WLC 및 Cisco Secure ACS 컨피그레이션을 통한 SSID를 기반으로 WLAN 액세스 제한 예

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[배경 정보](#)
[네트워크 설정](#)
[구성](#)
[WLC 구성](#)
[Cisco Secure ACS 구성](#)
[무선 클라이언트 구성 및 확인](#)
[문제 해결](#)
[문제 해결 명령](#)
[관련 정보](#)

소개

이 문서에서는 SSID(Service Set Identifier)를 기반으로 사용자별 액세스를 WLAN으로 제한하는 컨피그레이션 예를 제공합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 기본 작동을 위해 WLC(Wireless LAN Controller) 및 LAP(Lightweight Access Point)를 구성하는 방법에 대한 지식
- Cisco ACS(Secure Access Control Server) 구성 방법에 대한 기본 지식
- LWAPP(Lightweight Access Point Protocol) 및 무선 보안 방법에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 4.0을 실행하는 Cisco 2000 Series WLC

- Cisco 1000 Series LAP
- Cisco Secure ACS Server 버전 3.2
- 펌웨어 2.6을 실행하는 Cisco 802.11a/b/g Wireless Client Adapter
- Cisco Aironet Desktop Utility(ADU) 버전 2.6

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

표기 규칙

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

배경 정보

SSID 기반 WLAN 액세스를 사용하면 WLAN에 연결하기 위해 사용자가 사용하는 SSID를 기반으로 사용자를 인증할 수 있습니다.Cisco Secure ACS 서버는 사용자를 인증하는 데 사용됩니다.인증은 Cisco Secure ACS에서 두 단계로 이루어집니다.

1. EAP 인증
2. Cisco Secure ACS의 NAR(Network Access Restrictions)에 기반한 SSID 인증

EAP 및 SSID 기반 인증이 성공하면 사용자가 WLAN에 액세스할 수 있습니다. 그렇지 않으면 사용자가 연결 해제됩니다.

Cisco Secure ACS는 NAR 기능을 사용하여 SSID를 기반으로 사용자 액세스를 제한합니다.NAR은 Cisco Secure ACS에서 사용자가 네트워크에 액세스하기 전에 충족해야 하는 추가 조건의 정의입니다.Cisco Secure ACS는 AAA 클라이언트에서 보낸 속성의 정보를 사용하여 이러한 조건을 적용합니다.NAR을 설정할 수 있는 방법에는 여러 가지가 있지만 모두 AAA 클라이언트에서 보낸 일치하는 특성 정보를 기반으로 합니다.따라서 유효 NAR을 사용하려면 AAA 클라이언트가 전송하는 특성의 형식과 내용을 이해해야 합니다.

NAR을 설정할 때 필터의 작동 여부를 양성으로 선택할 수 있습니다.즉, NAR에서 AAA 클라이언트에서 NAR에 저장된 정보로 전송된 정보의 비교를 기반으로 네트워크 액세스를 허용할지 거부할지를 지정합니다.그러나 NAR에 작동하기에 충분한 정보가 없으면 기본적으로 액세스가 거부됩니다.

특정 사용자 또는 사용자 그룹에 대해 NAR을 정의하고 적용할 수 있습니다.자세한 내용은 네트워크 액세스 제한 백서를 참조하십시오.

Cisco Secure ACS는 두 가지 유형의 NAR 필터를 지원합니다.

1. **IP 기반 필터**—IP 기반 NAR 필터는 최종 사용자 클라이언트 및 AAA 클라이언트의 IP 주소를 기반으로 액세스를 제한합니다.이 유형의 NAR 필터에 대한 자세한 내용은 IP 기반 NAR 필터 정보를 참조하십시오.
2. **비 IP 기반 필터**—비 IP 기반 NAR 필터는 AAA 클라이언트에서 전송된 값의 간단한 문자열 비교를 기반으로 액세스를 제한합니다.값은 CLI(Calling Line ID) 번호, DNIS(Dialed Number Identification Service) 번호, MAC 주소 또는 클라이언트에서 시작되는 기타 값일 수 있습니다.이 유형의 NAR이 작동하려면 NAR 설명의 값이 어떤 형식이든 사용되는 형식을 포함하여 클라이언트에서 전송된 것과 정확히 일치해야 합니다.예를 들어 (217) 555-4534가 217-555-4534와 일치하지 않습니다.이 유형의 NAR 필터에 대한 자세한 내용은 비IP 기반 NAR 필터 정보를 참조하십시오.

이 문서에서는 비 IP 기반 필터를 사용하여 SSID 기반 인증을 수행합니다.비 IP 기반 NAR 필터(즉, DNIS/CLI 기반 NAR 필터)는 설정된 IP 기반 연결이 없는 경우 AAA 클라이언트의 제한에서 사용할 수 있는 허용 또는 거부된 발신/액세스 지점 목록입니다.비 IP 기반 NAR 기능은 일반적으로 CLI 번호와 DNIS 번호를 사용합니다.DNIS/CLI 필드 사용에는 예외가 있습니다.DNIS 필드에 SSID 이름을 입력하고 SSID 기반 인증을 수행할 수 있습니다.이는 WLC가 DNIS 특성, 즉 SSID 이름을 RADIUS 서버로 전송하기 때문입니다.따라서 사용자 또는 그룹에서 DNIS NAR을 구축할 경우 사용자별 SSID 제한을 생성할 수 있습니다.

RADIUS를 사용하는 경우 여기에 나열된 NAR 필드는 다음 값을 사용합니다.

- **AAA 클라이언트**—NAS-IP 주소(특성 4) 또는 NAS-IP 주소가 없는 경우 NAS 식별자(RADIUS 특성 32)가 사용됩니다.
- **Port**—NAS 포트(특성 5) 또는 NAS 포트가 없는 경우 NAS 포트 ID(특성 87)가 사용됩니다.
- **CLI** - calling-station-ID(특성 31)가 사용됩니다.
- **DNIS** - called-station-ID(특성 30)가 사용됩니다.

NAR 사용에 대한 자세한 내용은 네트워크 액세스 제한을 참조하십시오.

WLC가 DNIS 특성 및 SSID 이름으로 전송하므로 사용자별 SSID 제한을 생성할 수 있습니다 .WLC의 경우 NAR 필드에는 다음 값이 있습니다.

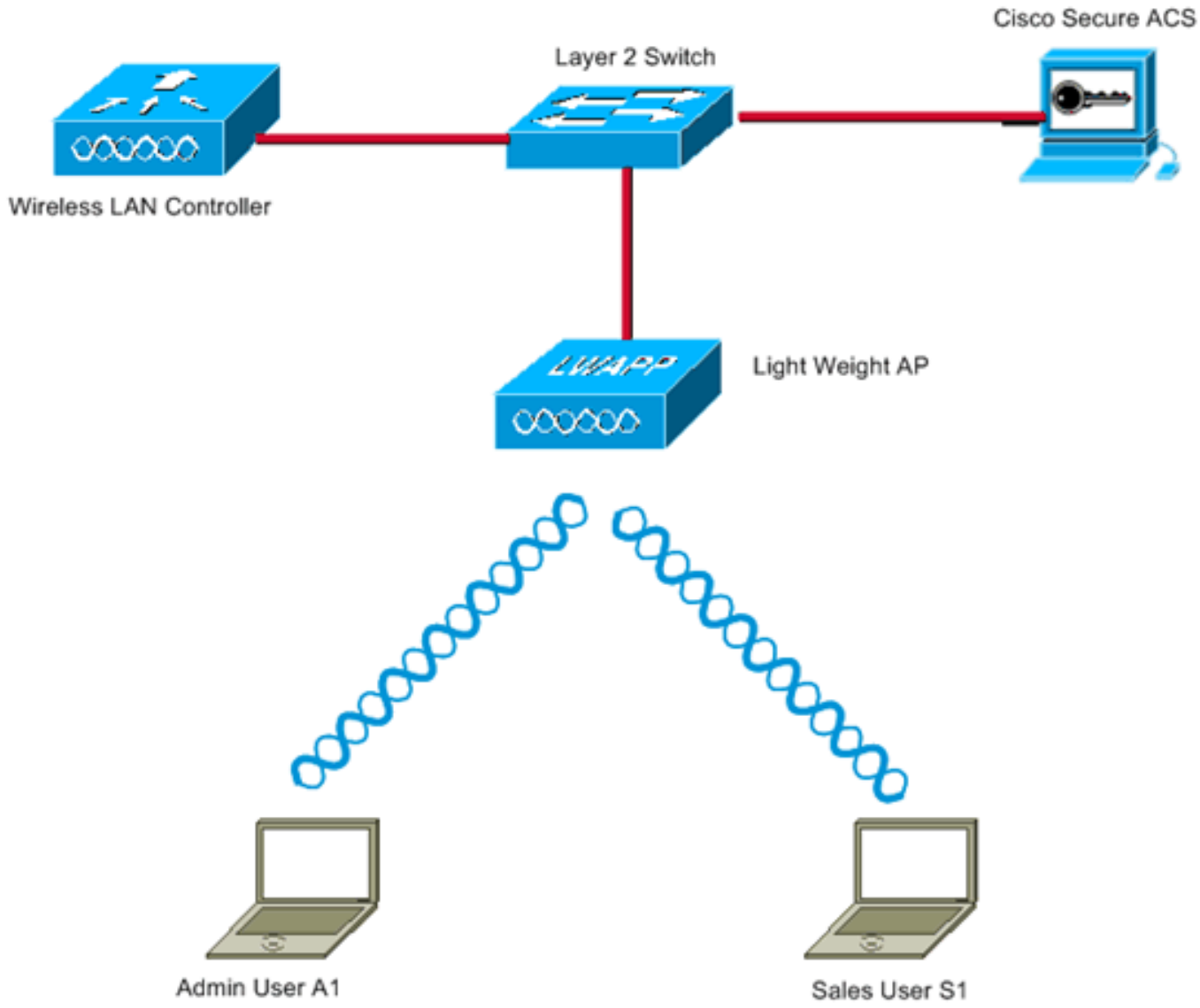
- **AAA 클라이언트** - WLC IP 주소
- **포트**—*
- **CLI** —*
- **DNIS**—*ssidname

이 문서의 나머지 부분에서는 이 작업을 수행하는 방법에 대한 구성 예를 제공합니다.

네트워크 설정

이 설정 예에서는 WLC가 LAP에 등록됩니다.2개의 WLAN이 사용됩니다.한 WLAN은 관리 부서 사용자를 위한 것이고 다른 WLAN은 영업 부서 사용자를 위한 것입니다.무선 클라이언트 A1(관리자 사용자) 및 S1(세일즈 사용자)이 무선 네트워크에 연결됩니다.관리자 사용자 A1이 WLAN **관리만** 액세스할 수 있고 WLAN **세일즈**에 대한 액세스가 제한되고 세일즈 사용자 S1이 WLAN **세일즈**에 액세스할 수 있어야 하며 WLAN **관리자**에 대한 액세스가 제한될 수 있도록 WLC 및 RADIUS 서버를 구성해야 합니다.모든 사용자는 레이어 2 인증 방법으로 LEAP 인증을 사용합니다.

참고: 이 문서에서는 WLC가 컨트롤러에 등록된 것으로 가정합니다.WLC를 처음 사용하고 기본 작동을 위해 WLC를 구성하는 방법을 모르는 경우 WLC(Wireless LAN Controller)에 대한 LAP(Lightweight AP) 등록을 참조하십시오.



WLC Management Interface IP address : 172.16.1.30/16
WLC AP-Manager Interface IP address: 172.16.1.31/16
Cisco Secure ACS server IP address: 172.16.1.60/16

SSID for the Admin department users : Admin
SSID for Sales department users: Sales

구성

이 설정에 대한 디바이스를 구성하려면 다음을 수행해야 합니다.

