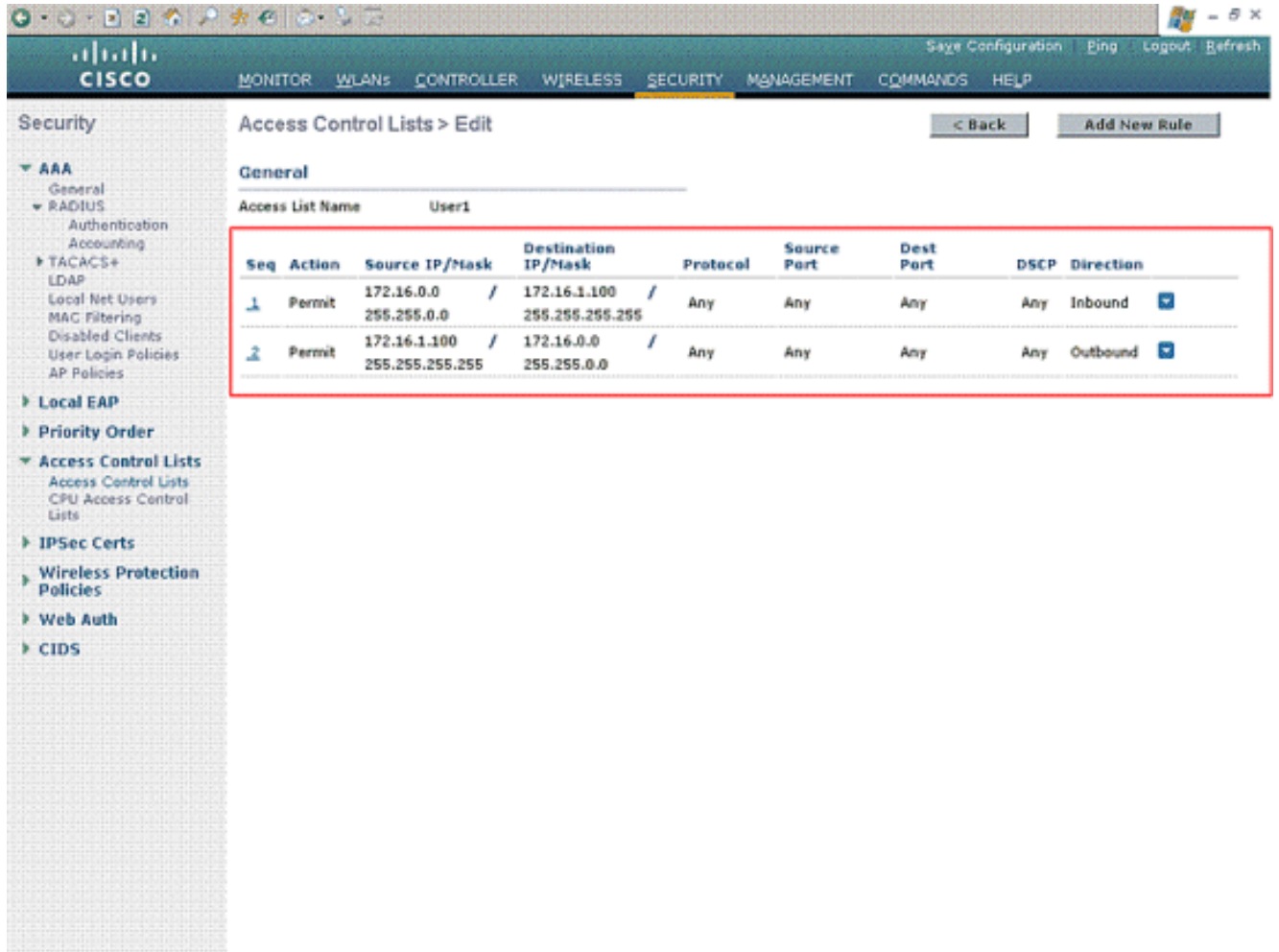
이 설정에 대해 두 개의 ACL을 생성해야 합니다.

