EAP-FAST 인증을 사용하는 Cisco Secure Services Client

목차

소개

이 문서에서는 Cisco CSSC(Secure Services Client)를 무선 LAN 컨트롤러, Microsoft Windows 200® 소프트웨어 및 EAP-FAST를 통한 Cisco ACS(Secure Access Control Server) 4.0으로 구성하는 방법에 대해 설명합니다.이 문서에서는 EAP-FAST 아키텍처를 소개하고 구축 및 구성 예를 제공합니다.CSSC는 네트워크에 사용자를 인증하고 적절한 액세스를 할당하기 위해 인프라에 사용자 자격 증명 통신을 제공하는 클라이언트 소프트웨어 구성 요소입니다.

다음은 이 문서에서 설명한 CSSC 솔루션의 몇 가지 장점입니다.

- EAP(Extensible Authentication Protocol)를 사용하여 WLAN/LAN에 대한 액세스 권한에 앞서 각 사용자(또는 디바이스)의 인증

- 서버, 인증자 및 클라이언트 구성 요소가 포함된 엔드 투 엔드 WLAN 보안 솔루션
- 유무선 인증을 위한 공통 솔루션
- 동적, 인증 프로세스에서 파생된 사용자별 암호화 키
- PKI(Public Key Infrastructure) 또는 인증서에 대한 요구 사항 없음(인증서 확인 옵션)
- 액세스 정책 할당 및/또는 NAC 지원 EAP 프레임워크

참고: 보안 무선 구축에 대한 자세한 내용은 Cisco SAFE 무선 청사진을 참조하십시오.

802.1x 인증 프레임워크는 802.11i(Wireless LAN Security) 표준의 일부로 통합되어 802.11 무선 LAN 네트워크에서 레이어 2 기반 인증, 권한 부여 및 어카운팅 기능을 지원합니다.현재 유무선 네트워크 모두에서 구축할 수 있는 여러 EAP 프로토콜이 있습니다.일반적으로 구축된 EAP 프로토콜에는 LEAP, PEAP 및 EAP-TLS가 포함됩니다.이러한 프로토콜 외에도 Cisco는 유무선 LAN 네트워크 모두에서 구축을 위해 사용 가능한 표준 기반 EAP 프로토콜로서 EAP-FAST(Secure Tunnel)를 통한 EAP Flexible Authentication을 정의 및 구현했습니다.EAP-FAST 프로토콜 사양은 IETF 웹 사이트에서 공개적으로 사용 가능합니다 .

다른 EAP 프로토콜과 마찬가지로 EAP-FAST는 TLS 터널 내에서 EAP 트랜잭션을 암호화하는 클라이언트 서버 보안 아키텍처입니다.이 점에서 PEAP 또는 EAP-TTLS와 유사하지만, EAP-FAST 터널 설정은 인증 세션을 보호하기 위해 서버 X.509 인증서를 사용하는 PEAP/EAP-TTLS와 각 사용자에게 고유한 강력한 공유 비밀 키를 기반으로 한다는 점에서 다릅니다. 이러한 공유 암호 키는 PAC(Protected Access Credentials)라고 하며 클라이언트 디바이스에 자동으로(Automatic 또는 In-band Provisioning) 또는 수동으로(Manual 또는 Out-of-band Provisioning) 배포할 수 있습니다.공유 비밀을 기반으로 한 악수는 PKI 인프라를 기반으로 하는 핸드셰이크보다 더 효율적이기 때문에 EAP-FAST는 보호된 인증 교환을 제공하는 EAP 중 가장 빠르고 덜 프로세서 집약적인 유형입니다 .EAP-FAST는 무선 LAN 클라이언트 또는 RADIUS 인프라에 인증서가 필요 없지만 내장 프로비저닝 메커니즘이 포함되어 있으므로 간단하게 배포할 수 있도록 설계되었습니다.

다음은 EAP-FAST 프로토콜의 주요 기능 중 일부입니다.

- Windows 사용자 이름/암호를 사용하는 SSO(Single Sign-On)
- 로그인 스크립트 실행 지원
- 서드파티 신청자가 없는 WPA(Wi-Fi Protected Access) 지원(Windows 2000 및 XP에만 해당)
- PKI 인프라를 필요로 하지 않는 간단한 구축
- Windows 암호 에이징(서버 기반 암호 만료 지원)
- Cisco Trust Agent for Network Admission Control과 적절한 클라이언트 소프트웨어 통합

사전 요구 사항

요구 사항

이 문서에서는 테스트를 용이하게 하기 위해 특정 구성만 다루므로 설치 관리자가 기본 Windows 2003 설치 및 Cisco WLC 설치에 대해 알고 있다고 가정합니다.

Cisco 4400 Series 컨트롤러의 초기 설치 및 구성 정보는 빠른 시작 가이드를 참조하십시오.Cisco 4400 Series Wireless LAN Controller.Cisco 2000 Series 컨트롤러의 초기 설치 및 구성 정보는 빠른 시작 가이드를 참조하십시오.Cisco 2000 Series Wireless LAN Controller.

시작하기 전에 최신 서비스 팩 소프트웨어와 함께 Microsoft Windows Server 2000을 설치하십시오 .컨트롤러 및 LAP(Lightweight Access Point)를 설치하고 최신 소프트웨어 업데이트가 구성되어 있는지 확인합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 4.0.155.5을 실행하는 Cisco 2006 또는 4400 Series 컨트롤러
- Cisco 1242 LWAPP AP
- Windows 2000(Active Directory 포함)
- Cisco Catalyst 3750G Switch
- Windows XP with CB21AG Adapter Card and Cisco Secure Services Client Version 4.05

표기 규칙

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

설계 매개변수

데이터베이스

WLAN 네트워크를 구축하고 인증 프로토콜을 찾는 경우 일반적으로 사용자/머신 인증에 현재 데이터베이스를 사용하는 것이 좋습니다.Windows Active Directory, LDAP 또는 OTP(One Time Password) 데이터베이스(즉, RSA 또는 SecureID)를 사용할 수 있는 일반적인 데이터베이스입니다. 이러한 모든 데이터베이스는 EAP-FAST 프로토콜과 호환되지만, 구축을 계획할 때 고려해야 하는 일부 호환성 요구 사항이 있습니다.클라이언트에 대한 PAC 파일의 초기 구축은 익명 자동 프로비저닝, 인증된 프로비저닝(현재 클라이언트 X.509 인증서를 통해) 또는 수동 프로비저닝을 통해 수행됩니다.이 문서에서는 익명 자동 프로비저닝 및 수동 프로비저닝이 고려됩니다.

자동 PAC 프로비저닝에서는 ADHP(Authenticated Diffie-Hellman Key Agreement Protocol)를 사용하여 보안 터널을 설정합니다.보안 터널은 익명으로 또는 서버 인증 메커니즘을 통해 설정할 수 있습니다.설정된 터널 연결 내에서 MS-CHAPv2를 사용하여 클라이언트를 인증하고 인증에 성공하면 PAC 파일을 클라이언트에 배포합니다.PAC가 성공적으로 프로비저닝되면 PAC 파일을 사용하여 보안 네트워크 액세스를 얻기 위해 새 EAP-FAST 인증 세션을 시작할 수 있습니다.

자동 PAC 프로비저닝은 사용 중인 데이터베이스와 관련이 있습니다. 자동 프로비저닝 메커니즘은 MSCHAPv2를 사용하므로 사용자를 인증하는 데 사용되는 데이터베이스는 이 비밀번호 형식과 호환되어야 합니다.MSCHAPv2 형식(예: OTP, Novell 또는 LDAP)을 지원하지 않는 데이터베이스와 함께 EAP-FAST를 사용하는 경우 사용자 PAC 파일을 배포하기 위해 일부 다른 메커니즘(수동 프로비저닝 또는 인증된 프로비저닝)을 사용해야 합니다.이 문서에서는 Windows 사용자 데이터베이스를 사용하여 자동 프로비저닝을 보여 줍니다.

암호화

EAP-FAST 인증에서는 특정 WLAN 암호화 유형을 사용할 필요가 없습니다.사용할 WLAN 암호화 유형은 클라이언트 NIC 카드 기능에 의해 결정됩니다.특정 구축의 NIC 카드 기능에 따라 WPA2(AES-CCM) 또는 WPA(TKIP) 암호화를 사용하는 것이 좋습니다.Cisco WLAN 솔루션을 사용하면 공통 SSID에서 WPA2 및 WPA 클라이언트 장치를 모두 사용할 수 있습니다.

클라이언트 장치가 WPA2 또는 WPA를 지원하지 않는 경우 동적 WEP 키를 사용하여 802.1X 인증을 배포할 수 있지만 WEP 키에 대해 잘 알려진 익스플로잇 때문에 이 WLAN 암호화 메커니즘은 권장되지 않습니다.WEP 전용 클라이언트를 지원하는 데 필요한 경우 세션 시간 초과 간격을 사용하는 것이 좋습니다. 이 경우 클라이언트가 자주 사용하는 간격으로 새 WEP 키를 파생시켜야 합니다

.일반적인 WLAN 데이터 전송률에 권장되는 세션 간격은 30분입니다.

Single Sign-on 및 머신 자격 증명

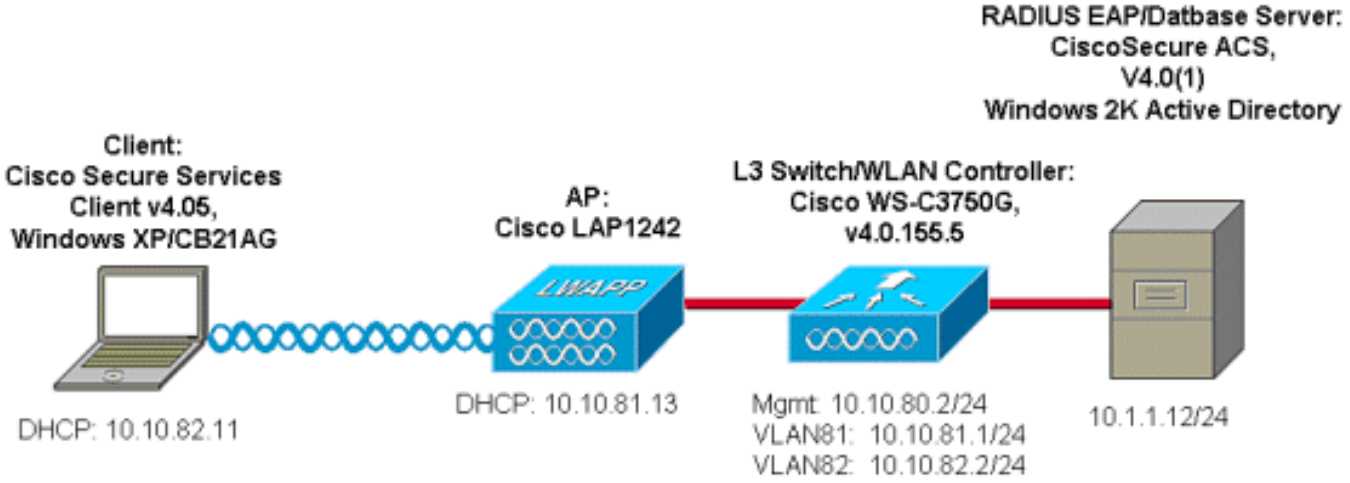
Single Sign-On은 단일 사용자 로그인 또는 여러 애플리케이션 또는 여러 디바이스에 액세스하는 데 사용할 인증 자격 증명 항목의 기능을 의미합니다.이 문서에서 Single Sign-On은 WLAN에 대한 인증을 위해 PC에 로그온하는 데 사용되는 자격 증명을 사용하는 것을 의미합니다.

Cisco Secure Services Client를 사용하면 사용자의 로그온 자격 증명을 사용하여 WLAN 네트워크도 인증할 수 있습니다.사용자가 PC에 로그온하기 전에 네트워크에 PC를 인증하려면 저장된 사용자 자격 증명 또는 컴퓨터 프로필에 연결된 자격 증명을 사용해야 합니다.이러한 방법 중 하나는 사용자가 로그온하는 경우와 달리 PC가 부팅될 때 로그온 스크립트를 실행하거나 드라이브를 매핑하려는 경우에 유용합니다.

네트워크 다이어그램

이 문서에 사용된 네트워크 다이어그램입니다.이 네트워크에는 4개의 서브넷이 사용됩니다.이러한 디바이스를 다른 네트워크로 분할할 필요는 없지만, 이 경우 실제 네트워크와 가장 유연하게 통합할 수 있습니다.Catalyst 3750G Integrated Wireless LAN Controller는 공통 섀시에 POE(Power Over Ethernet) 스위치 포트, L3 스위칭 및 WLAN 컨트롤러 기능을 제공합니다.

1. 네트워크 10.1.1.0은 ACS가 상주하는 서버 네트워크입니다.
2. 네트워크 10.10.80.0은 WLAN 컨트롤러에서 사용하는 관리 네트워크입니다.
3. 네트워크 10.10.81.0은 AP가 상주하는 네트워크입니다.
4. 네트워크 10.10.82.0은 WLAN 클라이언트에 사용됩니다.



