

# RADIUS 서버를 사용한 EAP 인증

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기규칙](#)

[구성](#)

[네트워크 EAP 또는 EAP를 통한 개방 인증](#)

[인증 서버 정의](#)

[클라이언트 인증 방법 정의](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제 해결 절차](#)

[문제 해결 명령](#)

[관련 정보](#)

## 소개

이 문서에서는 RADIUS 서버에서 액세스하는 데이터베이스에 대해 무선 사용자의 EAP(Extensible Authentication Protocol) 인증을 위한 Cisco IOS® 기반 액세스 포인트의 샘플 컨피그레이션을 제공합니다.

액세스 포인트가 EAP에서 수행하는 패시브 역할(클라이언트에서 인증 서버로 향하는 유선 패킷으로 무선 패킷을 연결하며 그 반대의 경우) 때문에 이 컨피그레이션은 거의 모든 EAP 방법과 함께 사용됩니다. 이러한 방법에는 LEAP, PEAP(Protected EAP)-MS-CHAP(Challenge Handshake Authentication Protocol) 버전 2, PEAP-GTC(Generic Token Card), FAST(Secure Tunneling)를 통한 EAP-Flexible Authentication via TLS(EAP-Transport Layer Security), TTLS(EAP-Tunneled TLS)가 포함됩니다. 이러한 각 EAP 방법에 대해 인증 서버를 적절히 구성해야 합니다.

이 문서에서는 이 문서의 컨피그레이션 예에서 Cisco Secure ACS인 AP(Access Point) 및 RADIUS 서버를 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- Cisco IOS GUI 또는 CLI에 대해 잘 알고 있습니다.
- EAP 인증의 이면에 있는 개념에 익숙합니다.

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS를 실행하는 Cisco Aironet AP 제품.
- 네트워크에서 하나의 가상 LAN(VLAN)만 가정
- 사용자 데이터베이스에 성공적으로 통합되는 RADIUS 인증 서버 제품입니다.다음은 Cisco LEAP 및 EAP-FAST에 대해 지원되는 인증 서버입니다.Cisco ACS(Secure Access Control Server)Cisco CAR(Access Registrar)펑크 스틸 벨트드 RADIUS인터링크 장점Microsoft PEAP-MS-CHAP 버전 2 및 PEAP-GTC에 대해 지원되는 인증 서버입니다.Microsoft IAS(인터넷 인증 서비스)Cisco Secure ACS펑크 스틸 벨트드 RADIUS인터링크 장점Microsoft에서 인증할 수 있는 추가 인증 서버입니다.**참고:** GTC 또는 일회성 비밀번호는 클라이언트와 서버 측 모두에서 추가 소프트웨어를 필요로 하는 추가 서비스와 하드웨어 또는 소프트웨어 토큰 생성기를 필요로 합니다.EAP-TLS, EAP-TTLS 및 기타 EAP 방법에 대해 해당 제품과 함께 인증 서버가 지원되는지 여부는 클라이언트 신청자 제조업체에 문의하십시오.

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 규칙](#)을 참조하십시오.

## 구성

이 구성은 IOS 기반 AP에서 EAP 인증을 구성하는 방법을 설명합니다. 이 문서의 예에서 LEAP는 RADIUS 서버를 사용하는 EAP 인증 방법으로 사용됩니다.

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

대부분의 비밀번호 기반 인증 알고리즘과 마찬가지로 Cisco LEAP는 사전 공격에 취약합니다. 이는 Cisco LEAP의 새로운 공격이나 새로운 취약성이 아닙니다. 강력한 비밀번호 정책을 생성하는 것이 사전 공격을 완화하는 가장 효과적인 방법입니다. 여기에는 강력한 비밀번호 사용 및 정기적 비밀번호 만료 등이 포함됩니다. 사전 공격에 대한 자세한 [내용과](#) 예방 방법에 대한 자세한 내용은 [Cisco LEAP의 사전 공격](#)을 참조하십시오.

이 문서에서는 GUI와 CLI에 모두 이 컨피그레이션을 사용합니다.

- AP의 IP 주소는 10.0.0.106입니다.
- RADIUS 서버(ACS)의 IP 주소는 10.0.0.3입니다.

