9800 WLC에서 LWA의 일반적인 문제 해결

목차

소개

이 문서에서는 LWA(Local Web Authentication)를 사용하여 WLAN에 연결하는 클라이언트와 관련된 일반적인 문제에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음에 대한 기본 지식을 갖춘 것을 권장합니다.

- Cisco WLC(Wireless LAN Controller) 9800 시리즈.
- LWA(Local Web Authentication) 및 해당 컨피그레이션에 대한 일반적인 이해.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9800-CL WLC
- Cisco Access Point 9120AXI

- 9800 WLC Cisco IOS® XE 버전 17.9.3

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

배경 정보

LWA는 WLC에서 구성할 수 있는 WLAN 인증 유형으로, 연결을 시도하는 최종 클라이언트가 목록에서 WLAN을 선택한 후 사용자에게 포털을 제공합니다. 이 포털에서 사용자는 WLAN에 대한 연결을 완료하기 위해 사용자 이름 및 비밀번호(선택한 컨피그레이션에 따라)를 입력할 수 있습니다.

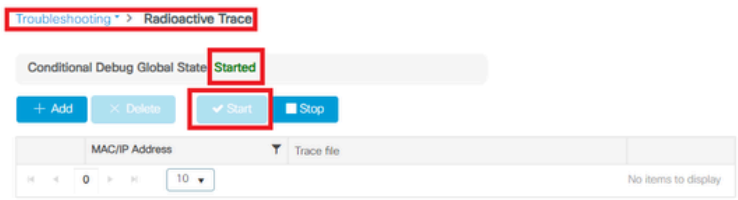
9800 WLC에서 LWA를 구성하는 방법에 대한 자세한 내용은 로컬 웹 인증 구성 가이드를 참조하십시오.

9800 WLC의 방사성(RA) 흔적

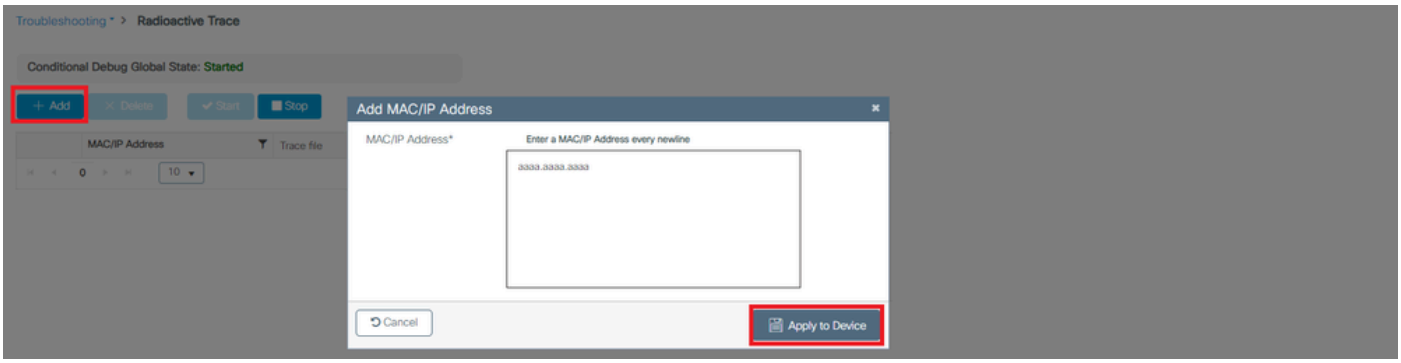
방사성 추적은 WLC 및 클라이언트 연결과 관련된 다양한 문제를 해결할 때 사용할 수 있는 훌륭한 문제 해결 도구입니다. RA 추적을 수집하려면 다음 단계를 수행합니다.

GUI에서 다음과 같이 표시되어야 합니다.

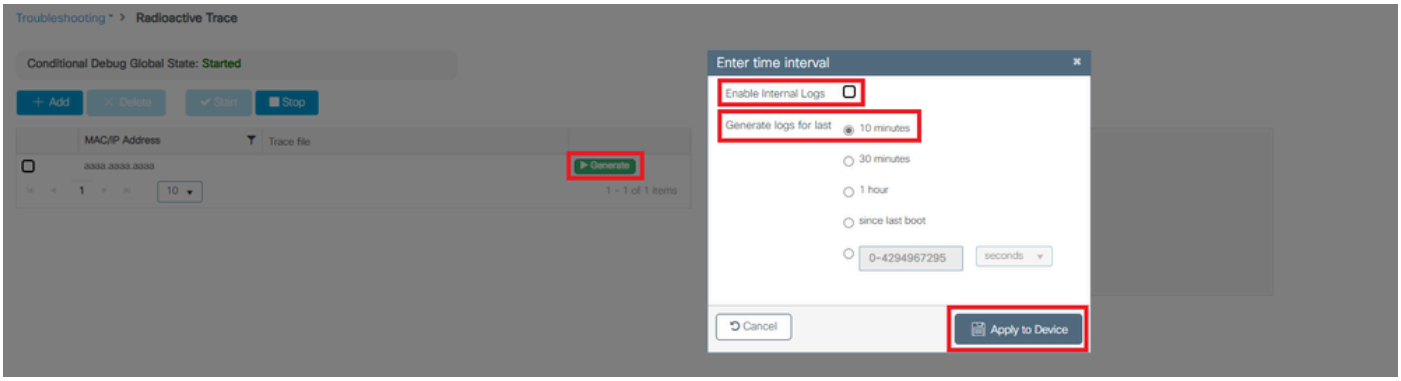
1. Troubleshooting(트러블슈팅) > Radioactive Trace(방사능 추적)로 이동합니다.
2. Start(시작)를 클릭하여 Conditional Debug Global State(조건부 디버그 전역 상태)를 활성화합니다.
3. + Add(추가)를 클릭합니다. 팝업 창이 열립니다. 클라이언트의 MAC 주소를 입력합니다. 모든 MAC 주소 형식이 허용됩니다(aabb.cdd.eff, AABB.CDD.EEEE, aa:bb:cc:dd:ee:ff 또는 AA:BB:CC:dd:EE:FF). 그런 다음 Apply to Device(디바이스에 적용)를 클릭합니다.
4. 고객이 문제를 3~4회 재현하도록 합니다.
5. 문제가 재현되면 Generate(생성)를 클릭합니다.
6. 새 팝업 창이 열립니다. 지난 10분 동안 로그를 생성합니다. (이 경우 내부 로그를 활성화할 필요가 없습니다.) Apply to Device(디바이스에 적용)를 클릭하고 파일이 처리될 때까지 기다립니다.
7. 파일이 생성되면 다운로드 아이콘을 클릭합니다.