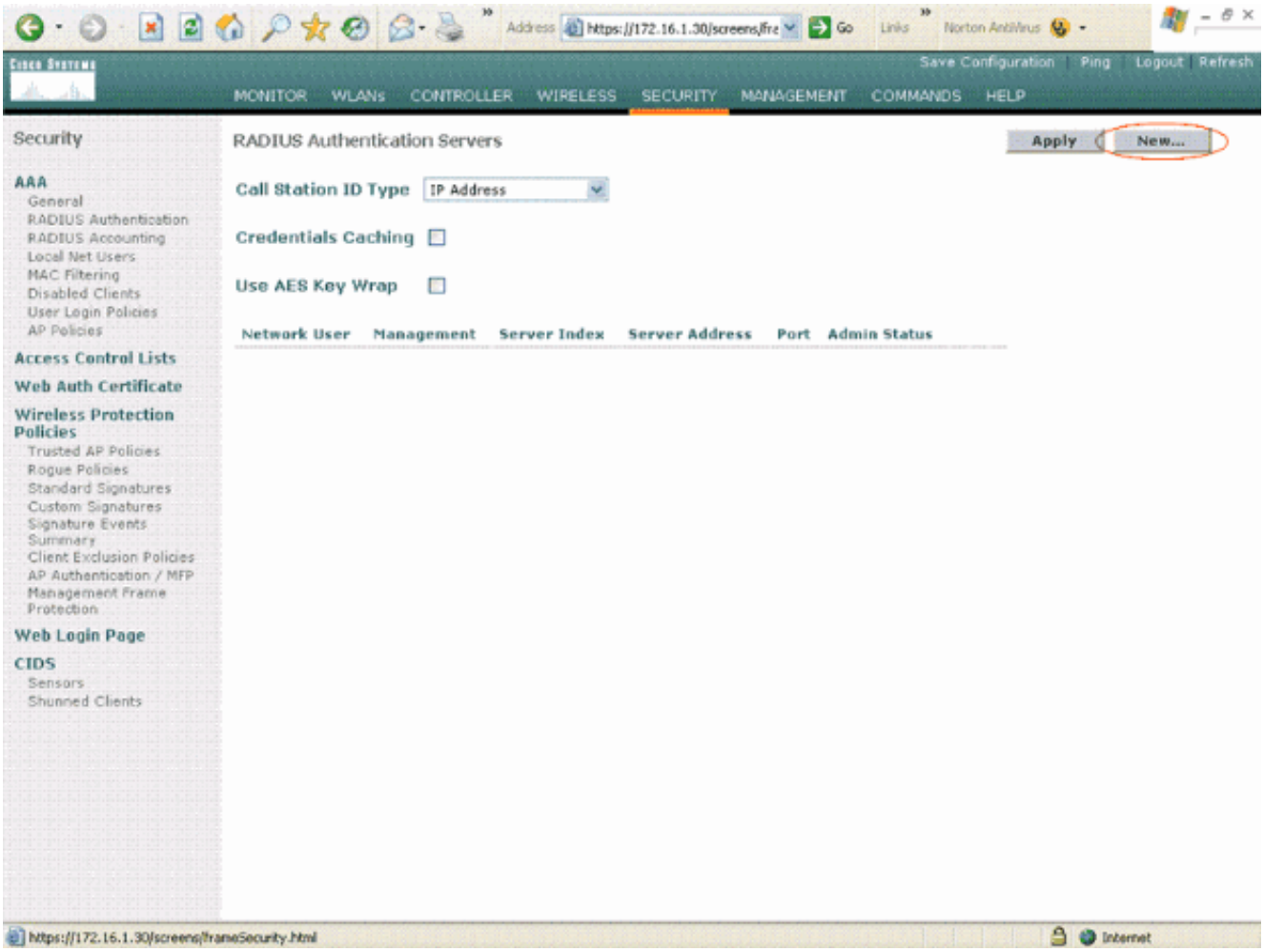
1. 2개의 WLAN 및 RADIUS 서버에 대한 WLC를 구성합니다.
2. Cisco Secure ACS를 구성합니다.
3. 무선 클라이언트를 구성하고 확인합니다.

WLC 구성

이 설정에 대한 WLC를 구성하려면 다음 단계를 완료합니다.

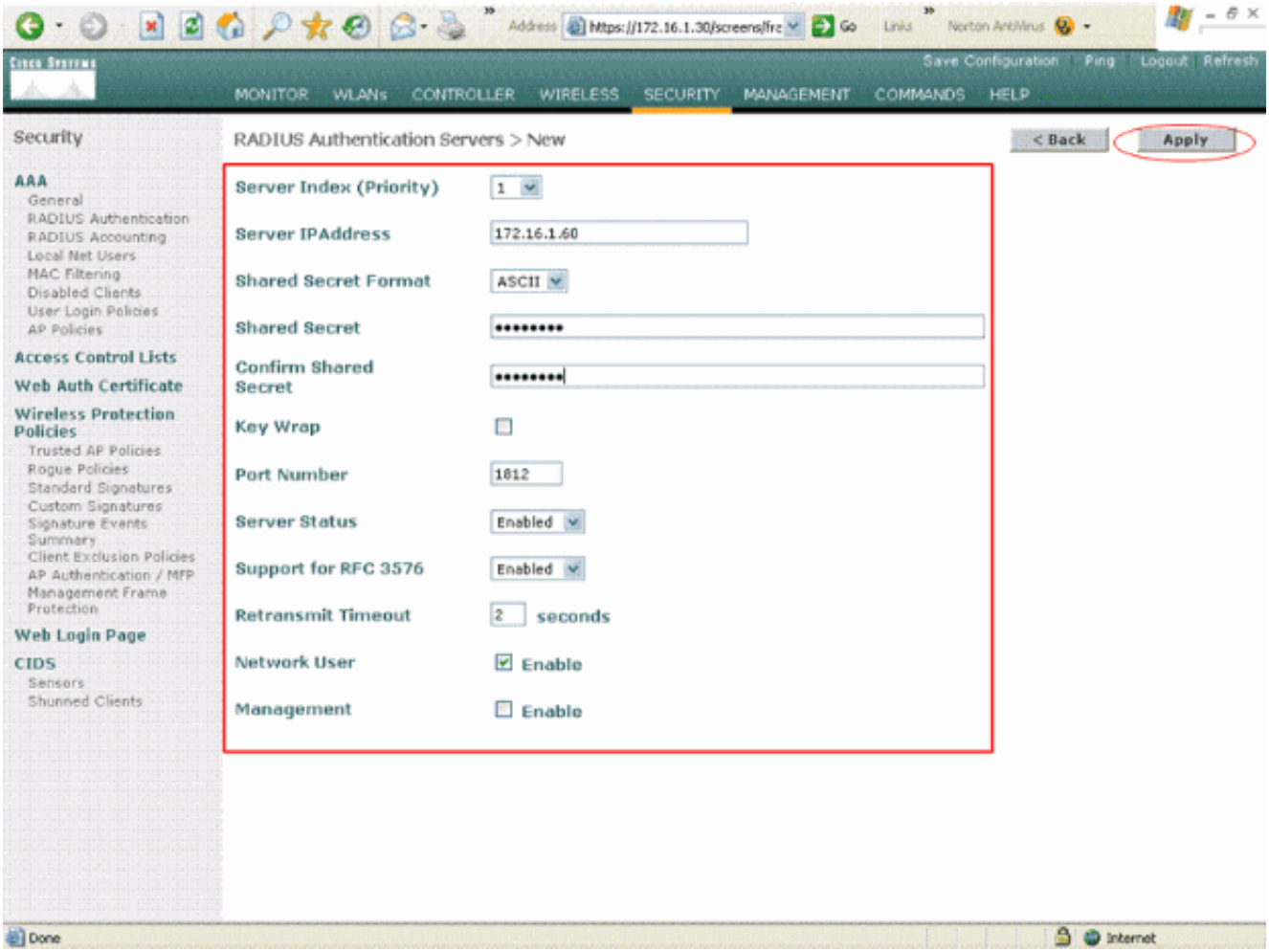
1. 사용자 자격 증명을 외부 RADIUS 서버로 전달하도록 WLC를 구성해야 합니다.그런 다음 외부 RADIUS 서버(이 경우 Cisco Secure ACS)에서 사용자 자격 증명을 검증하고 무선 클라이언트에 대한 액세스를 제공합니다.다음 단계를 완료하십시오.RADIUS **Authentication** Servers 페이지를 표시하려면 컨트롤러 GUI에서 Security(보안) > RADIUS Authentication(RADIUS 인증)을 선택합니다

.



RADIUS 서버 매개변수를 정의하려면 New(새로 만들기)를 클릭합니다.이러한 매개변수에는 RADIUS 서버 IP 주소, 공유 암호, 포트 번호 및 서버 상태가 포함됩니다.Network User and Management(네트워크 사용자 및 관리) 확인란은 RADIUS 기반 인증이 관리 및 네트워크 사용자에게 적용되는지 여부를 결정합니다.이 예에서는 Cisco Secure ACS를 IP 주소가 172.16.1.60인 RADIUS 서버로 사용합니다

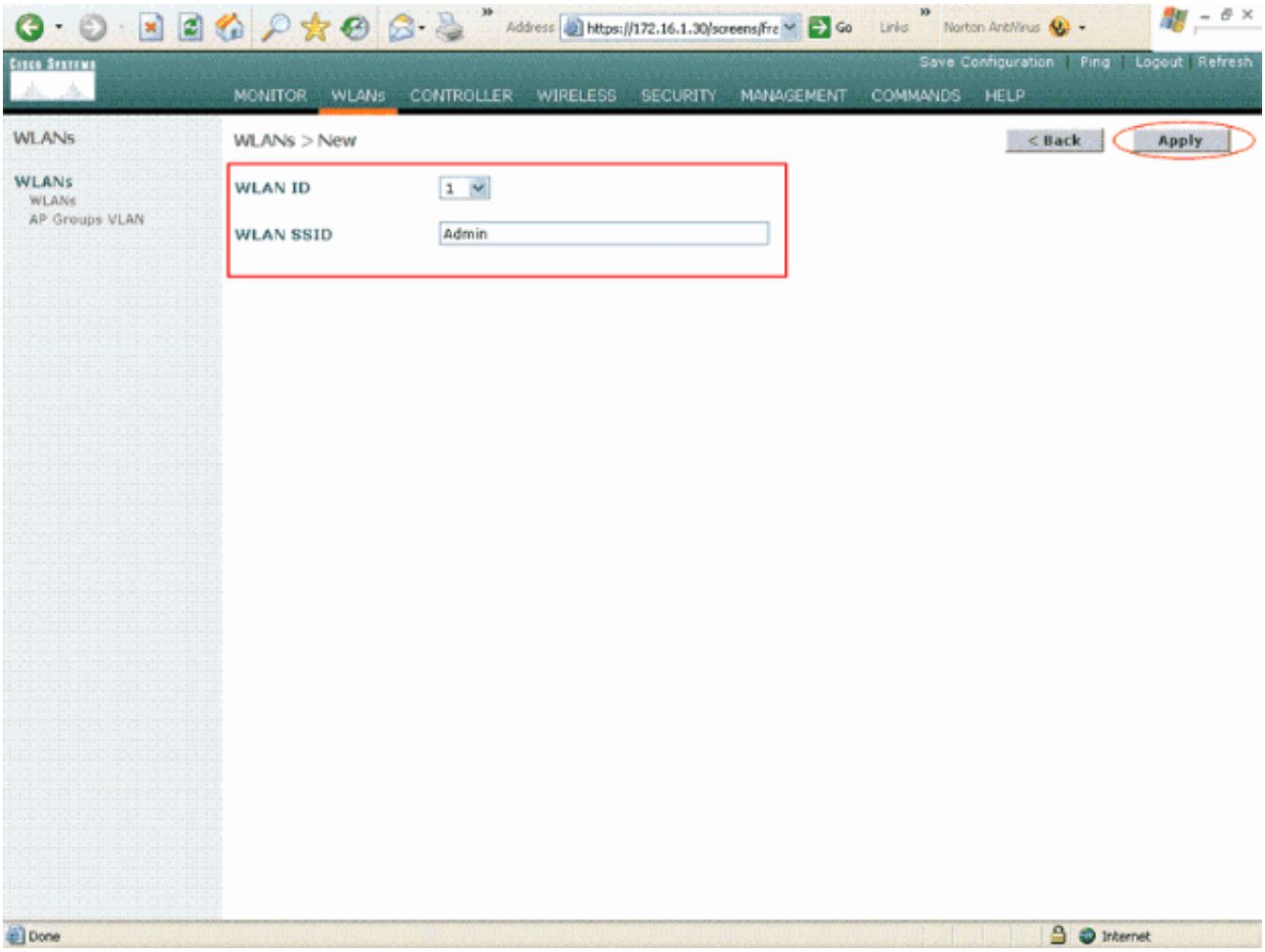
.



