ACKSYS
COMMUNICATIONS & SYSTEMS

APPLICATION NOTE

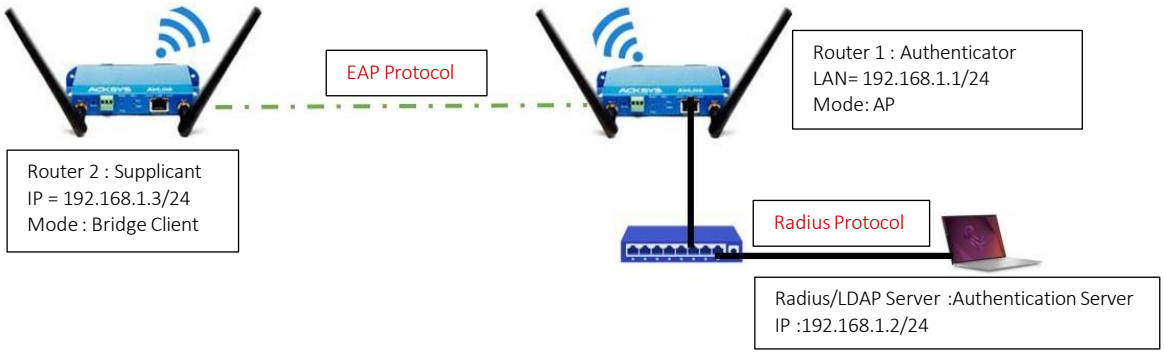
WaveOS 제품을 통한 Radius 보안 서버 설정

WaveOS 제품을 통한 Radius 보안 서버 설정

Introduction

Radius 는 Remote Authentication Dial In User Service 의 약자로, 사용자의 인증, 계정 및 권한 부여에 사용되는 중앙 집중 보안 서버입니다.

ACKSYS 라우터는 RADIUS Server 와 호환되는 RADIUS Client 로 설정할 수 있습니다. EAP 와 같은 RADIUS 인증 프로토콜을 통해 Wi-Fi, VPN 및 기타 응용 프로그램에 연결하여 사용자 연결을 허용하거나 거부할 수 있습니다.



Radius Server Configuration and requirements

WPA2-Enterprise 의 설정 요구 사항은 다음과 같습니다:

- 서버는 네트워크에서 Client 가 신뢰하는 CA(Certificate Authority)의 인증서를 호스팅해야 합니다.
- WPA2-Enterprise SSID 를 브로드 캐스트 하는 모든 AccessPoint 는 공유된 보안 값을 가진 RADIUS Server 에서 RADIUS Client 또는 인증자로 설정되어야 합니다.
- RADIUS 서버에는 인증할 사용자 기반 또는 Ldap 서버가 있어야 합니다.
- RADIUS 서버는 Wi-Fi Client와 동일한 EAP 인증을 지원해야 합니다.(예: 테스트용 PEAPv2)

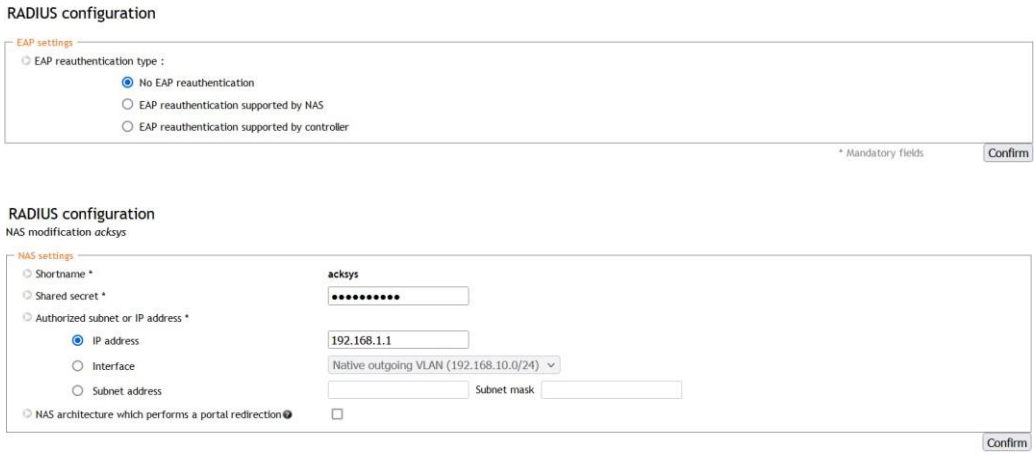
WaveOS 제품을 통한 Radius 보안 서버 설정

Radius Client(인증자) AP 추가

RADIUS 인증 서버를 사용하도록 설정하기 전에 RADIUS 서버에 대한 다음 정보가 있어야 합니다 :
(예시)