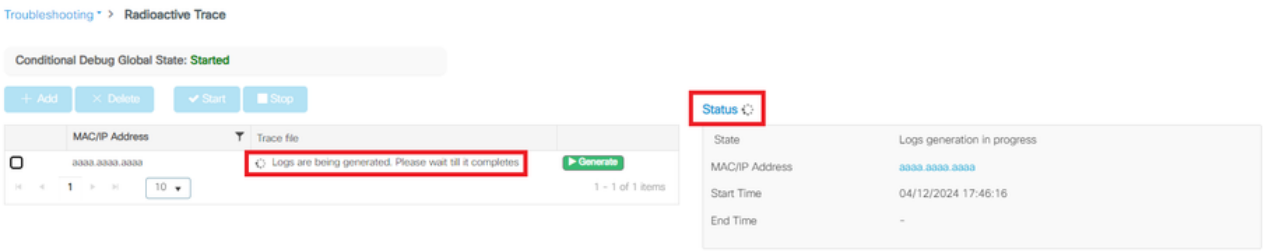
조건부 디버깅 사용



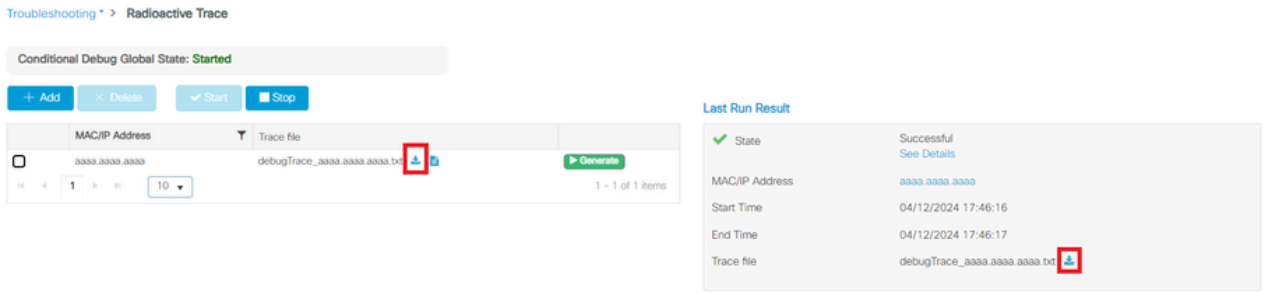
클라이언트 MAC 주소 추가



지난 10분 동안 로그 생성



파일이 생성될 때까지 대기파일



을 다운로드합니다

CLI에서:

<#root>

```
WLC# debug wireless mac
<mac-address>
 monitor-time 600
```

부트플래시의 새 파일은 ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log라고 생성됩니다

<#root>

```
WLC# more bootflash:
ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

분석을 위해 외부 서버에 파일 복사

<#root>

```
WLC# copy bootflash:
ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
 ftp://username:password@<ftp-server-ip>/path/RATRACE_FILENAME.txt
```

Radioactive Tracing에 대한 자세한 내용은 이 링크를 참조하십시오.

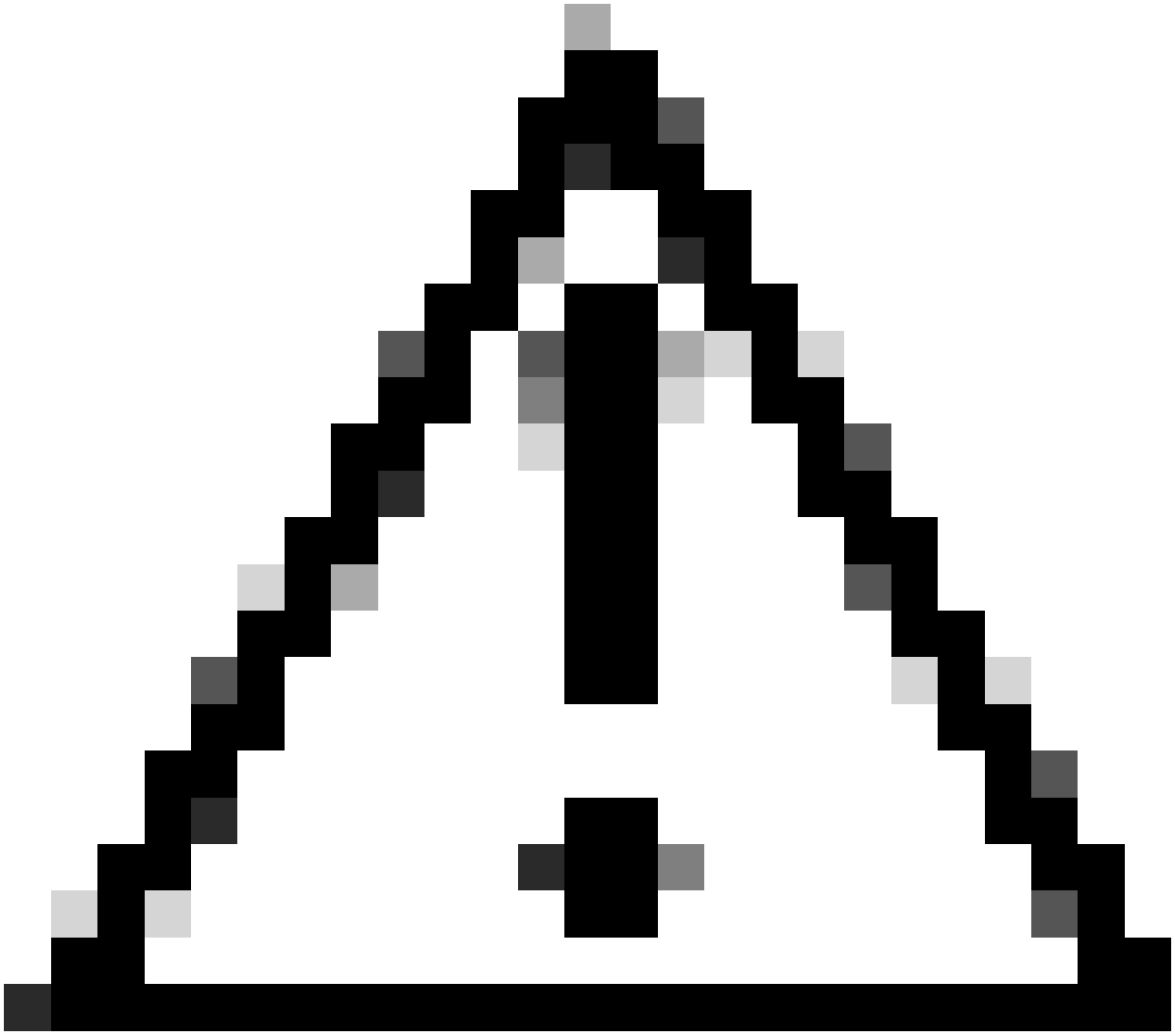
예상 플로우

LWA의 작동 시나리오를 이해하려면 정보를 참조하십시오.

클라이언트가 클라이언트 관점에서 겪는 단계

1. 최종 클라이언트가 WLAN에 연결됩니다.
2. 클라이언트가 할당된 IP 주소를 가져옵니다.
3. 포털이 최종 클라이언트에 표시됩니다.
4. 최종 클라이언트가 로그인 자격 증명을 입력합니다.
5. 최종 클라이언트가 인증되었습니다.
6. 최종 클라이언트는 인터넷을 탐색할 수 있습니다.

클라이언트가 WLC의 관점에서 거치는 단계



주의: RA(Radio Active) 추적의 많은 로그가 단순화를 위해 누락되었습니다.

최종 클라이언트가 WLAN에 연결됨

<#root>