Apply를 **클릭합니다**.

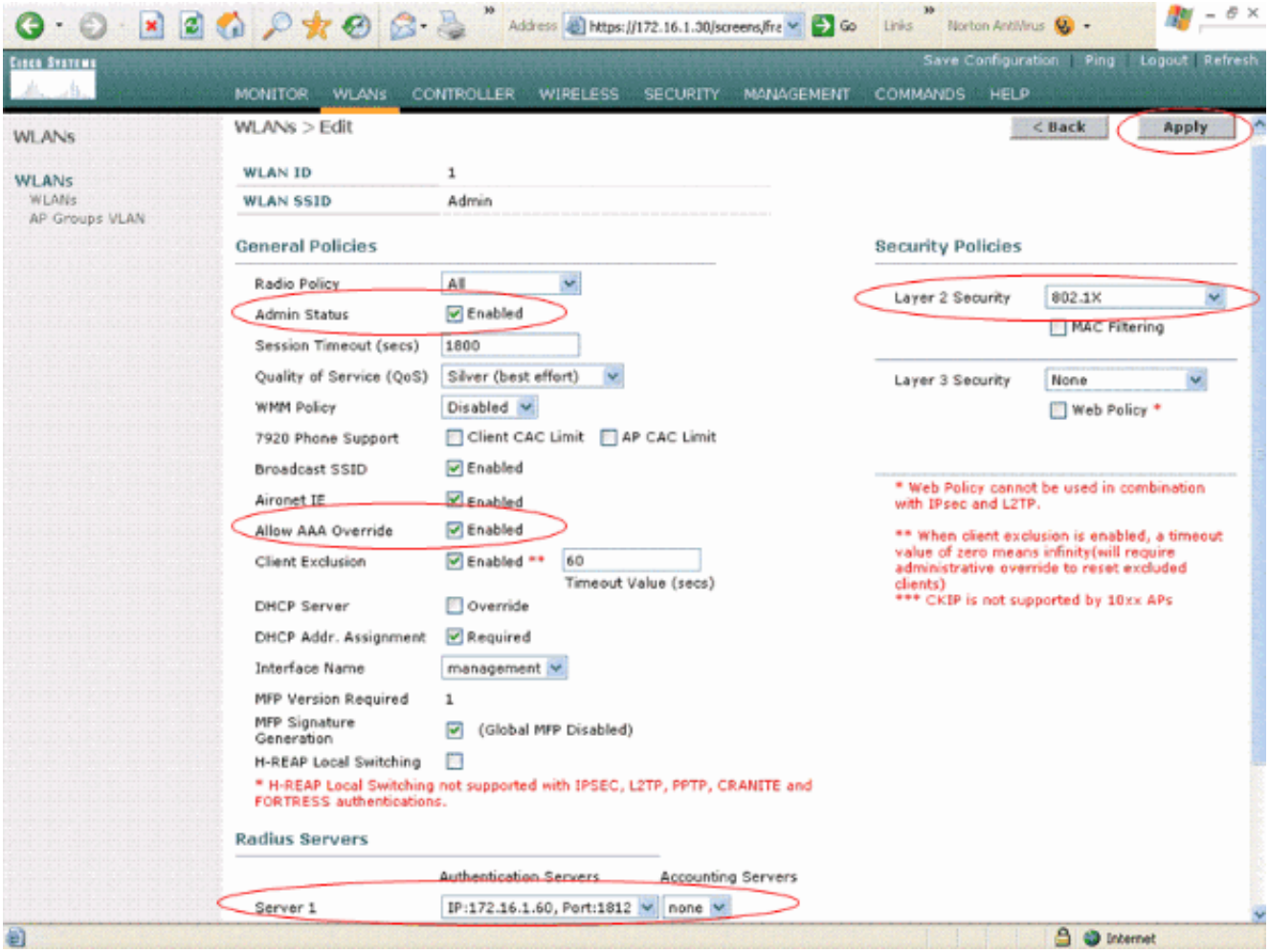
2. SSID **관리자**로 관리 부서에 대해 WLAN 1개를 구성하고 SSID **세일즈**로 판매 부서에 대해 다른 WLAN을 **구성합니다**.이 작업을 수행하려면 다음 단계를 완료하십시오.WLAN**을** 생성하려면 컨트롤러 GUI에서 WLANs를 클릭합니다.WLANs 창이 나타납니다.이 창에는 컨트롤러에 구성된 WLAN이 나열됩니다.새 WLAN을 구성하려면 **New**(새로 만들기)를 클릭합니다.이 예에서는 관리 부서의 **Admin이라는** WLAN을 생성하고 WLAN ID는 **1**입니다. Apply(적용)를 **클릭합니다**

.



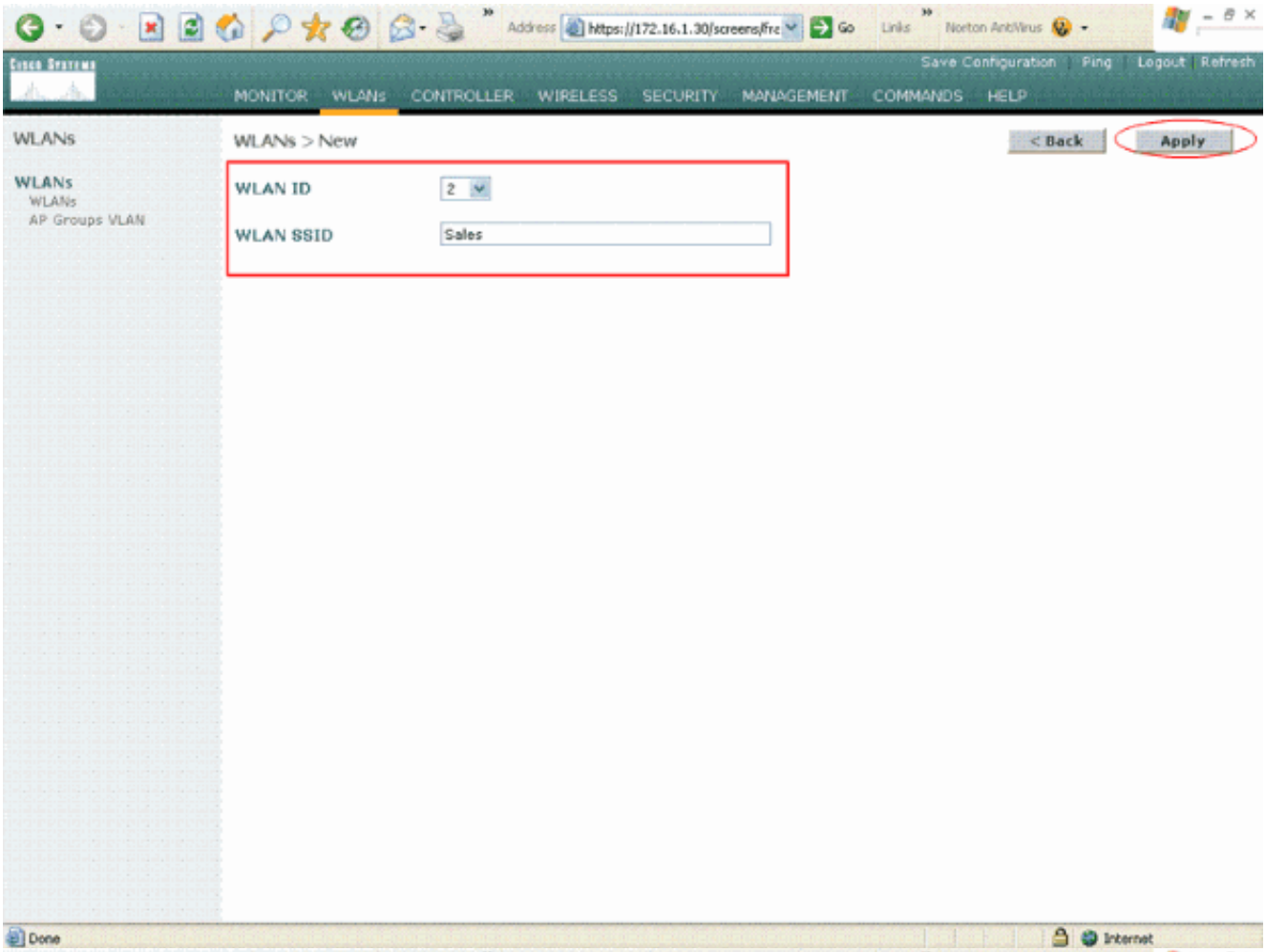
WLAN **> Edit(편집)** 창에서 WLAN에 해당하는 매개변수를 정의합니다.Layer 2 Security 풀다운 메뉴에서 **802.1x**를 선택합니다.기본적으로 레이어 2 보안 옵션은 802.1x입니다.이렇게 하면 WLAN에 대한 802.1x/EAP 인증이 활성화됩니다.일반 정책에서 **AAA 재정의** 상자**를** 선택합니다.AAA Override(AAA 재정의)가 활성화되고 클라이언트에 충돌하는 AAA 및 컨트롤러 WLAN 인증 매개변수가 있으면 AAA 서버에서 클라이언트 인증을 수행합니다.RADIUS Servers(RADIUS 서버) 아래의 풀다운 메뉴에서 적절한 RADIUS 서버를 선택합니다.다른 매개변수는 WLAN 네트워크의 요구 사항에 따라 수정할 수 있습니다.Apply를 **클릭합니다**

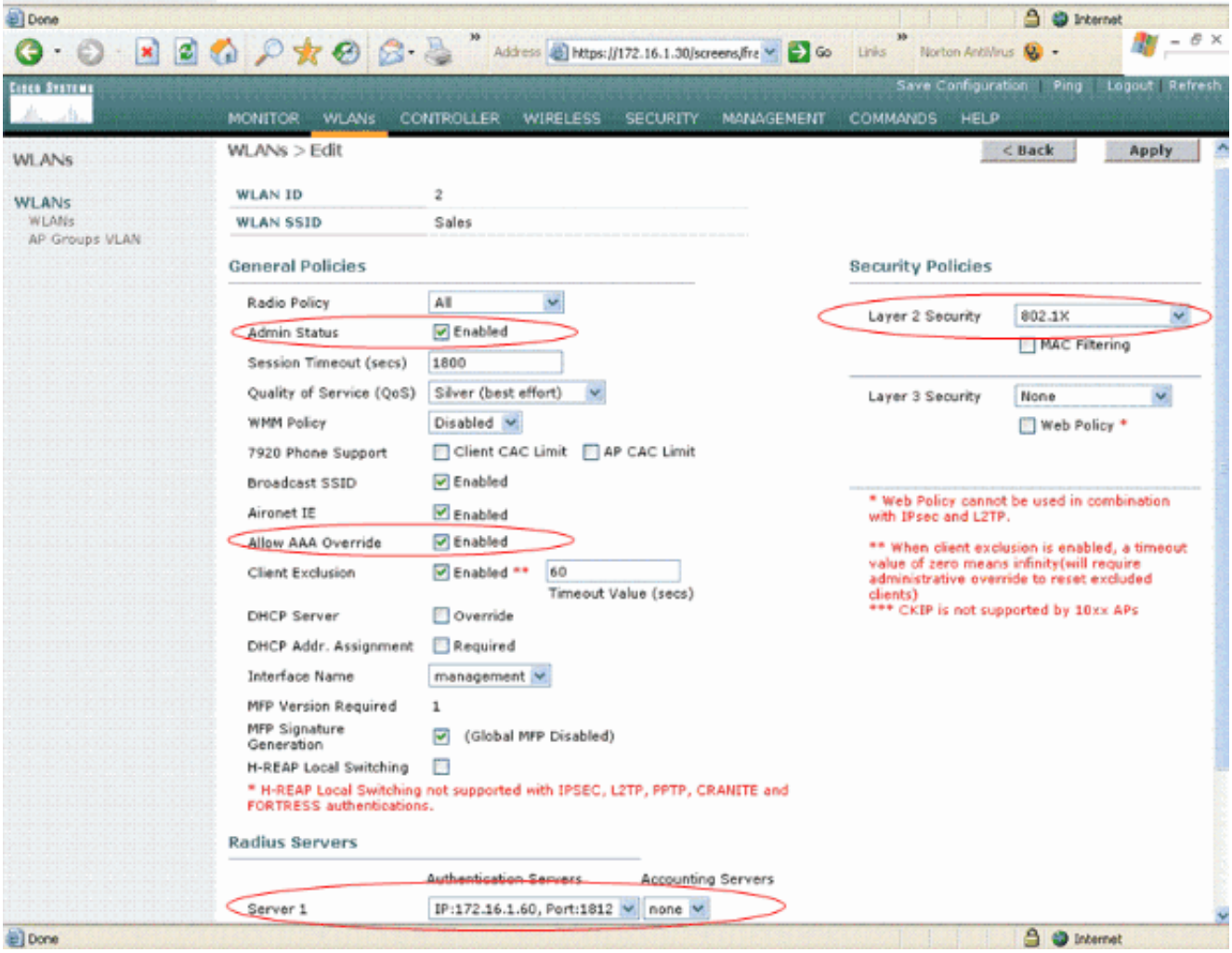
.