ACS(Access Control Server) 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

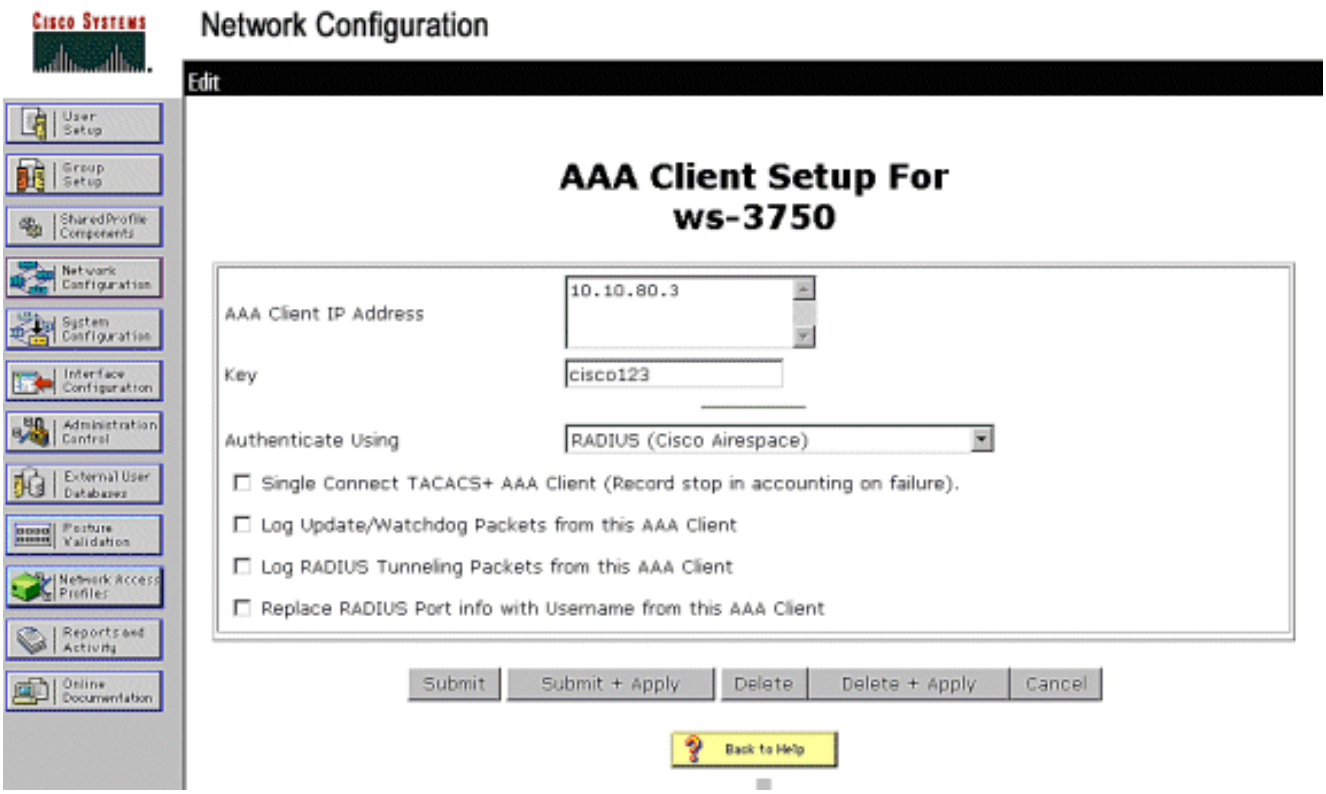
참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

ACS에서 AAA-Client(NAS)로 액세스 포인트 추가

이 섹션에서는 Windows Active Directory를 사용하여 대역 내 PAC 프로비저닝을 외부 데이터베이스로 사용하여 EAP-FAST용 ACS를 구성하는 방법에 대해 설명합니다.

1. ACS > **Network Configuration(네트워크 컨피그레이션)에 로그온하고 Add Entry(항목 추가)를** 클릭합니다.
2. WLAN Controller name(WLAN 컨트롤러 이름), IP address(IP 주소), shared secret key(공유 비밀 키)를 입력하고 Authenticate Using(인증 사용)에서 RADIUS(Cisco Airespace)를 선택합니다. 여기에는 RADIUS IETF 속성도 포함됩니다.**참고:** NDG(Network Device Groups)가 활성화된 경우 먼저 적절한 NDG를 선택하고 WLAN 컨트롤러를 추가합니다.NDG에 대한 자세한 내용은 ACS 컨피그레이션 가이드를 참조하십시오.
3. Submit **+ Restart를 클릭합니다**

.

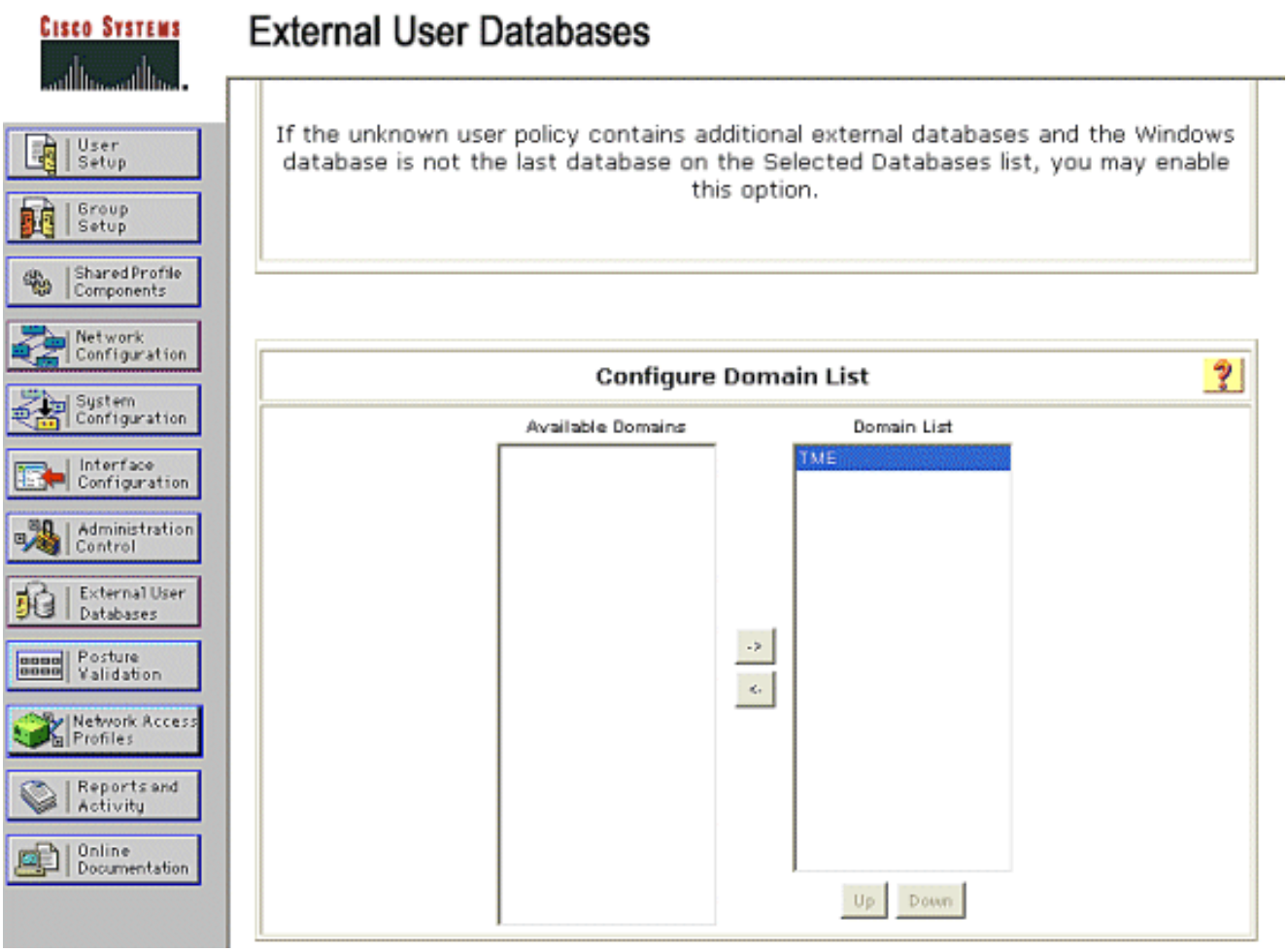


외부 데이터베이스를 쿼리하기 위해 ACS 구성

이 섹션에서는 외부 데이터베이스를 쿼리하기 위해 ACS를 구성하는 방법에 대해 설명합니다.

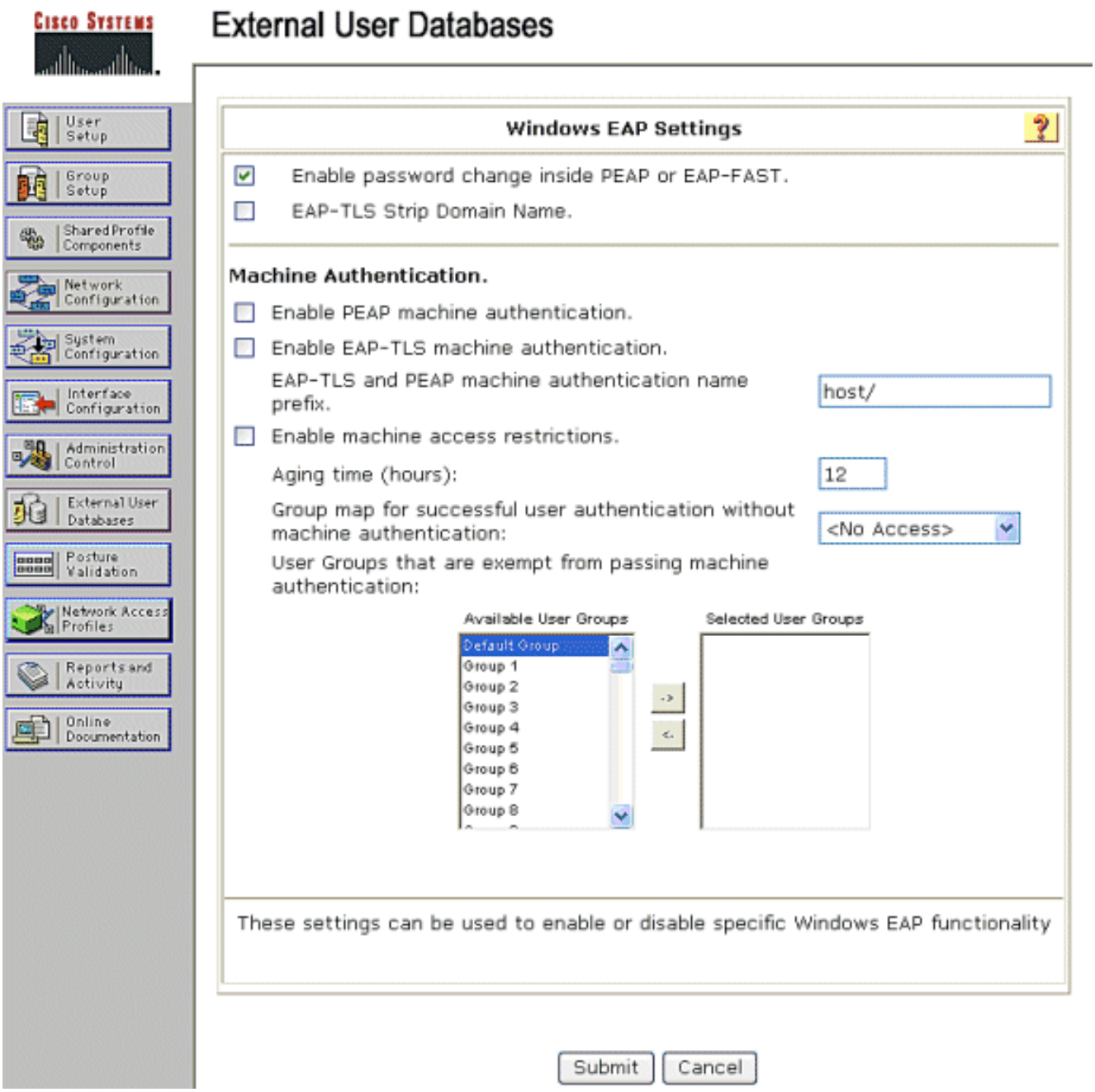
1. 외부 **사용자 데이터베이스 > 데이터베이스 구성 > Windows 데이터베이스 > 구성을 클릭합니다**.
2. Configure Domain List(도메인 목록 구성)에서 **Domains**(사용 가능한 도메인)를 Available Domains(도메인 목록)로 이동합니다.**참고:** ACS 응용 프로그램이 인증을 위해 이러한 도메인을 탐지하고 사용하려면 ACS를 실행하는 서버가 이러한 도메인에 대한 지식을 가지고 있어야 합니다

.