```
MAC: aaaa.bbbb.cccc

Association received

. BSSID d4e8.801a.3063, WLAN LWA-SSID, Slot 0 AP d4e8.801a.3060, APD4E8.8019.608C, old BSSID d4e8.801a.
MAC: aaaa.bbbb.cccc Received Dot11 association request. Processing started,SSID: LWA-SSID, Policy profi
MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
MAC: aaaa.bbbb.cccc Dot11 ie validate ext/supp rates. Validation Passed for Supported rates radio_type
MAC: aaaa.bbbb.cccc WiFi direct: Dot11 validate P2P IE. P2P IE not present.
MAC: aaaa.bbbb.cccc dot11 send association response. Framing association response with resp_status_code
MAC: aaaa.bbbb.cccc Dot11 Capability info byte1 1, byte2: 14
MAC: aaaa.bbbb.cccc WiFi direct: skip build Assoc Resp with P2P IE: Wifi direct policy disabled
MAC: aaaa.bbbb.cccc Clearing old call info.
MAC: aaaa.bbbb.cccc dot11 send association response. Sending assoc response of length: 161 with resp_st
MAC: aaaa.bbbb.cccc
```

Association success.

AID 1, Roaming = True, WGB = False, 11r = False, 11w = False Fast roam = False
MAC: aaaa.bbbb.cccc DOT11 state transition: S_DOT11_ASSOCIATED -> S_DOT11_ASSOCIATED

L2 인증

<#root>

MAC: aaaa.bbbb.cccc Starting L2 authentication. Bssid in state machine:d4e8.801a.3063 Bssid in request
MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_L2_AUTH_IN_PROGRESS
MAC: aaaa.bbbb.cccc L2 Authentication initiated. method WEBAUTH, Policy VLAN 0, AAA override = 1
[aaaa.bbbb.cccc:capwap_90400002] -

authc_list: forwebauth

[aaaa.bbbb.cccc:capwap_90400002] - authz_list: Not present under wlan configuration
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH
MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH
MAC: aaaa.bbbb.cccc

L2 Authentication of station is successful.

, L3 Authentication : 1

클라이언트가 할당된 IP 주소를 가져옵니다.

<#root>

MAC: aaaa.bbbb.cccc Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE
MAC: aaaa.bbbb.cccc

Received ip learn response. method: IPLEARN_METHOD_DHCP

L3 인증

<#root>

MAC: aaaa.bbbb.cccc Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
MAC: aaaa.bbbb.cccc

L3 Authentication initiated. LWA

MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH

클라이언트가 IP 주소를 가져옵니다.

<#root>

```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
RX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
TX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
RX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
TX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE ->
```

S_IPLEARN_COMPLETE

포털 처리

<#root>

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

HTTP GET request

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

Parse GET, src [X.X.X.X] dst [Z.Z.Z.Z] url [http://connectivitycheck.gstatic.com/generate_204]

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 8
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

State GET_REDIRECT -> GET_REDIRECT

```
[...]
```

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

GET rcvd when in GET_REDIRECT state

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

HTTP GET request

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

Parse GET, src [X.X.X.X] dst [192.0.2.1] url [https://<virtual-ip-address>:443/login.html?redirect=http:

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 10
```

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

Param-map used: lwa-parameter_map

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

State GET_REDIRECT -> LOGIN

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

Sending Webauth login form

, len 8076
[...]
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

POST rcvd when in LOGIN state

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 get url: /login.html
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 4
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State LOGIN -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 45876/176 IO state READING -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

State AUTHENTICATING -> AUTHC_SUCCESS

WLC는 연결 최종 클라이언트에 적용될 정보를 처리합니다.