- ACL1: User1에 대한 액세스를 172.16.1.100 서버에만 제공
- ACL2: User2에 대한 액세스를 172.16.1.50 서버에만 제공하려면

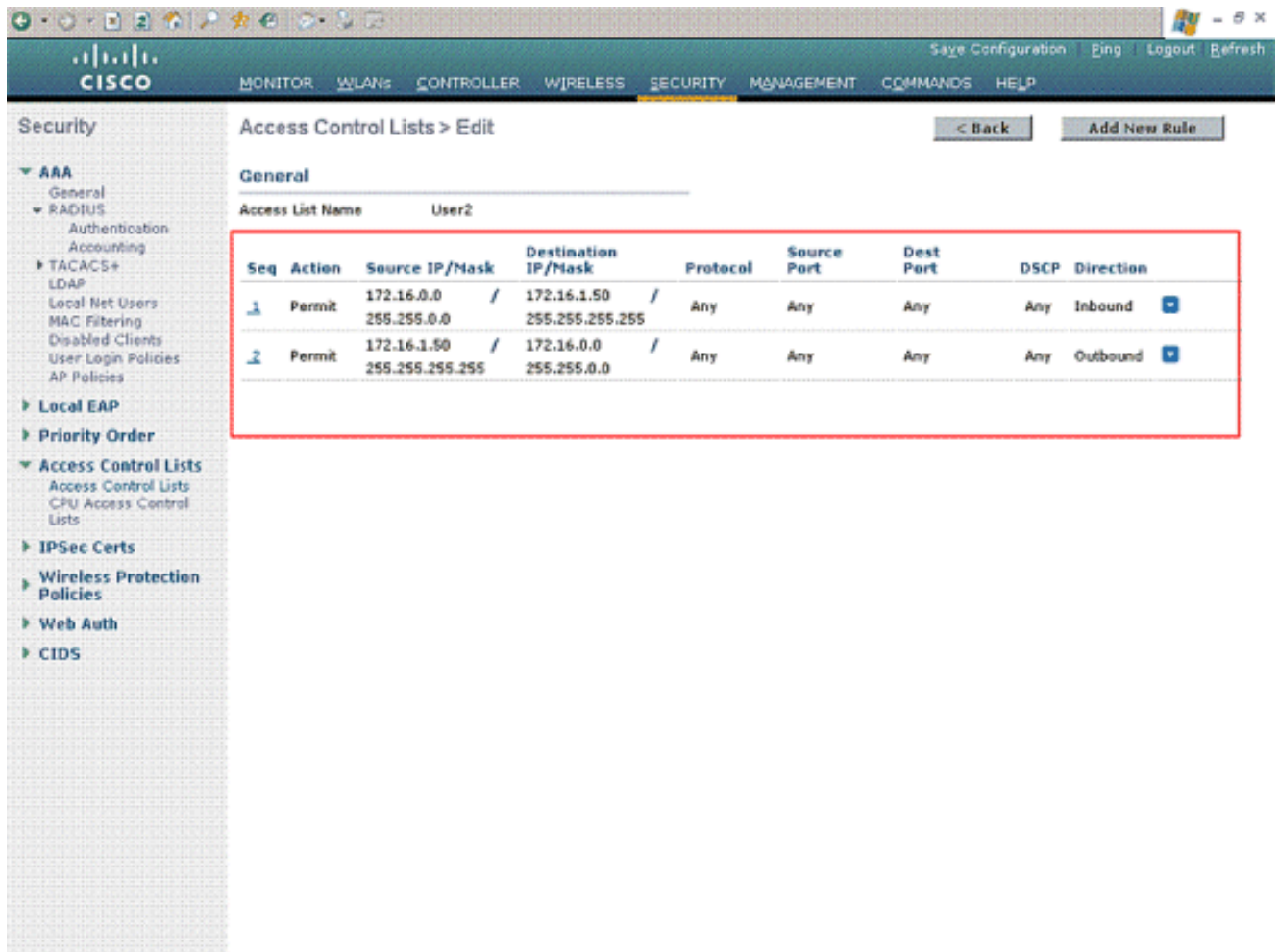
WLC에서 ACL을 구성하려면 다음 단계를 완료합니다.

