Converged Access 5760, 3850 및 3650 Series WLC EAP-FAST with Internal RADIUS Server Configuration 예

목차

소개

이 문서에서는 클라이언트 인증을 위해 Cisco Extensible Authentication Protocol-Flexible Authentication via Secure Protocol(이 예에서 EAP-FAST)을 수행하는 RADIUS 서버 역할을 하기 위해 Cisco Converged Access 5760, 3850 및 3650 Series WLC(Wireless LAN Controller)를 구성하는 방법에 대해 설명합니다.

일반적으로 외부 RADIUS 서버는 사용자를 인증하는 데 사용되며 경우에 따라 실행 가능한 솔루션이 아닙니다.이러한 경우 Converged Access WLC는 RADIUS 서버 역할을 할 수 있습니다. WLC에 구성된 로컬 데이터베이스에 대해 사용자가 인증됩니다.이를 로컬 RADIUS 서버 기능이라고 합니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 이러한 주제에 대해 알고 있는 것이 좋습니다.

- Converged Access 5760, 3850 및 3650 Series WLC를 사용하는 Cisco IOS® GUI 또는 CLI
- EAP(Extensible Authentication Protocol) 개념
- SSID(Service Set Identifier) 컨피그레이션
- RADIUS

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 5760 Series WLC 릴리스 3.3.2(NGWC[Next Generation Wiring Closet])
- Cisco 3602 Series AP(Lightweight Access Point)
- Intel PROset 신청자가 있는 Microsoft Windows XP
- Cisco Catalyst 3560 Series 스위치

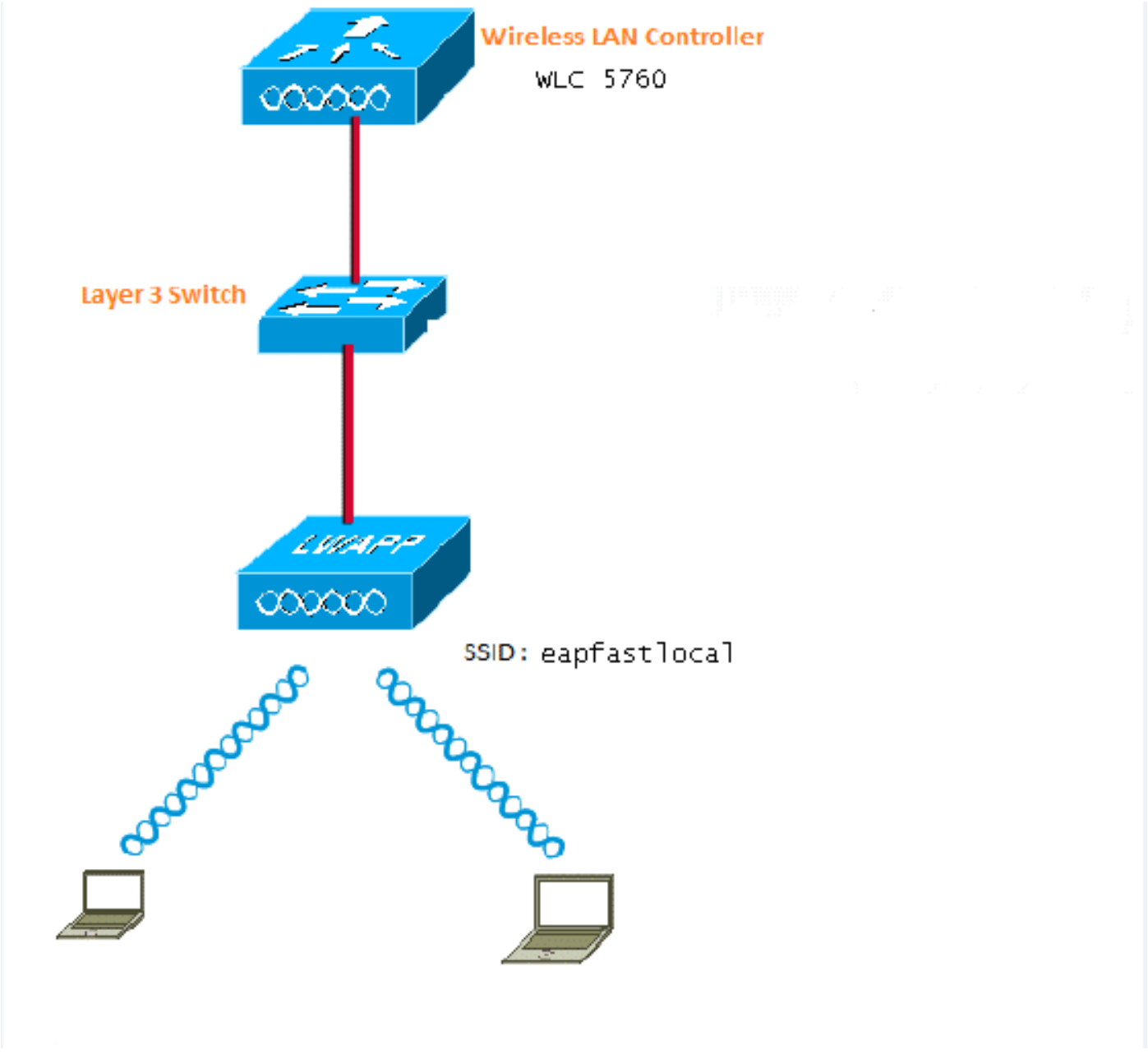
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램

이 이미지는 네트워크 다이어그램의 예를 제공합니다.