- **Shortname** — NAS를 식별할 이름(사용자 지정 이름 사용)
- **An external RADIUS server** — 192.168.1.2 (IP 주소 및 RADIUS 포트)
- **Shared secret** — acksys(대소문자 구분 암호)
- **Authentication methods** — 장치에서 사용하는 인증 방법을 허용하도록 RADIUS 서버를 설정합니다. 예: WPA2 Enterprise
- **Authorized subnet or IP address** — Radius 서버에 접속하도록 승인된 인증자 IP 주소

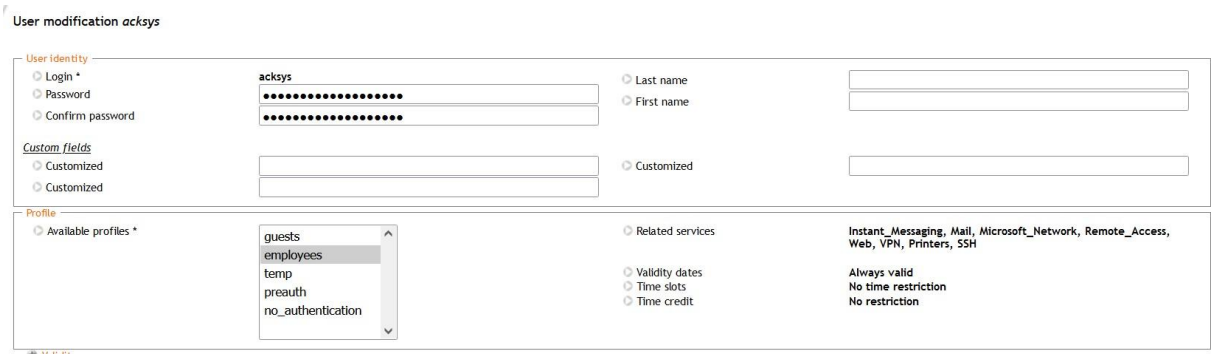
Radius Server 설정 예시:



Radius 서버에 사용자 추가

Ldap 서버는 Radius 서버에 내장되어 있으며 별도의 외부 Ldap 서버를 생성할 필요가 없습니다.

- **User Database**
  - User Database 에는 RADIUS 서버가 사용자에 대한 인증 및 권한 부여를 수행하는 데 필요한 자격 증명과 사용자 정보가 포함되어 있습니다..



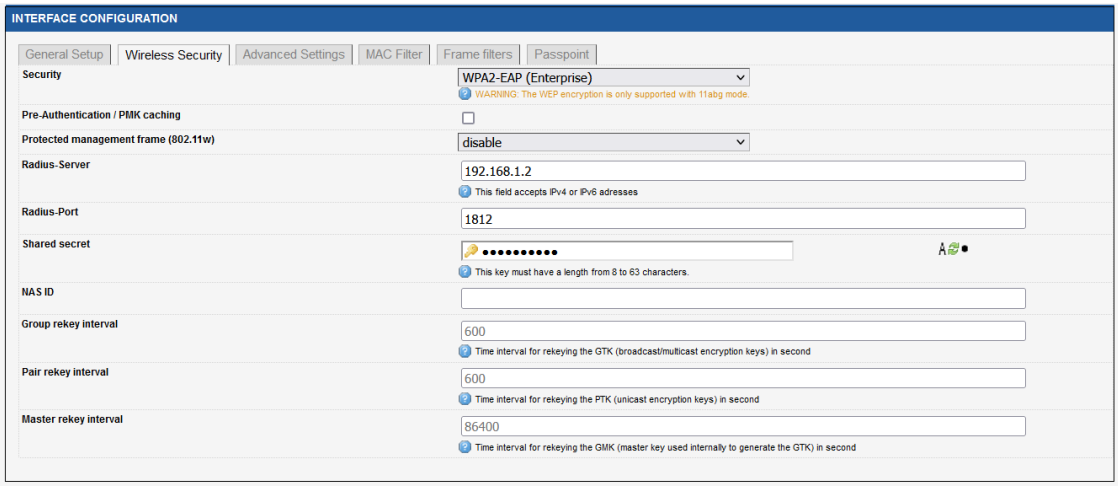
WaveOS 제품을 통한 Radius 보안 서버 설정

ACKSYS Router configuration

모든 Acksys 라우터는 인증자 및 신청자로서 Radius 서버와 호환되지만 무선 클라이언트 인증을 담당하지는 않습니다. AP는 클라이언트와 RADIUS 서버 사이의 중개자 역할만 합니다.