<#root>

[aaaa.bbbb.cccc:capwap_90400002]

Authc success from WebAuth, Auth event success

[aaaa.bbbb.cccc:capwap_90400002] Raised event

APPLY_USER_PROFILE

(14)
[aaaa.bbbb.cccc:capwap_90400002] Raised event RX_METHOD_AUTHC_SUCCESS (3)
[aaaa.bbbb.cccc:capwap_90400002] SM will not send event Template Deactivated to PRE for 0xAE000012
[aaaa.bbbb.cccc:capwap_90400002] SM will not send event Template Deactivated to PRE for 0xAE000012

Authentication Success.

Resolved Policy bitmap:4 for client aaaa.bbbb.cccc
Applying Attribute :

username 0 "cisco"

Applying Attribute : aaa-author-type 0 1 (0x1)
Applying Attribute : aaa-author-service 0 16 (0x10)
Applying Attribute : clid-mac-addr 0 3a e6 3b 9a fc 4a
Applying Attribute : addr 0 0xac104206
Applying Attribute : addrv6 0 "þ€"
Applying Attribute : addrv6 0 " ?Ì??"
Applying Attribute : addrv6 0 " ?Ì??"
Applying Attribute : addrv6 0 " ?Ì??"
Applying Attribute : target-scope 0 0 [client]
Applying Attribute : audit-session-id 0 "1A4210AC0000001C5B12A51C"
Applying Attribute : aaa-unique-id 0 28 (0x1c)
Applying Attribute : client-iif-id 0 4261415483 (0xfe000a3b)

```
Applying Attribute :
```

vlan-id 0 100 (0xa63)

```
Applying Attribute : session-linksec-secured 0 False
Applying Attribute : nas-ip-address 0 0x0
Applying Attribute : nas-ipv6-Address 0 ""
Applying Attribute : interface 0 ""
Applying Attribute : port-type 0 19 [802.11 wireless]
Applying Attribute : nas-port 0 10014 (0x40eba)
Applying Attribute :
```

cisco-wlan-ssid 0 "LWA-SSID"

```
Applying Attribute :
```

wlan-profile-name 0 "LWA-SSID"

```
Applying Attribute : dnis 0 "d4-e8-80-1a-30-60:LWA-SSID"
Applying Attribute : formatted-clid 0 "3a-e6-3b-9a-fc-4a"
Applying Attribute : bsn-wlan-id 0 16 (0x10)
Applying Attribute : nas-identifier-wireless 0 "LWA-SSID"
Applying Attribute : timeout 0 86400 (0x15180)
Applying Attribute : priv-lvl 0 1 (0x1)
Applying Attribute : timeout 0 86400 (0x15180)
Applying Attribute :
```

method 0 1 [webauth]

```
Applying Attribute : clid-mac-addr 0 3a e6 3b 9a fc 4a
Applying Attribute : intf-id 0 2420113410 (0x90400002)
[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr username(45
[aaaa.bbbb.cccc:capwap_90400002] SM Notified attribute
```

Add/Update username cisco

```
[aaaa.bbbb.cccc:capwap_90400002]
```

Received User-Name cisco for client aaaa.bbbb.cccc

```
[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr auth-domain
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Success'
[aaaa.bbbb.cccc:capwap_90400002] Context changing state from 'Running' to 'Authc Success'
[aaaa.bbbb.cccc:capwap_90400002]
```

Username cisco received

```
[aaaa.bbbb.cccc:capwap_90400002]
```

WLAN ID 16 received

WLC가 연결된 최종 클라이언트에 사용자 프로필 적용

```
Applied User Profile: aaa-author-type 0 1 (0x1)
Applied User Profile: aaa-author-service 0 16 (0x10)
Applied User Profile: clid-mac-addr 0 3a e6 3b 9a fc 4a
Applied User Profile: target-scope 0 0 [client]
Applied User Profile: aaa-unique-id 0 28 (0x1c)
Applied User Profile: client-iif-id 0 4261415483 (0xfe000a3b)
Applied User Profile: vlan-id 0 100 (0xa63)
Applied User Profile:session-linksec-secured 0 False
Applied User Profile: nas-ip-address 0 0x0
Applied User Profile: nas-ipv6-Address 0 ""
Applied User Profile: interface 0 ""
Applied User Profile: port-type 0 19 [802.11 wireless]
Applied User Profile: nas-port 0 10014 (0x40eba)
Applied User Profile:

cisco-wlan-ssid 0 "LWA-SSID"


Applied User Profile:

 wlan-profile-name 0 "LWA-SSID"


Applied User Profile:nas-identifier-wireless 0 "LWA-SSID"
Applied User Profile: priv-lvl 0 1 (0x1)
Applied User Profile: method 0 1 [webauth]
Applied User Profile:

clid-mac-addr 0 3a e6 3b 9a fc 4a


Applied User Profile: intf-id 0 2420113410 (0x90400002)
Applied User Profile:

 username 0 "cisco"


Applied User Profile: bsn-wlan-id 0 16 (0x10)
Applied User Profile: timeout 0 86400 (0x15180)
Applied User Profile: timeout 0 86400 (0x15180)
MAC: aaaa.bbbb.cccc Link-local bridging not enabled for this client, not checking VLAN validity
[aaaa.bbbb.cccc:capwap_90400002]

User Profile applied successfully - REPLACE

[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr method(757)



[aaaa.bbbb.cccc:capwap_90400002]

Raised event AUTHZ_SUCCESS (11)

[aaaa.bbbb.cccc:capwap_90400002]

Context changing state from 'Authc Success' to 'Authz Success'
```

웹 인증 완료

<#root>

```
MAC: aaaa.bbbb.cccc
```

L3 Authentication Successful.

