무선 도메인 서비스 구성

목차

소개

이 문서에서는 WDS(Wireless Domain Services)의 개념을 소개합니다. 또한 이 문서에서는 하나의 AP(Access Point) 또는 WLSM(Wireless LAN Services Module)을 WDS로 구성하고 다른 하나 이상을 인프라 AP로 구성하는 방법에 대해 설명합니다. 이 문서의 절차에서는 작동 중인 WDS를 안내하고 클라이언트가 WDS AP 또는 인프라 AP에 연결할 수 있도록 합니다. 이 문서는 빠른 보안 로밍을 구성하거나 네트워크에 WLSE(Wireless LAN Solutions Engine)를 도입하여 기능을 사용할 수 있는 기반을 설정하려고 합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 무선 LAN 네트워크 및 무선 보안 문제에 대해 철저히 숙지하십시오.
- 현재 EAP(Extensible Authentication Protocol) 보안 방법을 알고 있어야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어를 사용하는 AP
- Cisco IOS Software 릴리스 12.3(2)JA2 이상
- Catalyst 6500 Series Wireless LAN Services Module

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 인터페이스 BVI1의 지워진(기본) 컨피그레이션과 IP 주소로 시작되므로 Cisco IOS 소프트웨어 GUI 또는 CLI(Command Line Interface)에서 디바이스에 액세스할 수 있습니다. 라이브 네트워크에서 작업하는 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

무선 도메인 서비스

WDS는 Cisco IOS Software의 AP와 Catalyst 6500 Series WLSM의 기반이 되는 새로운 기능입니다. WDS는 다음과 같은 다른 기능을 활성화하는 핵심 기능입니다.

- 빠른 보안 로밍
- WLSE 상호 작용
- 무선 관리

다른 WDS 기반 기능이 작동하기 전에 WDS와 WLSM에 참여하는 AP 간의 관계를 설정해야 합니다. WDS의 목적 중 하나는 사용자 자격 증명을 검증하고 클라이언트 인증에 필요한 시간을 단축하기 위해 인증 서버가 필요하지 않게 하는 것입니다.

WDS를 사용하려면 하나의 AP 또는 WLSM을 WDS로 지정해야 합니다. WDS AP는 인증 서버와의 관계를 설정하려면 WDS 사용자 이름 및 비밀번호를 사용해야 합니다. 인증 서버는 외부 RADIUS 서버이거나 WDS AP의 로컬 RADIUS 서버 기능일 수 있습니다. WLSM이 서버에 대해 인증할 필요는 없지만 WLSM은 인증 서버와 관계가 있어야 합니다.

인프라 AP라고 하는 다른 AP는 WDS와 통신합니다. 등록 전에 인프라 AP는 WDS에 대해 자신을 인증해야 합니다. WDS의 인프라 서버 그룹은 이 인프라 인증을 정의합니다.

WDS에서 하나 이상의 클라이언트 서버 그룹이 클라이언트 인증을 정의합니다.

클라이언트가 인프라 AP에 연결하려고 시도하면 인프라 AP는 검증을 위해 사용자의 자격 증명을 WDS에 전달합니다. WDS에 처음으로 자격 증명이 표시되면 WDS는 인증 서버로 전환하여 자격 증명을 검증합니다. 그런 다음 WDS는 동일한 사용자가 인증을 다시 시도할 때 인증 서버로 돌아갈 필요가 없도록 자격 증명을 캐시합니다. 재인증의 예는 다음과 같습니다.

- 키 재지정
- 로밍
- 사용자가 클라이언트 디바이스를 시작할 때

RADIUS 기반 EAP 인증 프로토콜은 다음과 같은 WDS를 통해 터널링될 수 있습니다.

- LEAP(Lightweight EAP)
- 보호된 EAP(PEAP)
- EAP-전송 계층 보안(EAP-TLS)

- 보안 터널링을 통한 EAP-Flexible 인증(EAP-FAST)

또한 MAC 주소 인증은 외부 인증 서버 또는 WDS AP에 대한 로컬 목록에 대해 터널링할 수 있습니다. WLSM은 MAC 주소 인증을 지원하지 않습니다.

WDS 및 인프라 AP는 WLCCP(WLAN Context Control Protocol)라는 멀티캐스트 프로토콜을 통해 통신합니다. 이러한 멀티캐스트 메시지는 라우팅할 수 없으므로 WDS와 관련 인프라 AP는 동일한 IP 서브넷에 있고 동일한 LAN 세그먼트에 있어야 합니다. WDS와 WLSE 사이에서 WLCCP는 포트 2887에서 TCP 및 UDP(User Datagram Protocol)를 사용합니다. WDS와 WLSE가 서로 다른 서브넷에 있는 경우 NAT(Network Address Translation)와 같은 프로토콜에서 패킷을 변환할 수 없습니다.

WDS 디바이스로 구성된 AP는 최대 60개의 참여 AP를 지원합니다. WDS 디바이스로 구성된 ISR(Integrated Services Router)은 최대 100개의 참여 AP를 지원합니다. 또한 WLSM 기반 스위치는 최대 600개의 참여 AP와 최대 240개의 모빌리티 그룹을 지원합니다. 단일 AP는 최대 16개의 모빌리티 그룹을 지원합니다.

참고: 인프라 AP는 WDS 디바이스와 동일한 버전의 IOS를 실행하는 것이 좋습니다. 이전 버전의 IOS를 사용하는 경우 AP가 WDS 디바이스를 인증하지 못할 수 있습니다. 또한 최신 버전의 IOS를 사용하는 것이 좋습니다. 무선 다운로드 페이지에서 최신 버전의 IOS를 찾을 수 있습니다.

WDS 장치의 역할

WDS 디바이스는 무선 LAN에서 여러 작업을 수행합니다.

- WDS 기능을 광고하고 무선 LAN에 가장 적합한 WDS 장치를 선택하는 데 참여합니다. WDS용 무선 LAN을 구성할 때 하나의 디바이스를 기본 WDS 후보로, 하나 이상의 추가 디바이스를 백업 WDS 후보로 설정합니다. 기본 WDS 디바이스가 오프라인 상태가 되면 백업 WDS 디바이스 중 하나가 작동합니다.
- 서브넷의 모든 AP를 인증하고 각 AP와 보안 통신 채널을 설정합니다.
- 서브넷의 AP에서 무선 데이터를 수집하고, 데이터를 집계하여 네트워크의 WLSE 디바이스에 전달합니다.
- 참여 AP에 연결된 모든 802.1x 인증 클라이언트 디바이스에 대한 패스스루 역할을 합니다.
- 동적 키를 사용하는 서브넷에 모든 클라이언트 디바이스를 등록하고, 해당 디바이스에 대한 세션 키를 설정하고, 보안 자격 증명을 캐시합니다. 클라이언트가 다른 AP로 로밍하면 WDS 디바이스는 클라이언트의 보안 자격 증명을 새 AP에 전달합니다.

WDS 디바이스를 사용하는 액세스 포인트의 역할

무선 LAN의 AP는 다음 활동에서 WDS 장치와 상호 작용합니다.

- 현재 WDS 디바이스를 검색하고 추적하고 WDS 광고를 무선 LAN에 릴레이합니다.
- WDS 디바이스로 인증하고 WDS 디바이스에 대한 보안 통신 채널을 설정합니다.
- 연결된 클라이언트 디바이스를 WDS 디바이스에 등록합니다.
- WDS 디바이스에 무선 데이터를 보고합니다.

구성

WDS는 순서가 지정된 모듈형 방식으로 구성을 나타냅니다. 각 개념은 앞에 오는 개념을 기반으로

합니다. WDS는 비밀번호, 원격 액세스, 무선 설정 등의 다른 구성 항목을 생략하여 핵심 주제에 초점을 맞추고 있습니다.

이 섹션에서는 이 문서에 설명된 기능을 구성하는 데 필요한 정보를 제공합니다.

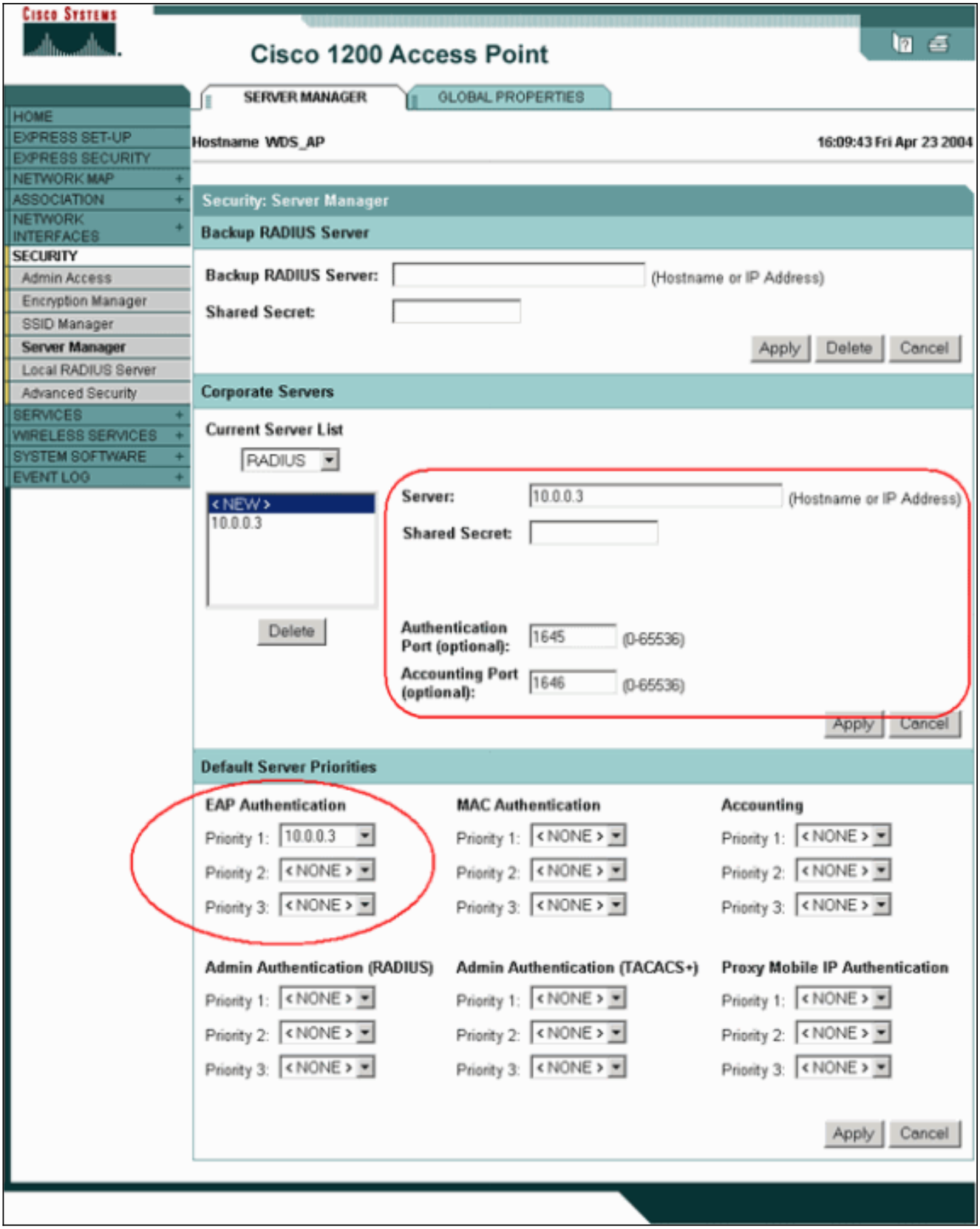
참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

AP를 WDS로 지정

첫 번째 단계는 AP를 WDS로 지정하는 것입니다. WDS AP는 인증 서버와 통신하는 유일한 AP입니다.