구성 개요

이 컨피그레이션은 다음 두 단계로 완료됩니다.

1. CLI 또는 GUI를 사용하여 로컬 EAP 방법 및 관련 인증 및 권한 부여 프로파일에 대한 WLC를 구성합니다.

2. WLAN을 구성하고 인증 및 권한 부여 프로필이 있는 방법 목록을 매핑합니다.

CLI로 WLC 구성

CLI로 WLC를 구성하려면 다음 단계를 완료합니다.

1. WLC에서 AAA 모델을 활성화합니다.

```
aaa new-model
```

2. 인증 및 권한 부여를 정의합니다.

```
aaa local authentication eapfast authorization eapfast

aaa authentication dot1x eapfast local
aaa authorization credential-download eapfast local
aaa authentication dot1x default local
```

3. 로컬 EAP 프로파일 및 방법(이 예에서는 EAP-FAST가 사용됨)을 구성합니다.

```
eap profile eapfast
 method fast
!
```

4. 고급 EAP-FAST 매개변수를 구성합니다.

```
eap method fast profile eapfast
 description test
 authority-id identity 1
 authority-id information 1
 local-key 0 cisco123
```

5. WLAN을 구성하고 로컬 권한 부여 프로파일을 WLAN에 매핑합니다.

```
wlan eapfastlocal 13 eapfastlocal
 client vlan VLAN0020
 local-auth eapfast
 session-timeout 1800
 no shutdown
```

6. 클라이언트 연결을 지원하도록 인프라를 구성합니다.

```
ip dhcp snooping vlan 12,20,30,40,50
ip dhcp snooping
!
```

```
ip dhcp pool vlan20
 network 20.20.20.0 255.255.255.0
 default-router 20.20.20.251
 dns-server 20.20.20.251


interface TenGigabitEthernet1/0/1
 switchport trunk native vlan 12
 switchport mode trunk
 ip dhcp relay information trusted
 ip dhcp snooping trust
```

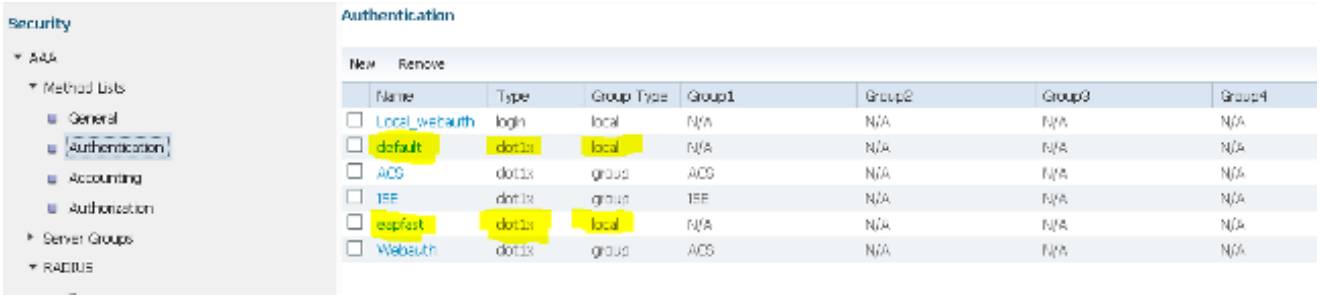
GUI를 사용하여 WLC 구성

GUI를 사용하여 WLC를 구성하려면 다음 단계를 완료합니다.

1. 인증을 위한 방법 목록을 구성합니다.

   eapfast **Type을 Dot1x로 구성합니다**.

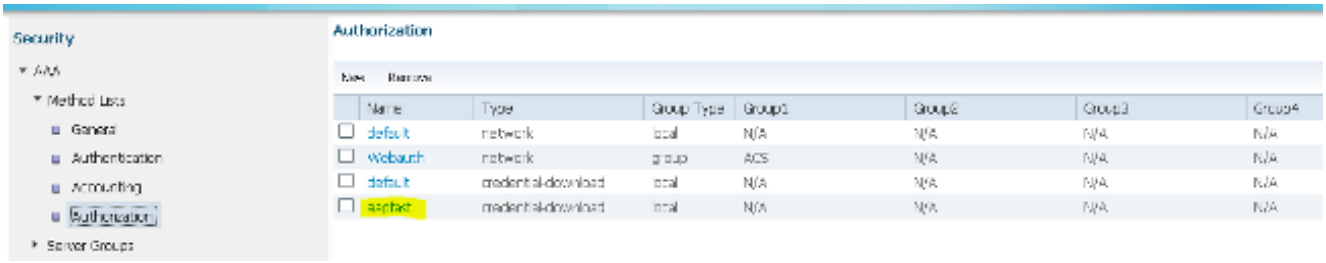
   빠른 그룹 유형**을** 로컬으로 **구성합니다**.



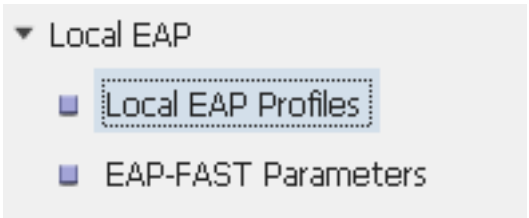
2. 권한 부여를 위한 방법 목록을 구성합니다.

   eapfast Type을 Credential-**Download로 구성합니다**.