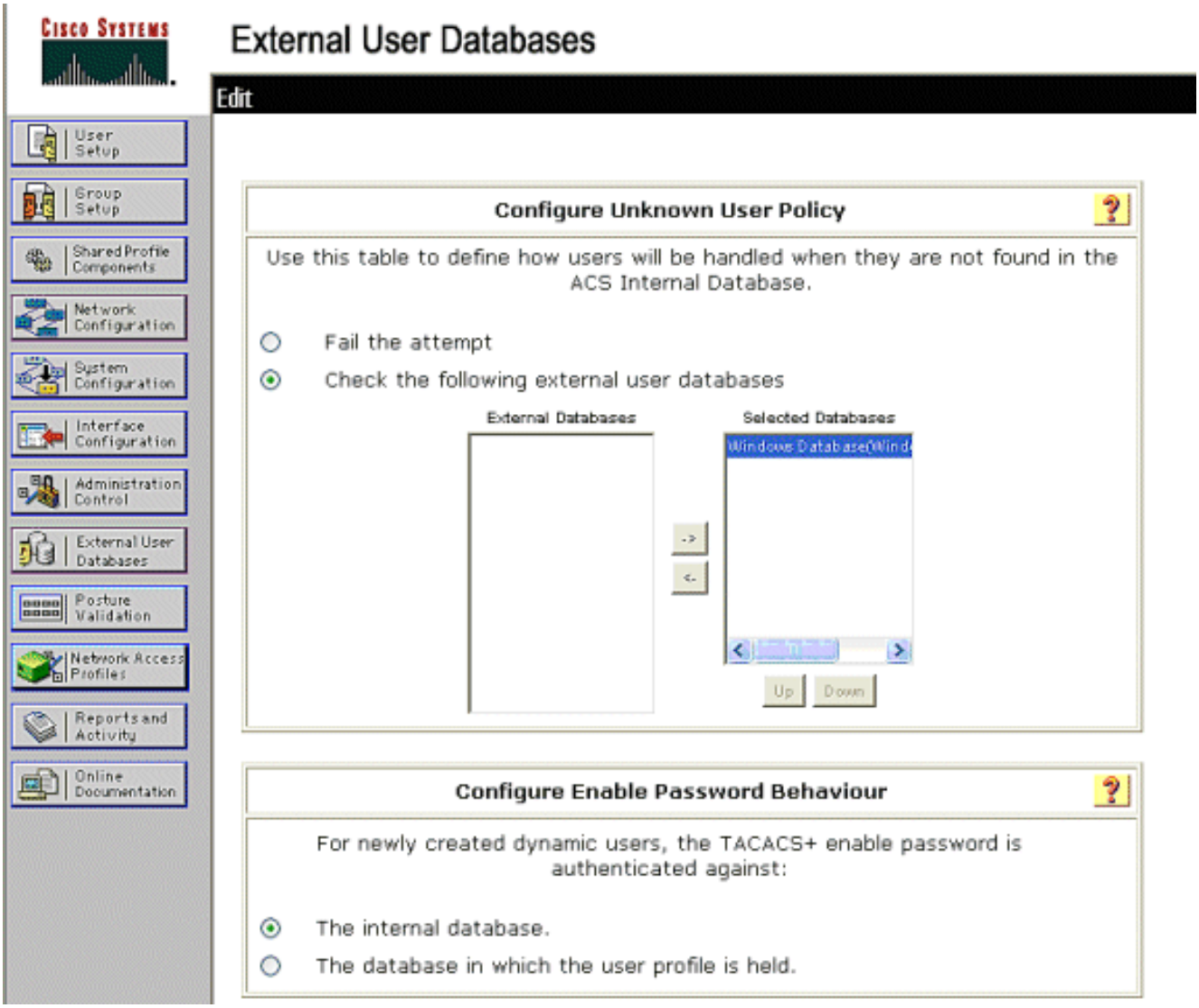
3. Windows EAP 설정에서 PEAP 또는 EAP-FAST 세션 내에서 비밀번호 변경을 허용하도록 옵션을 구성합니다.EAP-FAST 및 Windows 비밀번호 에이징에 대한 자세한 내용은 Cisco Secure ACS 4.1용 컨피그레이션 가이드를 참조하십시오.
4. Submit(제출)**을 클릭합니다.참고:** Windows 외부 데이터베이스에서 액세스 권한을 제어하도록 Windows 사용자 데이터베이스 구성에서 EAP-FAST에 대한 전화 접속 권한 기능을 활성화할 수도 있습니다.Windows 데이터베이스 컨피그레이션 페이지에서 암호 변경에 대한 MS-CHAP 설정은 비 EAP MS-CHAP 인증에만 적용됩니다.EAP-FAST와 함께 비밀번호 변경을 활성화하려면 Windows EAP 설정에서 비밀번호 변경을 활성화해야 합니다

.



5. External **User Database(외부 사용자 데이터베이스) > Unknown User Policy(알 수 없는 사용자 정책)**를 클릭하고 **Check the following external user databases(다음 외부 사용자 데이터베이스 확인)** 라디오 버튼을 선택합니다.
6. Windows 데이터베이스를 외부 데이터베이스에서 **선택한 데이터베이스**로 **이동합니다**.
7. Submit(제출)**을 클릭합니다.참고:** 이 시점부터 ACS는 Windows DB를 확인합니다.ACS 로컬 데이터베이스에서 사용자를 찾을 수 없으면 ACS 기본 그룹에 사용자를 배치합니다.데이터베이스 그룹 매핑에 대한 자세한 내용은 ACS 설명서를 참조하십시오.**참고:** ACS는 Microsoft Active Directory 데이터베이스를 쿼리하여 사용자 자격 증명을 확인하므로 Windows에서 추가 액세스 권한 설정을 구성해야 합니다.자세한 내용은 Cisco Secure ACS for Windows Server 설치 설명서를 참조하십시오

.



ACS에서 EAP-FAST 지원 활성화

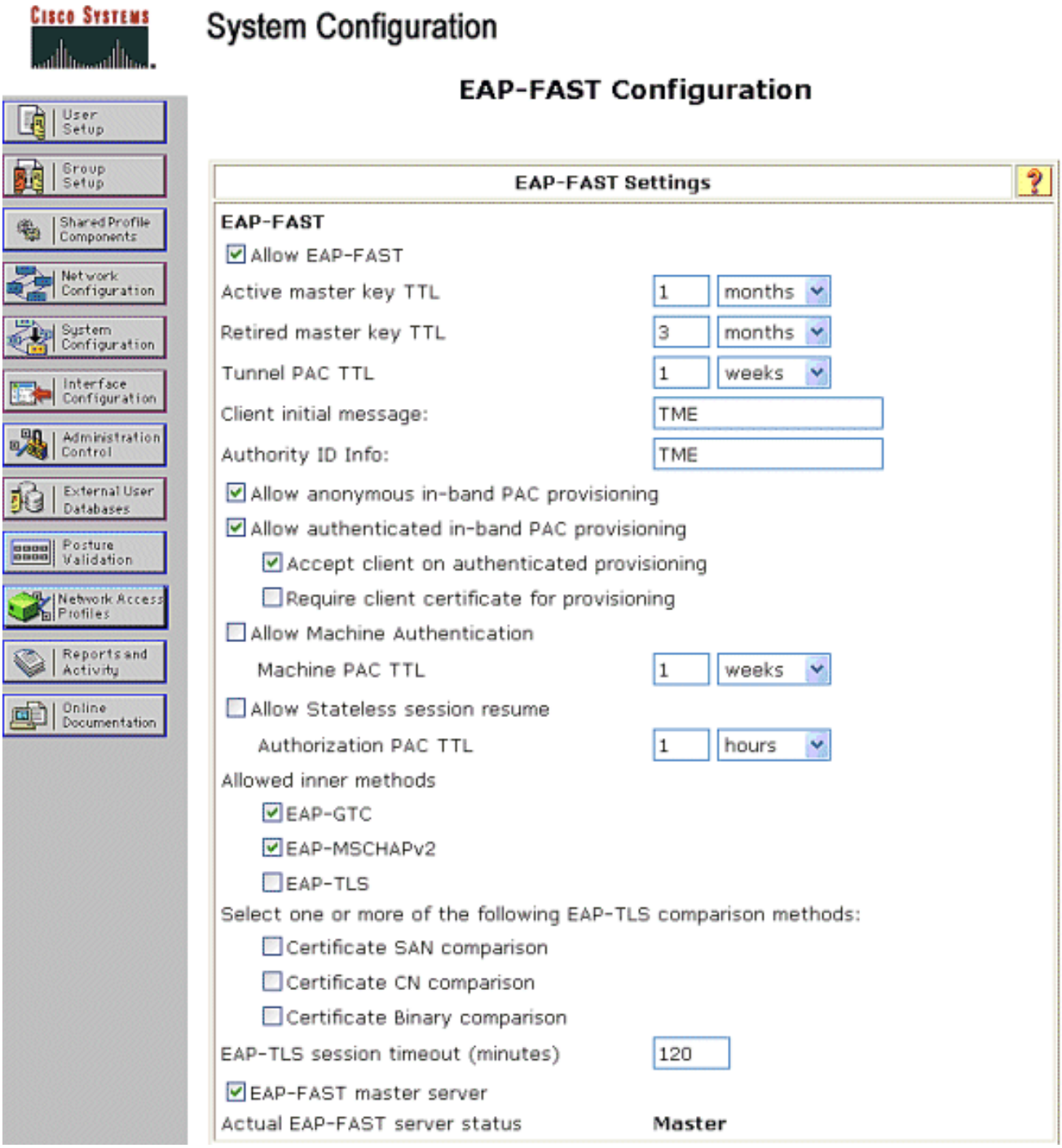
이 섹션에서는 ACS에서 EAP-FAST 지원을 활성화하는 방법에 대해 설명합니다.

1. System Configuration(**시스템 컨피그레이션) > Global Authentication Setup(전역 인증 설정) > EAP-FAST Configuration(EAP-FAST 컨피그레이션)으로 이동합니다**.
2. Allow **EAP-FAST(EAP-FAST 허용)를 선택합니다**.
3. 다음 권장 사항을 구성합니다.마스터 키 TTL/폐기된 마스터 키 TTL/PAC TTL.이러한 설정은 Cisco Secure ACS에서 기본적으로 구성됩니다.마스터 키 TTL:1개월폐기 키 TTL:3개월PAC TTL:1주
4. Authority **ID Info** 필드**를** 입력합니다.이 텍스트는 PAC Authority의 선택이 컨트롤러인 일부 EAP-FAST 클라이언트 소프트웨어에 표시됩니다.**참고:** Cisco Secure Services Client는 PAC 기관에 대해 이 설명 텍스트를 사용하지 않습니다.
5. Allow in-band **PAC provisioning(대역 내 PAC 프로비저닝 허용)** 필드를 선택합니다.이 필드는 올바르게 활성화된 EAP-FAST 클라이언트에 대해 자동 PAC 프로비저닝을 활성화합니다.이 예에서는 자동 프로비저닝이 사용됩니다.
6. 허용된 **내부 방법을 선택합니다**.EAP-GTC 및 EAP-MSCHAP2. EAP-FAST v1 및 EAP-FAST v1a 클라이언트의 작동을 허용합니다.(Cisco Secure Services Client는 EAP-FAST v1a를 지원합니다.) EAP-FAST v1 클라이언트를 지원할 필요가 없는 경우, EAP-MSCHAPv2를 내부 방법으로 활성화해야 합니다.
7. EAP-**FAST 마스터 서버** 확인란을 선택하여 이 EAP-FAST 서버를 마스터로 활성화합니다.이

렇게 하면 다른 ACS 서버가 이 서버를 마스터 PAC 기관으로 활용하여 네트워크의 각 ACS에 대한 고유 키 제공을 방지할 수 있습니다.자세한 내용은 ACS 컨피그레이션 가이드를 참조하십시오.

8. Submit **+Restart를 클릭합니다**

.



Cisco WLAN 컨트롤러

이 구축 가이드에서 Cisco WS3750G WLC(Integrated Wireless LAN Controller)는 Cisco AP1240 LAP(Lightweight AP)와 함께 사용하여 CSSC 테스트를 위한 WLAN 인프라를 제공합니다.컨피그레이션은 모든 Cisco WLAN 컨트롤러에 적용됩니다.사용된 소프트웨어 버전은 4.0.155.5입니다.

무선 LAN 컨트롤러 구성

컨트롤러에 대한 LAP의 기본 작동 및 등록

기본 작업을 위해 WLC를 구성하려면 CLI(Command Line Interface)에서 시작 컨피그레이션 마법사를 사용합니다.또는 GUI를 사용하여 WLC를 구성할 수 있습니다.이 문서에서는 CLI에서 시작 컨피그레이션 마법사를 사용하여 WLC의 컨피그레이션에 대해 설명합니다.