ACL:[]
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING ->

S_AUTHIF_WEBAUTH_DONE

최종 클라이언트에 적용된 AAA 특성

<#root>

[Applied attribute : username 0 "

cisco

"]
[Applied attribute : bsn-wlan-id 0 16 (0x10)]
[Applied attribute : timeout 0 86400 (0x15180)]
[Applied attribute : timeout 0 86400 (0x15180)]
[Applied attribute :bsn-vlan-interface-name 0 "

myvlan

"]

최종 클라이언트가 실행 상태에 도달함

<#root>

Managed client RUN state notification: aaaa.bbbb.cccc
MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS ->

S_CO_RUN

일반적인 문제 해결 시나리오

인증 실패

고려 사항

- 포털에 올바른 자격 증명을 입력한 후 "인증 실패"라고 표시됩니다.
- WLC는 "웹 인증 보류 중" 상태의 클라이언트를 표시합니다.
- 초기 스플래시 페이지가 다시 사용자에게 표시됩니다.

WLC RA 추적

<#root>

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State LOGIN -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 40828/176 IO state READING -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

Param-map used: lwa-parameter_map

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State AUTHENTICATING ->
```

AUTHC_FAIL [INVALID CREDENTIALS]

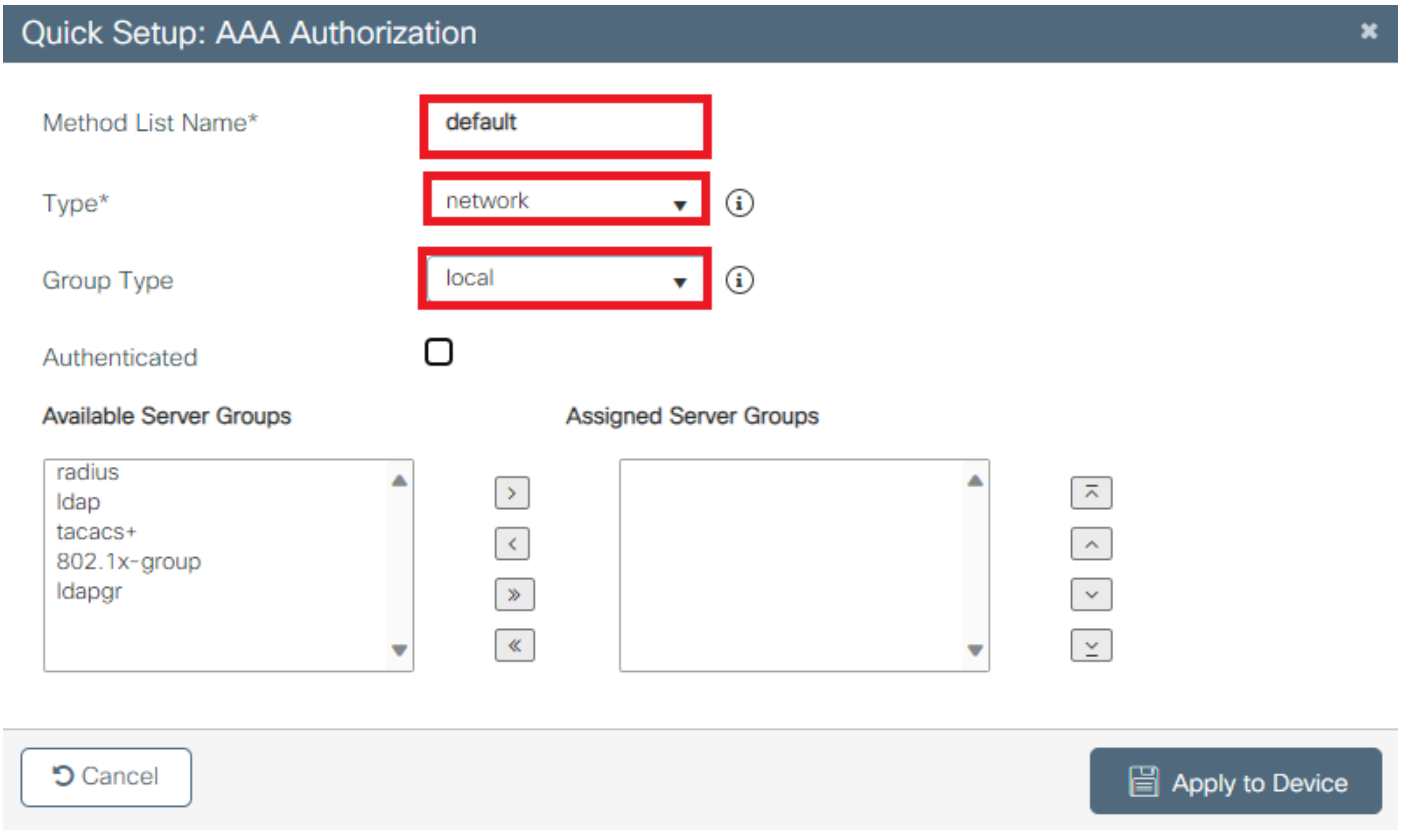
```
[aaaa.bbbb.cccc:capwap_90400002] Authc failure from WebAuth, Auth event fail
[aaaa.bbbb.cccc:capwap_90400002] (Re)try failed method WebAuth - aaaa.bbbb.cccc
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Failed'
```

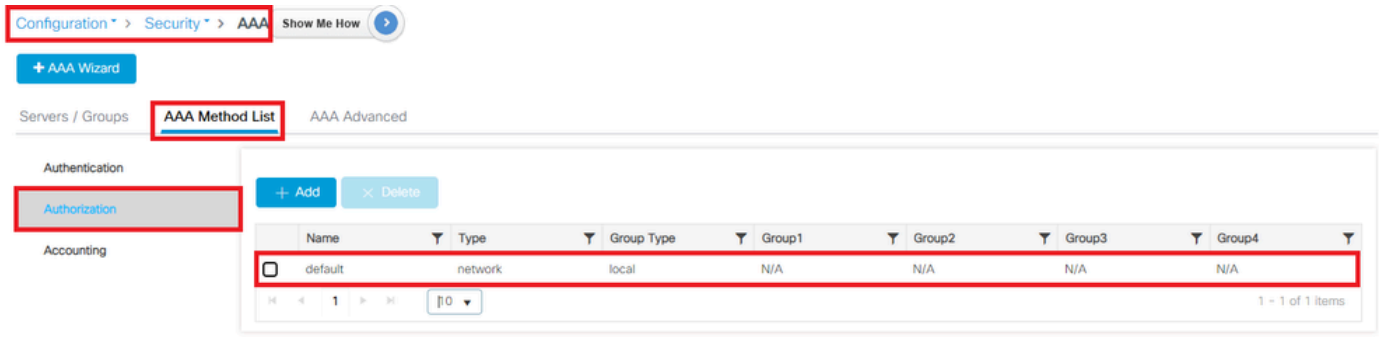
권장 솔루션

네트워크 권한 부여를 위한 기본 AAA 방법 목록이 WLC 컨피그레이션에 있는지 확인합니다.

GUI에서 다음과 같이 표시되어야 합니다.

1. Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 메서드 목록) > Authorization(권한 부여)으로 이동합니다. + Add(추가)를 클릭합니다.
2. 다음과 같이 구성합니다.
    1. 메서드 목록 이름: 기본값
    2. 유형: network
    3. 그룹 유형: local
3. Apply to Device(디바이스에 적용)를 클릭합니다.





CLI에서:

<#root>