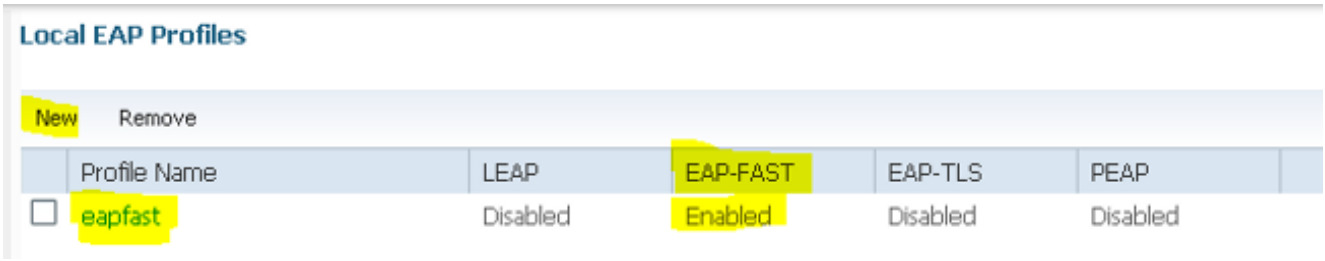
   빠른 그룹 유형**을** 로컬으로 **구성합니다**.



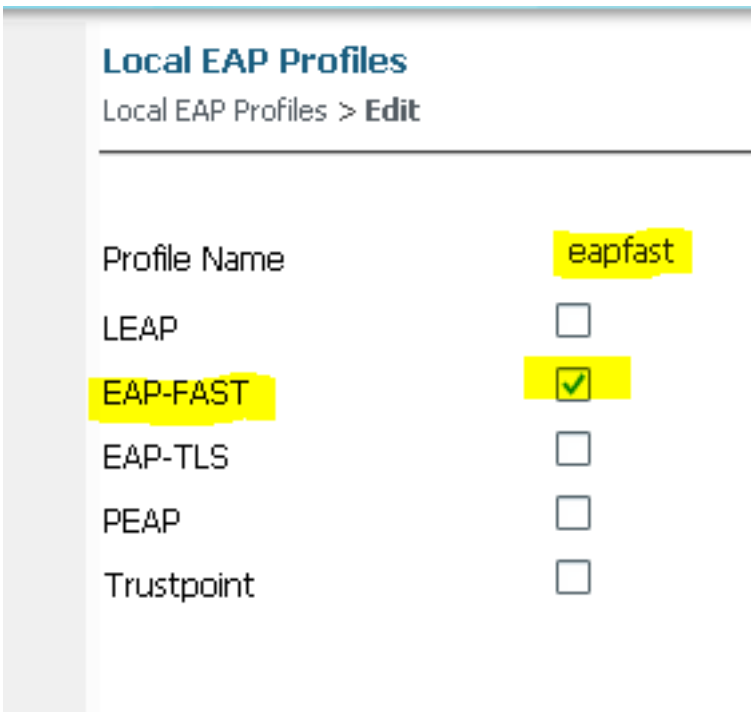
3. 로컬 EAP 프로파일을 구성합니다.



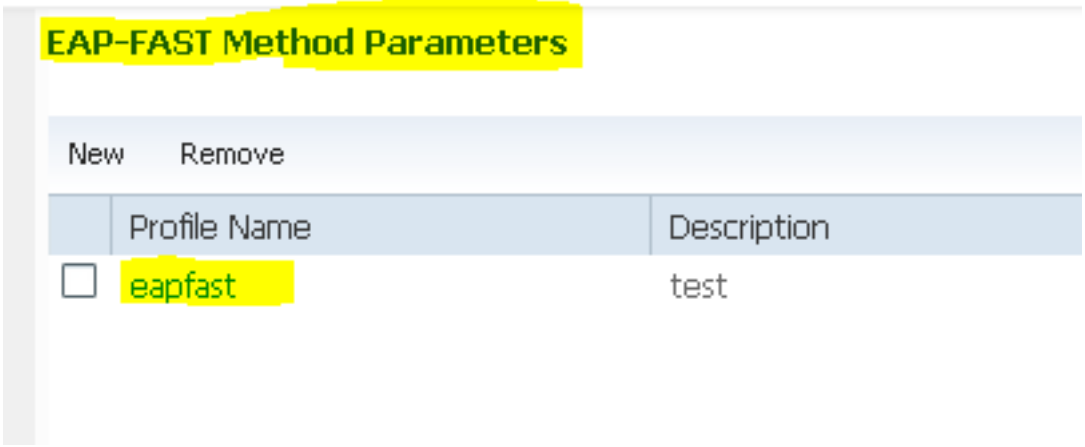
4. 새 프로필을 생성하고 EAP 유형을 선택합니다.