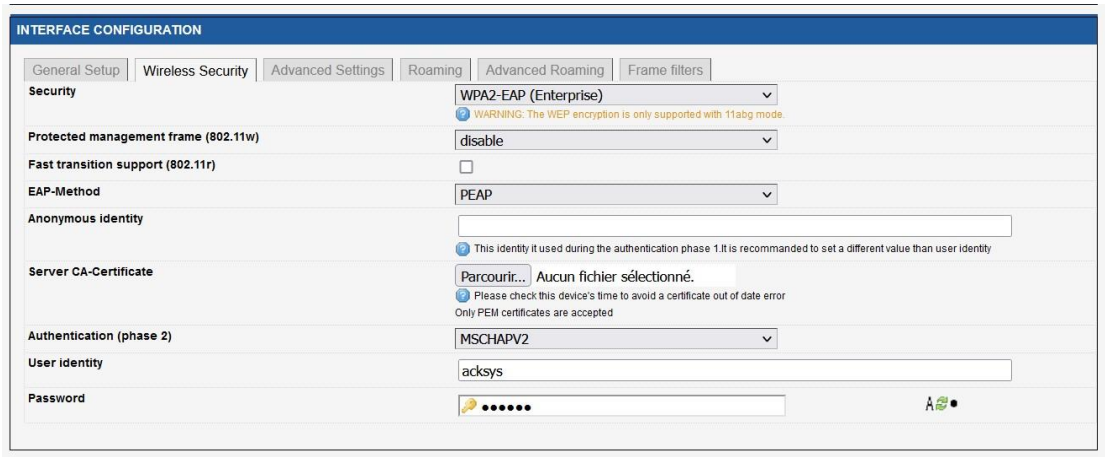
AccessPoint 모드일 경우의 설정 예시

- Wireless Security
  - WPA2-EAP (Enterprise)
  - Radius Server: 192.168.1.2
  - Radius-Port: 1812
  - Shared secret: Radius 서버와 동일한 암호 사용