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 **New**를 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 액세스가 거부되어야 합니다. 이를 위해 이러한 규칙을 정의해야 합니다. 무선 LAN 컨트롤러에서

ACL을 구성하는 방법에 대한 자세한 내용은 Wireless LAN Controller 컨피그레이션 예제의 ACL을 참조하십시오



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



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.

Cisco Secure ACS Server 구성

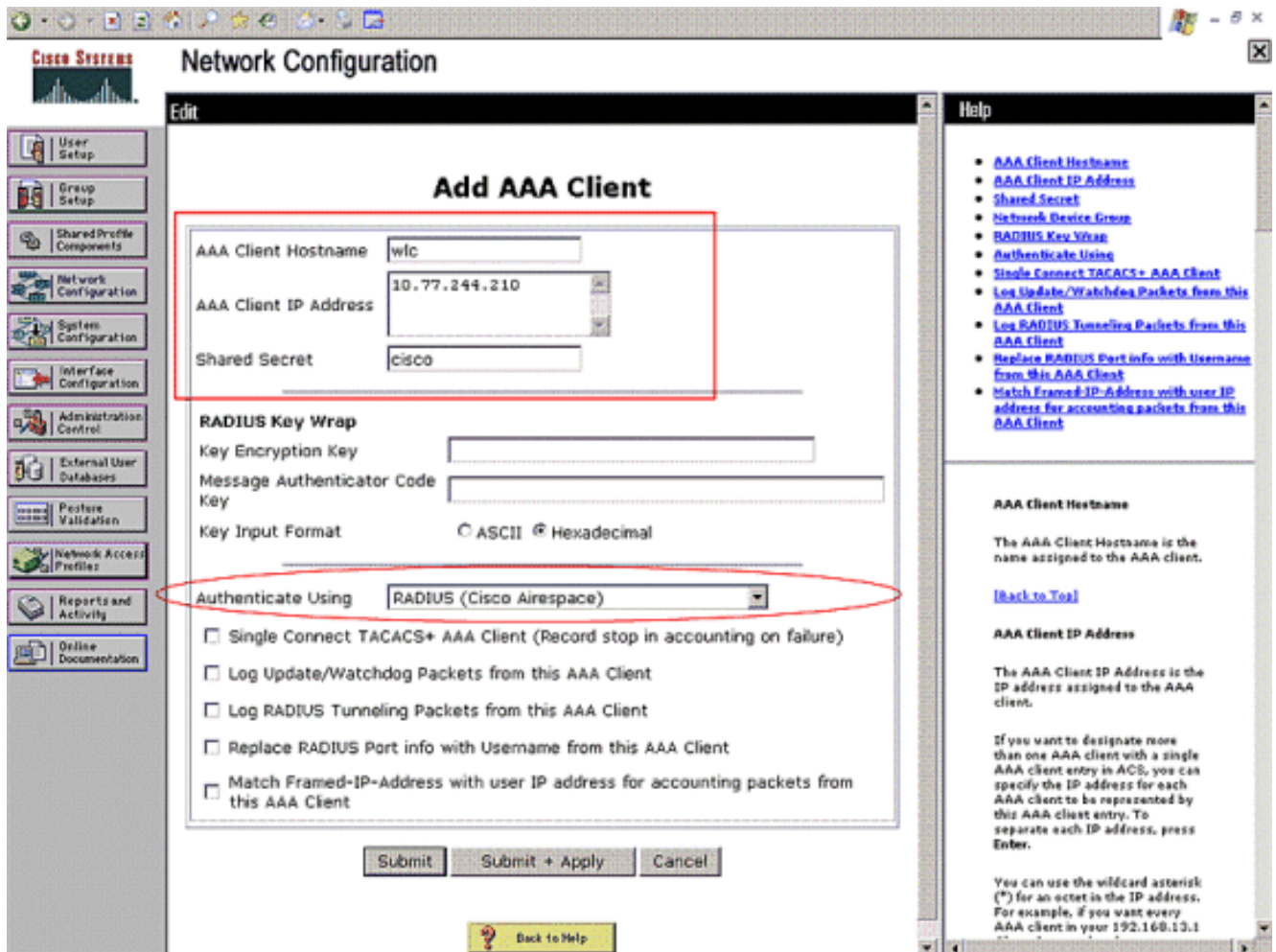
Cisco Secure ACS에서 무선 클라이언트를 인증하려면 다음 단계를 완료해야 합니다.