## 네트워크 EAP 또는 EAP를 통한 개방 인증

EAP/802.1x 기반 인증 방법에서는 네트워크 EAP와 EAP를 통한 개방 인증 간의 차이점이 무엇인지 질문할 수 있습니다. 이러한 항목은 관리 및 연결 패킷의 헤더에 있는 인증 알고리즘 필드의 값을 참조합니다. 대부분의 무선 클라이언트 제조업체는 이 필드를 값 0(Open 인증)으로 설정한 다음 연결 프로세스의 뒷부분에서 EAP 인증을 수행하고자 한다는 신호를 보냅니다. Cisco는 네트워크 EAP 플래그와의 연결 시작에서 값을 다르게 설정합니다.

네트워크에 다음과 같은 클라이언트가 있는 경우

- Cisco 클라이언트 - 네트워크 EAP를 사용합니다.
- 타사 클라이언트(CCX 호환 제품 포함) - EAP와 함께 Open을 사용합니다.
- Cisco 및 타사 클라이언트의 조합 - Network-EAP와 Open with EAP를 모두 선택합니다.

## 인증 서버 정의

EAP 컨피그레이션의 첫 번째 단계는 인증 서버를 정의하고 그 서버와의 관계를 설정하는 것입니다

1. 액세스 포인트 서버 관리자 탭(보안 > 서버 관리자 메뉴 항목 아래)에서 다음 단계를 완료합니다. Server(서버) 필드에 인증 서버의 IP 주소를 입력합니다. 공유 암호와 포트를 지정합니다. Apply(적용)를 클릭하여 정의를 생성하고 드롭다운 목록을 채웁니다. Default Server Priorities(기본 서버 우선순위) 아래에서 EAP Authentication type Priority 1(EAP 인증 유형 우선순위 1) 필드를 서버 IP 주소로 설정합니다. Apply를 클릭합니다

The screenshot shows the Cisco 1200 Access Point configuration interface. The top header displays 'Cisco 1200 Access Point' and 'SERVER MANAGER' tabs. The main content area is divided into several sections:

- Backup RADIUS Server:** Includes fields for 'Backup RADIUS Server:' (Hostname or IP Address) and 'Shared Secret:'. Buttons for 'Apply', 'Delete', and 'Cancel' are present.
- Corporate Servers:** Contains a 'Current Server List' with a dropdown menu set to 'RADIUS'. A list shows '< NEW >' and '10.0.0.3'. A 'Delete' button is below the list. To the right, there are fields for 'Server:' (10.0.0.3), 'Shared Secret:', 'Authentication Port (optional):' (1645), and 'Accounting Port (optional):' (1646). Buttons for 'Apply' and 'Cancel' are at the bottom right.
- Default Server Priorities:** This section is circled in red. It includes:
  - EAP Authentication:** Priority 1 is set to 10.0.0.3, Priority 2 is < NONE >, and Priority 3 is < NONE >.
  - MAC Authentication:** Priority 1, 2, and 3 are all set to < NONE >.
  - Accounting:** Priority 1, 2, and 3 are all set to < NONE >.
  - Admin Authentication (RADIUS):** Priority 1, 2, and 3 are all set to < NONE >.
  - Admin Authentication (TACACS+):** Priority 1 is set to 10.0.0.3, Priority 2 and 3 are < NONE >.
  - Proxy Mobile IP Authentication:** Priority 1, 2, and 3 are all set to < NONE >.

At the bottom of the interface, there are 'Close Window' and 'Copyright (c) 1992-2004 by Cisco Systems, Inc.' labels.