마찬가지로, 영업 부서의 WLAN을 생성하려면 b단계와 c단계를 반복합니다. 스크린샷은 다음과 같습니다

.


Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > New
< Back
Apply
WLAN ID
2
WLAN SSID
Sales


Done
Internet
Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > Edit
< Back
Apply
WLAN ID 2
WLAN SSID Sales
General Policies
Radio Policy All
Admin Status Enabled
Session Timeout (secs) 1800
Quality of Service (QoS) Silver (best effort)
WMM Policy Disabled
7920 Phone Support Client CAC Limit AP CAC Limit
Broadcast SSID Enabled
Aironet IE Enabled
Allow AAA Override Enabled
Client Exclusion Enabled ** 60
Timeout Value (secs)
DHCP Server Override
DHCP Addr. Assignment Required
Interface Name management
MFP Version Required 1
MFP Signature Generation (Global MFP Disabled)
H-REAP Local Switching
* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.
Security Policies
Layer 2 Security 802.1X
MAC Filtering
Layer 3 Security None
Web Policy *
* Web Policy cannot be used in combination with IPsec and L2TP.
** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)
*** CKIP is not supported by 10xx APs
Radius Servers
Authentication Servers
Accounting Servers
Server 1 IP:172.16.1.60, Port:1812 none
Done
Internet

Cisco Secure ACS 구성

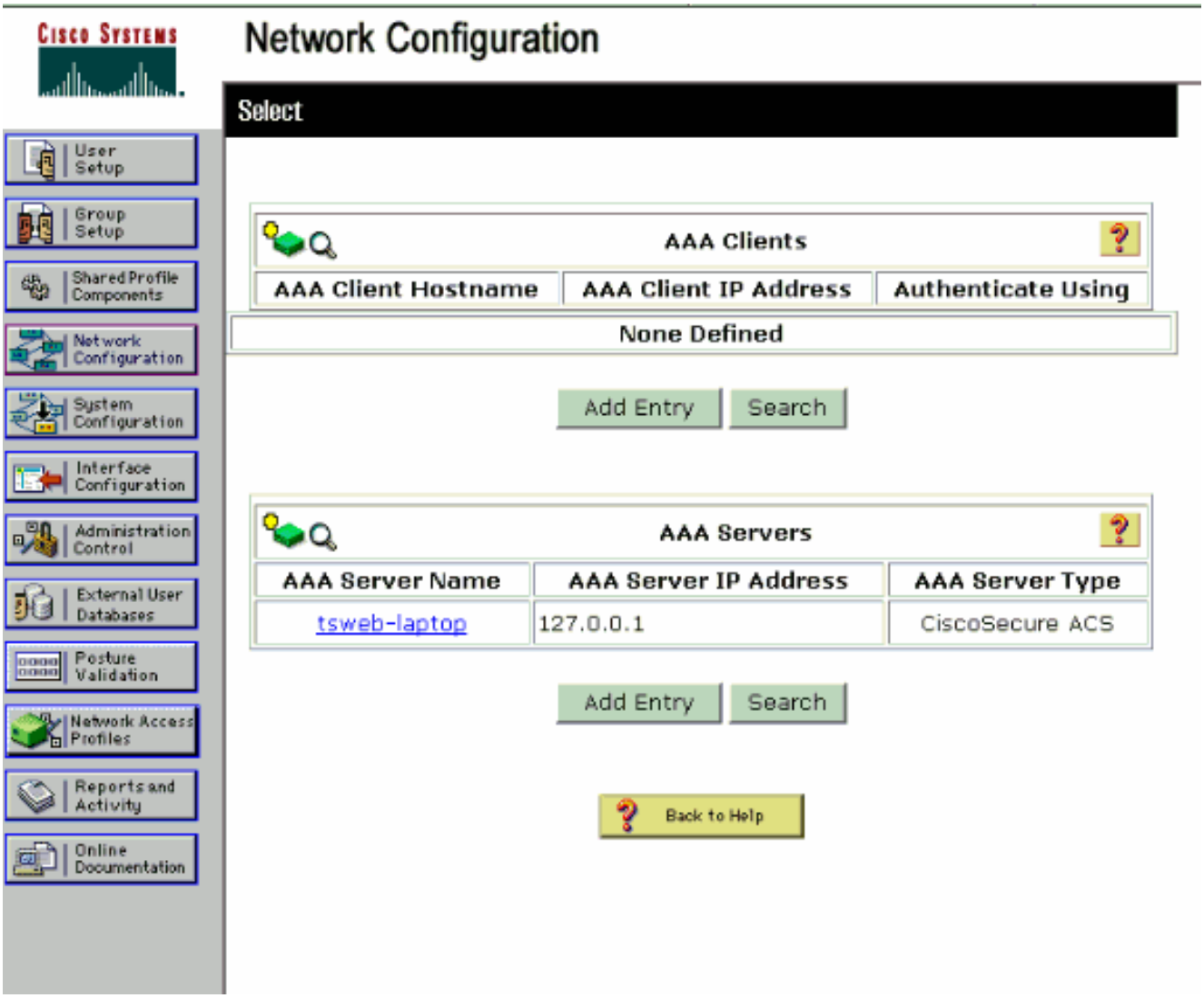
Cisco Secure ACS 서버에서 다음을 수행해야 합니다.

1. WLC를 AAA 클라이언트로 구성합니다.
2. 사용자 데이터베이스를 생성하고 SSID 기반 인증을 위한 NAR을 정의합니다.
3. EAP 인증을 활성화합니다.

Cisco Secure ACS에서 다음 단계를 완료합니다.

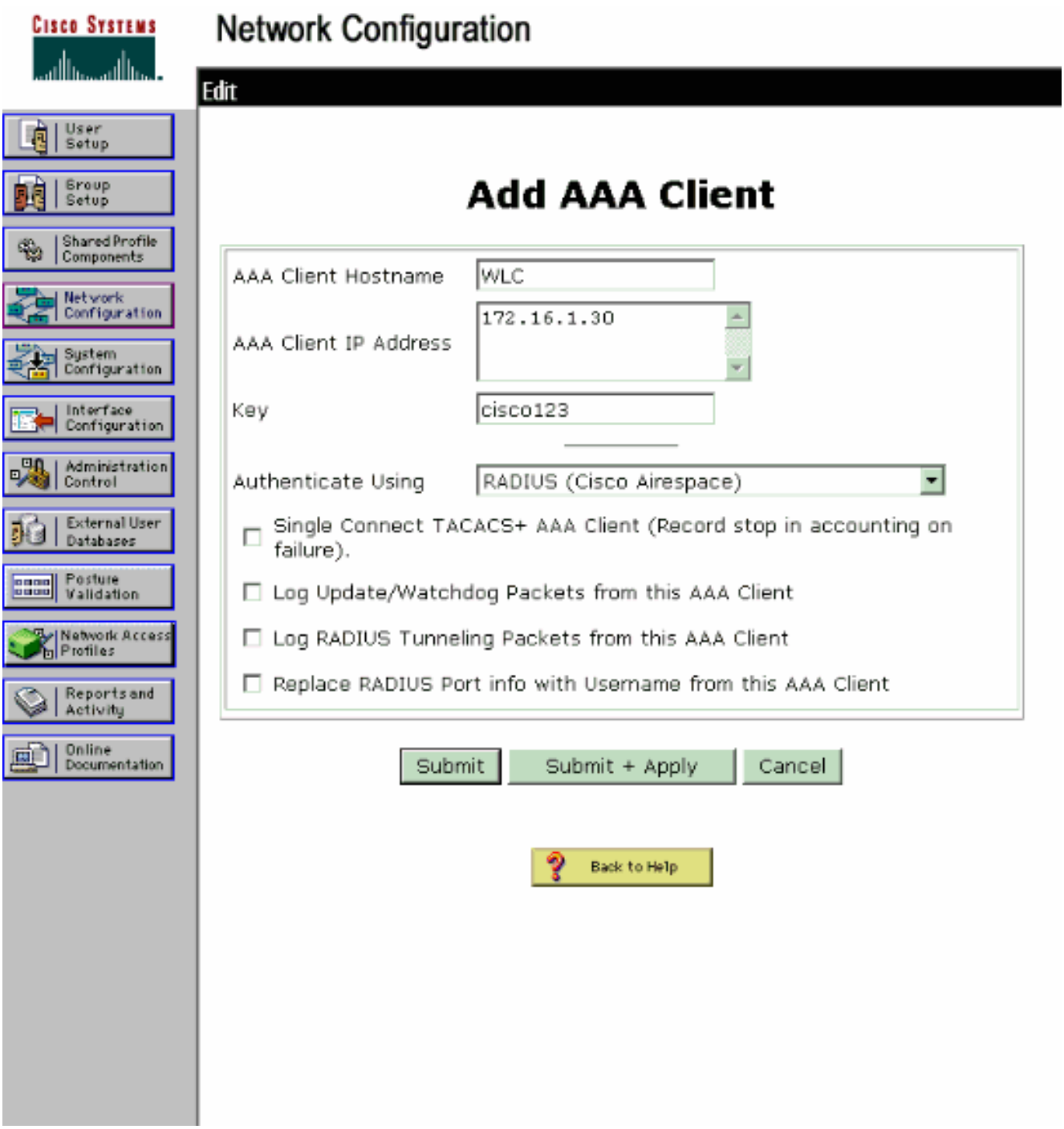
1. 컨트롤러를 ACS 서버에서 AAA 클라이언트로 정의하려면 ACS GUI에서 **Network Configuration(네트워크 컨피그레이션)**을 클릭합니다.AAA 클라이언트에서 Add Entry(항목 **추가)를 클릭합니다**

.