WLC가 처음 부팅되면 시작 컨피그레이션 마법사로 들어갑니다.구성 마법사를 사용하여 기본 설정을 구성합니다.CLI 또는 GUI를 통해 마법사에 액세스할 수 있습니다.이 출력은 CLI에서 시작 컨피그레이션 마법사의 예를 보여줍니다.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: ws-3750
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.10.80.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.80.2
Management Interface VLAN Identifier (0 = untagged):
Management Interface DHCP Server IP Address: 10.10.80.2
AP Manager Interface IP Address: 10.10.80.4
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Security
Network Name (SSID): Enterprise
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration.
```

이러한 매개변수는 기본 작업을 위해 WLC를 설정합니다.이 예제 컨피그레이션에서는 WLC가 **10.10.80.3**을 관리 인터페이스 IP 주소로, **10.10.80.4**를 AP-관리자 인터페이스 IP 주소로 사용합니다.

WLC에서 다른 기능을 구성하기 전에 LAP는 WLC에 등록해야 합니다.이 문서에서는 LAP가 WLC에 등록된 것으로 가정합니다.WLC에 AP를 등록하는 방법에 대한 자세한 내용은 WLAN Controller Failover for Lightweight Access Points 컨피그레이션 예의 Register the Lightweight AP to the WLCs 섹션을 참조하십시오.이 컨피그레이션 예와 관련하여 AP1240은 WLAN 컨트롤러(10.10.80.0/24)과 별도의 서브넷(10.10.81.0/24)에 구축되며 DHCP 옵션 43은 컨트롤러 검색에 사용됩니다.

Cisco Secure ACS를 통한 RADIUS 인증

사용자 자격 증명을 Cisco Secure ACS 서버에 전달하도록 WLC를 구성해야 합니다.그런 다음 ACS 서버는 구성된 Windows 데이터베이스를 통해 사용자 자격 증명을 확인하고 무선 클라이언트에 대한 액세스를 제공합니다.

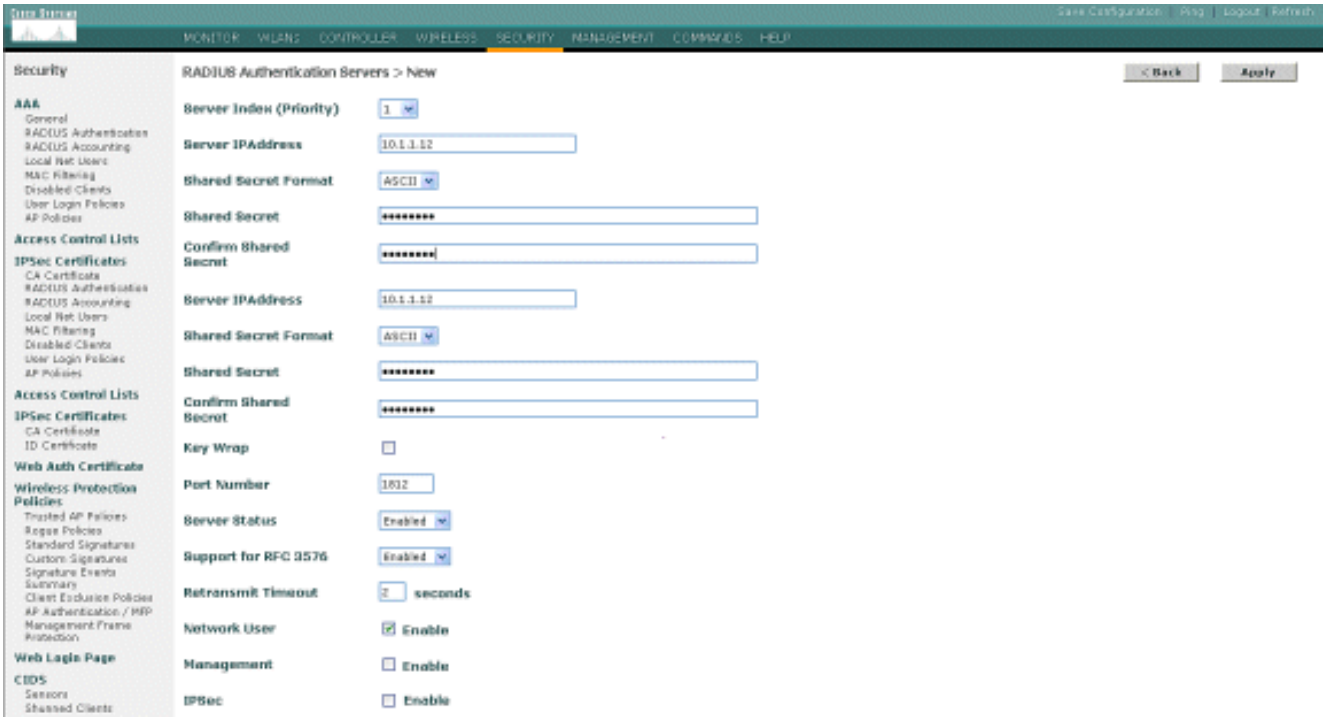
ACS 서버와의 통신을 위해 WLC를 구성하려면 다음 단계를 완료합니다.

1. RADIUS **Authentication** Servers(RADIUS 인증 서버) 페이지를 표시하려면 컨트롤러 GUI에서 Security(보안) 및 RADIUS Authentication(RADIUS 인증 서버)을 클릭합니다.그런 다음 **New(새로 만들기)**를 클릭하여 ACS 서버를 정의합니다

.

2. RADIUS 인증 서버 > 새 페이지에서 ACS 서버 매개변수를 정의합니다.이러한 매개변수에는 ACS IP 주소, 공유 암호, 포트 번호 및 서버 상태가 포함됩니다.**참고:** 포트 번호 1645 또는 1812는 RADIUS 인증을 위한 ACS와 호환됩니다.Network User and Management(네트워크 사용자 및 관리) 확인란은 RADIUS 기반 인증이 네트워크 사용자(예: WLAN 클라이언트) 및 관리(즉 관리 사용자)에 적용되는지 여부를 결정합니다. 예제 컨피그레이션에서는 Cisco Secure ACS를 IP 주소가 10.1.1.12인 RADIUS 서버로 사용합니다

.



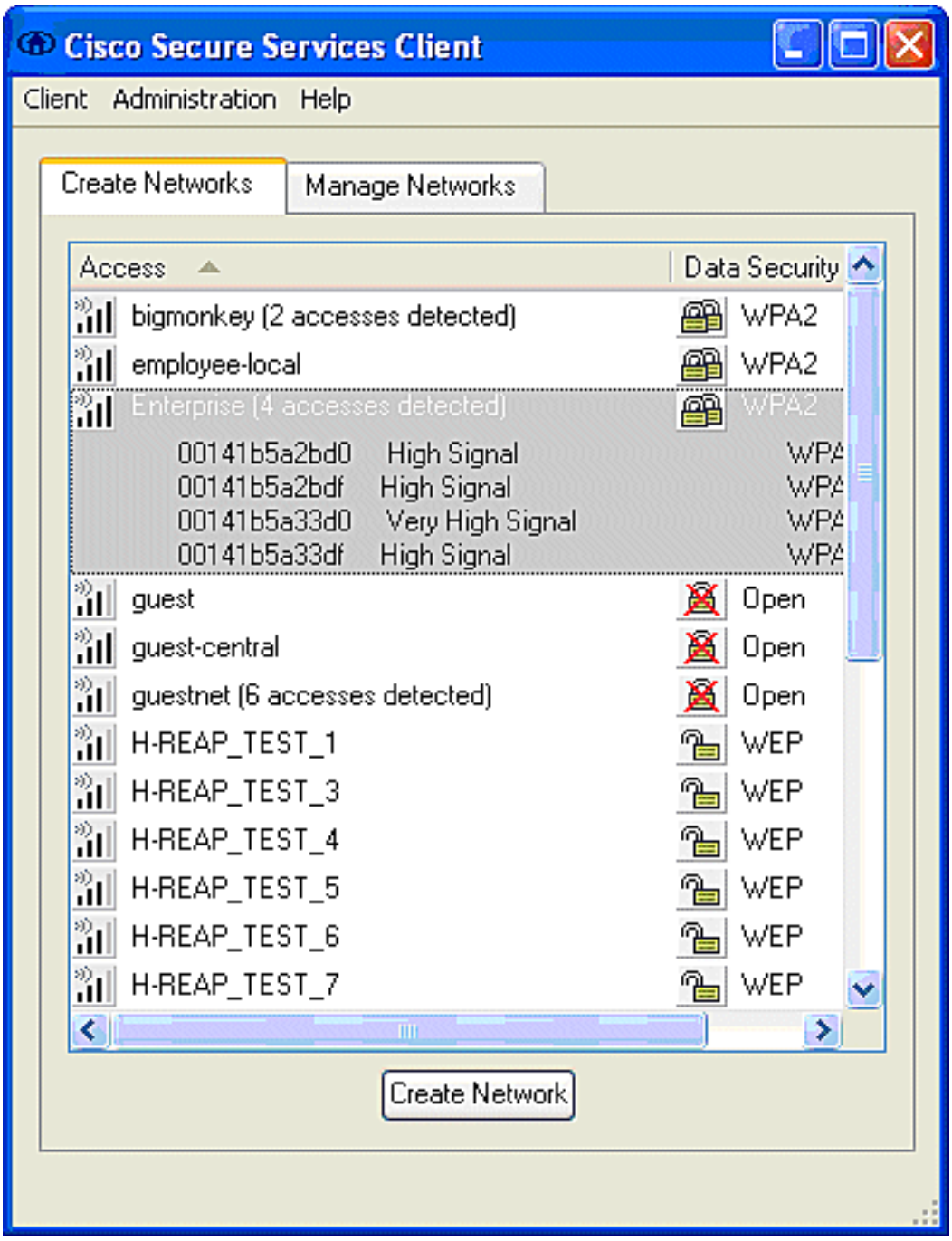
WLAN 매개변수 컨피그레이션

이 섹션에서는 Cisco Secure Services Client의 컨피그레이션에 대해 설명합니다.이 예에서 CSSC v4.0.5.4783은 Cisco CB21AG 클라이언트 어댑터와 함께 사용됩니다.CSSC 소프트웨어를 설치하기 전에 ADU(Aironet Desktop Utility)가 아니라 CB21AG용 드라이버만 설치되었는지 확인합니다.

소프트웨어가 설치되고 서비스로 실행되면 사용 가능한 네트워크를 검사하고 사용 가능한 네트워크를 표시합니다.

참고: CSSC는 Windows Zero Config를 비활성화합니다.

참고: 브로드캐스트에 대해 활성화된 SSID만 표시됩니다.



참고: WLAN 컨트롤러는 기본적으로 SSID를 브로드캐스트하므로 스캔된 SSID의 네트워크 생성 목록에 표시됩니다.네트워크 프로파일을 생성하려면 목록(Enterprise) 및 **Create Network** 라디오 버튼에서 **SSID**를 클릭하면 됩니다.

WLAN 인프라가 브로드캐스트 SSID를 비활성화하여 구성된 경우 SSID를 수동으로 추가해야 합니다.Access Devices(액세스 **디바이스**)에서 Add(추가) 라디오 버튼을 클릭하고 적절한 **SSID**(예: Enterprise)를 수동으로 입력합니다. 클라이언트에 대한 활성 프로브 동작(즉, 클라이언트가 구성된 SSID를 능동적으로 프로브하는 경우)을 구성합니다.Add **Access Device(액세스 디바이스 추가)** 창에서 SSID를 입력한 후 Actively search for this access device(이 액세스 디바이스**를** 적극적으로 검색)를 지정합니다.

참고: EAP 인증 설정이 먼저 프로파일에 대해 구성되지 않은 경우 포트 설정은 엔터프라이즈 모드(802.1X)를 허용하지 않습니다.

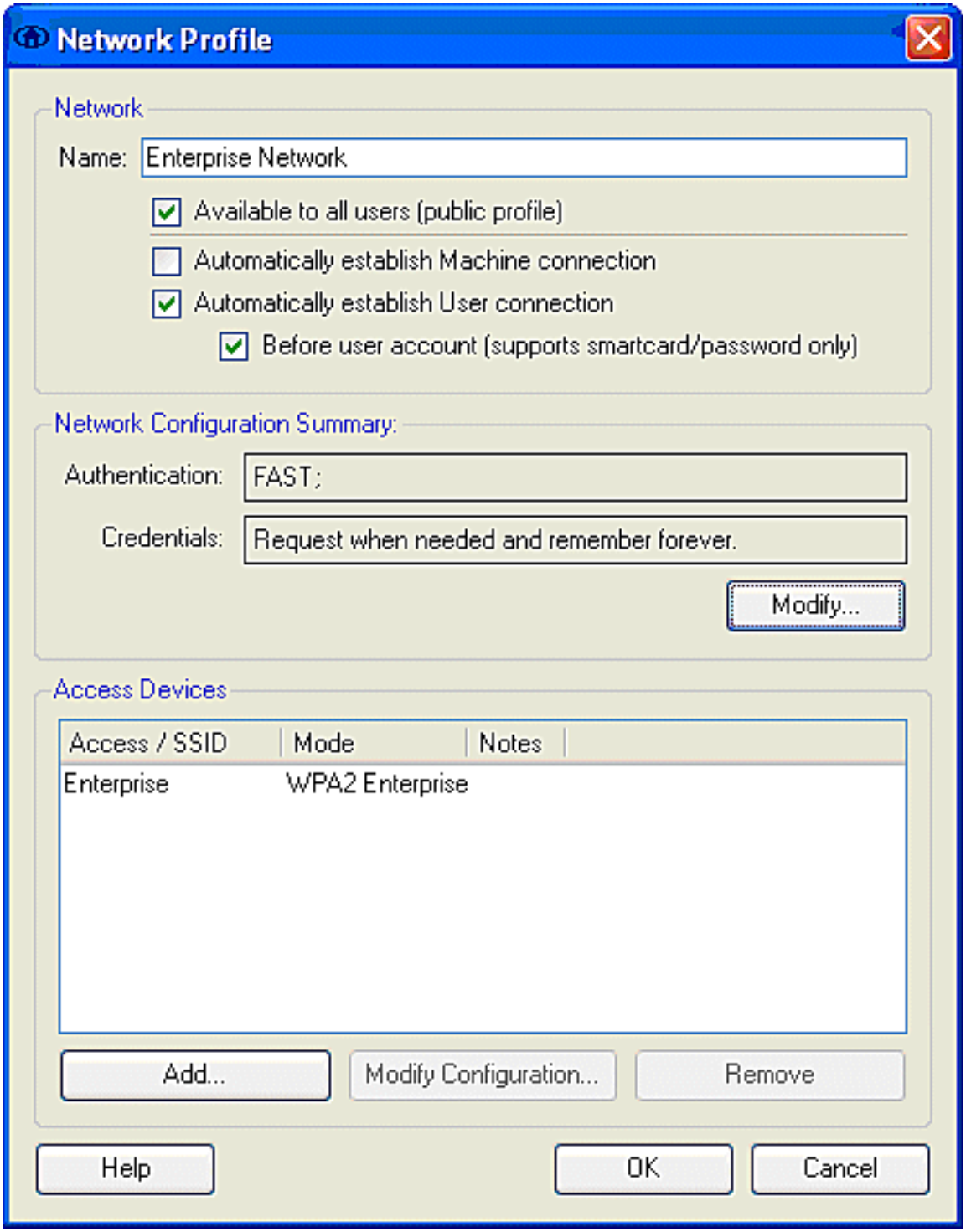
Create **Network**(네트워크 생성) 라디오 버튼이 Network Profile(네트워크 프로파일) 창을 실행하여

선택한(또는 구성된) SSID를 인증 메커니즘과 연결할 수 있습니다.프로필에 대한 설명 이름을 지정합니다.

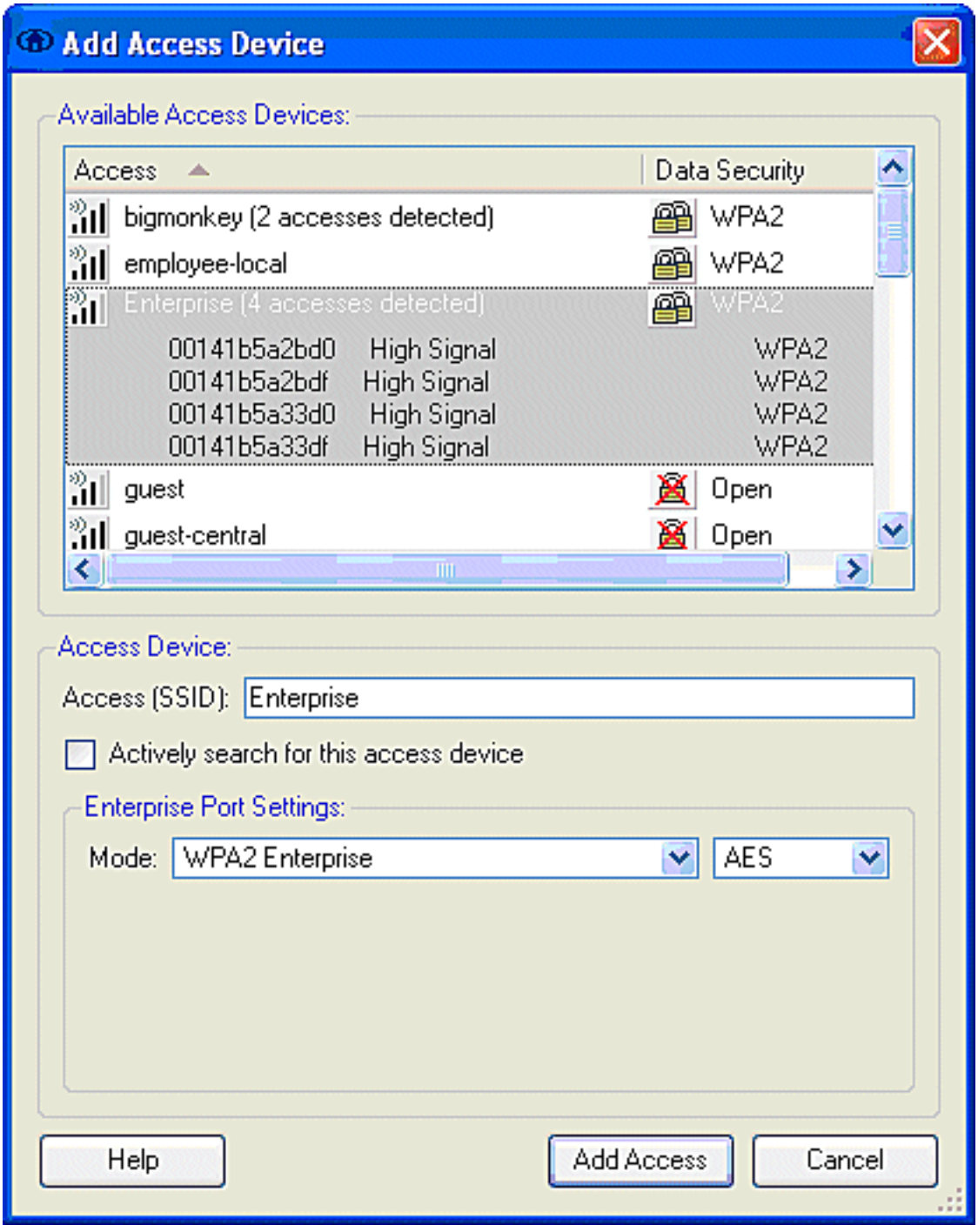
참고: 이 인증 프로파일에서 여러 WLAN 보안 유형 및/또는 SSID를 연결할 수 있습니다.

클라이언트가 RF 커버리지 범위에 있을 때 네트워크에 자동으로 연결되도록 하려면 **Automatically establish User connection을** 선택합니다.이 프로파일**을** 시스템의 다른 사용자 계정과 함께 사용하는 것이 바람직하지 않은 경우 **모든 사용자**에게 사용 가능을 선택 취소합니다.Automatically establish(**자동 설정**)를 선택하지 않으면 사용자가 CSSC 창을 열고 Connect(연결) 라디오 버튼을 사용하여 WLAN 연결을 수동으로 시작해야 합니다.

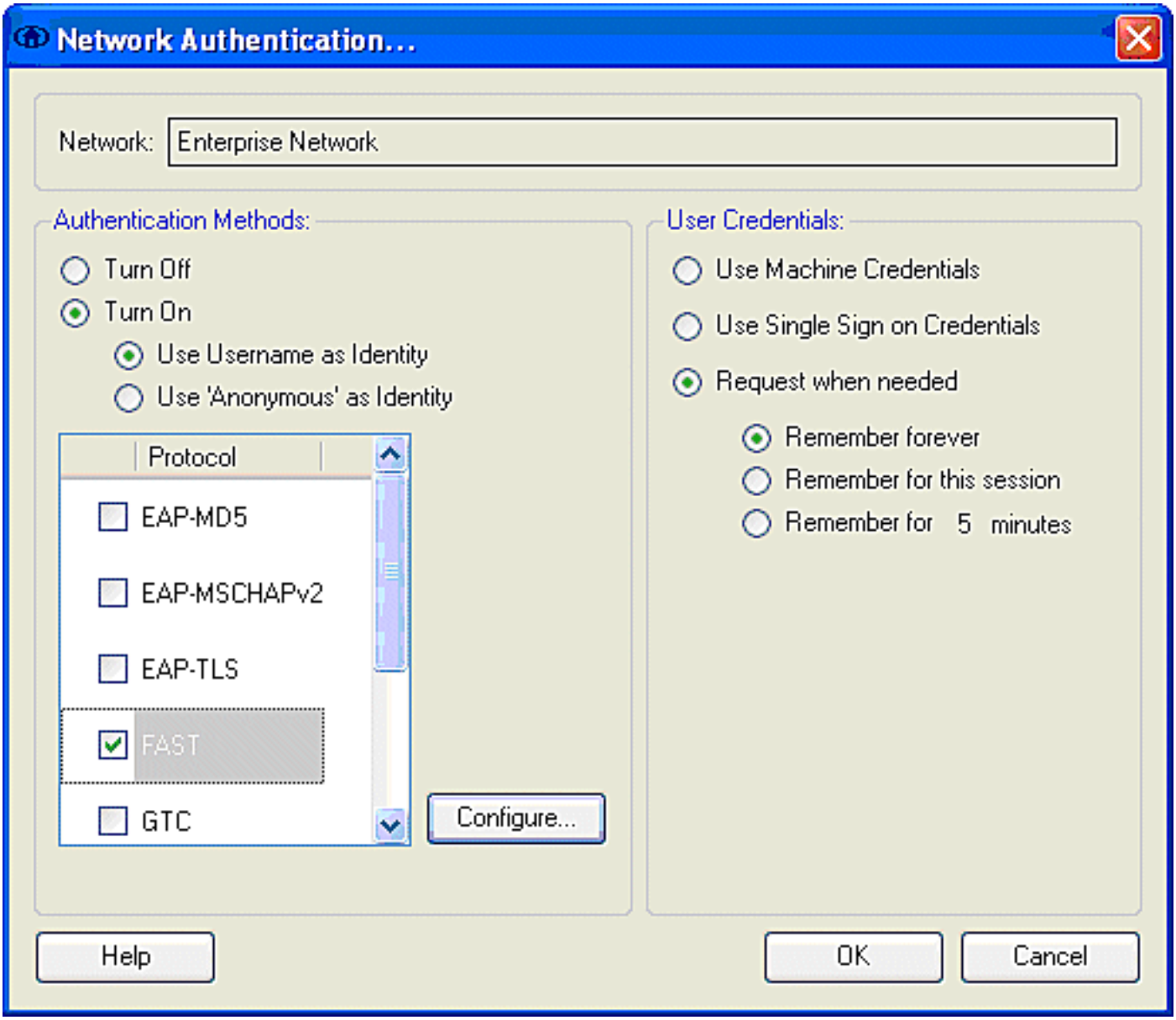
사용자가 로그온하기 전에 WLAN 연결을 시작하려면 **Before user account(사용자 계정** 전)를 선택합니다.이렇게 하면 저장된 사용자 자격 증명(EAP-FAST에서 TLS를 사용하는 경우 비밀번호 또는 인증서/스마트카드)을 사용하여 단일 로그인 작업이 허용됩니다.



참고: Cisco Aironet 350 Series Client Adapter와 함께 WPA/TKIP 작업을 수행하려면 WPA 핸드셰이크 해시 검증과 관련하여 현재 CSSC 클라이언트와 350 드라이버 간에 비호환성이 있으므로 WPA 핸드셰이크 검증을 비활성화해야 합니다.이 기능은 Client(클라이언트) **> Advanced Settings(고급 설정) > WPA/WPA2 Handshake Validation(WPA/WPA2 핸드셰이크 검증)에서 비활성화됩니다**.비활성화된 핸드셰이크 검증은 WPA(TKIP per-packet 키 및 메시지 무결성 확인)에 고유한 보안 기능을 허용하지만 초기 WPA 키 인증을 비활성화합니다.



Network Configuration Summary(네트워크 컨피그레이션 요약)에서 **Modify(수정)**를 클릭하여 EAP/자격 증명 설정을 구성합니다.Turn **On Authentication(인증 켜기)**을 지정하고 Protocol(프로토콜) 아래에서 **FAST**를 선택하고 **'Anonymous' as Identity**(초기 EAP 요청에서 사용자 이름 없음)를 선택합니다. 사용자 이름을 외부 EAP ID**로 사용**을 사용 할 수 있지만, 많은 고객이 초기 암호화되지 않은 EAP 요청에 사용자 ID를 표시 하기를 원하지 않습니다.네트워크 인증**에** 로그온 자격 증명을 사용하려면 Use Single Sign-on Credentials를 지정합니다.EAP-FAST 매개변수를 설정하려면 Configure를 클릭합니다.



FAST 설정에서 Validate Server Certificate(**서버 인증서 검증)를** 지정할 수 있습니다. 그러면 EAP-FAST 세션을 설정하기 전에 클라이언트가 EAP-FAST 서버(ACS) 인증서를 확인할 수 있습니다.이는 알 수 없거나 비인가 EAP-FAST 서버와의 연결에서 클라이언트 장치에 대한 보호 및 신뢰할 수 없는 소스에 대한 인증 자격 증명의 부주의로 전송 합니다.이렇게 하려면 ACS 서버에 인증서가 설치되어 있어야 하며 클라이언트에는 Root Certificate Authority 인증서가 설치되어 있어야 합니다 .이 예에서는 서버 인증서 검증이 활성화되지 않습니다.