- [Cisco Secure ACS에서 Wireless LAN Controller를 AAA 클라이언트로 구성합니다.](#)
- [Cisco Secure ACS에서 사용자 및 사용자 프로필을 구성합니다.](#)

Cisco Secure ACS에서 무선 LAN 컨트롤러를 AAA 클라이언트로 구성

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



참고: Cisco Secure ACS에 구성된 공유 암호는 RADIUS Authentication Servers(RADIUS 인증 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

Select

User:

List users beginning with letter/number:

A B C D E F G H I J K L M
 N O P Q R S T U V W X Y Z
 0 1 2 3 4 5 6 7 8 9

Help

- [User Setup and External User Databases](#)
- [Finding a Specific User in the ACS Internal Database](#)
- [Adding a User to the ACS Internal Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the ACS Internal Database](#)
- [Changing a Username in the ACS Internal User Database](#)
- [Remove Dynamic Users](#)

User Setup enables you to configure individual user information, add users, and delete users in the database. [User Setup and External User Databases](#)

Before ACS can authenticate users with an external user database:

- You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
- You must have configured the applicable parameters in the External User Databases section.

Note: User Setup configuration overrides Group Setup configuration.

If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.

External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who authenticate with an external user database. User Setup lets you configure individual user information, add users, and delete users in the ACS internal database.

Note: User Setup does not add or delete usernames in an external user database. [Back to Top](#)

Finding a Specific User in the ACS Internal Database

To find a user already in the ACS internal database, type the first few letters of the username in the User field, add an asterisk (*) as a wildcard, and click **Find**. From the list of usernames displayed, click the username whose information you want to view or change.

[Back to Top](#)

Adding a User to the ACS Internal Database

To add a new user or edit a configuration for an existing user, type a username

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

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

User Setup

Date exceeds: Sep 9 2007

Failed attempts exceed: 5

Failed attempts since last successful login: 0

Reset current failed attempts count on submit

Cisco Airespace RADIUS Attributes

[14179002] Aire-QoS-Level: Bronze

[14179003] Aire-DSCP: 0

[14179004] Aire-802.1P-Tag: 0

[14179005] Aire-Interface-Name:

[14179006] Aire-Acct-Name: User1

[Back to Help](#)

Submit Cancel

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IEEE RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top](#)

Deleting a Username

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 current user account from the database, click **Delete**. When asked to confirm your action, click **OK**.

[Back to Top](#)

Supplementary User Info

Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click **Interface**

3. 동일한 절차를 반복하여 User2를 만듭니다(여기에 표시됨).

Cisco Systems User Setup

Select

User:

List users beginning with letter/number:

A B C D E F G H I J K L M
 N O P Q R S T U V W X Y Z
 0 1 2 3 4 5 6 7 8 9

Help

- [User Setup and External User Databases](#)
- [Finding a Specific User in the ACS Internal Database](#)
- [Adding a User to the ACS Internal Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the ACS Internal Database](#)
- [Changing a Username in the ACS Internal User Database](#)
- [Remove Dynamic Users](#)

User Setup enables you to configure individual user information, add users, and delete users in the database. [User Setup and External User Databases](#)

Before ACS can authenticate users with an external user database:

- You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
- You must have configured the applicable parameters in the External User Databases section.