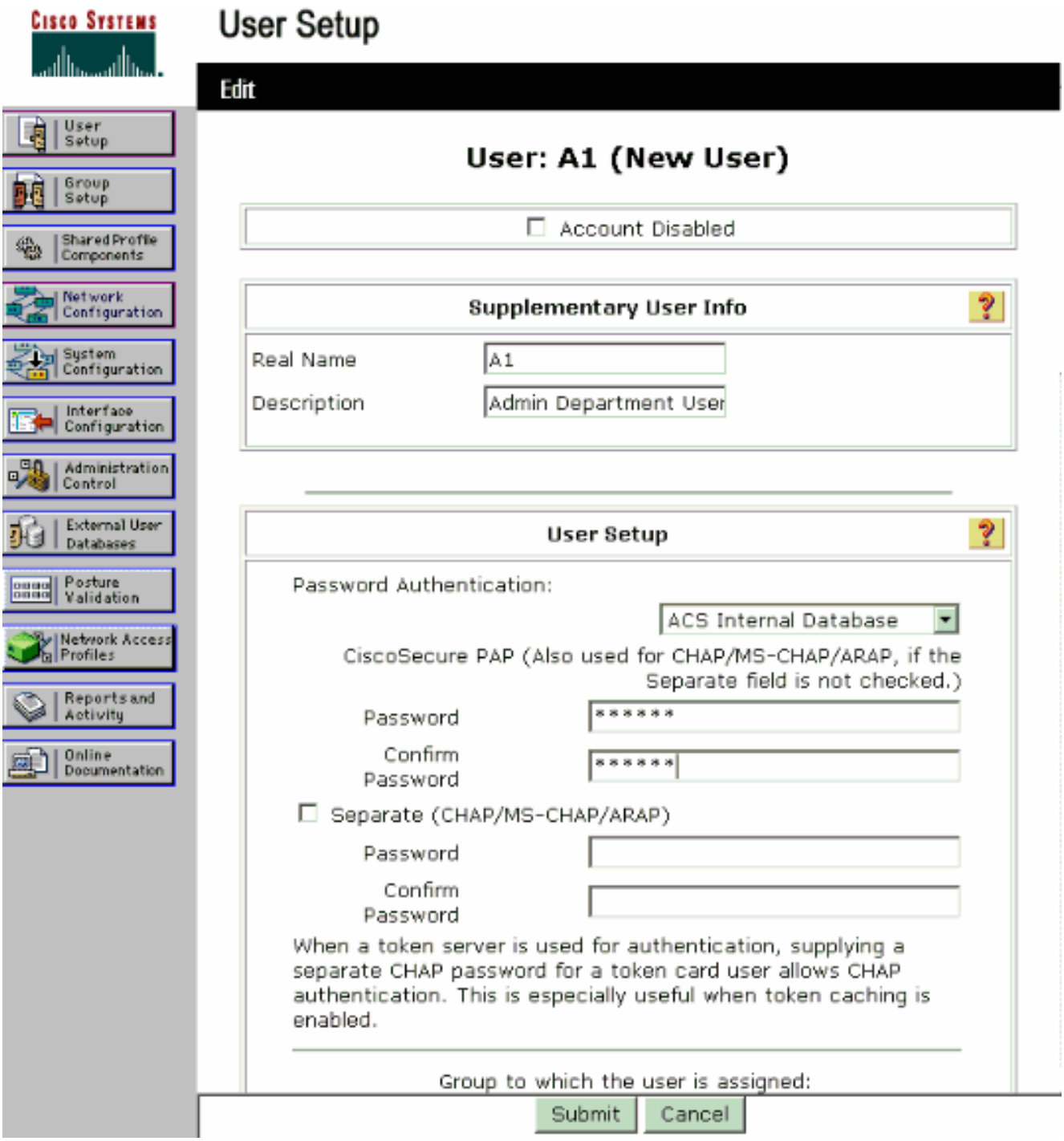
2. Network Configuration(네트워크 컨피그레이션) 페이지가 나타나면 WLC의 이름, IP 주소, 공유 암호 및 인증 방법(RADIUS Cisco Airespace)을 정의합니다

.



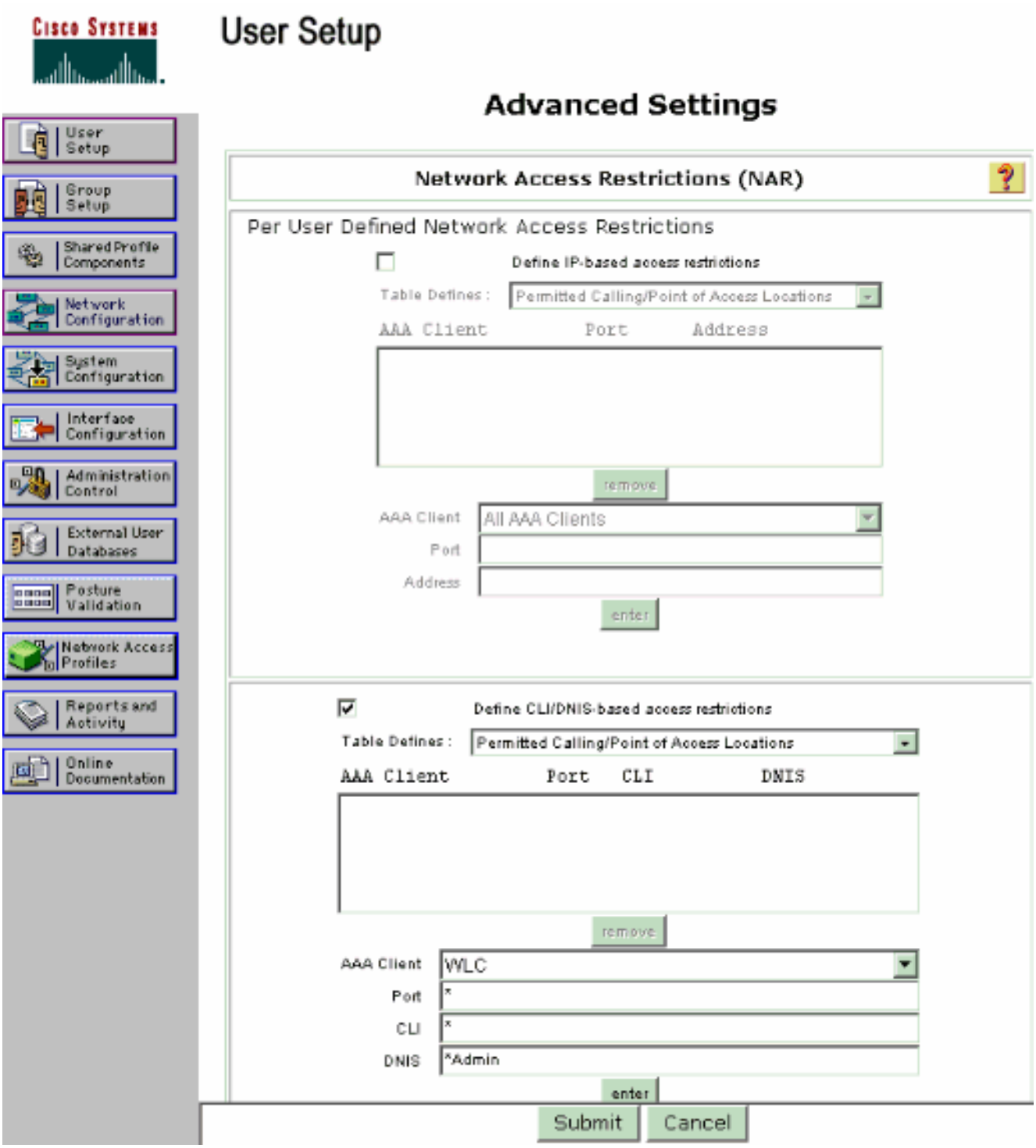
3. ACS GUI에서 **User Setup(사용자 설정)**을 클릭하고 사용자 이름을 입력한 다음 Add/**Edit(추가/수정)를 클릭합니다**.이 예에서는 사용자가 A1입니다.
4. User Setup 페이지가 나타나면 해당 사용자에 대한 모든 매개변수를 정의합니다.이 예에서는 LEAP 인증을 위해 이러한 매개변수가 필요하므로 사용자 이름, 비밀번호 및 보조 사용자 정보가 구성됩니다

.



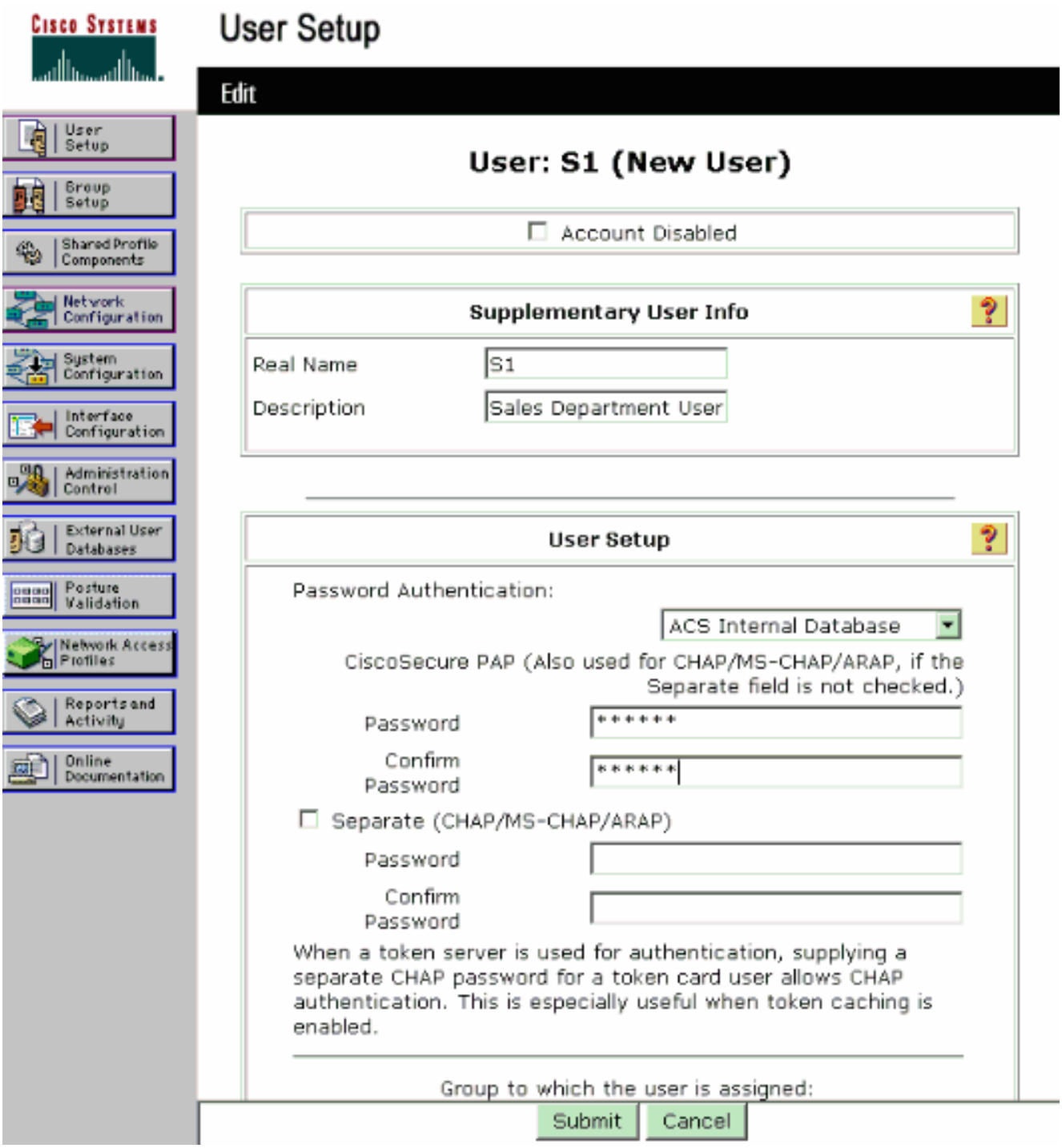
5. Network Access Restrictions 섹션이 표시될 때까지 User Setup 페이지를 아래로 스크롤합니다.User Interface of DNIS/CLI Access Restriction(DNIS/CLI 액세스 제한의 사용자 인터페이스)에서 Permitted Calling **/ Point of Access Locations(허용된 발신/POS 액세스 위치)를 선택하고** 다음 매개변수를 정의합니다.**AAA 클라이언트** - WLC IP 주소(예: 172.16.1.30)**포트**—*CLI—*DNIS—*ssidname
6. DNIS 특성은 사용자가 액세스할 수 있는 SSID를 정의합니다.WLC는 DNIS 특성의 SSID를 RADIUS 서버로 전송합니다.사용자가 Admin이라는 WLAN에만 액세스해야 하는 경우 DNIS 필드에 ***Admin**을 입력합니다.이렇게 하면 사용자가 Admin이라는 WLAN에만 액세스할 수 있습니다.Enter를 **클릭합니다.참고:** SSID는 항상 *로 **앞에 와야** 합니다.필수 항목입니다