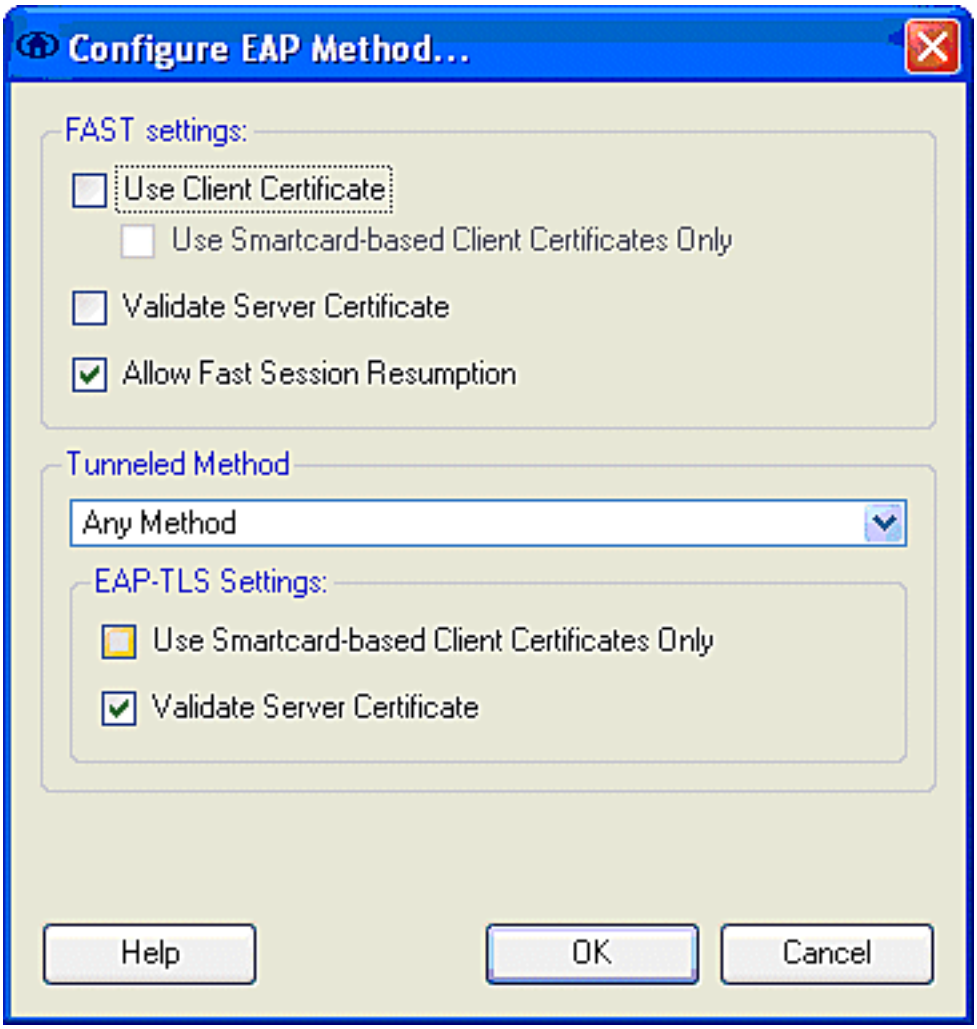
FAST 설정에서 **Allow Fast Session Resume(빠른 세션 재개 허용**)을 지정할 수 있습니다. 그러면 전체 EAP-FAST 재인증 요구 사항이 아닌 터널(TLS 세션) 정보를 기반으로 EAP-FAST 세션을 재개할 수 있습니다.EAP-FAST 서버 및 클라이언트가 초기 EAP-FAST 인증 교환 내에서 협상된 TLS 세션 정보에 대한 공통 지식을 가지고 있는 경우 세션 재개가 발생할 수 있습니다.

참고: EAP-FAST 서버 및 클라이언트는 모두 EAP-FAST 세션 재개에 대해 구성되어야 합니다.

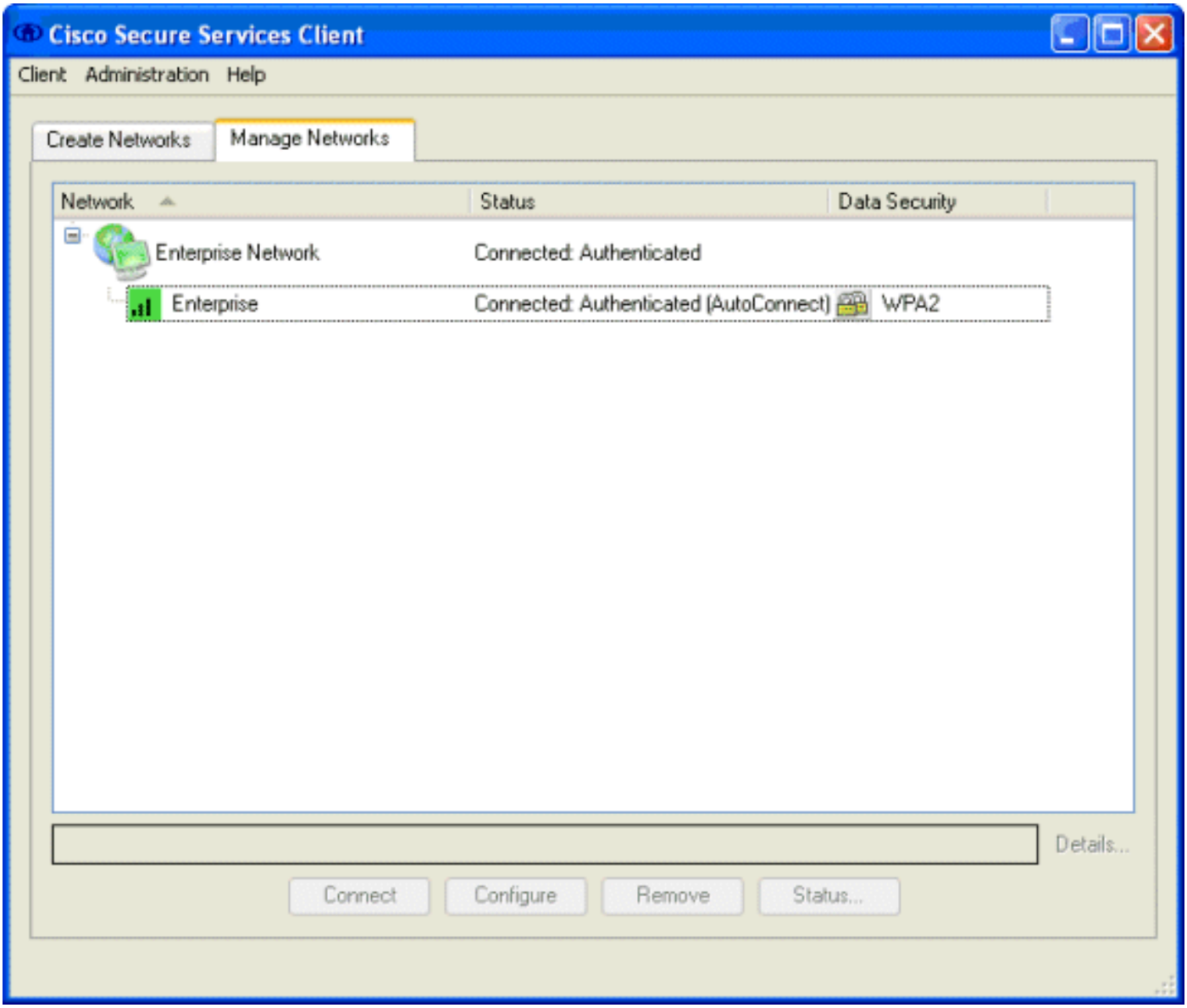
Tunneled Method(터널링된 방법) > EAP-TLS Settings(EAP-TLS 설정) 아래에서 PAC 자동 프로비저닝을 위한 EAP-MSCHAPv2 및 인증을 위한 EAP-GTC를 허용하는 **모든 방법**을 지정합니다 .Active Directory와 같은 Microsoft 형식 데이터베이스를 사용하는 경우 및 가 네트워크에서 EAP-FAST v1 클라이언트를 지원하지 않는 경우 MSCHAPv**2**만 터널링 방법으로 사용하도록 지정할 수도 있습니다.

참고: 이 창의 EAP-TLS 설정에서 서버 인증서 유효성 검사는 기본적으로 활성화되어 있습니다.이

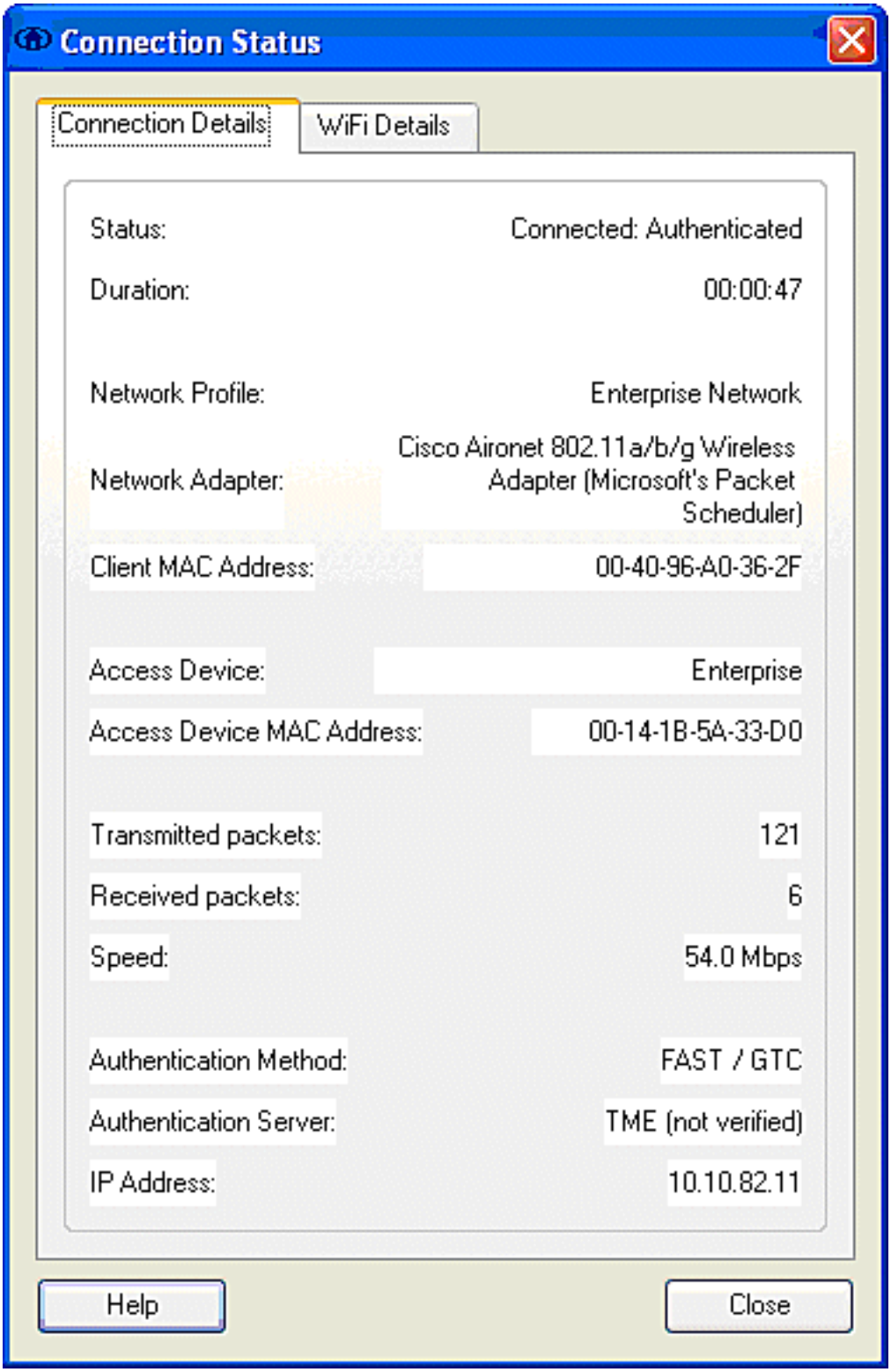
예에서는 내부 인증 방법으로 EAP-TLS를 사용하지 않으므로 이 필드는 적용되지 않습니다.이 필드가 활성화된 경우 EAP-TLS 내에서 클라이언트 인증서의 서버 유효성 검사 외에 클라이언트가 서버 인증서를 검증할 수 있습니다.

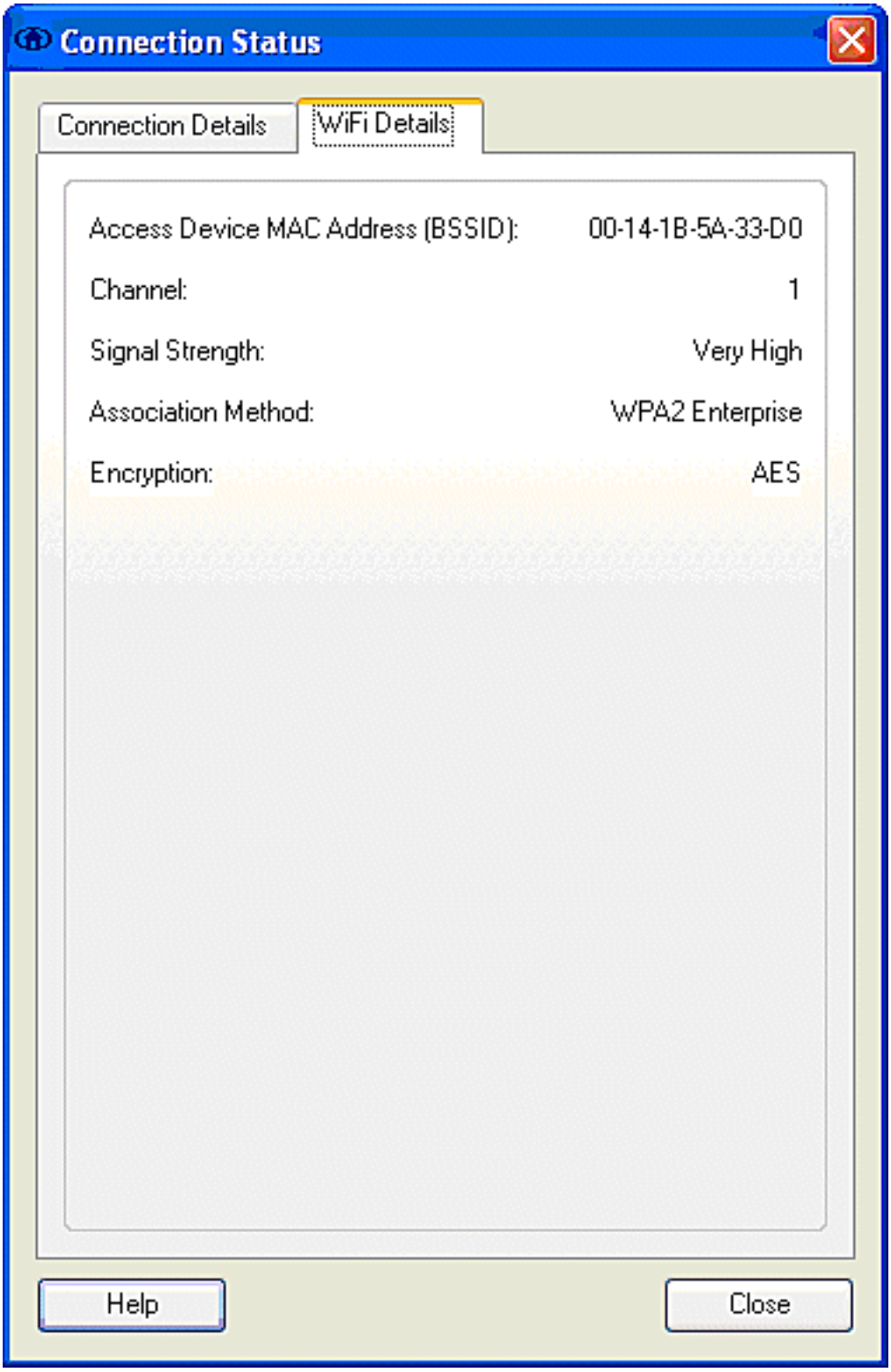


OK(**확인**)를 클릭하여 EAP-FAST 설정을 저장합니다.클라이언트가 프로파일 아래에 "자동으로 설정"되도록 구성되었으므로 네트워크와의 연결/인증이 자동으로 시작됩니다.네트워크 관리 탭에서 네트워크, 상태 및 데이터 보안 필드는 클라이언트의 연결 상태를 나타냅니다.이 예에서는 프로파일 엔터프라이즈 네트워크가 사용 중이며 네트워크 액세스 장치는 Connected:Authenticated를 나타내며 Autoconnect를 사용하는 SSID Enterprise입니다.데이터 보안 필드는 사용되는 802.11 암호화 유형을 나타내며, 이 예에서는 WPA2입니다.



클라이언트가 인증되면 Manage Networks(네트워크 관리) 탭의 Profile(프로파일) 아래에서 **SSID**를 선택하고 **Status(상태)**를 클릭하여 연결 세부사항을 쿼리합니다.Connection Details(연결 세부사항) 창은 클라이언트 디바이스, 연결 상태 및 통계, 인증 방법에 대한 정보를 제공합니다.WiFi 세부사항 탭은 RSSI, 802.11 채널 및 인증/암호화를 포함하는 802.11 연결 상태에 대한 세부사항을 제공합니다.


Connection Status
Connection Details
WiFi Details
Status:
Connected: Authenticated
Duration:
00:00:47
Network Profile:
Enterprise Network
Network Adapter:
Cisco Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:
00-40-96-A0-36-2F
Access Device:
Enterprise
Access Device MAC Address:
00-14-1B-5A-33-D0
Transmitted packets:
121
Received packets:
6
Speed:
54.0 Mbps
Authentication Method:
FAST / GTC
Authentication Server:
TME (not verified)
IP Address:
10.10.82.11
Help
Close



시스템 관리자는 표준 CSSC 배포에서 사용할 수 있는 진단 유틸리티인 Cisco Secure Services Client System Report를 사용할 수 있습니다.이 유틸리티는 시작 메뉴 또는 CSSC 디렉토리에서 사용할 수 있습니다.데이터를 가져오려면 데이터 **수집 > 클립보드로 복사 > 보고서 파일 찾기를** 클릭합니다.이렇게 하면 Microsoft File Explorer 창이 압축된 보고서 파일이 있는 디렉토리로 이동합니다.압축된 파일 내에서 가장 유용한 데이터는 로그(log_current) 아래에 있습니다.

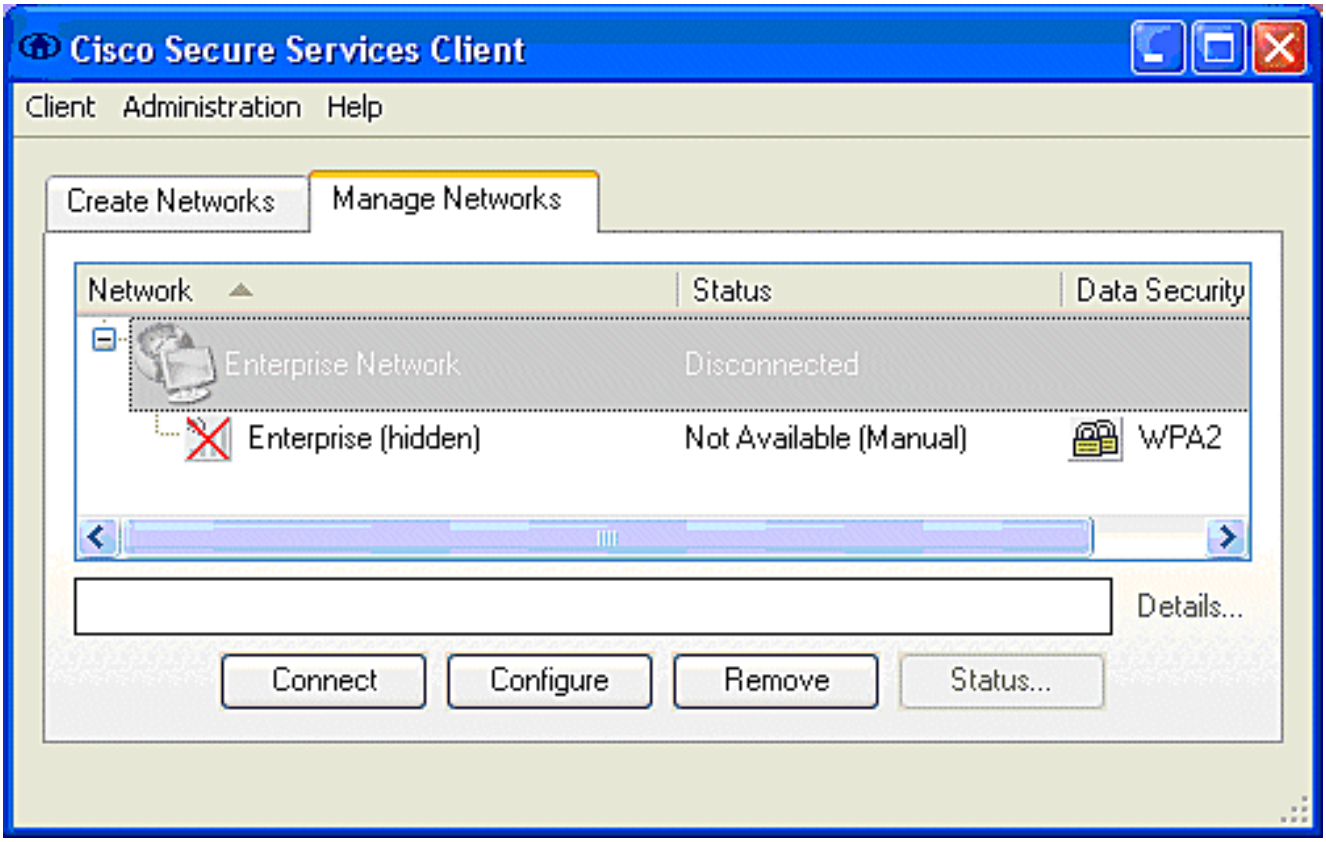
이 유틸리티는 WLAN 정보(SSID 탐지, 연결 상태 등)와 함께 CSSC, 인터페이스 및 드라이버 세부 사항의 현재 상태를 제공합니다. 이는 특히 CSSC와 WLAN 어댑터 간의 연결 문제를 진단하는 데 유용합니다.

작업 확인

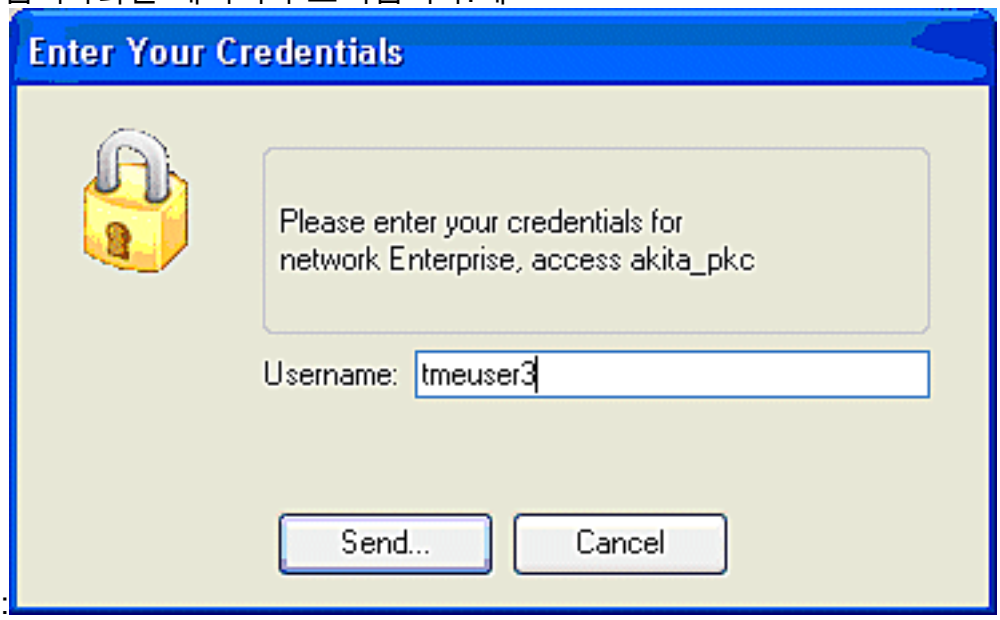
Cisco Secure ACS 서버, WLAN 컨트롤러, CSSC 클라이언트를 구성하고 정확한 컨피그레이션 및 데이터베이스 채우기를 구성한 후 WLAN 네트워크는 EAP-FAST 인증 및 보안 클라이언트 통신을 위해 구성됩니다.보안 세션의 진행률/오류를 확인하기 위해 모니터링할 수 있는 여러 지점이 있습니다.

컨피그레이션을 테스트하려면 EAP-FAST 인증을 사용하여 무선 클라이언트를 WLAN 컨트롤러와 연결하려고 합니다.

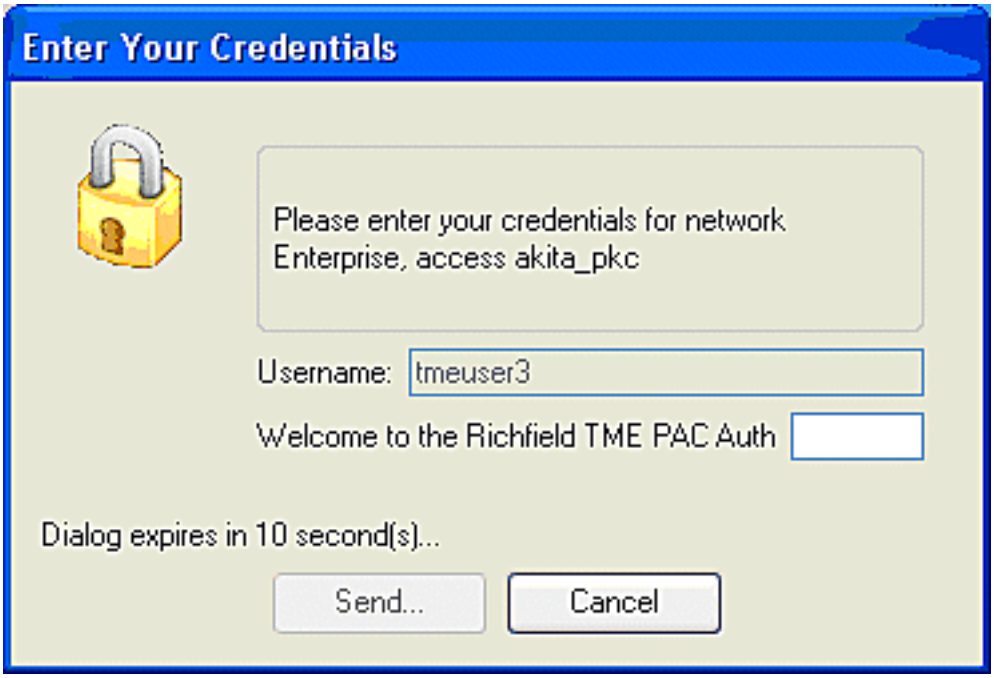
1. CSSC가 자동 연결을 위해 구성된 경우 클라이언트는 이 연결을 자동으로 시도합니다.자동 연결 및 단일 사인온 작업에 대해 구성되지 않은 경우 사용자는 **연결** 라디오 버튼을 통해 WLAN 연결을 시작해야 합니다.그러면 EAP 인증이 발생하는 802.11 연결 프로세스가 시작됩니다.예 :



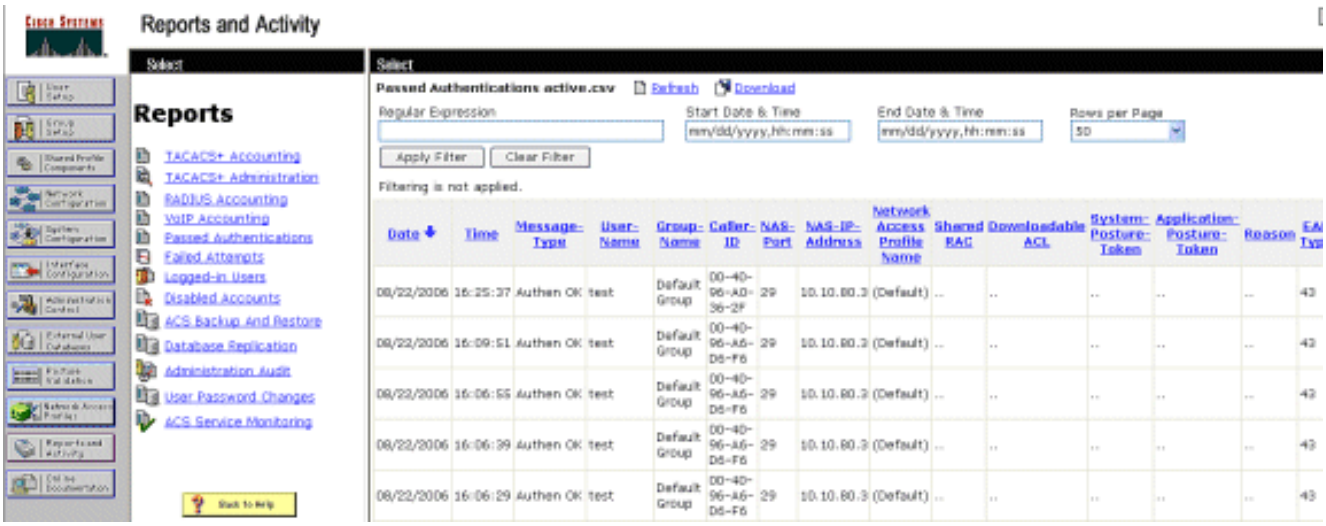
2. 그 후 EAP-FAST 인증(EAP-FAST PAC Authority 또는 ACS에서) 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.예



:

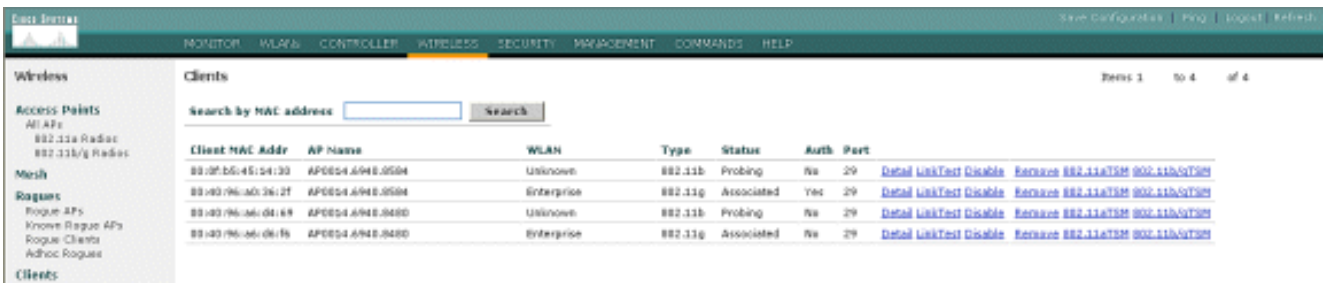


3. CSSC 클라이언트는 WLC를 통해 RADIUS 서버(Cisco Secure ACS)에 사용자 자격 증명을 전달하여 자격 증명을 검증합니다.ACS는 데이터와 구성된 데이터베이스(예 컨피그레이션, 외부 데이터베이스는 Windows Active Directory)를 비교하여 사용자 자격 증명을 확인하고 사용자 자격 증명이 유효할 때마다 무선 클라이언트에 대한 액세스를 제공합니다.ACS 서버의 Passed Authentications 보고서는 클라이언트가 RADIUS/EAP 인증을 통과했음을 보여줍니다 .예
:



4. RADIUS/EAP 인증에 성공하면 무선 클라이언트(이 예에서는 00:40:96:ab:36:2f)가 AP/WLAN 컨트롤러로 인증됩니다

.



부록

Cisco Secure ACS 및 Cisco WLAN Controller에서 제공되는 진단 및 상태 정보 외에도 EAP-FAST 인증을 진단하는 데 사용할 수 있는 추가 포인트가 있습니다.WLAN 스니퍼를 사용하거나 WLAN 컨트롤러에서 EAP 교환을 디버깅하지 않고 대부분의 인증 문제를 진단할 수 있지만, 이 참조 자료는 문제 해결을 돕기 위해 포함되어 있습니다.

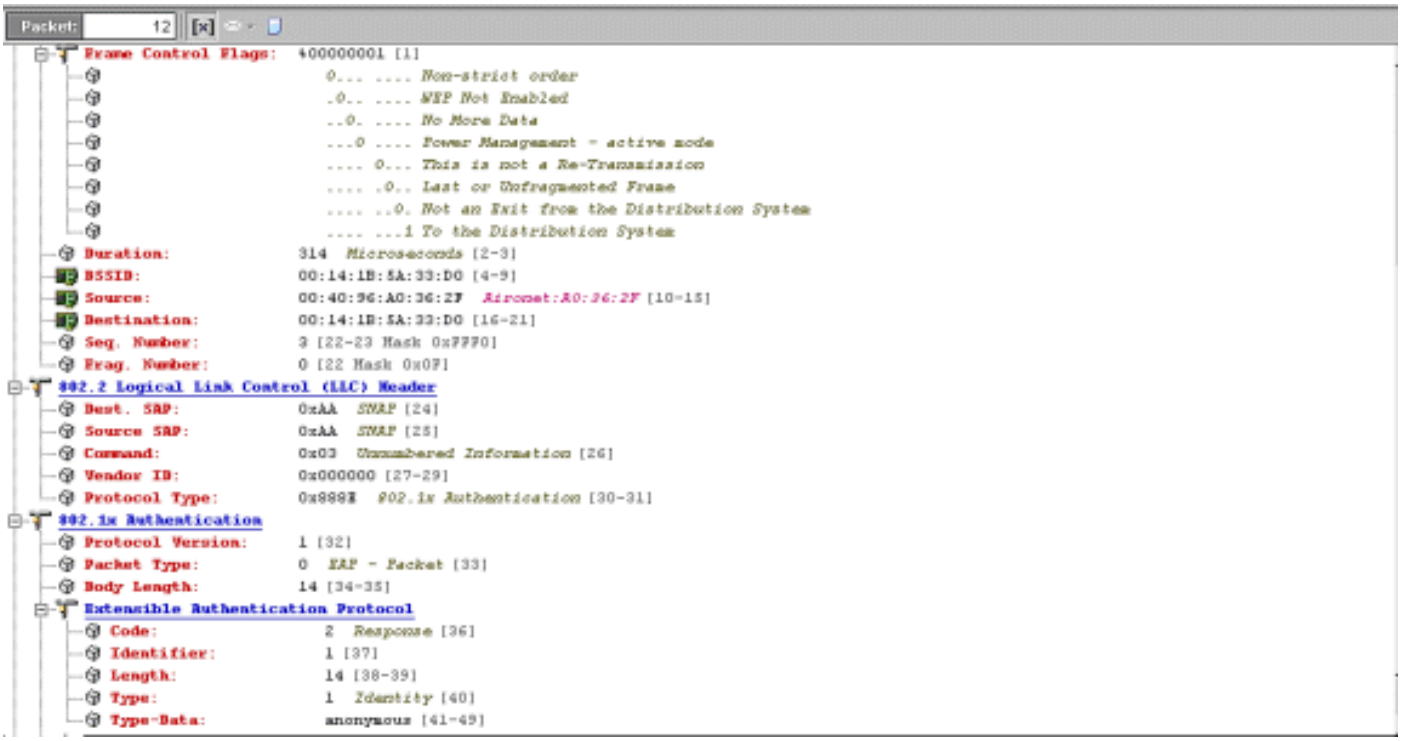
EAP-FAST Exchange용 스니퍼 캡처

이 802.11 스니퍼 캡처는 인증 교환을 보여줍니다.

Source	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary
00:14:1B:5A:33:D0	*	11	68%	36.0	101	00.033877	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0	*	11	70%	24.0	101	00.036453	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.1x	FC=.F......,SN=2868,FN= 0
Aironet:A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC=T.......,SN= 3,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.123517	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	67%	54.0	65	00.165611	802.1x	FC=.F......,SN=2870,FN= 0