AP를 WDS로 지정하려면 다음 단계를 완료하십시오.

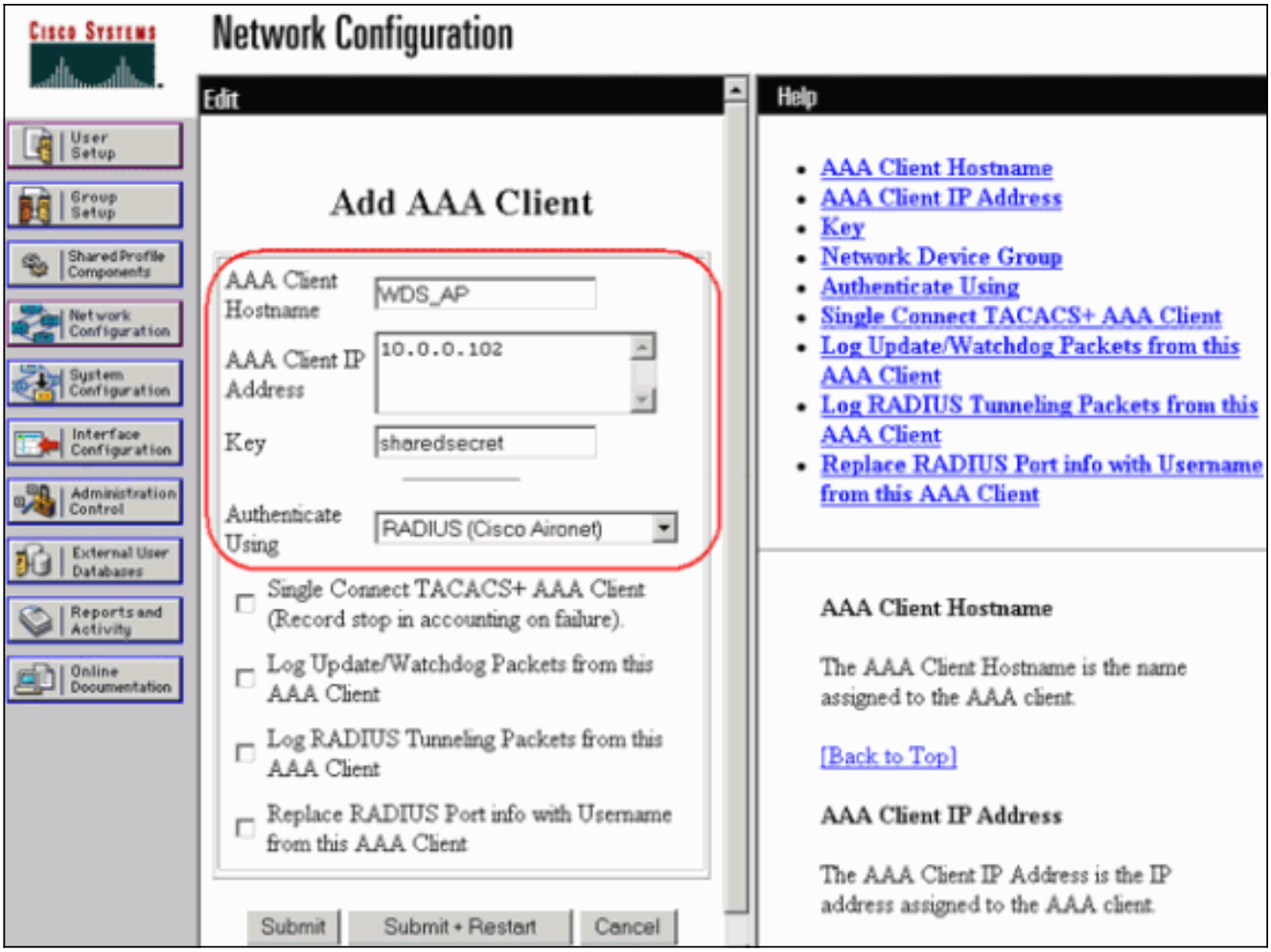
1. WDS AP에서 인증 서버를 구성하려면 **Security(보안) > Server Manager(서버 관리자)**를 선택하여 Server Manager(서버 관리자) 탭으로 이동합니다.Corporate Servers(회사 서버)의 Server(서버) 필드에 인증 서버의 IP 주소를 입력합니다.공유 암호와 포트를 지정합니다.Default Server Priorities 아래에서 Priority 1 필드를 적절한 인증 유형 아래의 해당 서버 IP 주소로 설정합니다
   .



또는 CLI에서 다음 명령을 실행합니다.

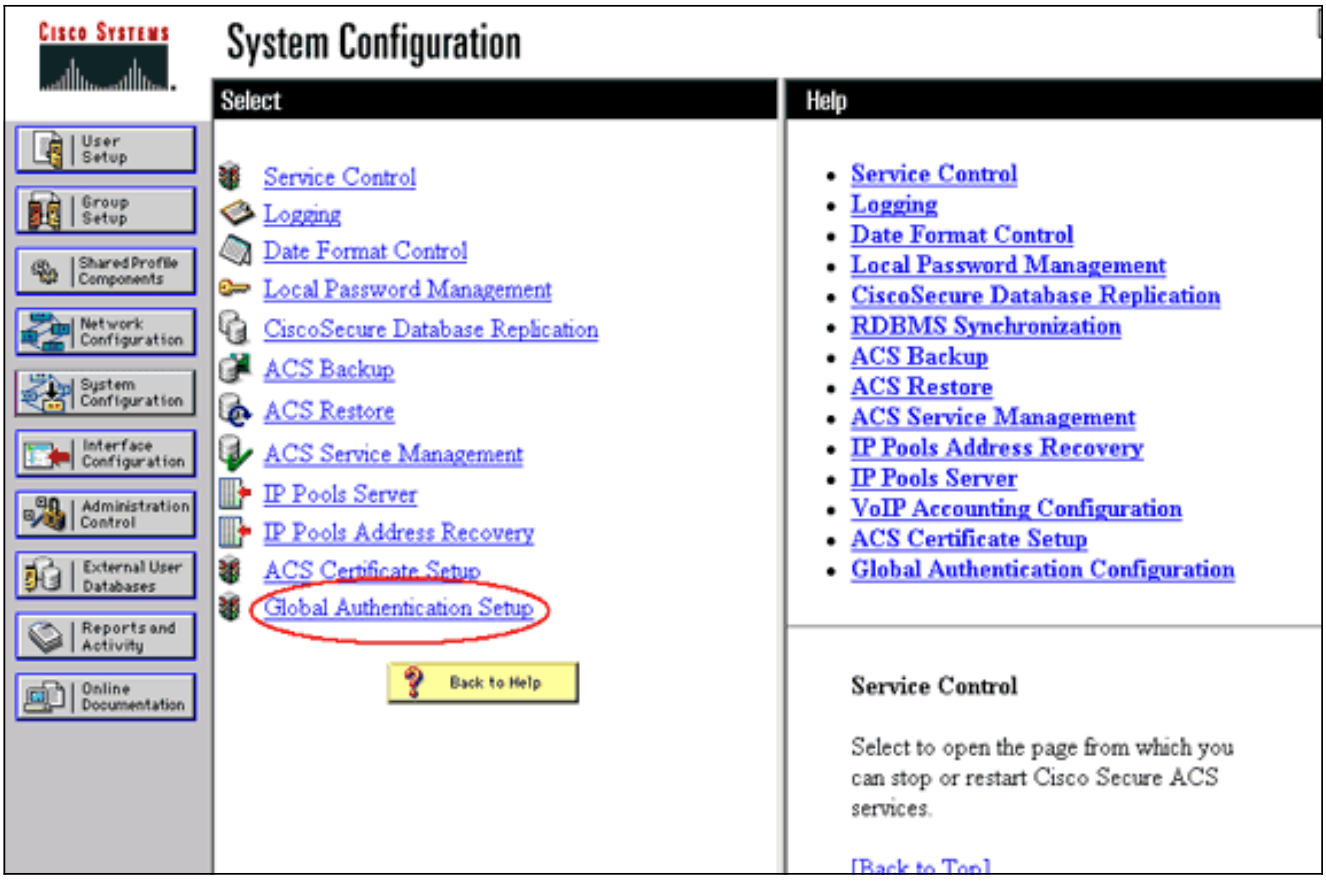
2. 다음 단계는 인증 서버의 WDS AP를 AAA(Authentication, Authorization, and Accounting) 클라이언트로 구성하는 것입니다. 이를 위해 WDS AP를 AAA 클라이언트로 추가해야 합니다. 다음 단계를 완료하십시오.**참고:** 이 문서에서는 Cisco Secure ACS 서버를 인증 서버로 사용합니다.Cisco ACS(Secure Access Control Server)에서 이는 WDS AP에 대해 이러한 특성을 정의하는 네트워크 구성 페이지에서 발생합니다.이름IP 주소공유 암호인증 방법RADIUS Cisco AironetRADIUS IETF(Internet Engineering Task Force)Submit(제출)을 **클릭합니다** .ACS가 아닌 다른 인증 서버는 제조업체의 설명서를 참조하십시오

.



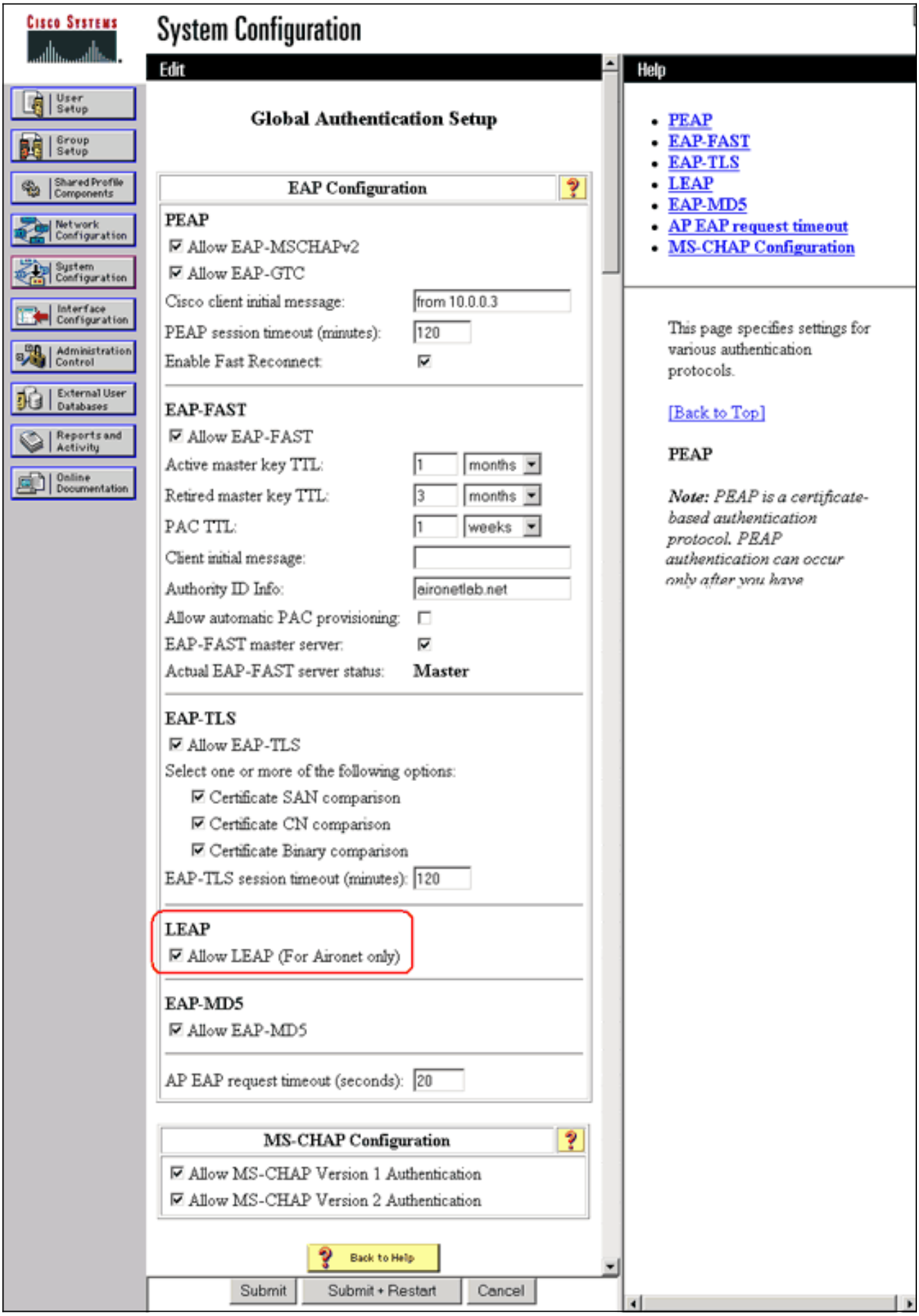
또한 Cisco Secure ACS에서 System Configuration - Global Authentication Setup 페이지에서 LEAP 인증을 수행하도록 ACS를 구성해야 합니다. 먼저 **System Configuration(시스템 컨피그레이션)**을 클릭한 다음 **Global Authentication Setup(전역 인증 설정)을 클릭합니다**