CLI에서 다음 명령을 실행할 수도 있습니다.

```
AP#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
AP(config)#aaa group server radius rad_eap
```

```
AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646
```

```

AP(config-sg-radius)#exit

AP(config)#aaa new-model

AP(config)#aaa authentication login eap_methods group rad_eap

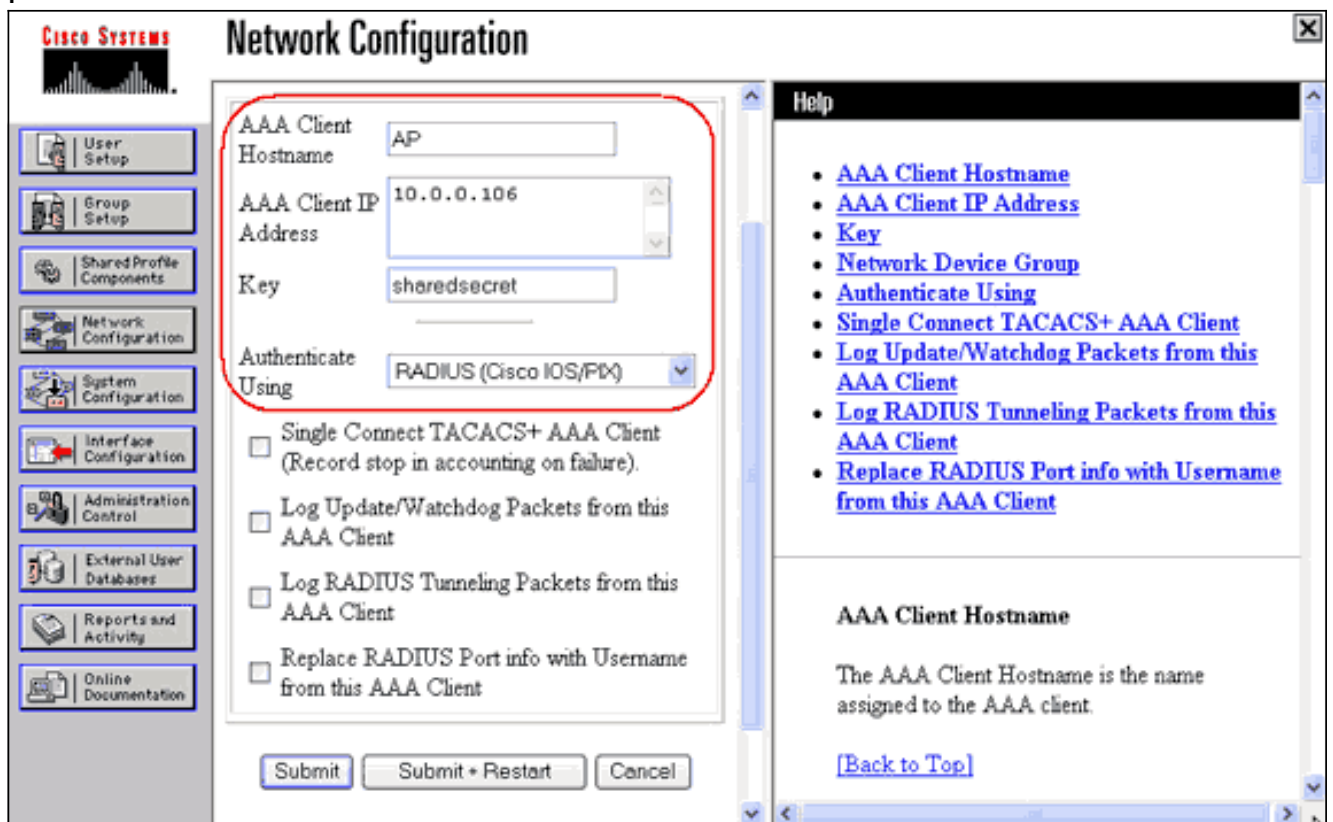
AP(config)#radius-server host 10.0.0.3 auth-port 1645
acct-port 1646 key labap1200ip102

AP(config)#end

AP#write memory

```

2. 액세스 포인트는 인증 서버에서 AAA 클라이언트로 구성해야 합니다. 예를 들어, Cisco Secure ACS에서는 액세스 포인트 이름, IP 주소, 공유 암호 및 인증 방법(RADIUS Cisco Aironet 또는 RADIUS Cisco IOS/PIX)이 정의된 [Network Configuration](#) 페이지에서 이러한 현상이 발생합니다. 다른 비 ACS 인증 서버에 대해서는 제조업체의 설명서를 참조하십시오




인증 서버가 원하는 EAP 인증 방법을 수행하도록 구성되어 있는지 확인합니다. 예를 들어, LEAP를 수행하는 Cisco Secure ACS의 경우 [System Configuration - Global Authentication Setup](#) 페이지에서 LEAP 인증을 구성합니다. System Configuration(시스템 컨피그레이션)을 클릭한 다음 [Global Authentication Setup\(전역 인증 설정\)](#)을 클릭합니다. 다른 비 ACS 인증 서버 또는 기타 EAP 방법은 제조업체의 설명서를 참조하십시오