Aironet:A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T.......,SN= 4,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.174228	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	68%	54.0	66	00.178863	802.1x	FC=.F......,SN=2871,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.200632	EAP Response	FC=T.......,SN= 5,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.203340	EAP Response	FC=T..R....,SN= 5,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.203639	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	70%	54.0	188	00.207634	802.1x	FC=.F......,SN=2872,FN= 0
Aironet:A0:36:2F		11	55%	1.0	105	00.216295	EAP Response	FC=T.......,SN= 6,FN= 0
Aironet:A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC=T..R....,SN= 6,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.217754	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	67%	54.0	99	00.222799	802.1x	FC=.F......,SN=2874,FN= 0
Aironet:A0:36:2F		11	55%	1.0	152	00.254189	EAP Response	FC=T.......,SN= 7,FN= 0
00:14:1B:5A:33:D0	#	11	68%	1.0	14	00.254499	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	64%	54.0	147	00.288950	802.1x	FC=.F.R....,SN=2875,FN= 0
Aironet:A0:36:2F		11	55%	1.0	232	00.318087	EAP Response	FC=T.......,SN= 8,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.318383	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	68%	54.0	44	00.326833	802.1x	FC=.F......,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	65%	54.0	44	00.326882	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	48.0	44	00.326922	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	157	00.326964	802.1x	FC=.F......,SN=2878,FN= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAP01-Key	FC=T.......,SN= 9,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.334019	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	65%	54.0	207	00.340467	802.1x	FC=.F......,SN=2879,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	207	00.341130	802.1x	FC=.F.R....,SN=2879,FN= 0
Aironet:A0:36:2F		11	57%	1.0	135	00.342542	EAP01-Key	FC=T.......,SN= 10,FN= 0

이 패킷은 초기 EAP-FAST EAP 응답을 표시합니다.

참고: CSSC 클라이언트에서 구성된 대로, 익명 은 초기 EAP 응답에서 외부 EAP ID로 사용됩니다.



WLAN 컨트롤러에서 디버그

다음 디버그 명령을 WLAN 컨트롤러에서 사용하여 인증 교환의 진행 상황을 모니터링할 수 있습니다.

- **디버그 aaa 이벤트 활성화**
- **디버그 aaa detail enable**
- **debug dot1x 이벤트 활성화**
- **디버그 dot1x 상태 활성화**

다음은 디버그를 사용하여 WLAN 컨트롤러에서 모니터링되는 CSSC 클라이언트와 ACS 간의 인증 트랜잭션 시작 예입니다.

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing RSN IE type 48,
   length 20 for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received RSN IE with
   0 PMKIDs from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
   moving mobile 00:40:96:a0:36:2f into Connecting state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-
   Request/Identity to mobile 00:40:96:a0:36:2f (EAP Id 1)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Identity Response
   (count=1) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f EAP State update from
   Connecting to Authenticating for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x - moving mobile
   00:40:96:a0:36:2f into Authenticating state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth
   Response state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AuthenticationRequest: 0x138dd764
Thu Aug 24 18:20:54 2006:       Callback.......0x10372764
Thu Aug 24 18:20:54 2006:       protocolType...0x00040001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:       Packet contains 15 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Successful transmission of
   Authentication Packet (id 84) to 10.1.1.12:1812, proxy state0
Thu Aug 24 18:20:54 2006: ****Enter processIncomingMessages: response code=11
Thu Aug 24 18:20:54 2006: ****Enter processRadiusResponse: response code=11
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Access-Challenge received from
   RADIUS server 10.1.1.12 for mobile 00:40:96:a0:36:2f rec7
Thu Aug 24 18:20:54 2006: AuthorizationResponse: 0x11c8a394
Thu Aug 24 18:20:54 2006:       structureSize..147
Thu Aug 24 18:20:54 2006:       resultCode.....255
Thu Aug 24 18:20:54 2006:       protocolUsed...0x00000001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:       Packet contains 4 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-Challenge
   for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Req state
   (id=249) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f WARNING:
   updated EAP-Identifer 1 ===> 249 for STA 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP Request from
   AAA to mobile 00:40:96:a0:36:2f (EAP Id 249)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAP Response from
   mobile 00:40:96:a0:36:2f (EAP Id 249, EAP Type 3)
```