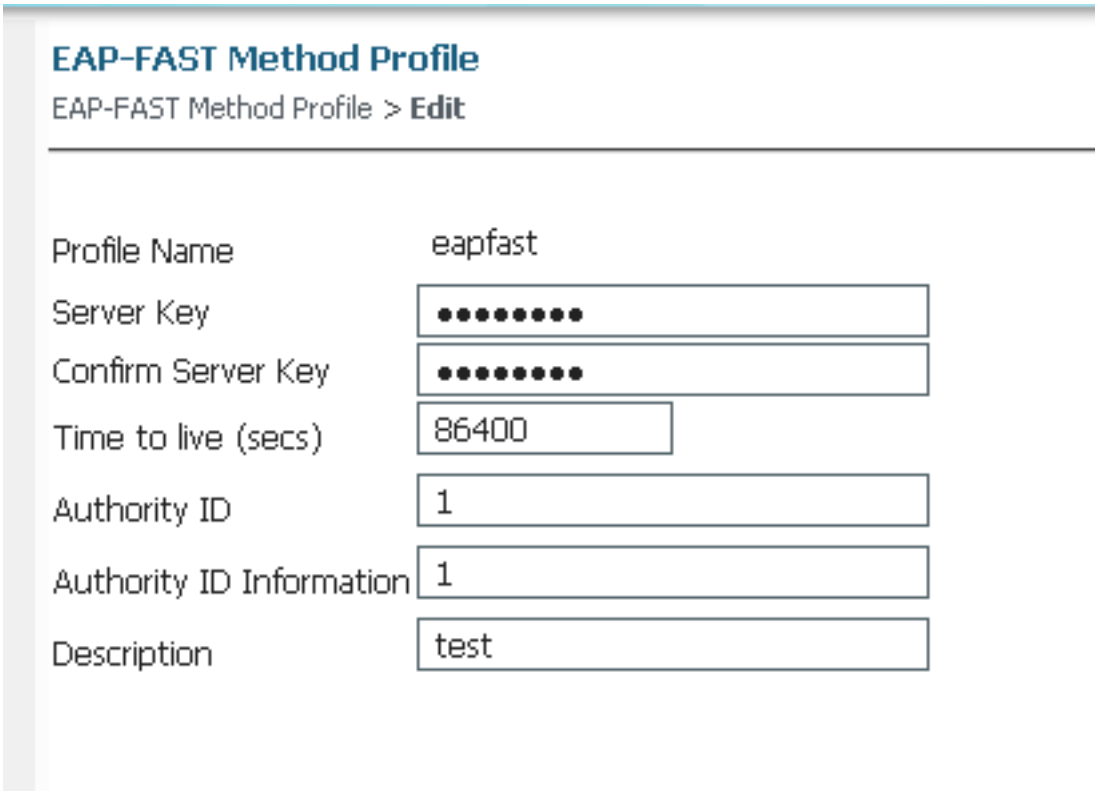
프로파일 이름이 **빠른** 경우 선택한 EAP 유형이 EAP-**FAST입니다**.



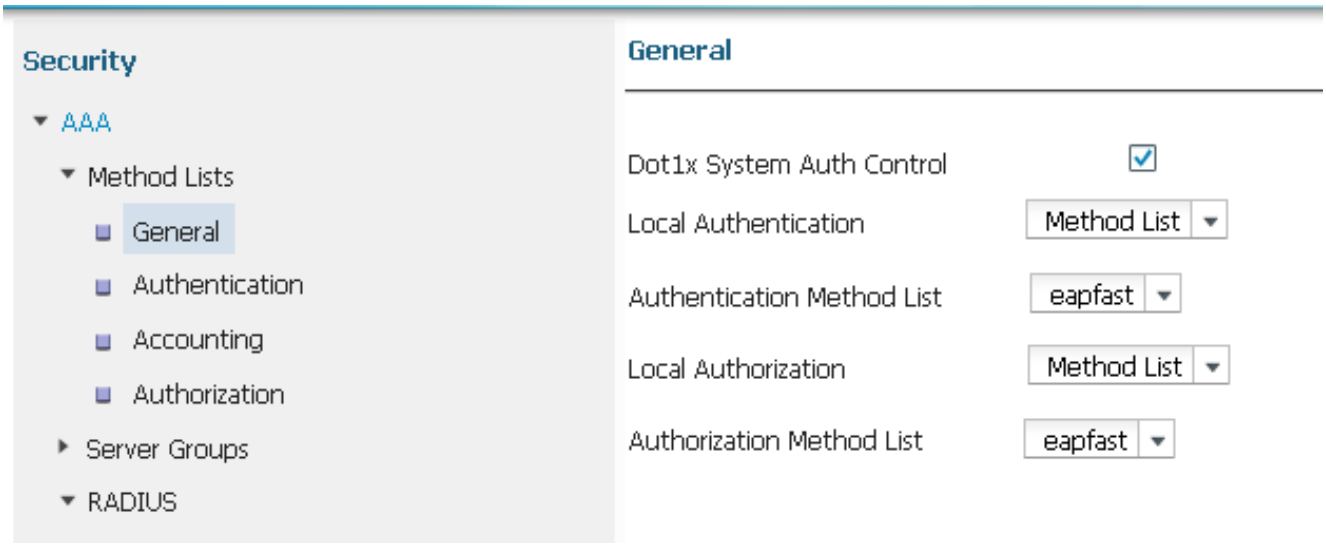
5. EAP-FAST 방법 매개변수를 구성합니다.