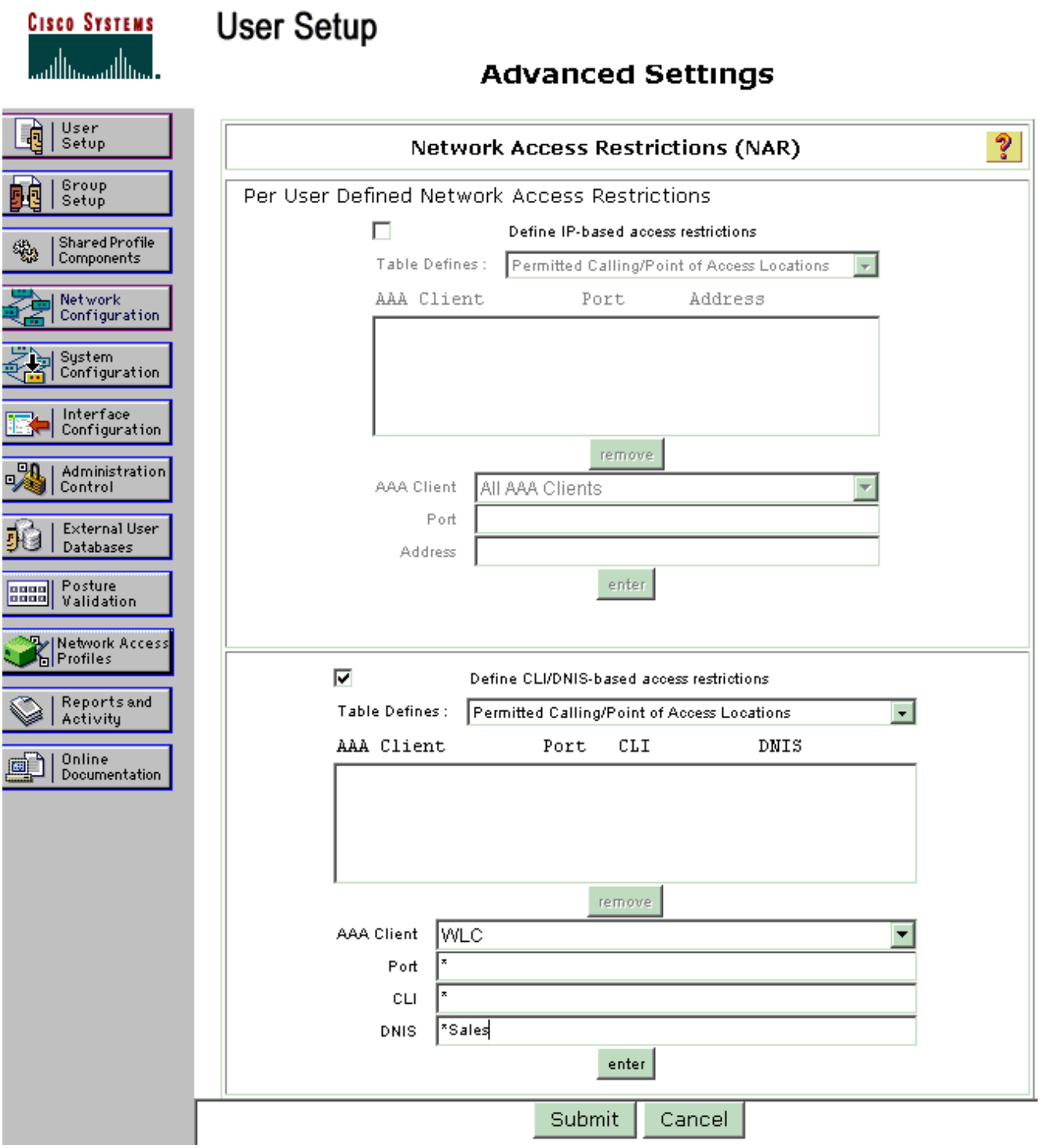
.



7. Submit(제출)**을 클릭합니다**.
8. 마찬가지로 영업 부서 사용자의 사용자를 생성합니다.스크린샷입니다

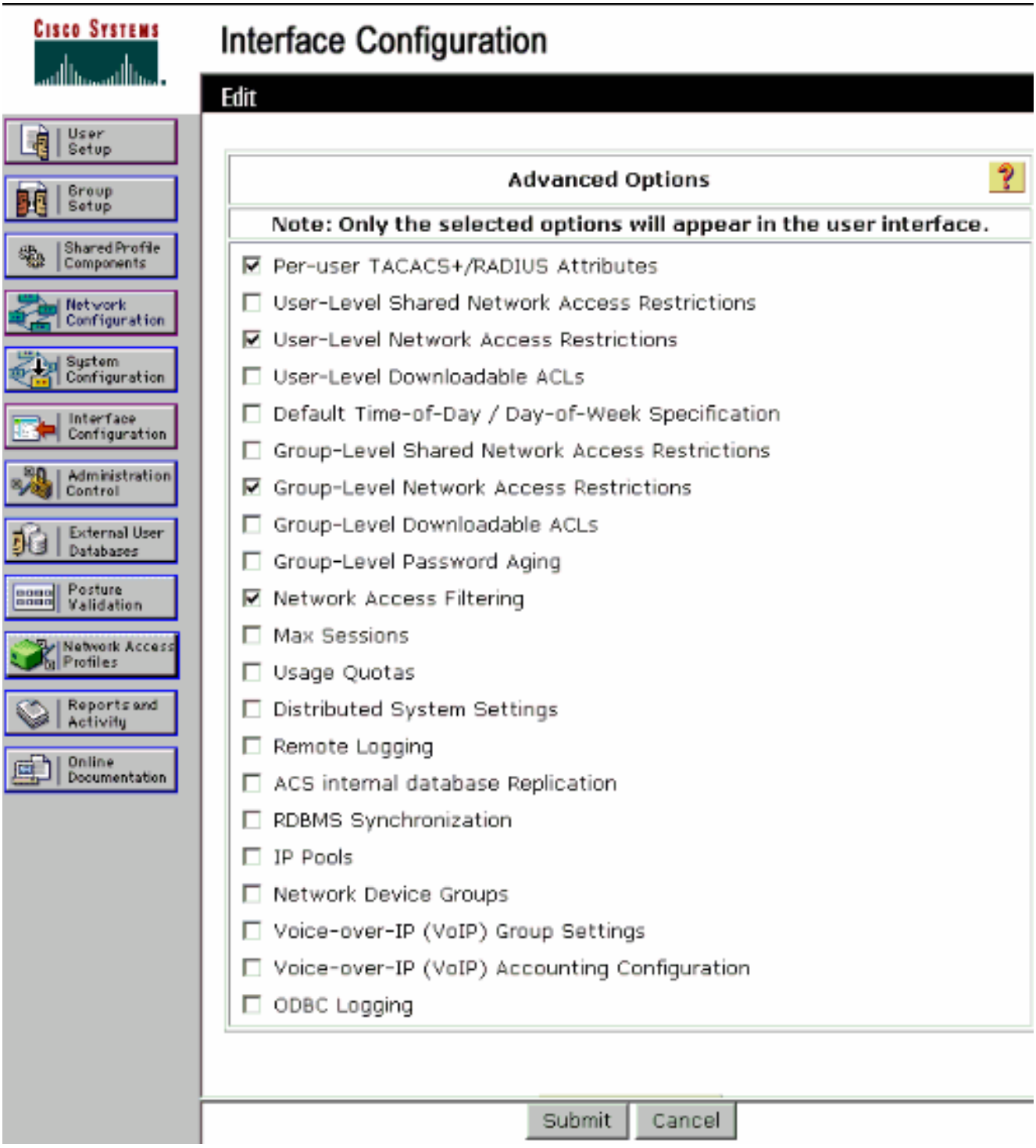
.

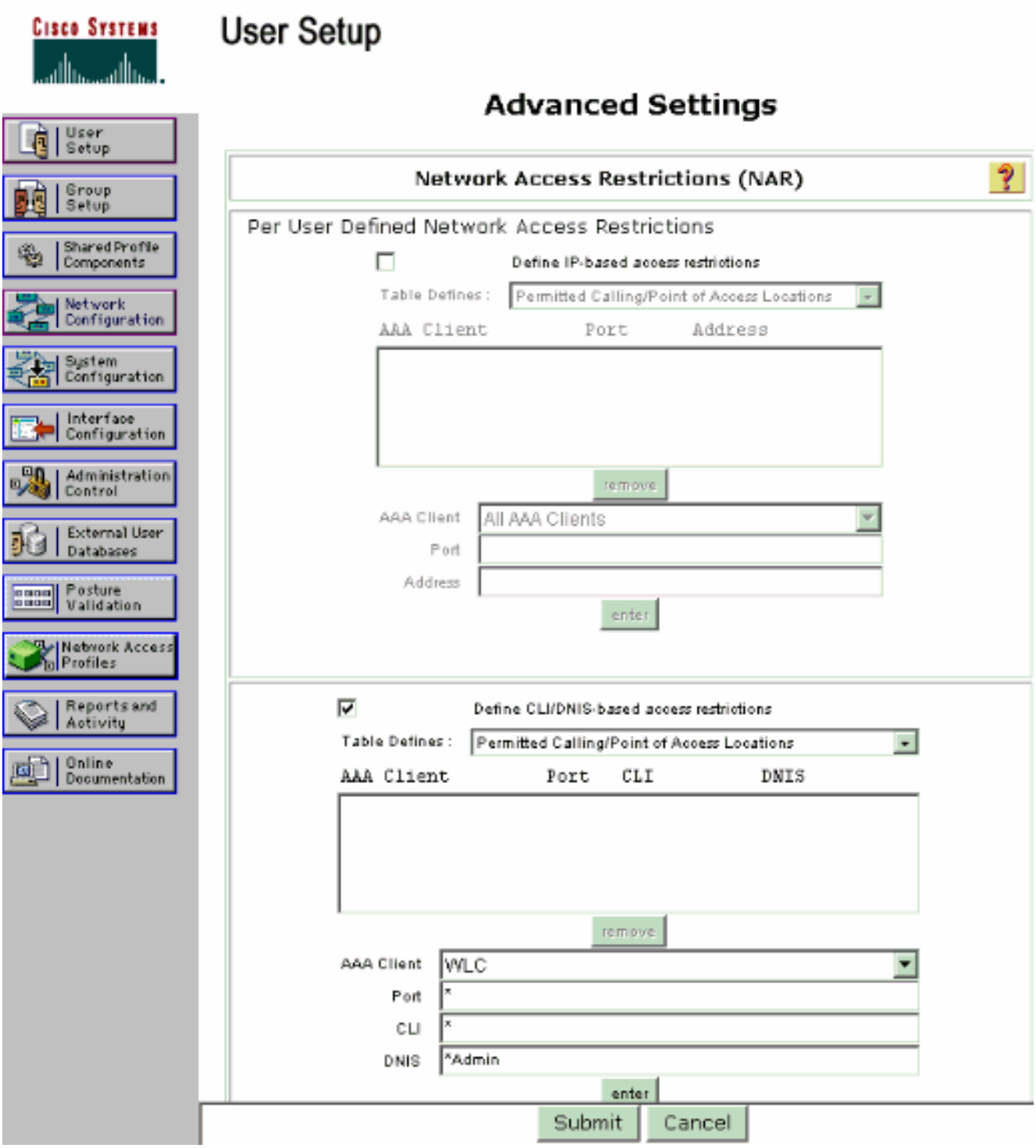

Cisco Systems
User Setup
Edit
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
User: S1 (New User)
Account Disabled
Supplementary User Info
Real Name
S1
Description
Sales Department User
User Setup
Password Authentication:
ACS Internal Database
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:
Submit
Cancel



9. 동일한 프로세스를 반복하여 데이터베이스에 사용자를 더 추가합니다.**참고:** 기본적으로 모든 사용자는 기본 그룹 아래에 그룹화됩니다.특정 사용자를 다른 그룹에 할당하려면 Windows Server 3.2용 Cisco Secure ACS 사용 설명서의 사용자 그룹 관리 섹션을 참조하십시오.**참고:** User Setup(사용자 설정) 창에 Network Access Restrictions(네트워크 액세스 제한) 섹션이 표시되지 않으면 활성화되지 않았기 때문일 수 있습니다.사용자에 대한 네트워크 액세스 제한을 활성화하려면 ACS GUI에서 **Interfaces(인터페이스) > Advanced Options(고급 옵션)**를 선택하고 **User-Level Network Access Restrictions(사용자 레벨 네트워크 액세스 제한)를** 선택하고 Submit(제출)을 **클릭합니다**.이렇게 하면 NAR이 활성화되고 User Setup(사용자 설정) 창에 나타납니다