.



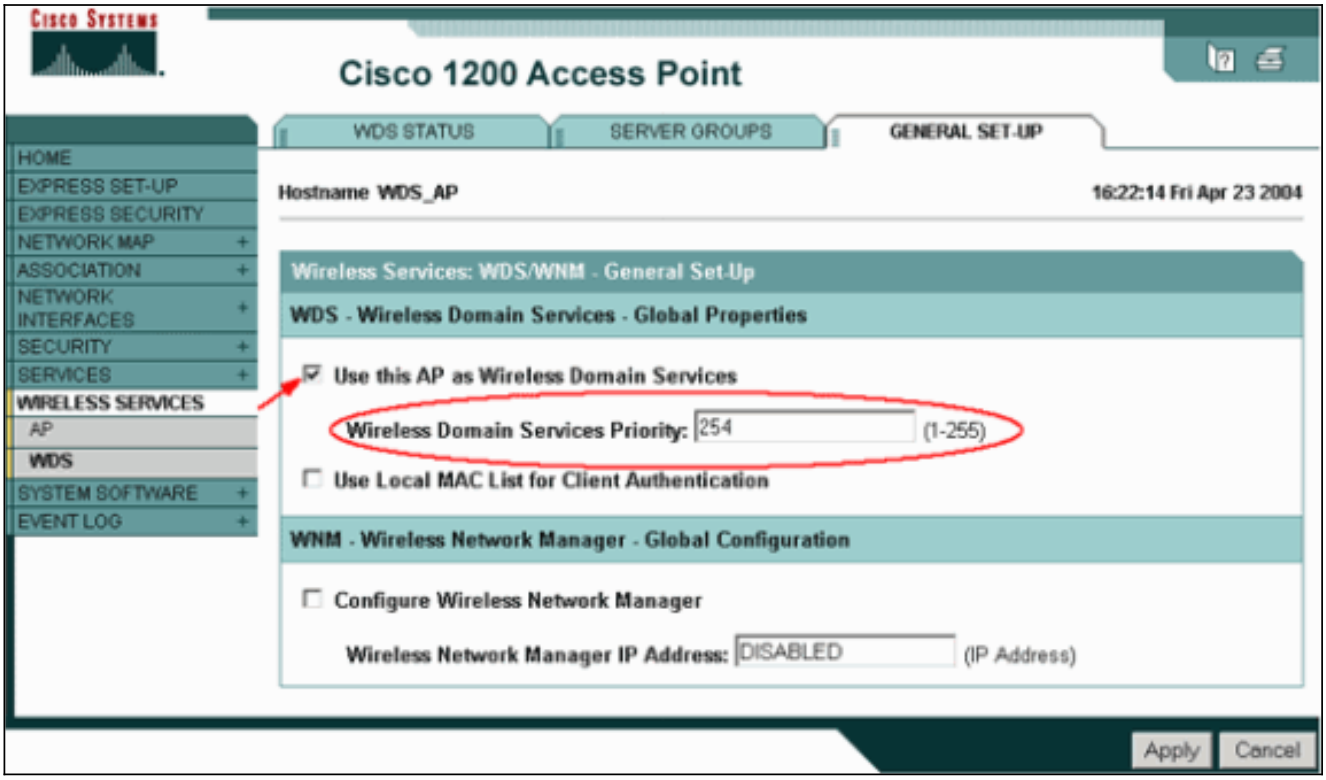
페이지를 아래로 스크롤하여 LEAP 설정으로 이동합니다. 확인란을 선택하면 ACS에서 LEAP를 인증합니다

.



3. WDS AP에서 WDS 설정을 구성하려면 WDS AP에서 **Wireless Services(무선 서비스) > WDS(WDS)**를 선택하고 **General Set-Up(일반 설정)** 탭을 클릭합니다. 다음 단계를 수행합니다.WDS-Wireless Domain Services - Global Properties 아래에서 Use this **AP as Wireless Domain Services**를 선택합니다.Wireless Domain Services Priority(무선 도메인 서비스 우선 순위) 필드의 값을 약 **254** 값으로 설정합니다. 첫 번째 값이기 때문입니다. 하나 이상의 AP 또는 스위치를 후보자로 구성하여 WDS를 제공할 수 있습니다. 우선 순위가 가장 높은 장치는 WDS를 제공합니다

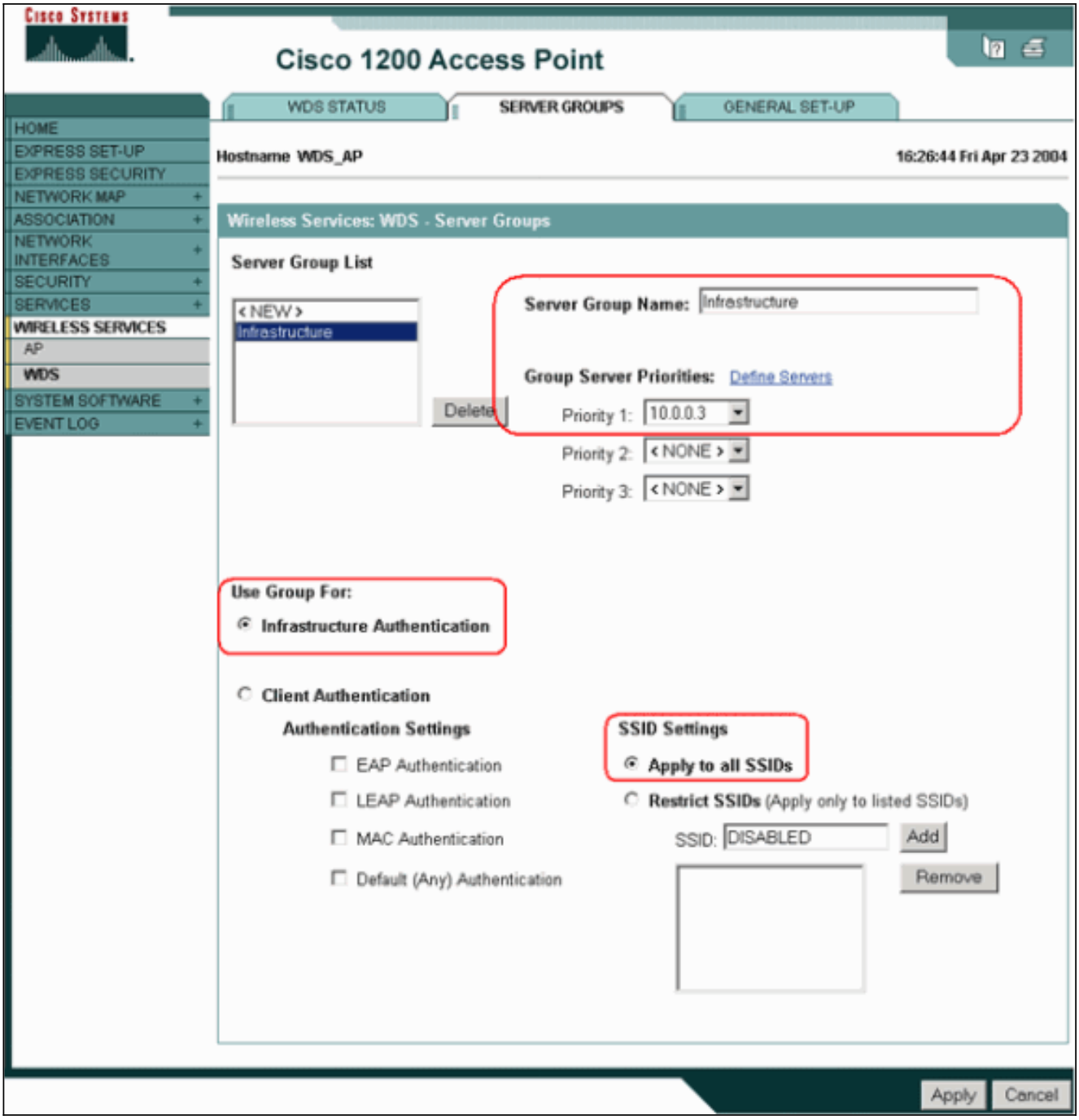
.



또는 CLI에서 다음 명령을 실행합니다.