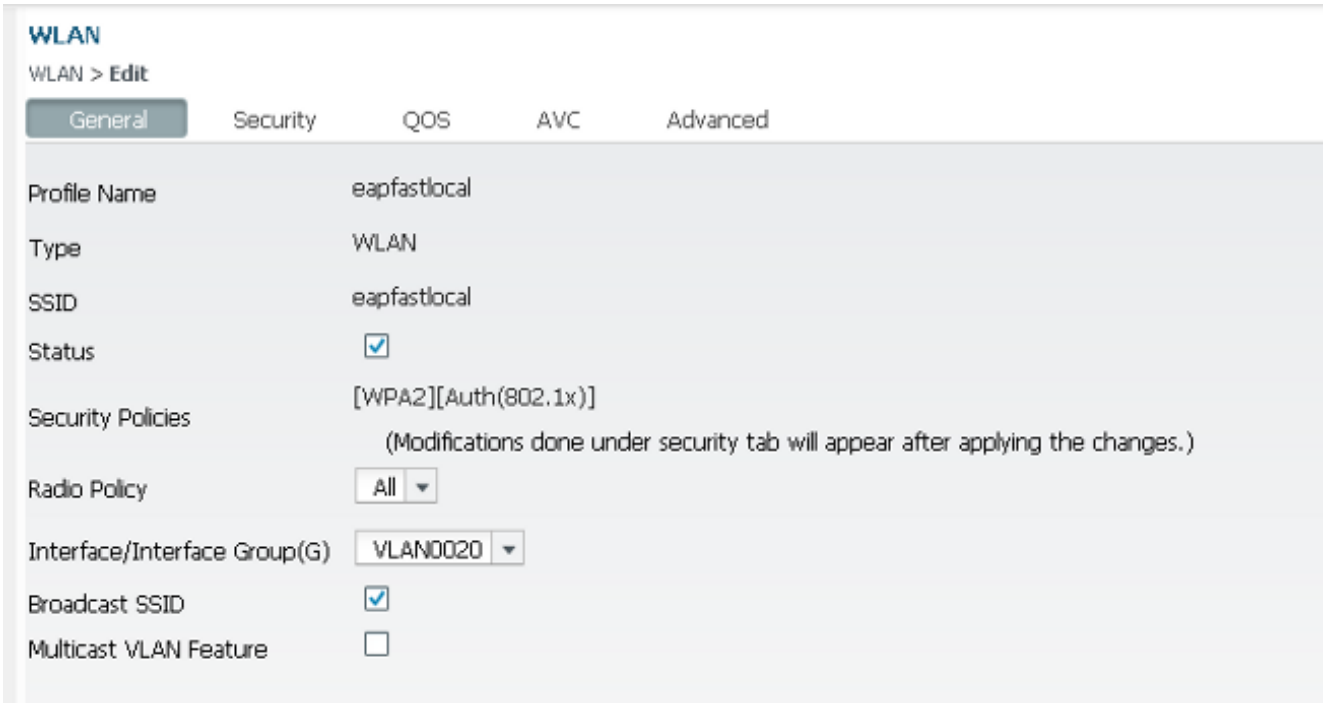
서버 키는 **Cisco123**로 **구성됩니다**.