**CISCO SYSTEMS** **System Configuration**

Select	Help
<ul style="list-style-type: none"> <li>User Setup</li> <li>Group Setup</li> <li>Shared Profile Components</li> <li>Network Configuration</li> <li>System Configuration</li> <li>Interface Configuration</li> <li>Administration Control</li> <li>External User Databases</li> <li>Reports and Activity</li> <li>Online Documentation</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">Service Control</a></li> <li><a href="#">Logging</a></li> <li><a href="#">Date Format Control</a></li> <li><a href="#">Local Password Management</a></li> <li><a href="#">CiscoSecure Database Replication</a></li> <li><a href="#">ACS Backup</a></li> <li><a href="#">ACS Restore</a></li> <li><a href="#">ACS Service Management</a></li> <li><a href="#">IP Pools Server</a></li> <li><a href="#">IP Pools Address Recovery</a></li> <li><a href="#">ACS Certificate Setup</a></li> <li><a href="#">Global Authentication Setup</a></li> </ul> <p style="text-align: center;"><a href="#">Back to Help</a></p>
	<ul style="list-style-type: none"> <li>• <a href="#">Service Control</a></li> <li>• <a href="#">Logging</a></li> <li>• <a href="#">Date Format Control</a></li> <li>• <a href="#">Local Password Management</a></li> <li>• <a href="#">CiscoSecure Database Replication</a></li> <li>• <a href="#">RDBMS Synchronization</a></li> <li>• <a href="#">ACS Backup</a></li> <li>• <a href="#">ACS Restore</a></li> <li>• <a href="#">ACS Service Management</a></li> <li>• <a href="#">IP Pools Address Recovery</a></li> <li>• <a href="#">IP Pools Server</a></li> <li>• <a href="#">VoIP Accounting Configuration</a></li> <li>• <a href="#">ACS Certificate Setup</a></li> <li>• <a href="#">Global Authentication Configuration</a></li> </ul> <hr/> <p><b>Service Control</b></p> <p>Select to open the page from which you can stop or restart Cisco Secure ACS services.</p> <p><a href="#">[Back to Top]</a></p>

이 이미지는 PEAP, EAP-FAST, EAP-TLS, LEAP 및 EAP-MD5에 대해 구성된 Cisco Secure ACS를 보여줍니다



# System Configuration

Edit

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

## Global Authentication Setup

**EAP Configuration** ?

**PEAP**

Allow EAP-MSCHAPv2

Allow EAP-GTC

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

---

**EAP-FAST**

Allow EAP-FAST

Active master key TTL:  months

Retired master key TTL:  months

PAC TTL:  weeks

Client initial message:

Authority ID Info:

Allow automatic PAC provisioning:

EAP-FAST master server:

Actual EAP-FAST server status: **Master**

---

**EAP-TLS**

Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

---

**LEAP**

Allow LEAP (For Aironet only)

---

**EAP-MD5**

Allow EAP-MD5

AP EAP request timeout (seconds):

---

**MS-CHAP Configuration** ?

Allow MS-CHAP Version 1 Authentication

Allow MS-CHAP Version 2 Authentication

### Help

- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP EAP request timeout](#)
- [MS-CHAP Configuration](#)

This page specifies settings for various authentication protocols.

[\[Back to Top\]](#)