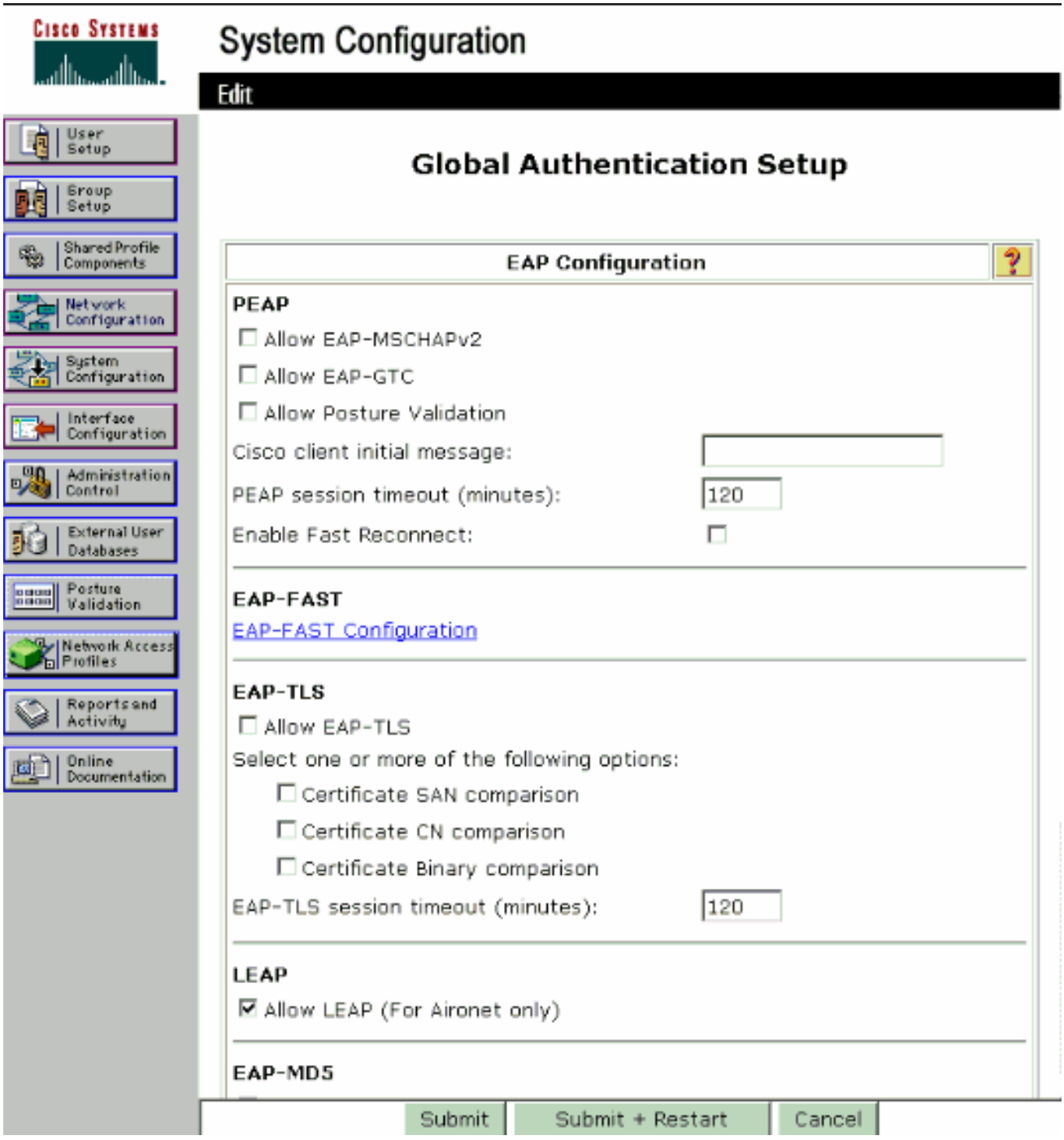
.


Cisco Systems
Interface Configuration
Edit
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Advanced Options
Note: Only the selected options will appear in the user interface.
Per-user TACACS+/RADIUS Attributes
User-Level Shared Network Access Restrictions
User-Level Network Access Restrictions
User-Level Downloadable ACLs
Default Time-of-Day / Day-of-Week Specification
Group-Level Shared Network Access Restrictions
Group-Level Network Access Restrictions
Group-Level Downloadable ACLs
Group-Level Password Aging
Network Access Filtering
Max Sessions
Usage Quotas
Distributed System Settings
Remote Logging
ACS internal database Replication
RDBMS Synchronization
IP Pools
Network Device Groups
Voice-over-IP (VoIP) Group Settings
Voice-over-IP (VoIP) Accounting Configuration
ODBC Logging
Submit
Cancel



10. EAP 인증을 활성화하려면 인증 서버가 원하는 EAP 인증 방법을 수행하도록 구성되었는지 확인하기 위해 **System Configuration** and **Global Authentication Setup**을 클릭합니다.EAP 컨피그레이션 설정에서 적절한 EAP 방법을 선택합니다.이 예에서는 LEAP 인증을 사용합니다 .완료되면 **Submit(제출)**을 클릭합니다

.

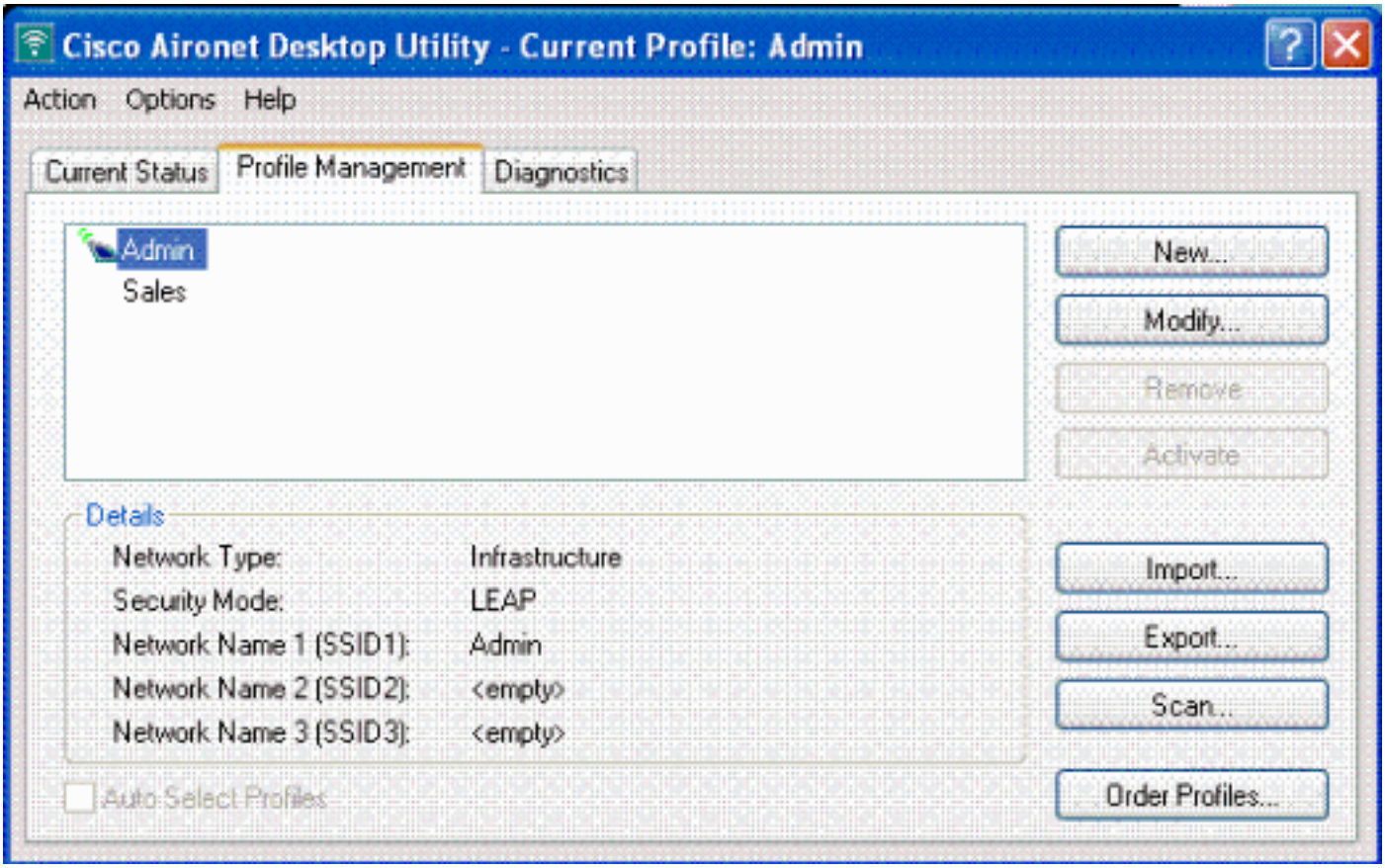


무선 클라이언트 구성 및 확인

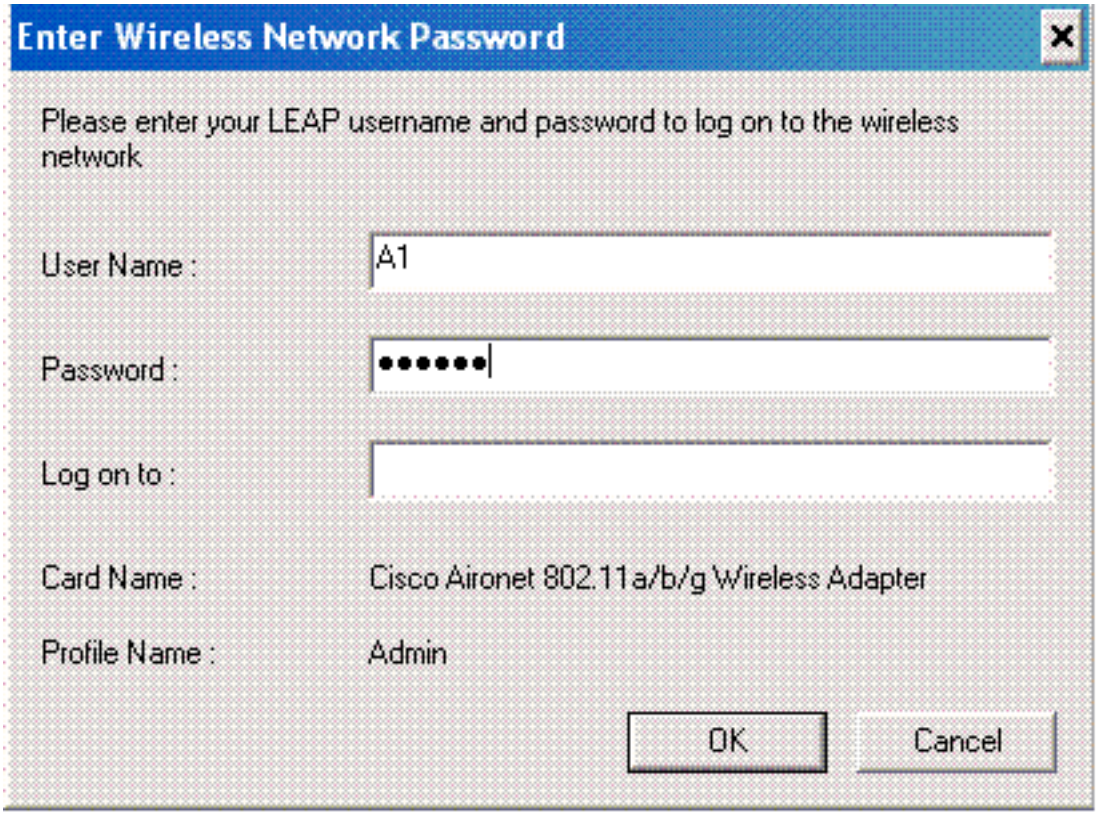
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.LEAP 인증을 사용하여 무선 클라이언트를 LAP에 연결하여 컨피그레이션이 예상대로 작동하는지 확인합니다.

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.

참고: ADU에서 두 개의 클라이언트 프로파일을 구성했음을 확인할 수 있습니다.SSID **관리자**가 있는 관리 부서 사용자와 SSID **Sales**가 있는 판매 부서 사용자의 다른 프로파일**을** 위한 **것입니다**.두 프로파일 모두 LEAP 인증을 위해 구성됩니다.



관리 부서의 무선 사용자에 대한 프로파일이 활성화되면 사용자에게 LEAP 인증을 위한 사용자 이름/비밀번호를 입력하라는 메시지가 표시됩니다.예를 들면 다음과 같습니다.