컨트롤러 디버그(WPA2 인증 사용)에서 EAP 교환을 성공적으로 완료했습니다.

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-
   Accept for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Applying new AAA
   override for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Override values for station
   00:40:96:a0:36:2f source: 4, valid bits: 0x0
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout:
   -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, r1'
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Unable to apply override
   policy for station 00:40:96:a0:36:2f - VapAllowRadiusOverride E
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Creating a new PMK Cache Entry
   for station 00:40:96:a0:36:2f (RSN 2)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Adding BSSID
   00:14:1b:5a:33:d0 to PMKID cache for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: New PMKID: (16)
Thu Aug 24 18:20:54 2006:      [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b
   72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-Success
   to mobile 00:40:96:a0:36:2f (EAP Id 0)
Thu Aug 24 18:20:54 2006: Including PMKID in M1  (16)
Thu Aug 24 18:20:54 2006:
   [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to
   mobile 00:40:96:a0:36:2f state INITPMK (message 1), repl0
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend
   Auth Success state (id=0) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Auth Success
   while in Authenticating state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
   moving mobile 00:40:96:a0:36:2f into Authenticated state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-
   Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version
   (1) in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key
   in PKT_START state (message 2) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission
   timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message
   to mobile 00:40:96:a0:36:2f state PTKINITNEGOTIATING (messa1
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received
   EAPOL-Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1)
   in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in
   PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AccountingMessage
   Accounting Interim: 0x138dd764
Thu Aug 24 18:20:54 2006: Packet contains 20 AVPs:
Thu Aug 24 18:20:54 2006:
   AVP[01] User-Name.................enterprise (10 bytes)
Thu Aug 24 18:20:54 2006: AVP[02]
   Nas-Port..........................0x0000001d (29) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[03]
   Nas-Ip-Address....................0x0a0a5003 (168448003) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[04]
   Class.............................CACS:0/28b5/a0a5003/29 (22 bytes)
Thu Aug 24 18:20:54 2006: AVP[05]
   NAS-Identifier....................ws-3750 (7 bytes)
Thu Aug 24 18:20:54 2006: AVP[06]
   Airespace / WLAN-Identifier........0x00000001 (1) (4 bytes)
```