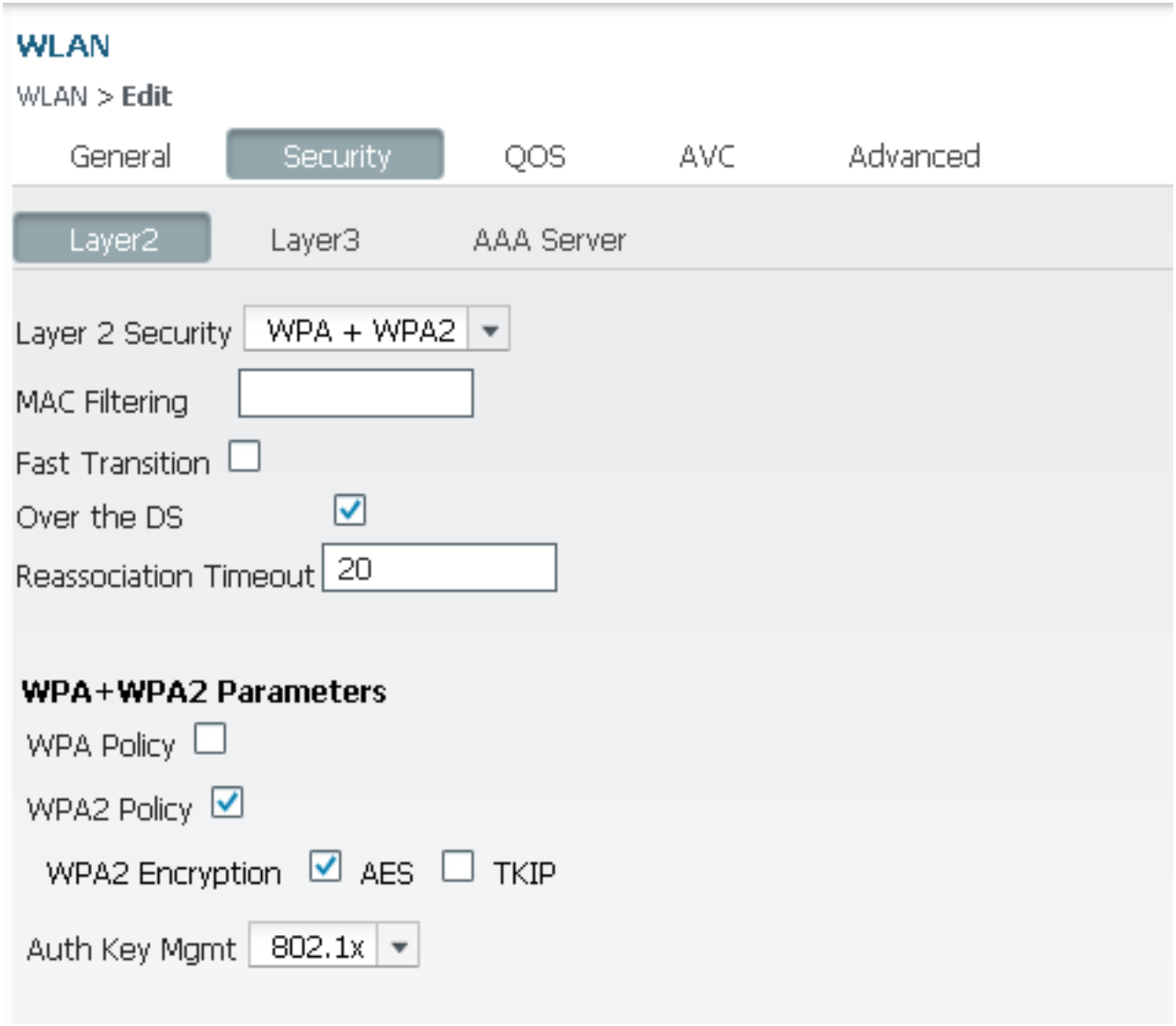


6. Dot**1x System Auth Control(Dot1x 시스템 인증 제어)** 확인란을 선택하고 Method Lists(방법 목록)에 대해 eapfast를 선택합니다.로컬 EAP 인증을 수행하는 데 도움이 됩니다.