```
WLC# configure terminal
WLC(config)# aaa authorization default network local
```

포털이 사용자에게 표시되지 않지만 클라이언트가 연결된 것으로 표시됨

최종 클라이언트에서 발생할 수 있는 동작

- 최종 클라이언트는 자신의 장치를 "연결됨"으로 인식합니다.

- 최종 클라이언트에 포털이 표시되지 않습니다.
- 최종 클라이언트는 자격 증명을 입력하지 않습니다.
- 최종 클라이언트에 할당된 IP 주소가 있습니다.
- WLC는 클라이언트를 "실행" 상태로 표시합니다.

WLC RA 추적

클라이언트가 할당된 IP 주소를 가져오면 즉시 WLC에서 "Run" 상태로 전환됩니다. 사용자 특성에는 최종 클라이언트에 할당된 VLAN만 표시됩니다.

<#root>

```
MAC: aaaa.bbbb.cccc

Client IP learn successful. Method: DHCP IP: X.X.X.X


[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr addr(8)
[aaaa.bbbb.cccc:capwap_90400002] SM Notified attribute Add/Update addr X.X.X.X
MAC: aaaa.bbbb.cccc IP-learn state transition:

 S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE


MAC: aaaa.bbbb.cccc Received ip learn response. method: IPLEARN_METHOD_DHCP
[ Applied attribute :bsn-vlan-interface-name 0 "
```

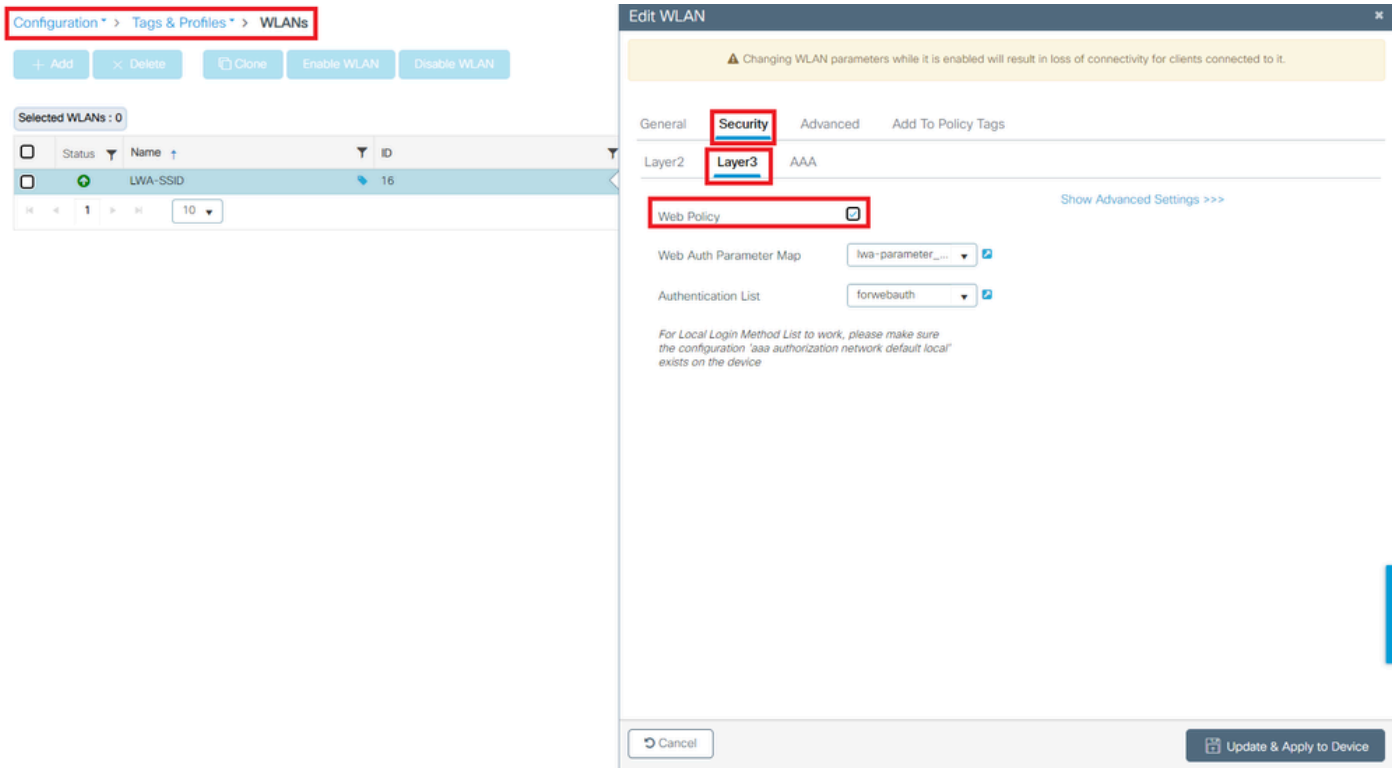
```
myvlan