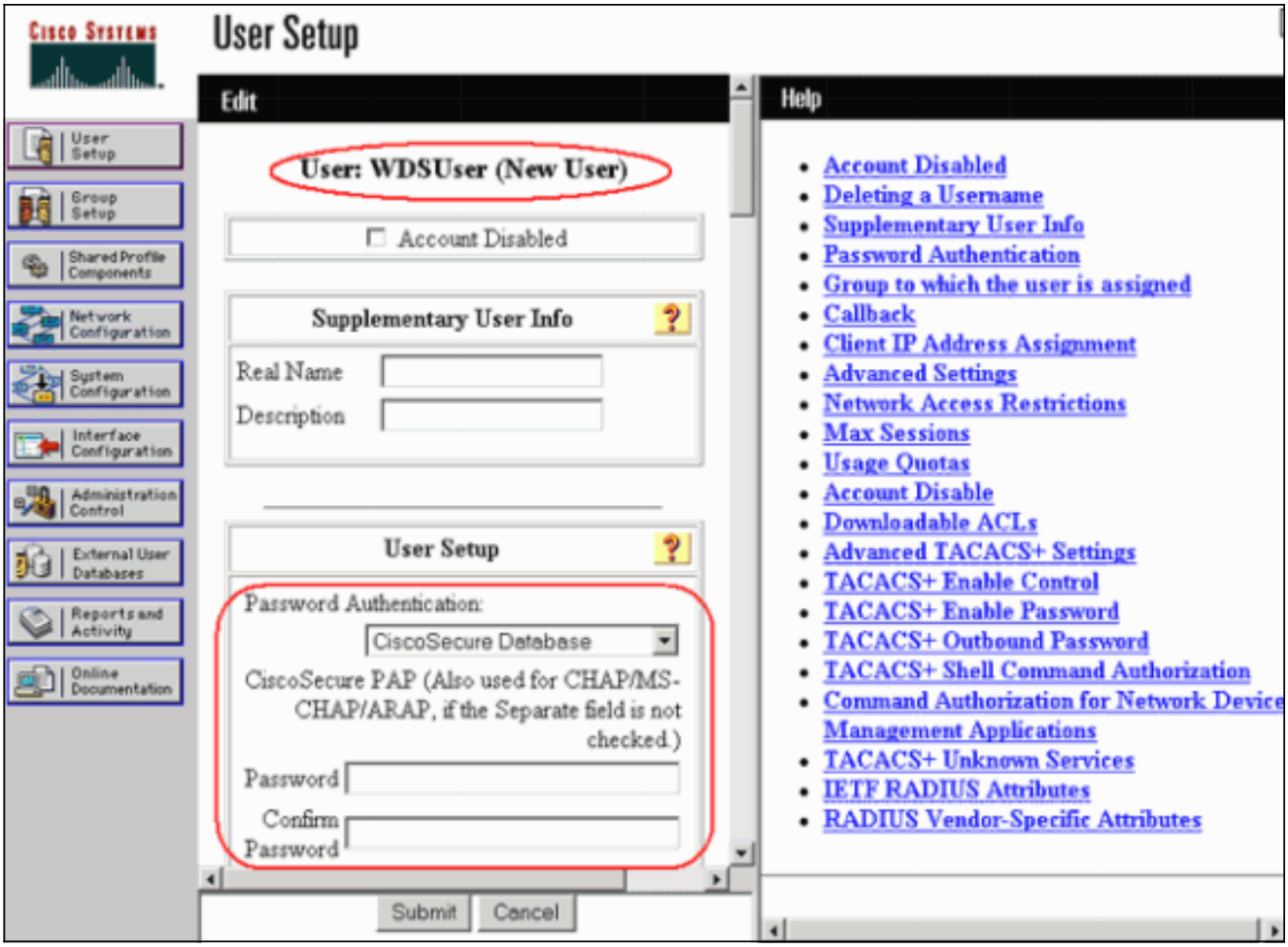
4. Wireless **Services(무선 서비스) > WDS(WDS)**를 선택하고 **Server Groups(서버 그룹)** 탭으로 이동합니다.다른 AP, 인프라 그룹을 인증하는 서버 그룹 이름을 정의합니다.Priority 1을 이전에 구성한 인증 서버로 설정합니다.Use **Group For:(그룹 사용 대상:)을 클릭합니다. 인프라 인증** 라디오 버튼.관련 SSID(Service Set Identifier)에 설정을 적용합니다

.



또는 CLI에서 다음 명령을 실행합니다.

5. WDS 사용자 이름 및 비밀번호를 인증 서버의 사용자로 구성합니다.Cisco Secure ACS에서는 WDS 사용자 이름 및 비밀번호를 정의하는 User Setup 페이지에서 이러한 문제가 발생합니다. ACS가 아닌 다른 인증 서버는 제조업체의 설명서를 참조하십시오.**참고:** WDS 사용자를 많은 권한 및 권한이 할당된 그룹에 두지 마십시오. WDS에는 제한된 인증만 필요합니다
.



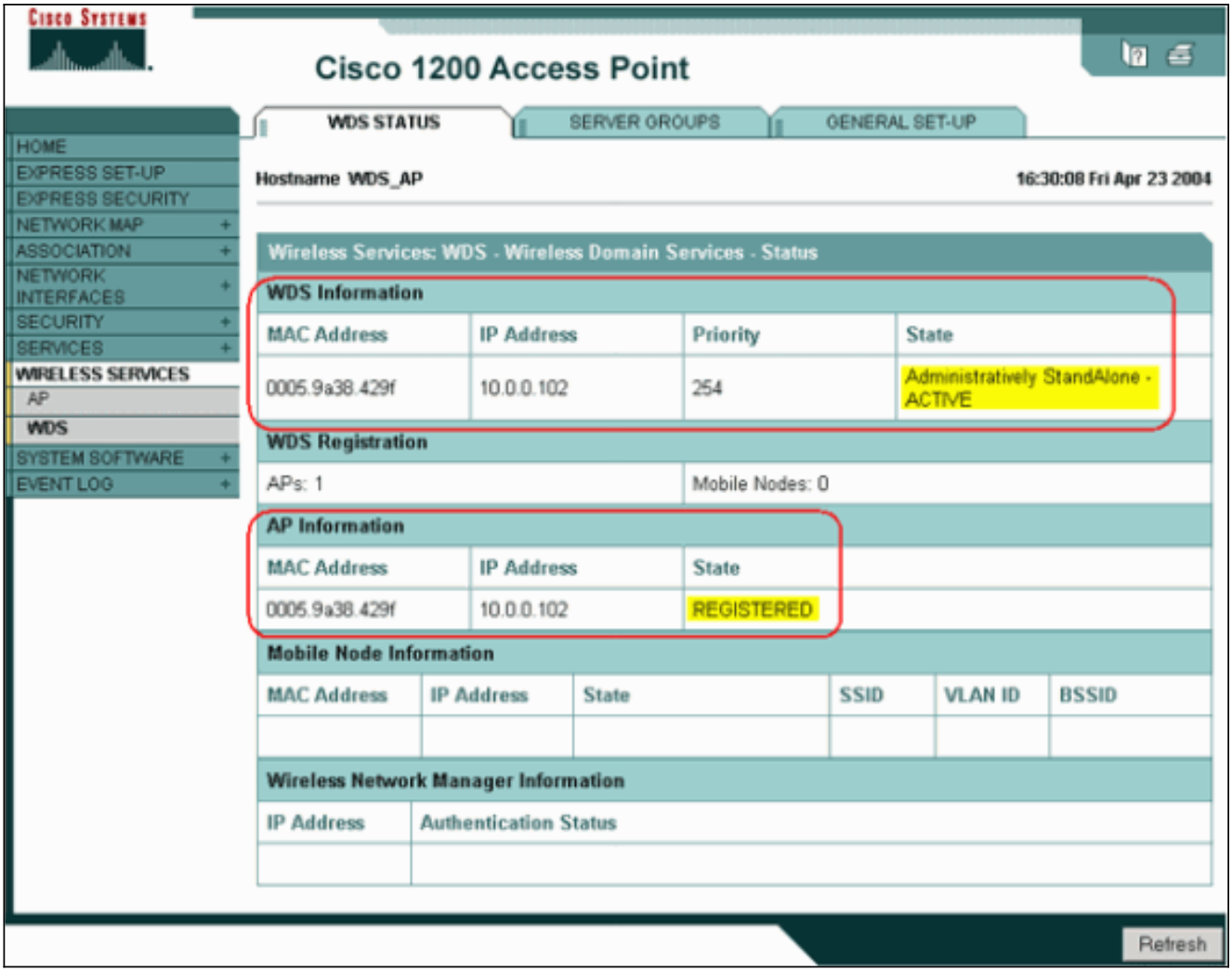
6. Wireless **Services(무선 서비스) > AP**를 선택하고 **Enable(활성화)을** 클릭하여 Participate in SWAN infrastructure(SWAN 인프라에 참여) 옵션을 선택합니다. 그런 다음 WDS 사용자 이름 및 비밀번호를 입력합니다.WDS의 멤버를 지정하는 모든 디바이스에 대해 인증 서버에서 WDS 사용자 이름과 비밀번호를 정의해야 합니다

.

또는 CLI에서 다음 명령을 실행합니다.

7. 무선 **서비스 > WDS를 선택합니다**. WDS AP WDS Status(WDS AP WDS 상태) 탭에서 WDS Information(WDS 정보) 영역의 ACTIVE State(활성 상태)에 WDS AP가 나타나는지 확인합니다. AP는 AP Information(AP 정보) 영역에도 나타나야 하며 State(상태)는 REGISTERED(등록됨)로 표시됩니다.AP가 REGISTERED 또는 ACTIVE로 표시되지 않으면 인증 서버에서 오류 또는 실패한 인증 시도를 확인합니다.AP가 적절하게 등록되면 WDS의 서비스를 사용할 인프라 AP를 추가합니다

.



또는 CLI에서 다음 명령을 실행합니다.**참고:** 클라이언트 인증에 아직 프로비전이 없으므로 클라이언트 연결을 테스트할 수 없습니다.

WLSM을 WDS로 지정

이 섹션에서는 WLSM을 WDS로 구성하는 방법에 대해 설명합니다. WDS는 인증 서버와 통신하는 유일한 디바이스입니다.

참고: Supervisor Engine 720이 아닌 WLSM의 enable 명령 프롬프트에서 다음 명령을 실행합니다. WLSM의 명령 프롬프트로 이동하려면 Supervisor Engine 720의 `enable` 명령 프롬프트에서 다음 명령을 실행합니다.

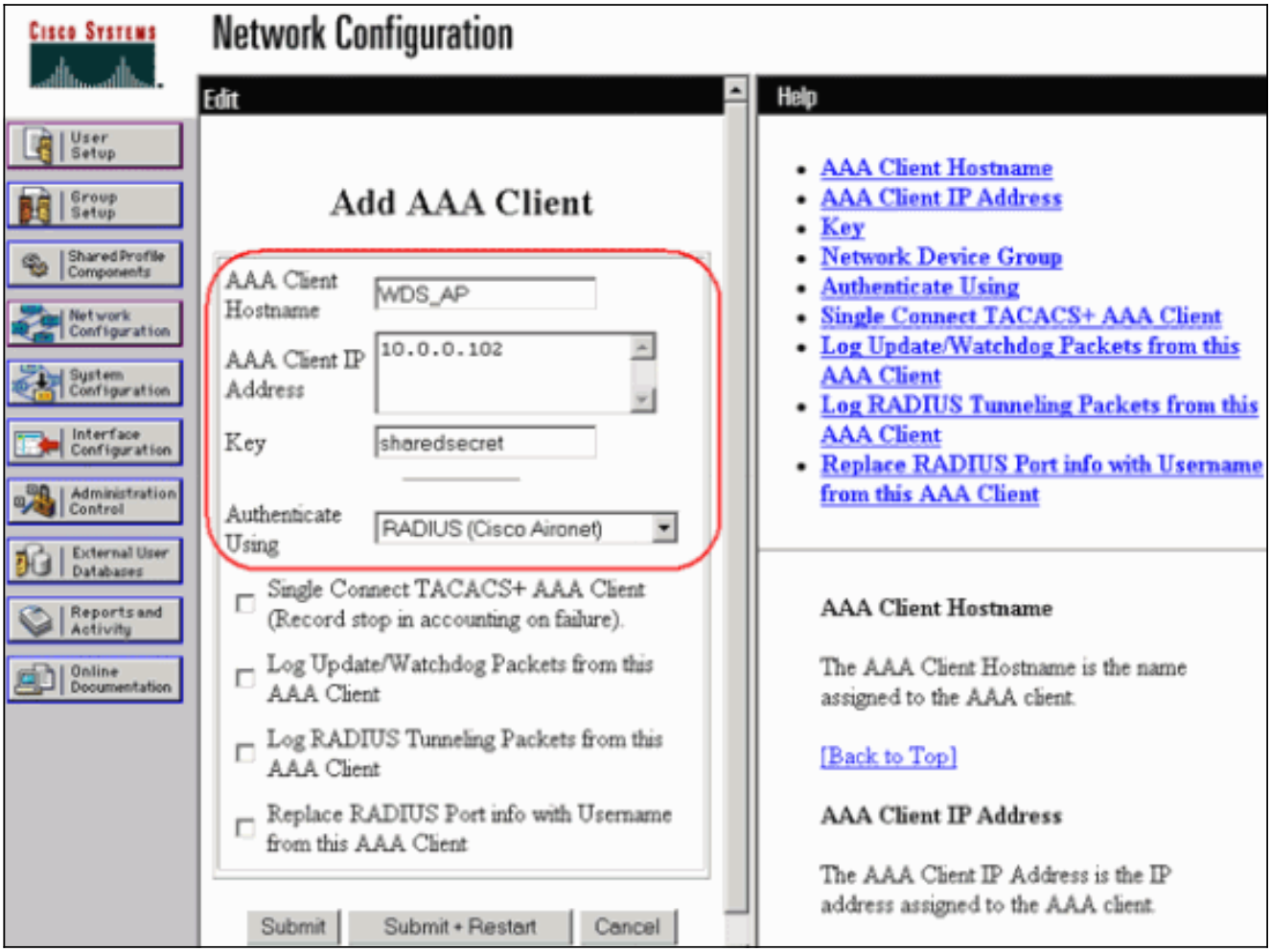
```
c6506#session slot x proc 1
!--- In this command, x is the slot number where the
WLSM resides. The default escape character is Ctrl-^,
then x. You can also type 'exit' at the remote prompt to
end the session Trying 127.0.0.51 ... Open User Access
Verification Username: <username> Password: <password>
wlan>enable
Password: <enable password>
wlan#
```