**PEAP**

*Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have*

? Back to Help

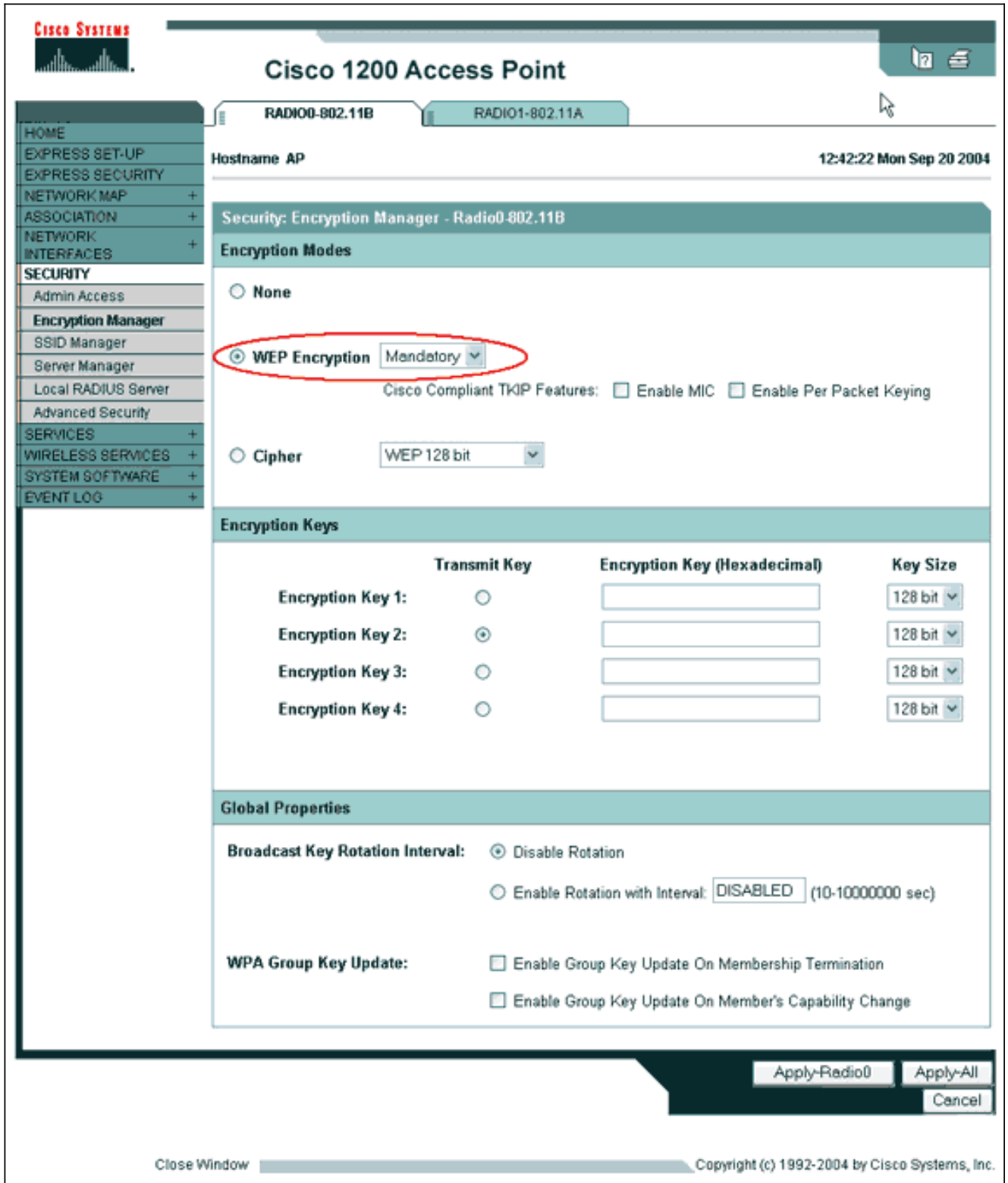
Submit
Submit + Restart
Cancel

[클라이언트 인증 방법 정의](#)

액세스 포인트가 클라이언트 인증 요청을 보낼 위치를 알게 되면 해당 방법을 허용하도록 구성합니다.

**참고:** 이러한 지침은 WEP 기반 설치를 위한 것입니다. WEP 대신 암호를 사용하는 WPA의 경우 [WPA 구성 개요](#)를 참조하십시오.

1. 액세스 포인트 암호화 관리자 탭(보안 > 암호화 관리자 메뉴 항목 아래)에서 다음 단계를 완료합니다. **WEP 암호화**를 사용하도록 지정합니다. **WEP가 필수임을 지정합니다**. 키 크기가 **128비트**로 설정되어 있는지 **확인합니다**. **Apply**를 클릭합니다