" ]
[ Applied attribute : timeout 0 1800 (0x708) ]
MAC: aaaa.bbbb.cccc Client QoS run state handler
Managed client RUN state notification: aaaa.bbbb.cccc
MAC: aaaa.bbbb.cccc Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN
```

권장 솔루션

WLAN에서 웹 정책이 활성화되었는지 확인합니다.

GUI에서 다음과 같이 표시되어야 합니다.

1. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs로 이동합니다.
2. LWA WLANs(LWA WLAN)를 선택합니다.
3. Security(보안) > Layer 3로 이동합니다.
4. 웹 정책 확인란이 활성화되어 있는지 확인합니다.



웹 정책을 사용하도록 설정해야 합니다.

CLI에서:

```
<#root>

WLC# configure terminal


WLC(config)# wlan

<wlan>
```

```
WLC(config-wlan)# shutdown
WLC(config-wlan)# security webauth
WLC(config-wlan)# no shutdown
```

포털이 사용자에게 표시되지 않으며 클라이언트가 연결되지 않음

최종 클라이언트에서 발생할 수 있는 동작

- 최종 클라이언트는 장치가 계속 연결을 시도하고 있음을 확인합니다.

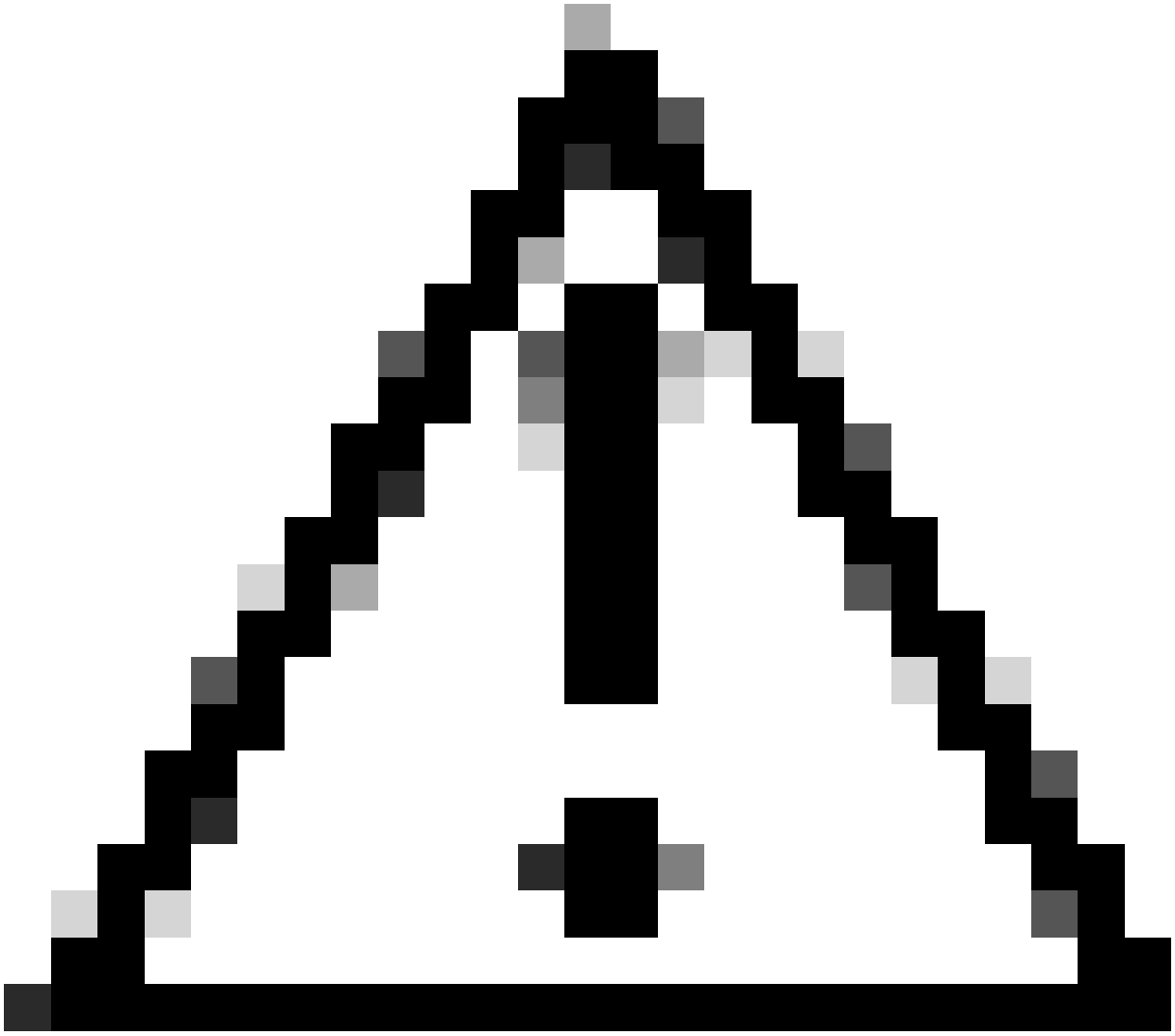
- 최종 클라이언트에 포털이 표시되지 않습니다.
- 최종 클라이언트에 할당된 IP 주소가 없습니다.
- WLC는 클라이언트를 "Webauth Pending" 상태로 표시합니다.

권장 솔루션

필요한 HTTP/HTTPS 서버를 활성화합니다. 이제 어떤 HTTP/HTTPS 서버를 활성화하여 네트워크 요구 사항에 완벽하게 적응할 수 있어야 할지를 더 효과적으로 제어할 수 있습니다. 웹 인증을 위한 HTTP 및 HTTPS 요청 구성에 대한 자세한 내용은 이 링크를 참조하십시오. 지원되는 여러 HTTP 조합이 있습니다. 예를 들어, HTTP는 webadmin에만 사용할 수 있고 HTTP는 webauth에 사용할 수 있습니다.

HTTP 및 HTTPS 액세스를 모두 사용하여 관리 디바이스 관리 및 웹 인증을 허용하려면 CLI에서 다음을 수행합니다.