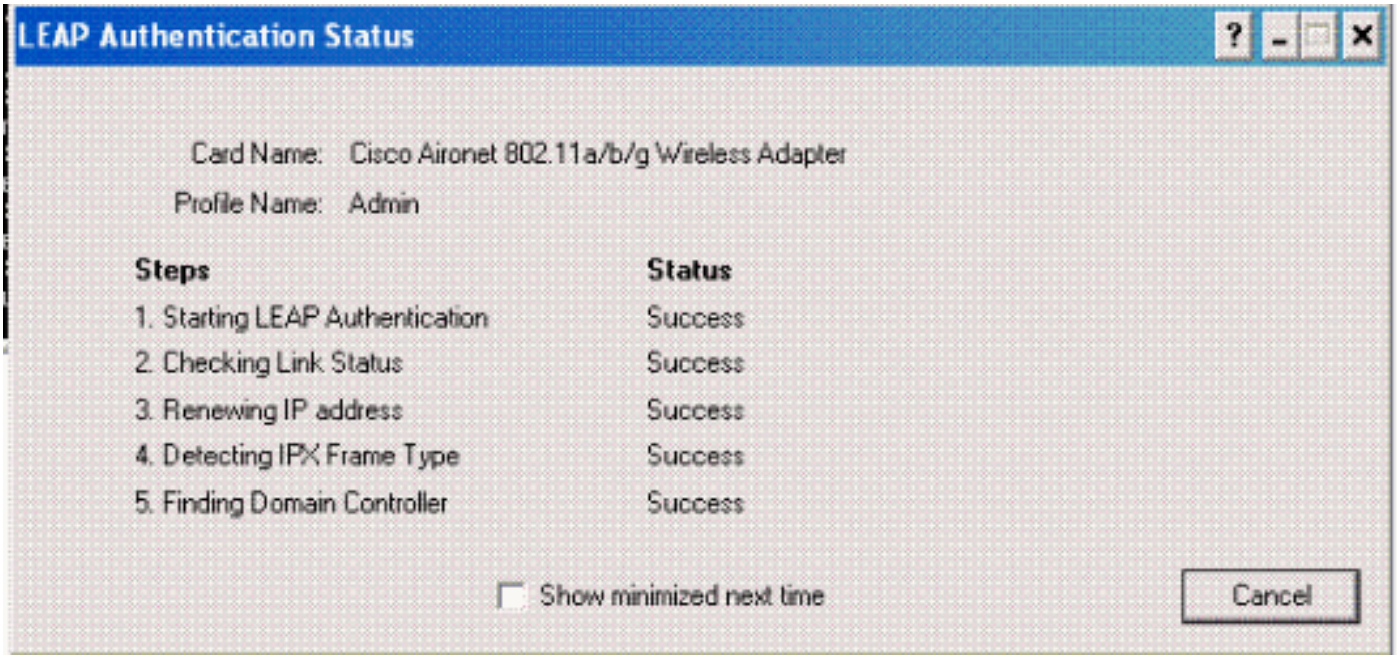


LAP와 WLC는 사용자 자격 증명을 외부 RADIUS 서버(Cisco Secure ACS)에 전달하여 자격 증명을 검증합니다.WLC는 검증을 위해 DNIS 특성(SSID 이름)을 포함한 자격 증명을 RADIUS 서버에 전달합니다.

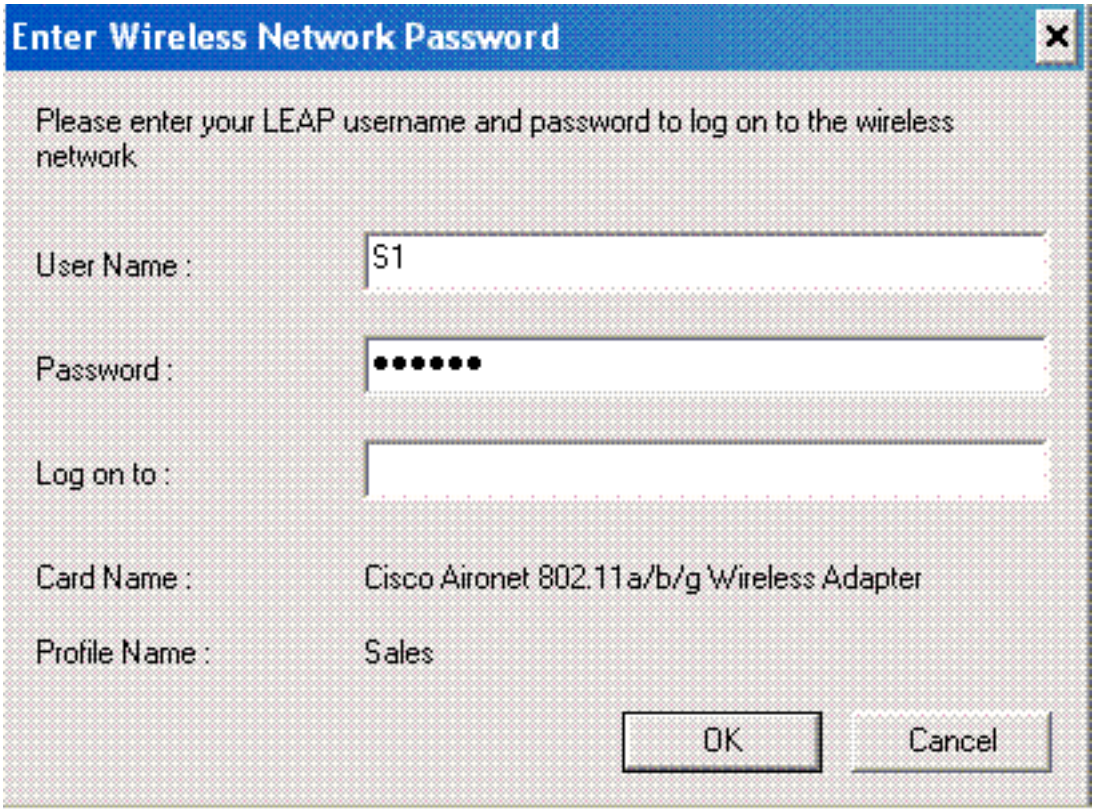
RADIUS 서버는 데이터를 사용자 데이터베이스(및 NAR)와 비교하여 사용자 자격 증명을 확인하고

사용자 자격 증명이 유효할 때마다 무선 클라이언트에 대한 액세스를 제공합니다.

RADIUS 인증에 성공하면 무선 클라이언트가 LAP와 연결됩니다.



Sales 부서의 사용자가 Sales 프로필을 활성화하면 LEAP 사용자 이름/비밀번호 및 SSID를 기반으로 RADIUS 서버에서 사용자를 인증합니다.



ACS 서버의 Passed Authentication(전달된 인증) 보고서는 클라이언트가 RADIUS 인증(EAP 인증 및 SSID 인증)을 통과했음을 보여줍니다. 예를 들면 다음과 같습니다.

Reports and Activity

Select

Passed Authentications active.csv Refresh Download

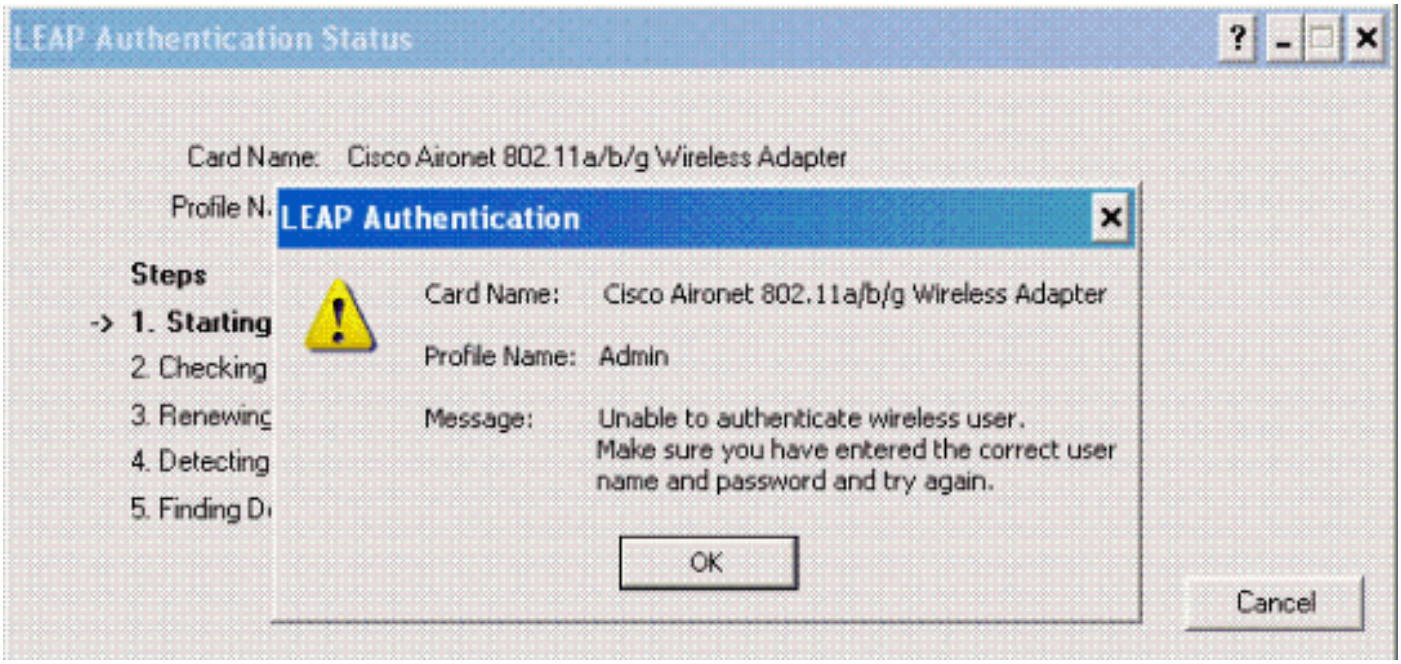
Regular Expression | Start Date & Time (mm/dd/yyyy,hh:mm:ss) | End Date & Time (mm/dd/yyyy,hh:mm:ss) | Rows per Page (50)

Apply Filter | Clear Filter

Filtering is not applied.

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address	Network Access Profile Name	Shared RAC	Downloadable ACL	System-Posture-Token	Application-Posture-Token	Reason	EAP Type	EAP Type Name
10/11/2006	14:48:40	Authen OK	S1	Default Group	00-40-96-AC-E6-57	1	172.16.1.30	(Default)	..	..	..	..	..	17	LEAP
10/11/2006	14:47:05	Authen OK	A1	Default Group	00-40-96-AC-E6-57	1	172.16.1.30	(Default)	..	..	..	..	..	17	LEAP

이제 세일즈 사용자가 **관리** SSID에 액세스하려고 하면 RADIUS 서버는 WLAN에 대한 사용자 액세스를 거부합니다.예를 들면 다음과 같습니다.



이렇게 하면 사용자가 SSID를 기반으로 액세스를 제한할 수 있습니다.N 기업 환경에서는 특정 부서에 속하는 모든 사용자를 단일 그룹으로 그룹화할 수 있으며 이 문서에서 설명한 대로 SSID를 사용하여 WLAN에 액세스할 수 있습니다.

문제 해결

문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug dot1x aaa enable** - 802.1x AAA 상호 작용의 디버그를 활성화합니다.
- **debug dot1x packet enable** - 모든 dot1x 패킷의 디버그를 활성화합니다.
- **debug aaa all enable** - 모든 AAA 메시지의 디버그를 구성합니다.

Cisco Secure ACS 서버에서 Passed Authentication(전달된 인증) 보고서 및 Failed Authentication(실패한 인증) 보고서를 사용하여 컨피그레이션을 트러블슈팅할 수도 있습니다.이러한 보고서는 ACS GUI의 **Reports and Activity** 창 아래에 있습니다.

관련 정보

- WLAN 컨트롤러(WLC)를 사용한 EAP 인증 컨피그레이션 예
- 무선 LAN 컨트롤러 웹 인증 컨피그레이션 예
- 무선 LAN 컨트롤러가 있는 AP 그룹 VLAN 컨피그레이션 예
- 무선 지원 페이지
- 기술 지원 및 문서 – Cisco Systems