참고: WLSM의 문제를 더 쉽게 해결하고 유지 보수하려면 WLSM에 대한 텔넷 원격 액세스를 구성합니다. 텔넷 원격 액세스 구성을 참조하십시오.

WLSM을 WDS로 지정하려면

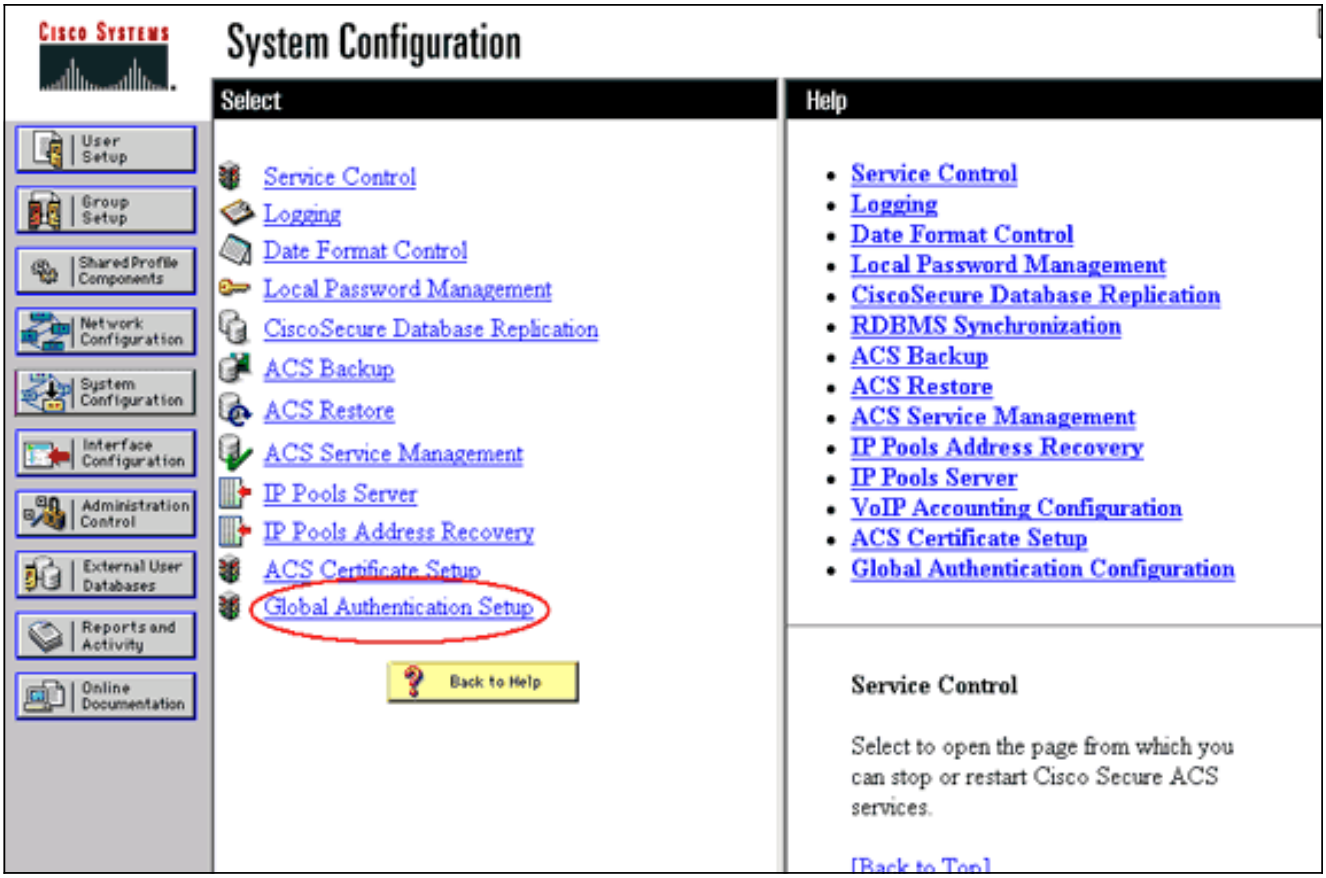
1. WLSM의 CLI에서 다음 명령을 실행하고 인증 서버와의 관계를 설정합니다.**참고:** WLSM에는 우선순위 제어가 없습니다. 네트워크에 여러 WLSM 모듈이 포함된 경우 WLSM은 이중화 컨피그레이션을 사용하여 기본 모듈을 결정합니다.
2. 인증 서버에서 WLSM을 AAA 클라이언트로 구성합니다.Cisco Secure ACS에서 WLSM에 대해 이러한 속성을 정의하는 네트워크 컨피그레이션 페이지에서 이가 발생합니다.이름IP 주소공유 암호인증 방법RADIUS Cisco AironetRADIUS IETFACS가 아닌 다른 인증 서버는 제조업체의 설명서를 참조하십시오

.



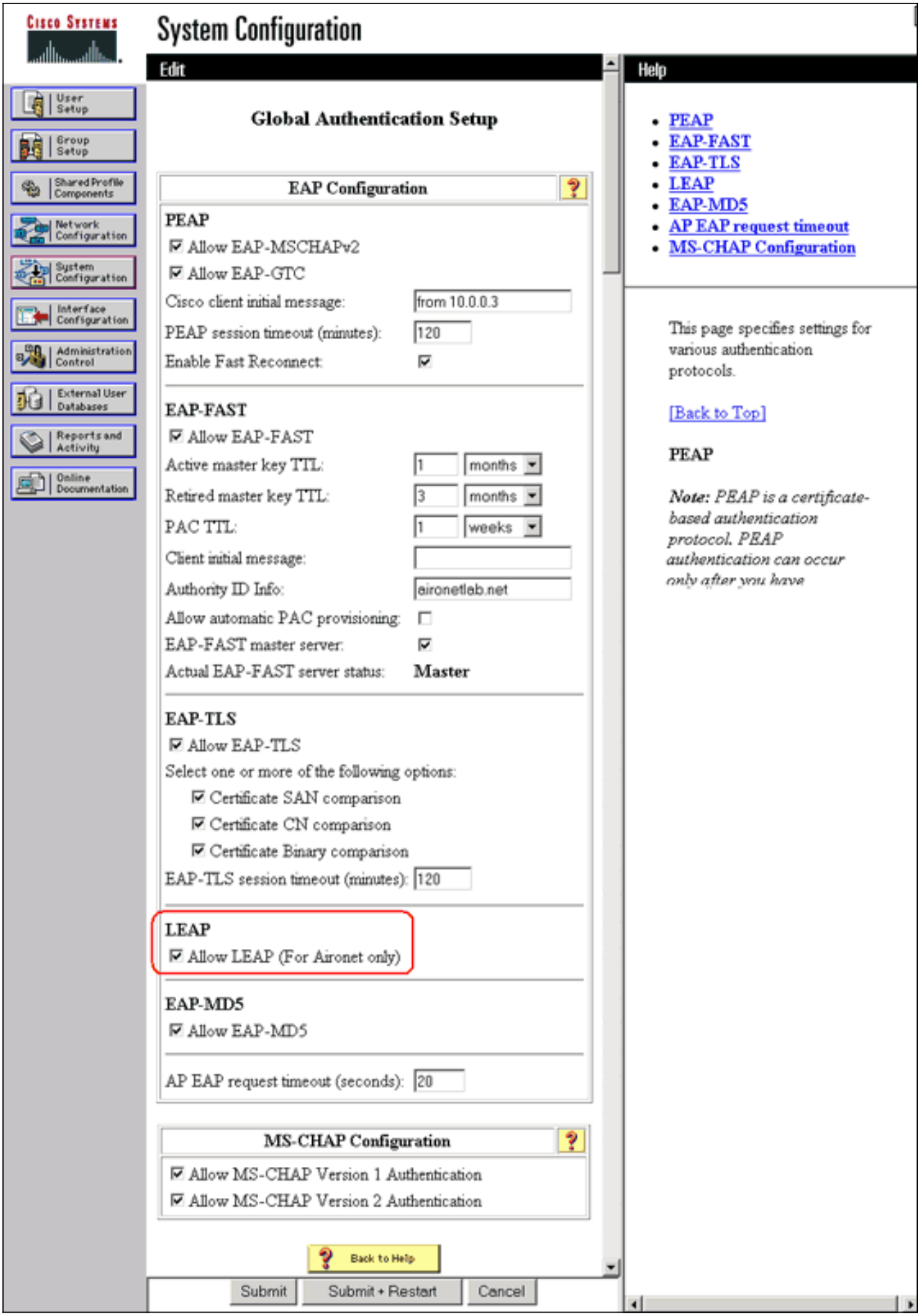
또한 Cisco Secure ACS에서 System Configuration - Global Authentication Setup 페이지에서 LEAP 인증을 수행하도록 ACS를 구성합니다. 먼저 **System Configuration(시스템 컨피그레이션)**을 클릭한 다음 **Global Authentication Setup(전역 인증 설정)을 클릭합니다**

.



페이지를 아래로 스크롤하여 LEAP 설정으로 이동합니다. 확인란을 선택하면 ACS에서 LEAP를 인증합니다

.



3. WLSM에서 다른 AP(인프라 서버 그룹)를 인증하는 방법을 정의합니다.
4. WLSM에서 클라이언트 장치(클라이언트 서버 그룹)를 인증하는 방법 및 클라이언트가 사용하는 EAP 유형을 정의합니다.**참고:** 이 단계에서는 클라이언트 인증 방법 정의 프로세스가 필요

하지 않습니다.

5. WLSM이 AP 및 인증 서버와 같은 외부 엔티티와 통신할 수 있도록 Supervisor Engine 720과 WLSM 간에 고유한 VLAN을 정의합니다. 이 VLAN은 다른 곳이나 네트워크의 다른 용도로 사용되지 않습니다. 먼저 Supervisor Engine 720에서 VLAN을 생성한 다음 다음 명령을 실행합니다.Supervisor Engine 720에서 다음을 수행합니다.WLSM에서 다음을 수행합니다.
6. 다음 명령을 사용하여 WLSM의 기능을 확인합니다.WLSM에서 다음을 수행합니다 .Supervisor Engine 720에서 다음을 수행합니다.