Client 모드일 경우의 설정 예시

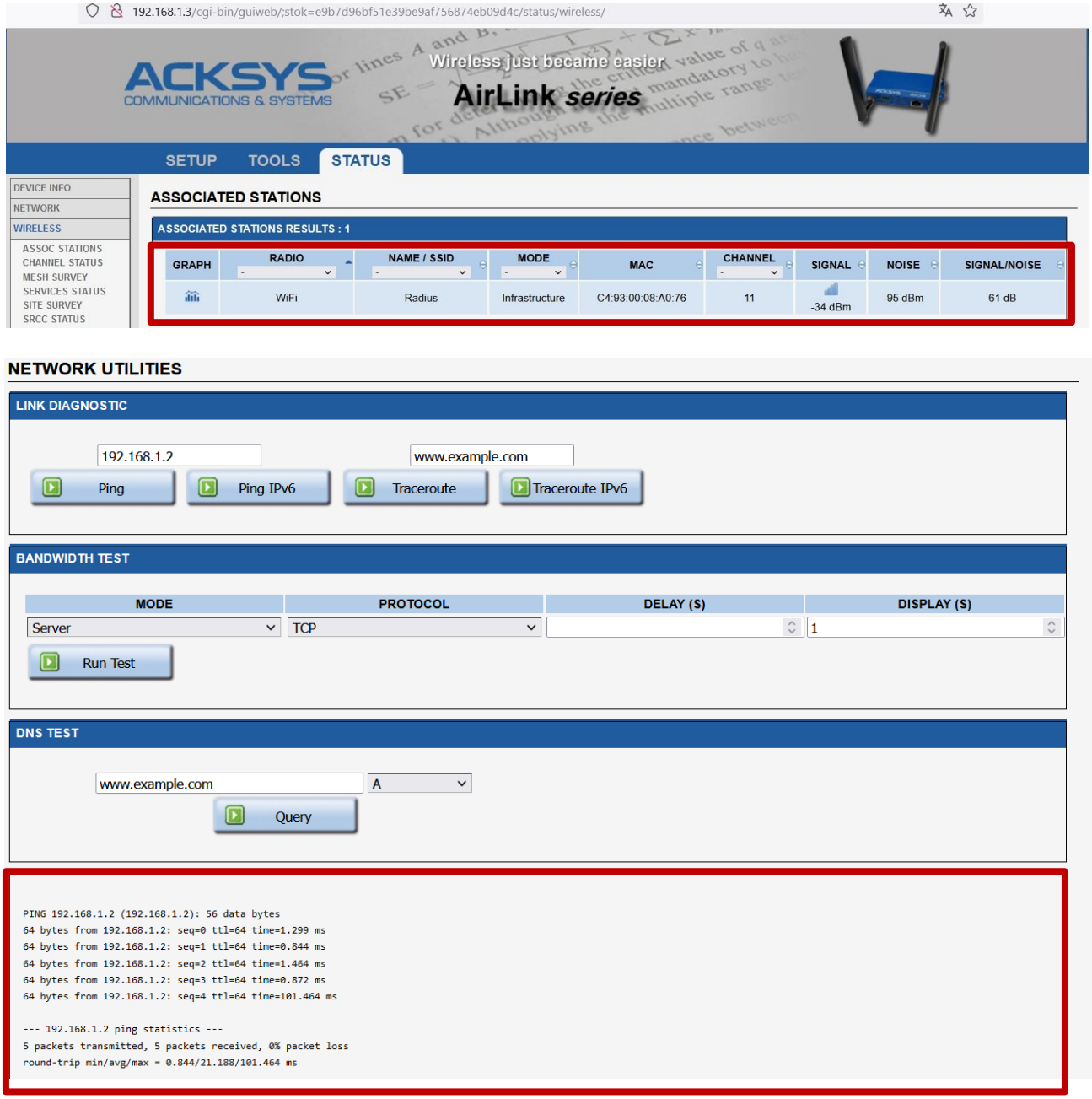
- Wireless Security
  - WPA2-EAP (Enterprise)
  - EAP-Method: PEAP
  - Server CA-Certificate: Radius 서버에서 .pem 인증서 가져오기
  - Authentication phase2: MSCHAPv2
  - User identity: acksys
  - Password: acksys



WaveOS 제품을 통한 Radius 보안 서버 설정

TESTING

웹 인터페이스 – Wireless 탭



Radius 서버에 대한 Supplicant의 IP 가 연결되어 User가 Radius 서버에서 인증되었음을 표시합니다.

WaveOS 제품을 통한 Radius 보안 서버 설정

```
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: RX EAPOL - hexdump(len=47): 02 00 00 2b 01 0b 00 2b 19 00 17 03 01 00 20 48 dc 57 af f
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: Received EAP-Packet frame
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: SUPP_BE entering state REQUEST
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: getSuppRsp
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: EAP entering state RECEIVED
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: Received EAP-Request id=11 method=25 vendor=0 vendorMethod=0
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: EAP entering state METHOD
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: SSL: Received packet(len=43) - Flags 0x00
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-PEAP: received 37 bytes encrypted data for Phase 2
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: OpenSSL: RX ver=0x0 content_type=256 (TLS header info/)
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: OpenSSL: Message - hexdump(len=5): [REMOVED]
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-PEAP: Decrypted Phase 2 EAP - hexdump(len=11): 01 0b 00 0b 21 80 03 00 02 00 01
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-PEAP: received Phase 2: code=1 identifier=11 length=11
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-PEAP: Phase 2 Request: type=33
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-TLV: Received TLVs - hexdump(len=6): 80 03 00 02 00 01
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-TLV: Result TLV - hexdump(len=2): 00 01
Wed Jan 24 15:48:45 2024 daemon.notice wpa_supplicant[7426]: EAP-TLV: TLV Result - Success - EAP-TLV/Phase2 Completed
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-PEAP: Encrypting Phase 2 data - hexdump(len=11): [REMOVED]
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: OpenSSL: TX ver=0x0 content_type=256 (TLS header info/)
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: OpenSSL: Message - hexdump(len=5): [REMOVED]
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: OpenSSL: TX ver=0x0 content_type=256 (TLS header info/)
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: OpenSSL: Message - hexdump(len=5): [REMOVED]
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: SSL: 74 bytes left to be sent out (of total 74 bytes)
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: method process -> ignore=FALSE methodState=DONE decision=UNCOND_SUCC eapRespData=
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: Session-Id - hexdump(len=65): 19 7a 2a 96 a6 64 84 fd 3f ea 5f f7 e3 a2 0f 44 2b
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: EAP entering state SEND_RESPONSE
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: EAP entering state IDLE
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: SUPP_BE entering state RESPONSE
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: txSuppRsp
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: TX EAPOL: dst=c4:93:00:08:a0:76
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: TX EAPOL - hexdump(len=84): 01 00 00 50 02 0b 00 50 19 00 17 03 01 00 20 c4 a8 49 da 4
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: nl80211: Send over control port dest=c4:93:00:08:a0:76 proto=0x888e len=84 no_encrypt=
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: SUPP_BE entering state RECEIVE
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: startWhen --> 0
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: l2_packet_receive: src=c4:93:00:08:a0:76 len=22
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: wlan0: RX EAPOL from c4:93:00:08:a0:76 to c4:93:00:0c:3c:85 (bridge)
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: wlan0: RX EAPOL from c4:93:00:08:a0:76
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: RX EAPOL - hexdump(len=8): 02 00 00 04 03 0b 00 04
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: Received EAP-Packet frame
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: SUPP_BE entering state REQUEST
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: getSuppRsp
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: EAP entering state RECEIVED
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: Received EAP-Success
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: Status notification: completion (param=success)
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: EAP entering state SUCCESS
Wed Jan 24 15:48:45 2024 daemon.notice wpa_supplicant[7426]: wlan0: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: SUPP_BE entering state RECEIVE
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: SUPP_BE entering state SUCCESS
```