CLI에서 다음 명령을 실행할 수도 있습니다.

```
AP#configure terminal
```



Enter configuration commands, one per line. End with CNTL/Z.

```
AP(config)#interface dot11radio 0
```

```
AP(config-if)#encryption mode wep mandatory
```

```
AP(config-if)#end
```

```
AP#write memory
```

2. 액세스 포인트 SSID Manager 탭(**Security(보안)**) > **SSID Manager(SSID 관리자)** 메뉴 항목 아래에서 다음 단계를 완료합니다.원하는 SSID를 선택합니다."Authentication Methods Accepted(인증 방법 수락)" 아래에서 **Open(열기)** 확인란을 선택하고 드롭다운 목록을 사용하여 EAP를 선택합니다.Cisco 클라이언트 카드가 있는 경우 **Network-EAP**라는 상자를 선택합니다. 네트워크 EAP 또는 EAP를 통한 인증 열기 섹션의 토론을 참조하십시오.Apply를 클릭합니다.

RADIO0-802.11B

RADIO1-802.11A

Hostname AP

12:47:46 Mon Sep 20 2004

- HOME
- EXPRESS SET-UP
- EXPRESS SECURITY
- NETWORK MAP +
- ASSOCIATION +
- NETWORK INTERFACES +
- SECURITY**
- Admin Access
- Encryption Manager
- SSID Manager**
- Server Manager
- Local RADIUS Server
- Advanced Security
- SERVICES +
- WIRELESS SERVICES +
- SYSTEM SOFTWARE +
- EVENT LOG +

## Security: SSID Manager - Radio0-802.11B

### SSID Properties

#### Current SSID List

< NEW >
labap1200

**SSID:**

**VLAN:**  [Define VLANs](#)

**Network ID:**  (0-4096)

Delete-Radio0

Delete-All

### Authentication Settings

#### Methods Accepted:

Open Authentication:

Shared Authentication:

Network EAP:

#### Server Priorities:

##### EAP Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

##### MAC Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

Portions of this image not relevant to the discussion have been edited for clarity

### Global Radio0-802.11B SSID Properties

**Set Guest Mode SSID:**

**Set Infrastructure SSID:**   Force Infrastructure Devices to associate only to this SSID

Apply

Cancel

CLI에서 다음 명령을 실행할 수도 있습니다.

```
AP#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
AP(config)#interface dot11radio 0
```

```
AP(config-if)#ssid labap1200
```

```
AP(config-if-ssid)#authentication open eap eap_methods
```

```
AP(config-if-ssid)#authentication network-eap eap_methods
```

```
AP(config-if-ssid)#end
```

```
AP#write memory
```

기본 EAP 컨피그레이션으로 기본 기능을 확인하면 나중에 추가 기능 및 키 관리를 추가할 수 있습니다. 더 복잡한 기능을 기능 기반 위에 계층화하여 문제 해결을 더 쉽게 합니다.

## 다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show** 명령은 [출력 인터프리터 틀](#)에서 지원되는데(등록된 고객만), 이 틀을 사용하면 **show** 명령 출력의 분석 결과를 볼 수 있습니다.

- **show radius server-group all** - AP에 구성된 모든 RADIUS 서버 그룹의 목록을 표시합니다.

## 문제 해결

### 문제 해결 절차

컨피그레이션 문제를 해결하려면 다음 단계를 완료하십시오.

1. 클라이언트 측 유틸리티 또는 소프트웨어에서 동일하거나 유사한 매개변수로 새 프로파일 또는 연결을 생성하여 클라이언트 컨피그레이션에서 손상된 것이 없도록 합니다.
2. 성공적인 인증을 방지하는 RF 문제의 가능성을 제거하려면 다음 단계와 같이 일시적으로 인증을 비활성화합니다. CLI에서 **no authentication open eap\_methods, no authentication network-eap\_methods** 및 **authentication open** 명령을 사용합니다. GUI의 SSID Manager 페이지에서 **Network-EAP**를 선택 취소하고 **Open(열기)**을 선택한 다음 드롭다운 목록을 다시 **No Additional(추가 없음)**로 설정합니다. 클라이언트가 성공적으로 연결되면 RF는 연결 문제에 기여하지 않습니다.
3. 공유 암호 암호가 액세스 포인트와 인증 서버 간에 동기화되었는지 확인합니다. 그렇지 않으면 다음 오류 메시지를 받을 수 있습니다.  
Invalid message authenticator in EAP request  
CLI에서 라인 **radius-server host x.x.x.x auth-port x acct-port x key <shared\_secret>** .GUI의 Server Manager(서버 관리자) 페이지에서 "Shared Secret(공유 암호)" 상자에 해당 서버에 대한 공유 암호를 다시 입력합니다. RADIUS 서버의 액세스 포인트에 대한 공유 암호 항목은 앞서 언급한 것과 동일한 공유 암호 암호를 포함해야 합니다.
4. RADIUS 서버에서 사용자 그룹을 제거합니다. RADIUS 서버에 의해 정의된 사용자 그룹과 기