AP를 인프라 디바이스로 지정

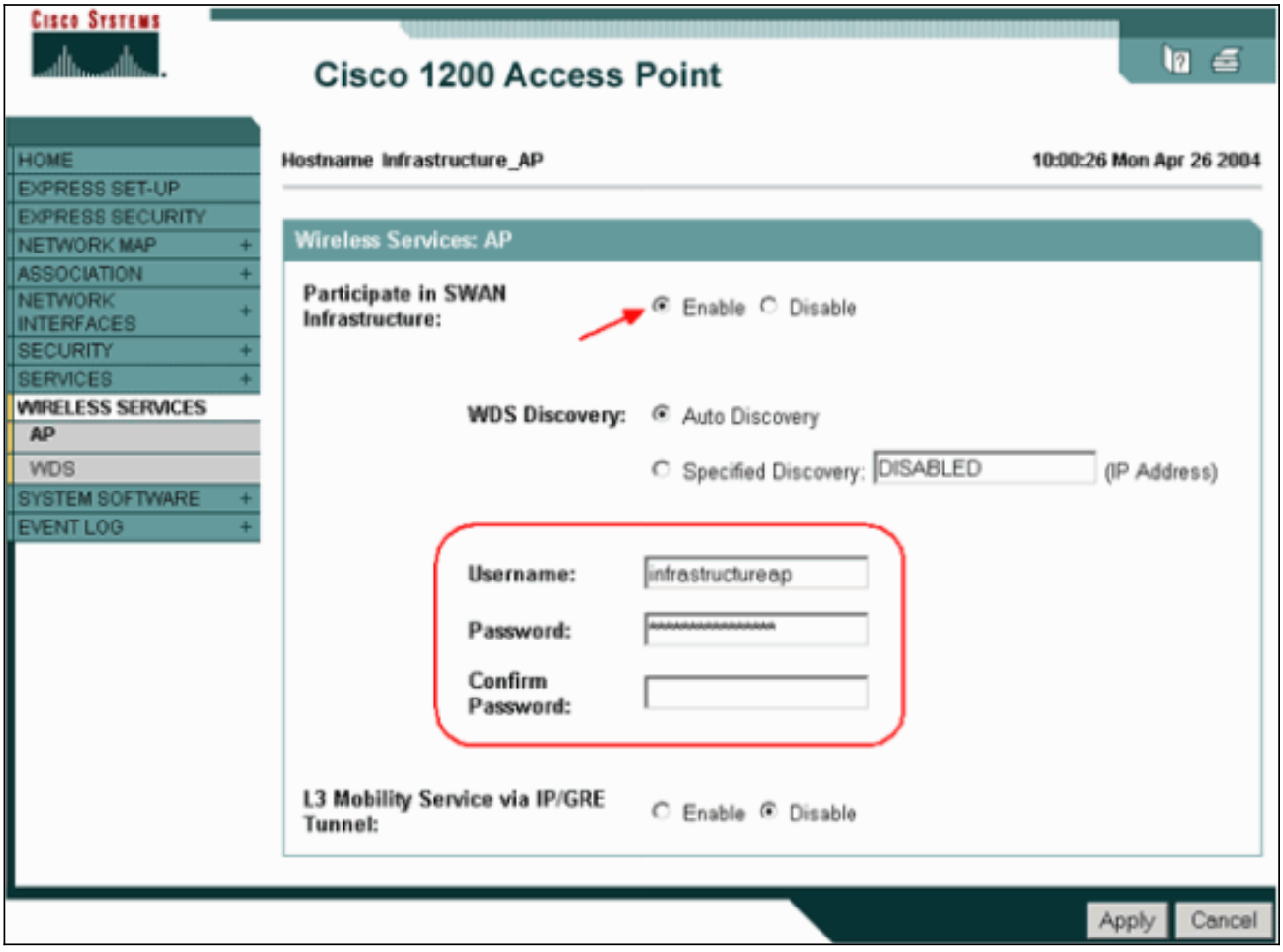
다음으로, 하나 이상의 인프라 AP를 지정하고 AP를 WDS에 연결해야 합니다. 클라이언트가 인프라 AP에 연결됩니다. 인프라 AP는 WDS AP 또는 WLSM에 인증을 수행하도록 요청합니다.

WDS의 서비스를 사용하는 인프라 AP를 추가하려면 다음 단계를 완료하십시오.

참고: 이 컨피그레이션은 WDS AP가 아니라 인프라 AP에만 적용됩니다.

1. 무선 **서비스 > AP를 선택합니다**. 인프라 AP에서 Enable for the **Wireless** Services(무선 서비스 옵션에 대해 활성화)를 선택합니다. 그런 다음 WDS 사용자 이름 및 비밀번호를 입력합니다.WDS의 멤버가 될 모든 디바이스에 대해 인증 서버에서 WDS 사용자 이름과 비밀번호를 정의해야 합니다

.

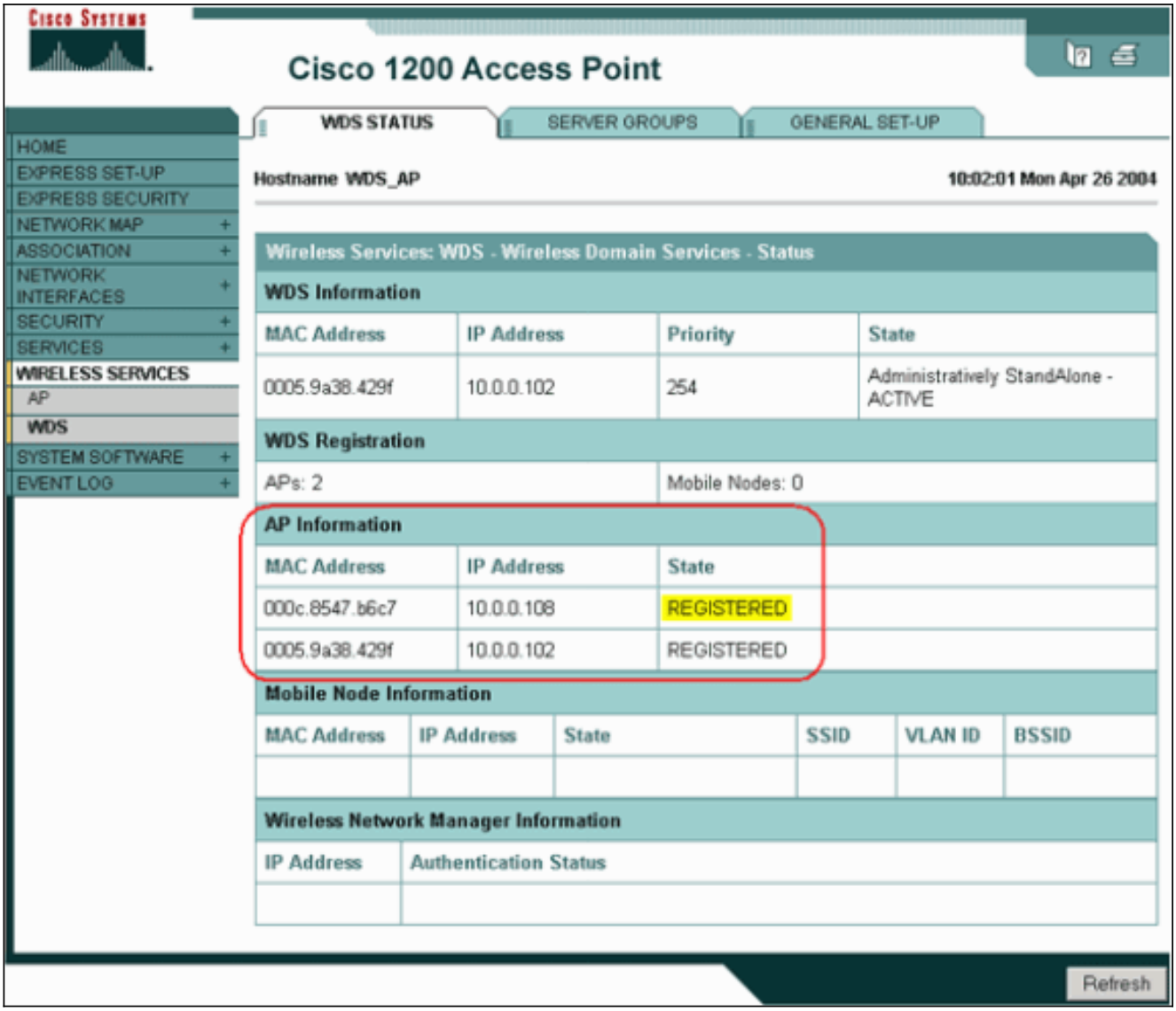


또는 CLI에서 다음 명령을 실행합니다.

2. 무선 **서비스 > WDS를 선택합니다**. WDS AP WDS Status(WDS WDS 상태) 탭에서 새 인프라 AP가 WDS Information(WDS 정보) 영역에 나타나고 State(상태)가 ACTIVE로, AP

Information(AP 정보) 영역에 State(상태)가 REGISTERED로 표시됩니다.AP가 ACTIVE 및/또는 REGISTERED로 나타나지 않으면 인증 서버에서 오류 또는 실패한 인증 시도를 확인합니다.AP가 ACTIVE 및/또는 REGISTERED로 나타나면 WDS에 클라이언트 인증 방법을 추가합니다

.



또는 CLI에서 다음 명령을 실행합니다.또는 WLSM에서 다음 명령을 실행합니다.그런 다음 인프라 AP에서 다음 명령을 실행합니다.**참고:** 클라이언트 인증에 아직 프로비전이 없으므로 클라이언트 연결을 테스트할 수 없습니다.