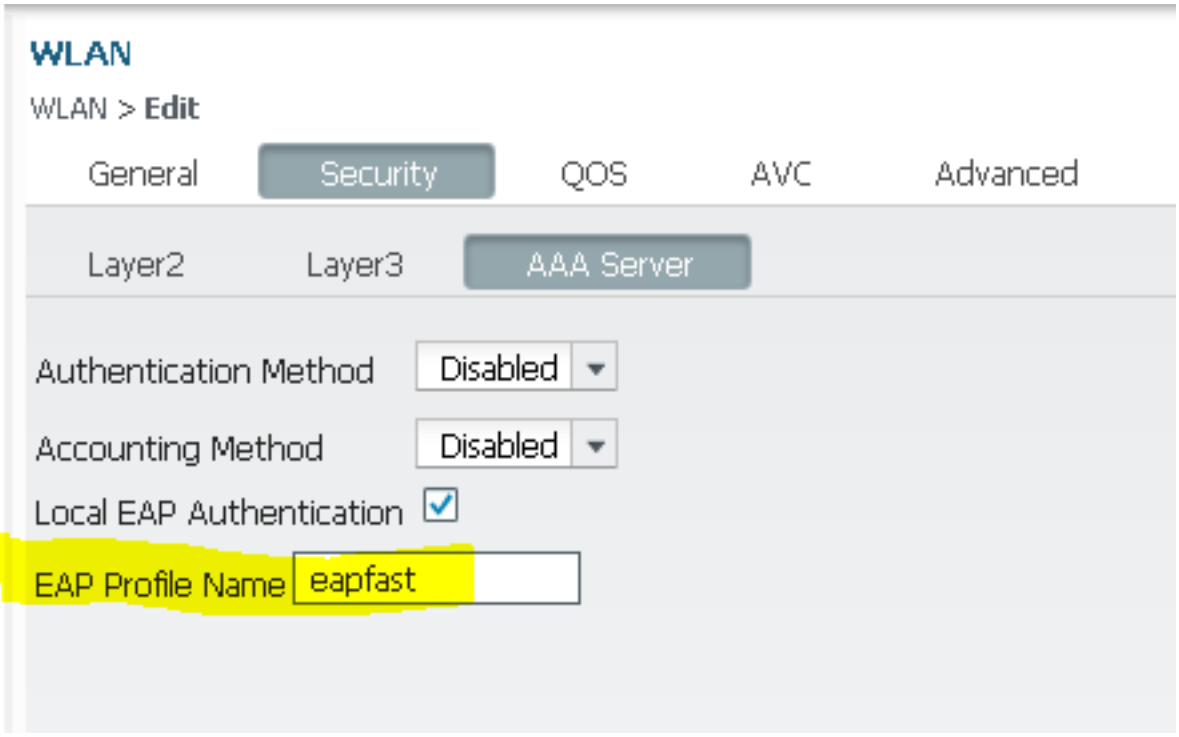


7. WPA2 AES 암호화를 위한 WLAN을 구성합니다.





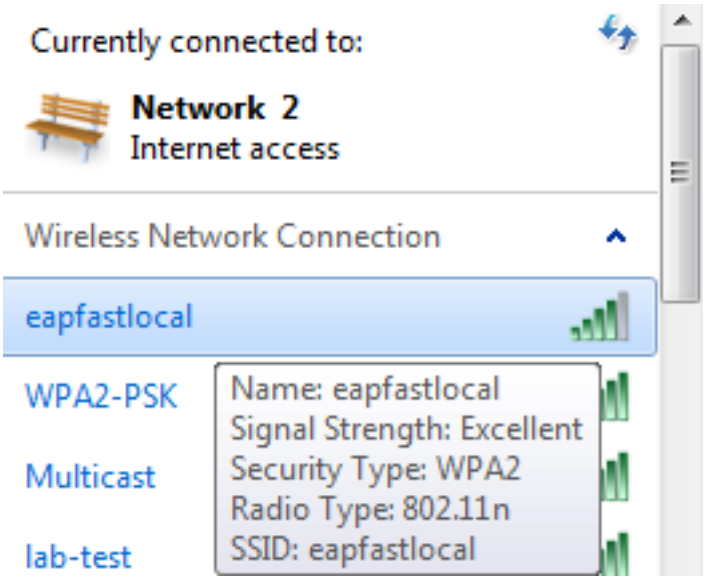
8. AAA **Server(AAA 서버)** 탭에서 EAP 프로파일 이름을 WLAN에 매핑합니다.



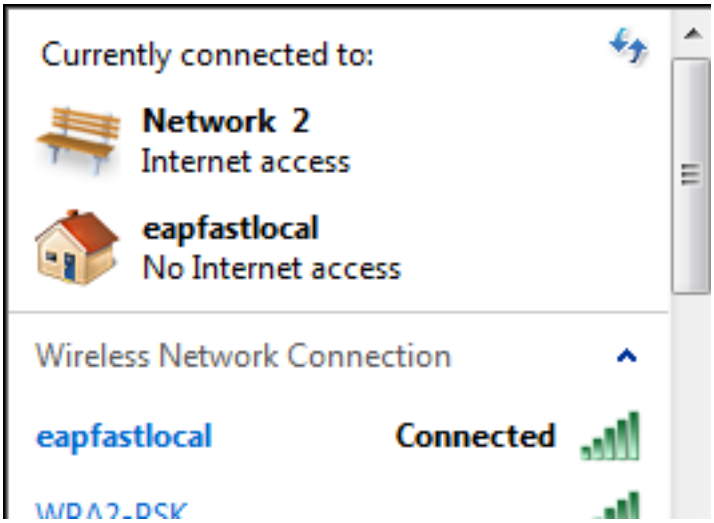
다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 다음 단계를 완료하십시오.

1. 클라이언트를 WLAN에 연결합니다.



2. PAC(Protected Access Credentials) 팝업이 나타나는지, 그리고 성공적으로 인증하려면 수락해야 하는지 확인합니다.



문제 해결

무선 문제를 해결하기 위해 추적을 사용하는 것이 좋습니다.추적은 순환 버퍼에 저장되며 프로세서 사용량이 많지 않습니다.

L2(Layer 2) 인증 로그를 얻으려면 다음 추적을 활성화합니다.

- **trace group-wireless secure level debug 설정**
- **set trace group-wireless-secure filter mac0021.6a89.51ca**

DHCP 이벤트 로그를 얻으려면 다음 추적을 활성화합니다.

- **추적 dhcp 이벤트 수준 디버그**
- **set trace dhcp events filter mac 0021.6a89.51ca**

다음은 성공적인 추적의 예입니다.

```
[04/10/14 18:49:50.719 IST 3 8116] 0021.6a89.51ca Association received from
 mobile on AP  c8f9.f983.4260

[04/10/14 18:49:50.719 IST 4 8116] 0021.6a89.51ca qos upstream policy is
 unknown and downstream policy is unknown
[04/10/14 18:49:50.719 IST 5 8116] 0021.6a89.51ca apChanged 1 wlanChanged 0
 mscb ipAddr 20.20.20.6, apf RadiusOverride 0x0, numIPv6Addr=0
[04/10/14 18:49:50.719 IST 6 8116] 0021.6a89.51ca Applying WLAN policy on MSCB.
[04/10/14 18:49:50.719 IST 7 8116] 0021.6a89.51ca Applying WLAN ACL policies
 to client

[04/10/14 18:49:50.719 IST 9 8116] 0021.6a89.51ca Applying site-specific IPv6
 override for station  0021.6a89.51ca  - vapId 13, site 'default-group',
 interface 'VLAN0020'
[04/10/14 18:49:50.719 IST a 8116] 0021.6a89.51ca Applying local bridging
 Interface Policy for station  0021.6a89.51ca  - vlan 20, interface 'VLAN0020'
[04/10/14 18:49:50.719 IST b 8116] 0021.6a89.51ca STA - rates (8):
 140 18 152 36 176 72 96 108 48 72 96 108 0 0 0 0

[04/10/14 18:49:50.727 IST 2f 8116] 0021.6a89.51ca Session Manager Call Client
```

57ca4000000048, uid 42, capwap id 50b94000000012,Flag 4, Audit-Session ID
0a6987b253468efb0000002a, method list

[04/10/14 18:49:50.727 IST 30 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.6a89.51ca, Ca3] Session update from Client[1] for 0021.6a89.51ca,
ID list 0x00000000
[04/10/14 18:49:50.727 IST 31 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.6a89.51ca, Ca3] (UPD): method: Dot1X, method list: none, aaa id:
0x0000002A
[04/10/14 18:49:50.727 IST 32 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.6a89.51ca, Ca3] (UPD): eap profile: eapfast