본 도메인의 사용자 그룹 간에 충돌이 발생할 수 있습니다. RADIUS 서버의 로그에서 실패한 시도 및 실패 원인을 확인합니다.

## 문제 해결 명령

일부 show 명령은 [출력 인터프리터 툴](#)에서 지원되는데(등록된 고객만), 이 툴을 사용하면 show 명령 출력의 분석 결과를 볼 수 있습니다.

[디버깅 인증](#)은 EAP와 관련된 디버깅 출력을 수집하고 해석하는 방법에 대한 상당한 상세 정보를 제공합니다.

참고: debug 명령을 실행하기 전에 디버그 명령에 [대한 중요 정보를 참조하십시오](#).

- **debug dot11 aaa authenticator state-machine** - 클라이언트와 인증 서버 간의 협상의 주요 부서(또는 상태)를 표시합니다. 다음은 성공적인 인증의 출력입니다.

```
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client: Sending
identity request to 0040.96ac.dd05
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client:
0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.930: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,EAP_START) for 0040.96ac.dd05
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client:
Sending identity request to 0040.96ac.dd05 (client)
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client: Client
0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.938: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96ac.dd05 data (User Name) to server
*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:
Started timer server_timeout 60 seconds
*Mar 1 02:37:47.017: dot11_auth_dot1x_run_rfsm: Executing
Action(SERVER_WAIT,SERVER_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.017: dot11_auth_dot1x_send_response_to_client:
Forwarding server message(Challenge) to client 0040.96ac.dd05
*Mar 1 02:37:47.018: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 20 seconds
*Mar 1 02:37:47.025: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.025: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96ac.dd05 data(User Credentials) to server
-----Lines Omitted for simplicity-----
*Mar 1 02:37:47.030: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 20 seconds
*Mar 1 02:37:47.041: dot11_auth_dot1x_run_rfsm: Executing Action
(SERVER_WAIT,SERVER_PASS) for 0040.96ac.dd05
*Mar 1 02:37:47.041: dot11_auth_dot1x_send_response_to_client:
Forwarding server message(Pass Message) to client
0040.96ac.dd05
*Mar 1 02:37:47.042: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 30 seconds
*Mar 1 02:37:47.043: %DOT11-6-ASSOC: Interface Dot11Radio0,
Station TACWEB 0040 .96ac.dd05 Associated KEY_MGMT[NONE] (Client stays
associated to the access point)
```

참고: 12.2(15)JA 이전 Cisco IOS Software 릴리스에서는 이 debug 명령의 구문은 debug dot11 aaa dot1x state-machine입니다.

- **debug dot11 aaa authenticator process** - 클라이언트와 인증 서버 간의 협상에 대한 개별 대화

항목을 표시합니다.참고: 12.2(15)JA 이전의 Cisco IOS Software 릴리스에서는 이 debug 명령의 구문은 debug dot11 aaa dot1x process입니다.