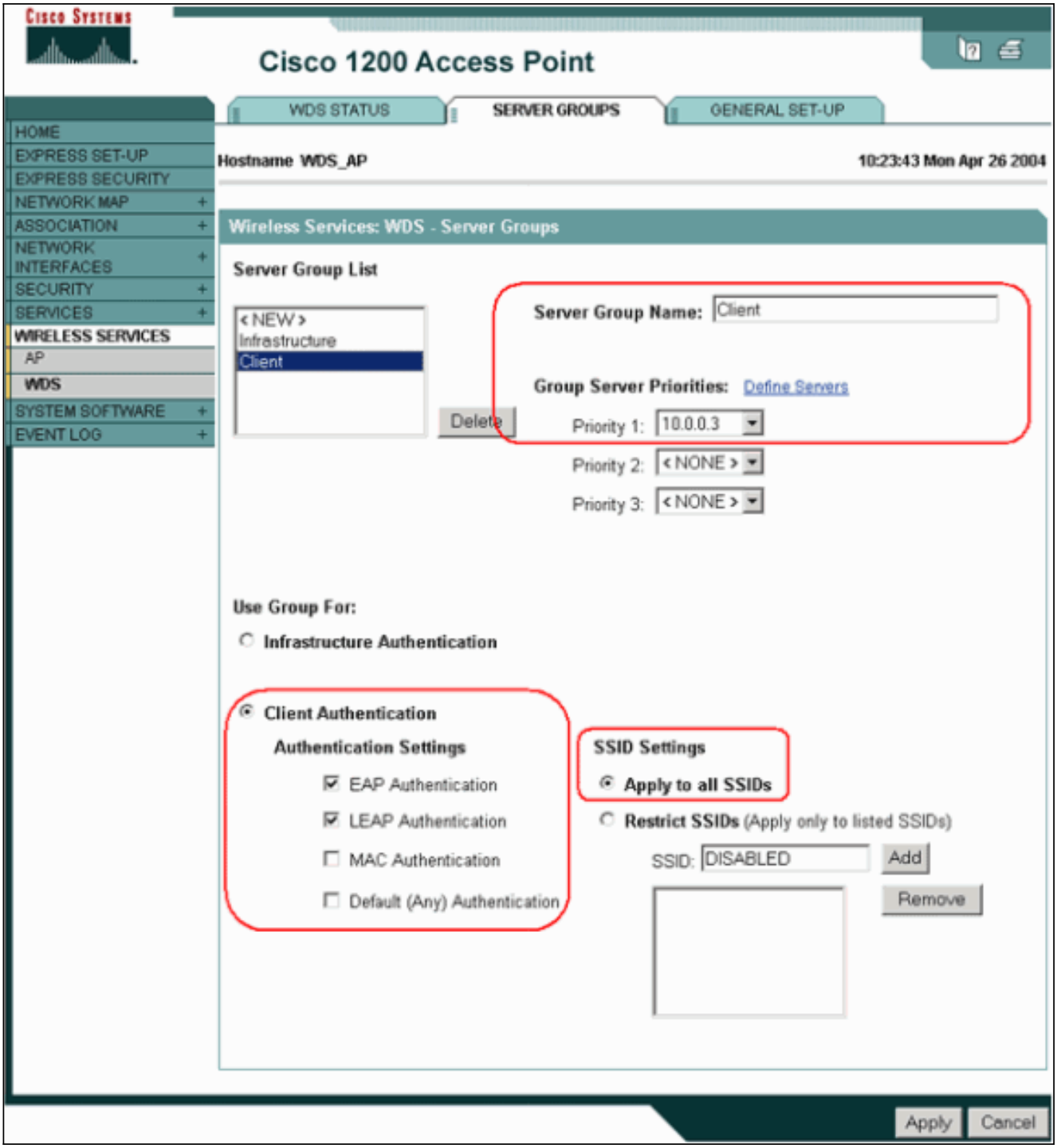
클라이언트 인증 방법 정의

마지막으로, 클라이언트 인증 방법을 정의합니다.

클라이언트 인증 방법을 추가하려면 다음 단계를 완료합니다.

1. 무선 **서비스 > WDS를 선택합니다**. WDS AP 서버 그룹 탭에서 다음 단계를 수행합니다.클라이언트를 인증하는 서버 그룹(클라이언트 그룹)을 정의합니다.Priority 1을 이전에 구성한 인증 서버로 설정합니다.적용 가능한 인증 유형(LEAP, EAP, MAC 등)을 설정합니다.관련 SSID에 설정을 적용합니다

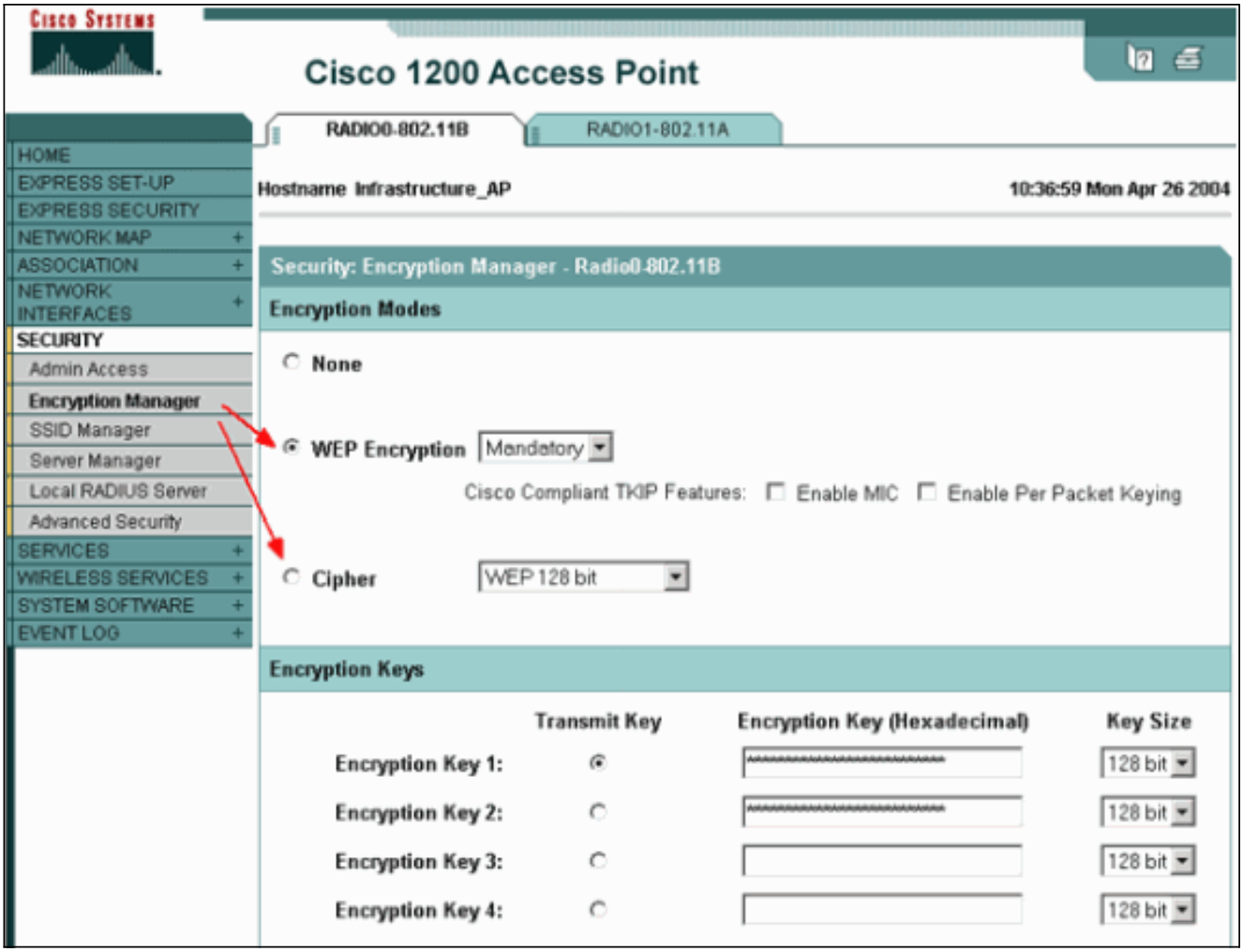
.



또는 CLI에서 다음 명령을 실행합니다.**참고:** WDS AP의 예는 전용이며 클라이언트 연결을 허용하지 않습니다.**참고:** 인프라 AP는 모든 요청을 처리할 WDS로 전달하므로 서버 그룹에 대해 인프라 AP에서 구성하지 마십시오.

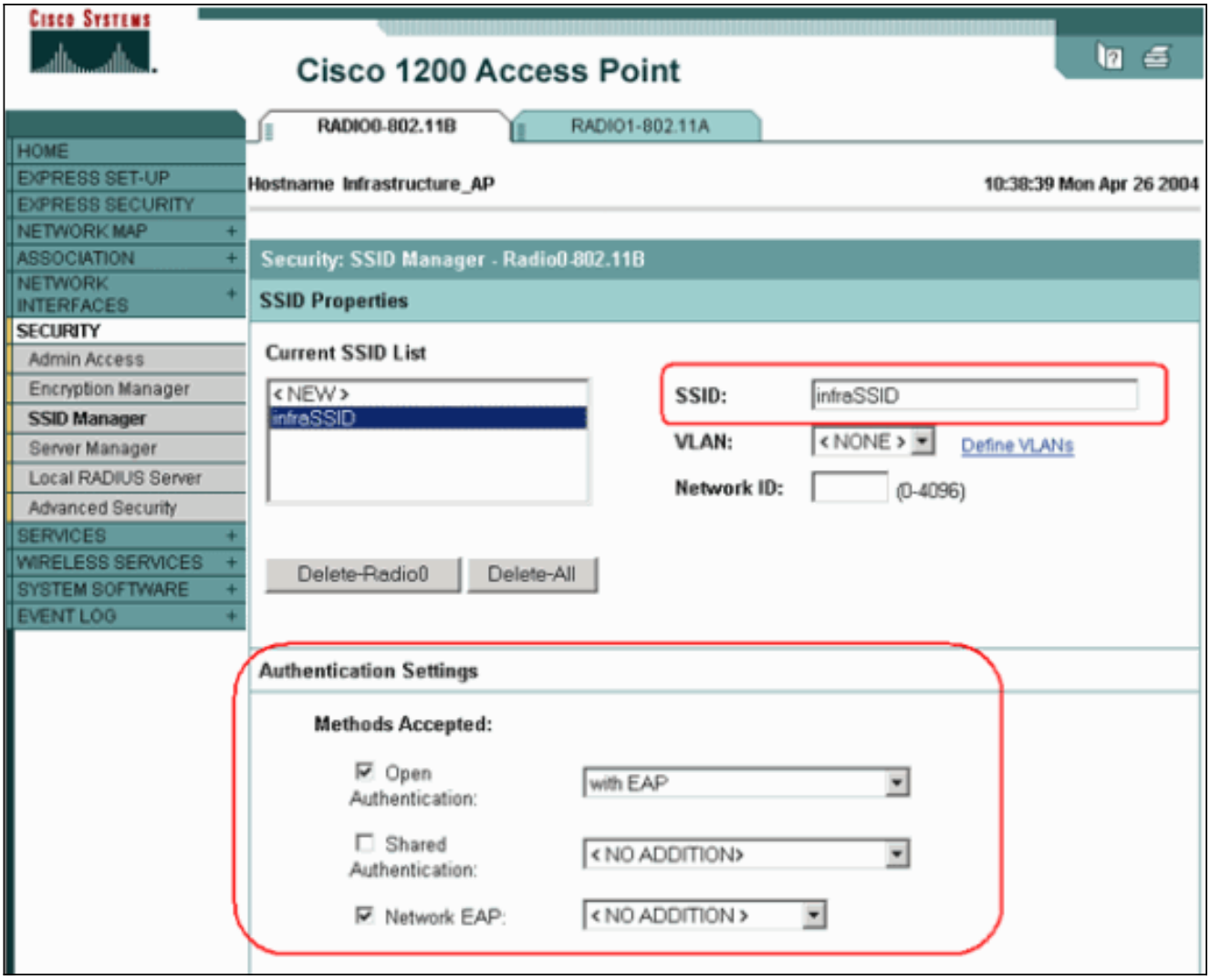
2. 인프라 AP 또는 AP에서 다음을 수행합니다.Security(**보안**) > Encryption Manager(**암호화 관리자**) 메뉴 항목에서 사용하는 인증 프로토콜에 필요한 **WEP Encryption**(**WEP 암호화**) 또는 **Cipher**(**암호**)를 클릭합니다

.