웹 인터페이스 접속 후 Status → Logs 로 이동하여 Radius log 를 검색하여 인증 로그를 확인할 수 있습니다.

```
Tue Feb  6 17:51:44 2024
        Packet-Type = Access-Accept
                Ldap-Id = "1"
                validitytype = "inherited"
                ProfileId = "3"
                Role = "3"
        Filter-Id = "3"
                Group = "3"
                Ldap-Id = "1"
                validitytype = "inherited"
                ProfileId = "3"
        Ruckus-Role = "3"
        Filter-Id = "3"
                Group = "3"
        User-Name = "acksys"
        MS-MPPE-Recv-Key = 0x8b921471761ef11dcf26d99f2f1f03fc87ac563f22729ac19f0017251bf86392
        MS-MPPE-Send-Key = 0xdb5b0f7f7b793a1795f3fa413ddfe8d88027e8c9469ad1eceed31eee043aa32d
        EAP-MSK = 0x8b921471761ef11dcf26d99f2f1f03fc87ac563f22729ac19f0017251bf86392db5b0f7f7b793a1795f3fa413ddfe8d88027e8c9469ad1eceed31eee043aa32d
        EAP-EMSK = 0x7bde907caf149ba71ae64b82b02d3b7b9a347fd76dec92d6cc70492502c04424cfa51557dfdad2c8582321eba9ced40a3fc9d6a43814f8eb0944a0e71d4afbdc
        EAP-Message = 0x030b0004
        Message-Authenticator = 0x00000000000000000000000000000000
```

```
Tue Feb  6 17:51:44 2024
        Packet-Type = Access-Request
        User-Name = "acksys"
        Called-Station-Id = "C4-93-00-08-A0-76:Radius"
        NAS-Port-Type = Wireless-802.11
        Service-Type = Framed-User
        NAS-Port = 1
        Calling-Station-Id = "C4-93-00-0C-3C-85"
        Connect-Info = "CONNECT 54Mbps 802.11g"
        Acct-Session-Id = "FF75B9DF1CE229F8"
        X-Ascend-Home-Agent-UDP-Port = 1027076
        X-Ascend-Multilink-ID = 1027076
        X-Ascend-Num-In-Multilink = 1027073
        Framed-MTU = 1400
        EAP-Message = 0x020b00501900170301002 0c4a849da45cf7516e7b779f57ad501d30bc023c33b7562c8340f9bf8109fc9f21703010020 1872ae8588cd6076582969379ba4ab3fe895f30fef7ec2175ae7560cc77deadc
        State = 0x22c15a072bca43a5acc4742b1618ed6a
        Message-Authenticator = 0xe89a2f251f8d74059ffd3fbc2ee354cc
        NAS-IP-Address = 192.168.1.1
```

Radius 서버에서 인증 세부 정보 로그 및 응답 로그를 확인합니다.