```
Thu Aug 24 18:20:54 2006: AVP[07]
   Acct-Session-Id.....................44ede3b0/00:40:
   96:a0:36:2f/14 (29 bytes)
Thu Aug 24 18:20:54 2006: AVP[08]
   Acct-Authentic.....................0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[09]
   Tunnel-Type........................0x0000000d (13) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[10]
   Tunnel-Medium-Type.................0x00000006 (6) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[11]
   Tunnel-Group-Id....................0x3832 (14386) (2 bytes)
Thu Aug 24 18:20:54 2006: AVP[12]
   Acct-Status-Type...................0x00000003 (3) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[13]
   Acct-Input-Octets..................0x000b99a6 (760230) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[14]
   Acct-Output-Octets.................0x00043a27 (277031) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[15]
   Acct-Input-Packets.................0x0000444b (17483) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[16]
   Acct-Output-Packets................0x0000099b (2459) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[17]
   Acct-Session-Time..................0x00000a57 (2647) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[18]
   Acct-Delay-Time....................0x00000000 (0) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[19]
   Calling-Station-Id.................10.10.82.11 (11 bytes)
Thu Aug 24 18:20:54 2006: AVP[20]
   Called-Station-Id..................10.10.80.3 (10 bytes)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f
   Stopping retransmission timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:57 2006: User admin authenticated
```

관련 정보

- Windows Server용 Cisco Secure ACS 설치 설명서
- Cisco Secure ACS 4.1용 구성 설명서
- WLC 및 Cisco Secure ACS 컨피그레이션을 통한 SSID를 기반으로 WLAN 액세스 제한 예
- ACS 4.0 및 Windows 2003을 사용하는 통합 무선 네트워크의 EAP-TLS
- RADIUS 서버 및 무선 LAN 컨트롤러 구성을 통한 동적 VLAN 할당 예
- 기술 지원 및 문서 – Cisco Systems