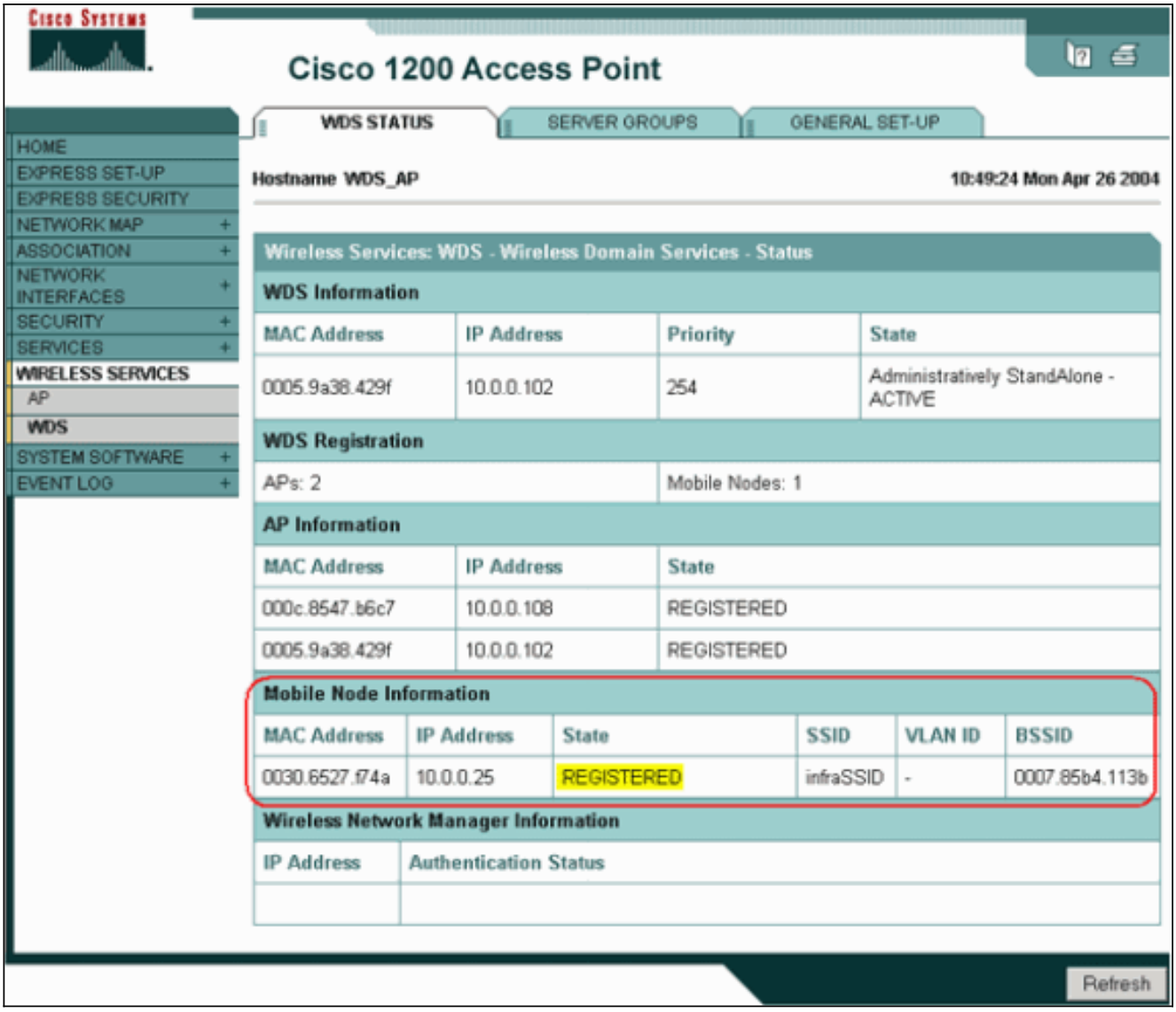
Security(**보안**) > **SSID Manager(SSID 관리자**) 메뉴 항목 아래에서 사용하는 인증 프로토콜에 필요한 인증 방법을 선택합니다

.



3. 이제 클라이언트가 인프라 AP에 인증되는지 여부를 성공적으로 테스트할 수 있습니다. WDS Status(WDS 상태) 탭(**Wireless Services(무선 서비스)** > WDS 메뉴 항목 아래)에 있는 WDS의 AP는 클라이언트가 Mobile Node Information(모바일 노드 정보) 영역에 나타나고 REGISTERED(등록됨) 상태가 있음을 나타냅니다.클라이언트가 나타나지 않으면 인증 서버에서 클라이언트에 의한 오류 또는 실패한 인증 시도를 확인합니다

.



또는 CLI에서 다음 명령을 실행합니다.**참고:** 인증을 디버깅해야 하는 경우 WDS AP는 인증 서버와 통신하는 디바이스이므로 WDS AP에서 디버깅해야 합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다. 이 목록에는 이러한 명령의 유용성을 더욱 명확하게 하기 위해 WDS 명령과 관련된 몇 가지 일반적인 질문이 나와 있습니다.

- **질문: WDS AP에서 이러한 항목에 권장되는 설정은 무엇입니까?radius-server 시간 초과radius 서버 데드 타임TKIP(Temporal Key Integrity Protocol) MIC(Message Integrity Check) 실패 전달 시간클라이언트 전달 시간EAP 또는 MAC 재인증 간격EAP 클라이언트 시간 초과(선택 사항)답변:** 이러한 특수 설정에 대한 기본 설정을 사용하여 컨피그레이션을 유지하고 타이밍 관련 문제가 있는 경우에만 사용하는 것이 좋습니다.다음은 WDS AP에 권장되는 설정입니다 .radius**-server timeout을 비활성화합니다**. AP가 요청을 재전송하기 전에 RADIUS 요청에 대한 응답을 기다리는 시간(초)입니다. 기본값은 5초입니다.radius**-server deadtime을 비활성화합니**

다. 모든 서버가 Dead(데드)로 표시되지 않는 한 이 기간 동안 추가 요청에 의해 RADIUS를 건너뜁니다.TKIP MIC 실패 전달 시간은 기본적으로 60초로 활성화됩니다. 전달 시간을 활성화할 경우 간격을 초 단위로 입력할 수 있습니다. AP가 60초 내에 두 개의 MIC 장애를 탐지하면 여기에 지정된 전달 기간 동안 해당 인터페이스의 모든 TKIP 클라이언트를 차단합니다.클라이언트 전달 시간은 기본적으로 비활성화되어야 합니다. Holdoff를 활성화한 경우 AP가 인증 실패 후 후속 인증 요청이 처리되기 전에 대기해야 하는 시간(초)을 입력합니다.EAP 또는 MAC 재인증 간격은 기본적으로 비활성화되어 있습니다. 재인증을 활성화할 경우 간격을 지정하거나 인증 서버에서 지정한 간격을 수락할 수 있습니다. 간격을 지정하도록 선택한 경우 인증된 클라이언트가 재인증되기 전에 AP가 대기하는 간격을 초 단위로 입력합니다.EAP 클라이언트 시간 초과(선택 사항)는 기본적으로 120초입니다. AP가 무선 클라이언트가 EAP 인증 요청에 응답할 때까지 대기해야 하는 시간을 입력합니다.

- **질문: TKIP 전달 시간에 대해서는 60초가 아니라 100ms로 설정해야 한다고 읽었습니다. 브라우저에서 1초로 설정된 것 같습니다. 1초가 가장 적게 선택할 수 있기 때문입니다.답변:** 100ms로 설정하는 구체적인 권장 사항은 없습니다. 단, 이 시간 동안 유일한 해결 방법이 증가하는 것으로 보고된 오류가 발생하지 않는 한 말입니다. 1초가 가장 낮은 설정입니다.
- **질문: 이 두 명령은 어떤 식으로든 클라이언트 인증에 도움이 됩니까? 그리고 WDS 또는 인프라 AP에서 클라이언트 인증이 필요합니까?radius-server 특성 6 on-for-login-authradius-server 특성 6 지원 다중답변:** 이러한 명령은 인증 프로세스에 도움이 되지 않으며 WDS 또는 AP에서 필요하지 않습니다.
- **질문: 인프라 AP에서는 AP가 WDS로부터 정보를 수신하므로 서버 관리자 및 전역 속성 설정이 필요하지 않다고 가정합니다. 인프라 AP에 이러한 특정 명령이 필요합니까?radius-server 특성 6 on-for-login-authradius-server 특성 6 지원 다중radius-server 시간 초과radius 서버 데드 타임 답변:** 인프라 AP에 대해 Server Manager와 Global Properties가 필요 없습니다. WDS에서 해당 작업을 처리하므로 다음 설정이 필요하지 않습니다.**radius-server 특성 6 on-for-login-authradius-server 특성 6 지원 다중radius-server 시간 초과radius 서버 데드 타임**radius-server **특성 32 include-in-access-req 형식 %h** 설정은 기본적으로 유지되며 필수 사항입니다.

AP는 레이어 2 디바이스입니다. 따라서 AP가 WDS 장치 역할을 하도록 구성된 경우 AP는 레이어 3 모빌리티를 지원하지 않습니다. WLSM을 WDS 디바이스로 구성하는 경우에만 레이어 3 모빌리티를 구현할 수 있습니다. Cisco Catalyst 6500 Series Wireless LAN Services Module의 Layer 3 Mobility Architecture 섹션을 참조하십시오. 자세한 내용은 백서

따라서 AP를 WDS 디바이스로 구성할 때 **mobility network-id** 명령을 사용하지 마십시오. 이 명령은 레이어 3 모빌리티에 적용되며 레이어 3 모빌리티를 올바르게 구성하려면 WLSM을 WDS 디바이스로 사용해야 합니다. **mobility network-id** 명령을 잘못 사용하면 다음 증상 중 일부를 볼 수 있습니다.

- 무선 클라이언트는 AP와 연결할 수 없습니다.
- 무선 클라이언트는 AP에 연결할 수 있지만 DHCP 서버에서 IP 주소를 수신하지 않습니다.
- VoWLAN(Voice over WLAN) 구축이 있을 경우 무선 전화가 인증되지 않습니다.
- EAP 인증이 발생하지 않습니다. **모빌리티 네트워크 ID**가 구성된 상태에서 AP는 EAP 패킷을 전달하기 위해 GRE(Generic Routing Encapsulation) 터널을 구축하려고 시도합니다. 터널이 설정되지 않은 경우 패킷은 어디로도 이동하지 않습니다.
- WDS 디바이스로 구성된 AP는 예상대로 작동하지 않으며 WDS 컨피그레이션이 작동하지 않습니다.**참고:** Cisco Aironet 1300 AP/Bridge는 WDS 마스터로 구성할 수 없습니다. 1300 AP/브리지는 이 기능을 지원하지 않습니다. 1300 AP/Bridge는 다른 AP 또는 WLSM을 WDS 마스터로 구성하는 인프라 디바이스로서 WDS 네트워크에 참여할 수 있습니다.

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 dot11 aaa authenticator all** - 클라이언트가 802.1x 또는 EAP 프로세스를 통해 연결 및 인증하면서 통과하는 다양한 협상을 표시합니다. 이 디버그는 Cisco IOS Software 릴리스 12.2(15)JA에서 도입되었습니다. 이 명령은 **디버그 dot11 aaa dot1x**를 해당 및 이후 릴리스에서 모두 사용하지 않습니다.
- **debug aaa authentication** - 일반 AAA 관점에서 인증 프로세스를 표시합니다.
- **debug wlccp ap** - AP가 WDS에 조인하는 경우 관련된 WLCCP 협상을 표시합니다.
- **debug wlccp packet** - WLCCP 협상에 대한 자세한 정보를 표시합니다.
- **debug wlccp leap-client**—인프라 디바이스가 WDS에 조인할 때 세부 정보를 표시합니다.

관련 정보

- WDS, Fast Secure Roaming 및 무선 관리 구성
- Catalyst 6500 Series Wireless LAN Services Module 컨피그레이션 참고
- 암호 그룹 및 WEP 구성
- 인증 유형 구성
- 무선 LAN 지원 페이지
- 기술 지원 및 문서 – Cisco Systems