[04/10/14 18:49:50.728 IST 4b 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
Posting AUTH_START for 0xF700000A
[04/10/14 18:49:50.728 IST 4c 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:entering request state
[04/10/14 18:49:50.728 IST 4d 278] ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
Sending EAPOL packet
[04/10/14 18:49:50.728 IST 4e 278] ACCESS-METHOD-DOT1X-INFO:[0021.6a89.51ca,Ca3]
Platform changed src mac of EAPOL packet
[04/10/14 18:49:50.728 IST 4f 278] ACCESS-METHOD-DOT1X-INFO:[0021.6a89.51ca,Ca3]
EAPOL packet sent to client 0xF700000A
[04/10/14 18:49:50.728 IST 50 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:idle request action
[04/10/14 18:49:50.761 IST 51 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL
message (len 5) from mobile
[04/10/14 18:49:50.761 IST 52 8116] 0021.6a89.51ca 1XA: Received EAPOL-Start
from mobile
[04/10/14 18:49:50.761 IST 53 8116] 0021.6a89.51ca 1XA: EAPOL-Start -
EAPOL start message from mobile as mobile is in Authenticating state, restart
authenticating

[04/10/14 18:49:50.816 IST 95 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:entering response state
[04/10/14 18:49:50.816 IST 96 278] ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
Response sent to the server from 0xF700000A
[04/10/14 18:49:50.816 IST 97 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:ignore response action
[04/10/14 18:49:50.816 IST 98 203] Parsed CLID MAC Address = 0:33:106:137:81:202
[04/10/14 18:49:50.816 IST 99 203] AAA SRV(00000000): process authen req
[04/10/14 18:49:50.816 IST 9a 203] AAA SRV(00000000): Authen method=LOCAL

[04/10/14 18:49:50.846 IST 11d 181] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.6a89.51ca, Ca3] Session authz status notification sent to Client[1] for
0021.6a89.51ca with handle FE000052, list 630007B2
[04/10/14 18:49:50.846 IST 11e 181]ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
Received Authz Success for the client 0xF700000A (0021.6a89.51ca)
[04/10/14 18:49:50.846 IST 11f 271] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
Posting AUTHZ_SUCCESS on Client 0xF700000A
[04/10/14 18:49:50.846 IST 120 271] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:entering authenticated state
[04/10/14 18:49:50.846 IST 121 271]ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
EAPOL success packet was sent earlier.

[04/10/14 18:49:50.846 IST 149 8116] 0021.6a89.51ca 1XA:authentication succeeded
[04/10/14 18:49:50.846 IST 14a 8116] 0021.6a89.51ca 1XK: Looking for BSSID
c8f9.f983.4263 in PMKID cache
[04/10/14 18:49:50.846 IST 14b 8116] 0021.6a89.51ca 1XK: Looking for BSSID
c8f9.f983.4263 in PMKID cache
[04/10/14 18:49:50.846 IST 14c 8116] 0021.6a89.51ca **Starting key exchange with**
mobile - data forwarding is disabled
[04/10/14 18:49:50.846 IST 14d 8116] 0021.6a89.51ca 1XA: **Sending EAPOL message**
to mobile, WLAN=13 AP WLAN=13
[04/10/14 18:49:50.858 IST 14e 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL

message (len 123) from mobile
[04/10/14 18:49:50.858 IST 14f 8116] 0021.6a89.51ca 1XA: Received EAPOL-Key from mobile
[04/10/14 18:49:50.858 IST 150 8116] 0021.6a89.51ca 1XK: **Received EAPOL-key in PTK_START state (msg 2) from mobile**
[04/10/14 18:49:50.858 IST 151 8116] 0021.6a89.51ca 1XK: Stopping retransmission timer
[04/10/14 18:49:50.859 IST 152 8116] 0021.6a89.51ca 1XA**: Sending EAPOL message to mobile, WLAN=13 AP WLAN=13**
[04/10/14 18:49:50.862 IST 153 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL message (len 99) from mobile
[04/10/14 18:49:50.862 IST 154 8116] 0021.6a89.51ca 1XA: Received EAPOL-Key from mobile
[04/10/14 18:49:50.862 IST 155 8116] 0021.6a89.51ca 1XK: **Received EAPOL-key in PTKINITNEGOTIATING state (msg 4) from mobile**

[04/10/14 18:49:50.863 IST 172 338] [WCDB] wcdb_ffcp_cb: client (0021.6a89.51ca) client (0x57ca4000000048): FFCP operation (UPDATE) return code (0)
[04/10/14 18:49:50.914 IST 173 273] dhcp pkt processing routine is called for pak with SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
[04/10/14 18:49:50.914 IST 174 219] sending dhcp packet outafter processing with SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
[04/10/14 18:49:50.914 IST 175 256] DHCPD: address 20.20.20.6 mask 255.255.255.0
[04/10/14 18:49:54.279 IST 176 273] dhcp pkt processing routine is called for pak with SMAC = 0021.6a89.51ca and SRC_ADDR = 20.20.20.6
[04/10/14 18:49:54.279 IST 177 219] sending dhcp packet outafter processing with SMAC = 0021.6a89.51ca and SRC_ADDR = 20.20.20.6