Note: User Setup configuration overrides Group Setup configuration.

If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.

External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who authenticate with an external user database. User Setup lets you configure individual user information, add users, and delete users in the ACS internal database.

Note: User Setup does not add or delete usernames in an external user database. [Back to Top](#)

Finding a Specific User in the ACS Internal Database

To find a user already in the ACS internal database, type the first few letters of the username in the User field, add an asterisk (*) as a wildcard, and click Find. From the list of usernames displayed, click the username whose information you want to view or change.

[Back to Top](#)

Adding a User to the ACS Internal Database

To add a new user or edit a configuration for an existing user, type a username

Cisco Systems User Setup

Edit

User: UserA (New User)

Account Disabled

Supplementary User Info

Real Name:

Description:

User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password:

Confirm Password:

Separate (CHAP/MS-CHAP/ARAP)

Password:

Confirm Password:

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:

Help

- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IEEE RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top](#)

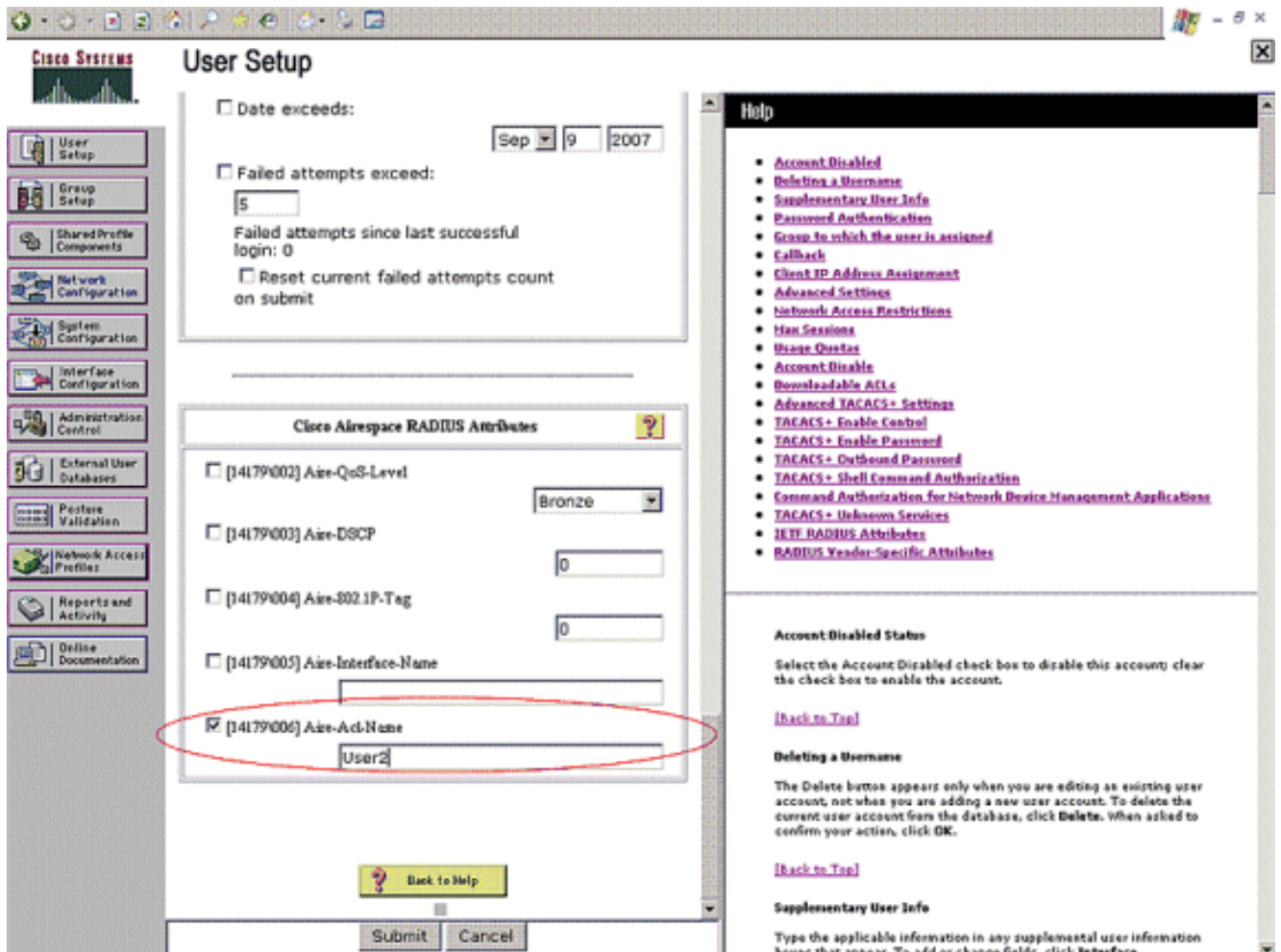
Deleting a Username

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 current user account from the database, click Delete. When asked to confirm your action, click OK.

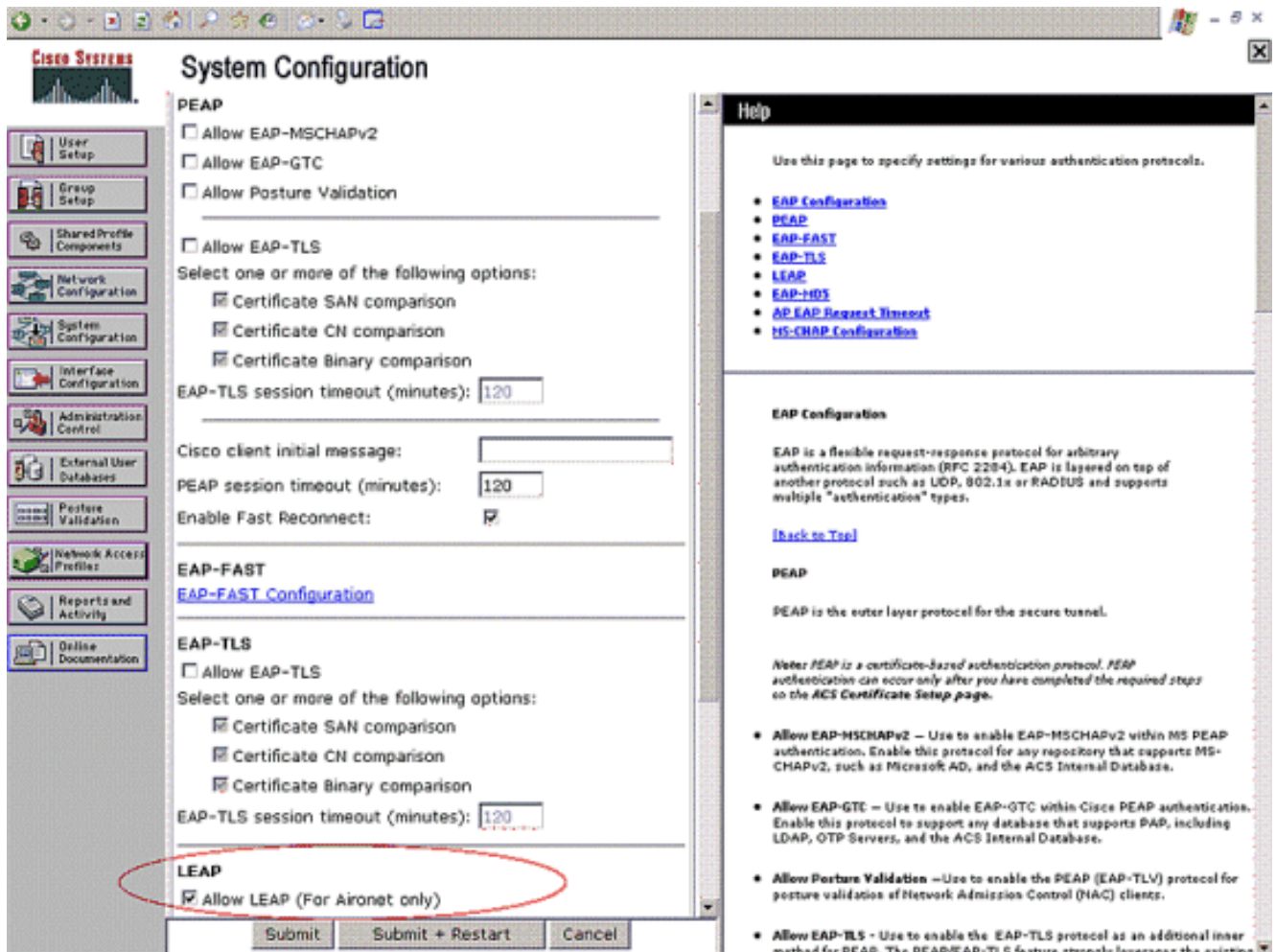
[Back to Top](#)