- debug radius authentication(디버그 radius 인증) - 서버와 클라이언트 간의 RADIUS 협상을 표시합니다. 이 협상은 둘 다 AP에 의해 브리지됩니다. 실패한 인증에 대한 출력입니다.

```
*Mar 1 02:34:55.086: RADIUS/ENCODE(00000031):Orig. component type = DOT11
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: ssid [264] 5
*Mar 1 02:34:55.086: RADIUS: 73 73 69 [ssi]
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: interface [157] 3
*Mar 1 02:34:55.087: RADIUS: 32 [2]
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.087: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.087: RADIUS(00000031): sending
*Mar 1 02:34:55.087: RADIUS(00000031): Send Access-Request
to 10.0.0.3 :164 5 id 1645/61, len 130
*Mar 1 02:34:55.088: RADIUS: authenticator 0F 6D B9 57 4B A3 F2 0E -
56 77 A4 7E D3 C2 26 EB
*Mar 1 02:34:55.088: RADIUS: User-Name [1] 8 "wirels"
*Mar 1 02:34:55.088: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 02:34:55.088: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0"
*Mar 1 02:34:55.088: RADIUS: Calling-Station-Id [31] 16 "0040.96ac.dd05"
*Mar 1 02:34:55.088: RADIUS: Service-Type [6] 6 Login [1]
*Mar 1 02:34:55.088: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.089: RADIUS: 73 8C 59 C4 98 51 53 9F 58 4D 1D EB A5
4A AB 88 [s?Y??QS?XM???J??]
*Mar 1 02:34:55.089: RADIUS: EAP-Message [79] 13
*Mar 1 02:34:55.089: RADIUS: NAS-Port-Id [87] 5 "299"
*Mar 1 02:34:55.090: RADIUS: NAS-IP-Address [4] 6 10.0.0.106
*Mar 1 02:34:55.090: RADIUS: Nas-Identifier [32] 4 "ap"
*Mar 1 02:34:55.093: RADIUS: Received from id 1645/61
10.0.0.3 :1645, Access-Challenge, len 79
*Mar 1 02:34:55.093: RADIUS: authenticator 72 FD C6 9F A1 53 8F D2 -
84 87 49 9B B4 77 B8 973
-----Lines Omitted-----
*Mar 1 02:34:55.117: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.118: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS(00000031): sending
*Mar 1 02:34:55.118: RADIUS(00000031): Send Access-Request to
10.0.0.3 :164 5 id 1645/62, len 168
*Mar 1 02:34:55.118: RADIUS: authenticator 49 AE 42 83 C0 E9 9A A7 -
07 0F 4E 7C F4 C7 1F 24
*Mar 1 02:34:55.118: RADIUS: User-Name [1] 8 "wirels"
*Mar 1 02:34:55.119: RADIUS: Framed-MTU [12] 6 1400
-----Lines Omitted-----
*Mar 1 02:34:55.124: RADIUS: Received from id 1645/62
10.0.0.3 :1645, Access-Reject, len 56
*Mar 1 02:34:55.124: RADIUS: authenticator A6 13 99 32 2A 9D A6 25 -
AD 01 26 11 9A F6 01 37
*Mar 1 02:34:55.125: RADIUS: EAP-Message [79] 6
*Mar 1 02:34:55.125: RADIUS: 04 15 00 04 [????]
*Mar 1 02:34:55.125: RADIUS: Reply-Message [18] 12
*Mar 1 02:34:55.125: RADIUS: 52 65 6A 65 63 74 65 64 0A 0D
[Rejected??]
*Mar 1 02:34:55.125: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.126: RADIUS(00000031): Received from id 1645/62
*Mar 1 02:34:55.126: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
*Mar 1 02:34:55.126: RADIUS/DECODE: Reply-Message fragments, 10, total 10 bytes
*Mar 1 02:34:55.127: %DOT11-7-AUTH_FAILED: Station
0040.96ac.dd05 Authentication failed
```

- debug aaa authentication—클라이언트 디바이스와 인증 서버 간의 인증에 대한 AAA 협상을

표시합니다.

## 관련 정보

- [디버그 인증](#)
- [인증 유형 구성](#)
- [로컬 RADIUS 서버의 LEAP 인증](#)
- [RADIUS 및 TACACS+ 서버 구성](#)
- [PEAP-MS-CHAPv2 머신 인증을 사용하여 Windows v3.2용 Cisco Secure ACS 구성](#)
- [EAP-TLS 머신 인증을 사용하는 Windows v3.2용 Cisco Secure ACS](#)
- [Microsoft IAS에서 PEAP/EAP 구성](#)
- [RADIUS 서버로 Microsoft IAS 문제 해결](#)
- [Microsoft 802.1X 인증 클라이언트](#)
- [기술 지원 및 문서 - Cisco Systems](#)