Supplementary User Info

Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click Interface



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



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

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

참고: 이 문서에서는 클라이언트 프로파일이 LEAP 인증을 위해 구성된 것으로 가정합니다. LEAP 인증을 위해 802.11 a/b/g 무선 클라이언트 어댑터를 구성하는 방법에 대한 자세한 내용은 EAP 인증 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 LEAP username and password to log on to the wireless network.

User Name :

Password :

Log on to :

Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter


Profile Name : Office

경량 AP와 WLC는 자격 증명을 확인하기 위해 외부 RADIUS 서버(Cisco Secure ACS)에 사용자 자격 증명을 전달합니다. RADIUS 서버는 데이터를 사용자 데이터베이스와 비교하고, 인증에 성공하면 사용자에게 대해 구성된 ACL 이름을 WLC에 반환합니다. 이 경우 ACL User1은 WLC로 반환됩니다.

Cisco Aironet Desktop Utility - Current Profile: Office-TSWEB

Action Options Help

Current Status Profile Management Diagnostics




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

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 LEAP username and password to log on to the wireless network.

User Name : User2

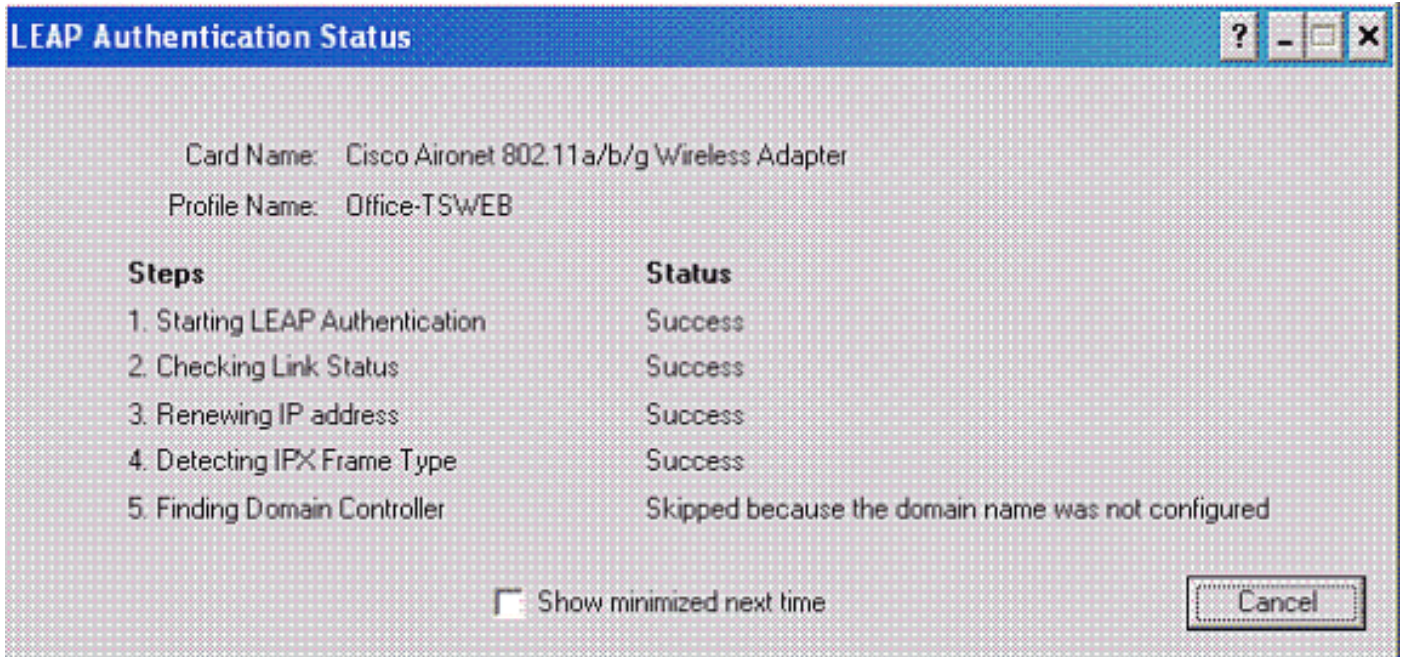
Password : ●●●●●●

Log on to :

Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name : Office

OK Cancel



무선 LAN 컨트롤러는 이 ACL을 User2에 적용합니다. 이 Ping 출력은 User2가 서버 172.16.1.50에만 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),
```

문제 해결

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

무선 LAN 컨트롤러에서 AAA 인증 문제를 해결하기 위해 이러한 디버그 명령을 사용할 수도 있습니다

- **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
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 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 2d
.....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-TSWEB..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1a
.....M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00 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 00 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 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
..%......9.
Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96 dc c3 55 ff 7c 51 4e 75
.....#.U.|QNu
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 1c c2 16 4f 06 03 01 00 04 18 0a 53 56 43 3d
...O.....SVC=
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.l...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
Thu Aug 16 14:42:54 2007:      protocolUsed.....0x00000001
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: 0xblabl04
Thu Aug 16 14:42:54 2007: Callback.....0x85ed228
Thu Aug 16 14:42:54 2007: protocolType.....0x00140001
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 61
....8....[.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 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1a
.....M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00 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 00 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 75
.....e.(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
..k.....9..<.
Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8 6c 07 8e fb 58 84 8d f6
.....=].l...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.!.....O'...%
Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 1e 33 b5 4e 69 90 e7 84 25
.....1.3.Ni...%
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
l.;.....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 79
....auth-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 인식할 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 시도 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
-----
User1             Yes
User2             Yes

```

- **show acl detailed <ACL_Name>** - 구성된 ACL에 대한 자세한 정보를 표시합니다.예를 들면 다음과 같습니다.**참고:** 출력의 일부 행이 공간 제약으로 인해 두 번째 라인으로 이동되었습니다.

```

Cisco Controller) >show acl detailed User1

```

Source

Destination

	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	172.16.1.100/255.255.255.255	172.16.0.0/255.255.0.0	
	Any	0-65535	0-65535	Any Permit

(Cisco Controller) >show acl detailed User2

	Source	Destination		
I	Dir	IP Address/Netmask	IP Address/Netmask	
	Prot	Range	Range	DSCP Action
1	In	172.16.0.0/255.255.0.0	172.16.1.50/255.255.255.255	
	Any	0-65535	0-65535	Any Permit
2	Out	172.16.1.50/255.255.255.255	172.16.0.0/255.255.0.0	
	Any	0-65535	0-65535	Any Permit

- **show client detail <MAC Address of the client>** - 무선 클라이언트에 대한 자세한 정보를 표시합니다.

문제 해결 정보

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 확인합니다. 이러한 보고서는 ACS 서버의 Reports and Activities에서 사용할 수 있습니다.

관련 정보

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