```
WLC# configure terminal
WLC(config)# ip http server
WLC(config)# ip http secure-server
```



주의: 이 두 서버가 모두 비활성화된 경우 WLC의 GUI(Graphical User Interface)에 액세스할 수 없습니다.

최종 클라이언트가 IP 주소를 가져오지 않습니다.

최종 클라이언트에서 발생할 수 있는 동작

- 최종 클라이언트는 디바이스가 IP 주소를 계속 가져오려고 시도하고 있음을 알 수 있습니다.
- WLC는 클라이언트를 "IP Learning" 상태로 표시합니다.

WLC RA 추적

제안 없이 디스커버리 요청.

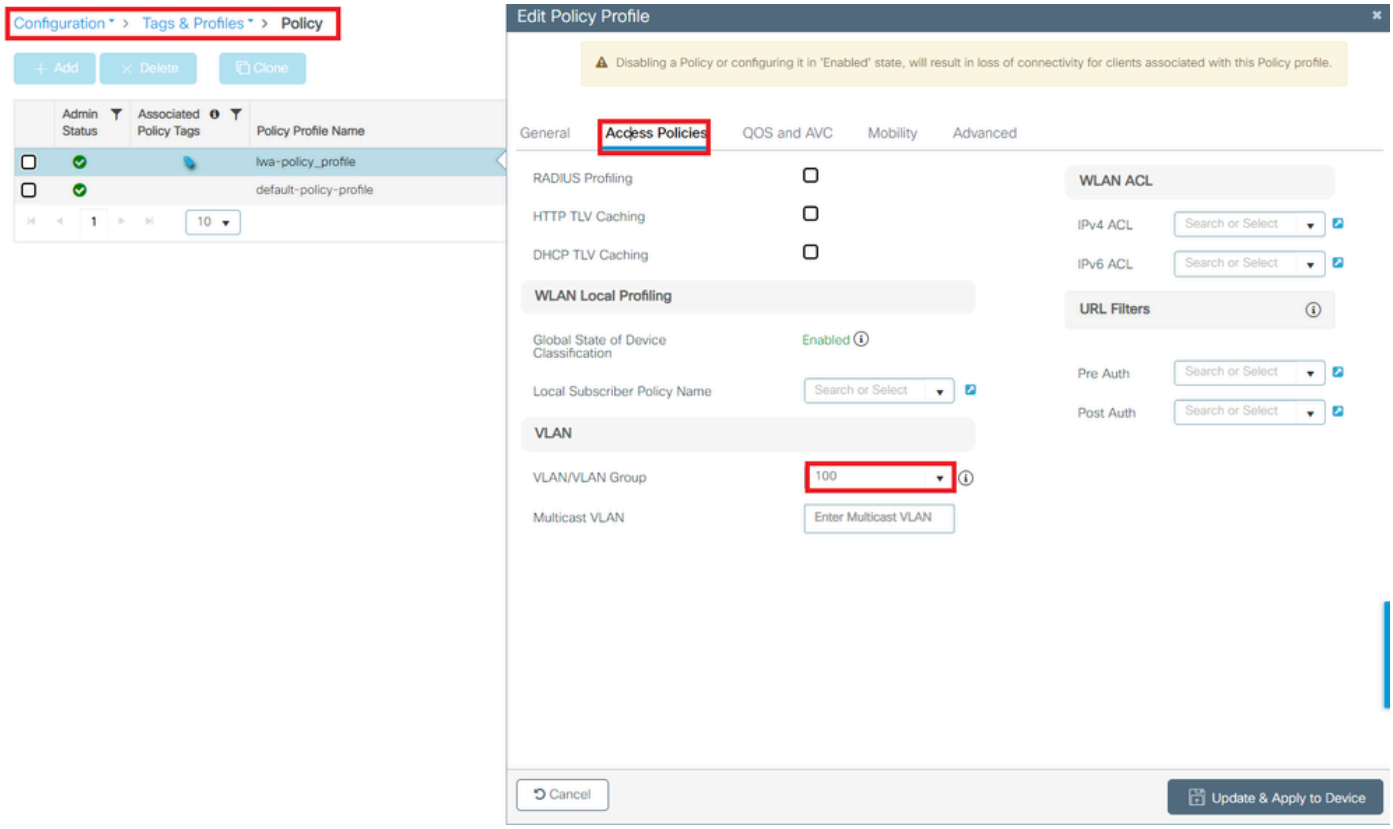
```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
```

권장 솔루션

첫째: 정책 프로필에 올바른 VLAN이 할당되었는지 확인합니다.

GUI에서 다음과 같이 표시되어야 합니다.

1. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동합니다.
2. 사용된 정책 프로필을 선택합니다.
3. 액세스 정책으로 이동합니다.
4. 올바른 VLAN을 선택합니다.



CLI에서:

<#root>

```
WLC# show wireless profile policy detailed
```

<policy-profile>

```
Policy Profile Name :
```

<policy-profile>

```
Description :
```

<policy-profile>

```
Status : ENABLED
VLAN :

VLAN-selected


[...]

WLC# configure terminal
WLC(config)# wireless profile policy

 <policy-profile>


WLC(config-wireless-policy)#

vlan <correct-vlan>
```

둘째: 사용자가 사용할 수 있는 DHCP 풀이 있는지 확인합니다. 컨피그레이션 및 연결 가능성을 확인합니다. RA 추적은 VLAN DHCP DORA 프로세스가 어떤 과정을 거치고 있는지 보여줍니다. 이 VLAN이 올바른 VLAN인지 확인합니다.

```
DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff src_i
DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y.Y,
DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff src_i
DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y.Y,
```

최종 클라이언트에 사용자 지정 포털이 표시되지 않음

최종 클라이언트에서 발생할 수 있는 동작

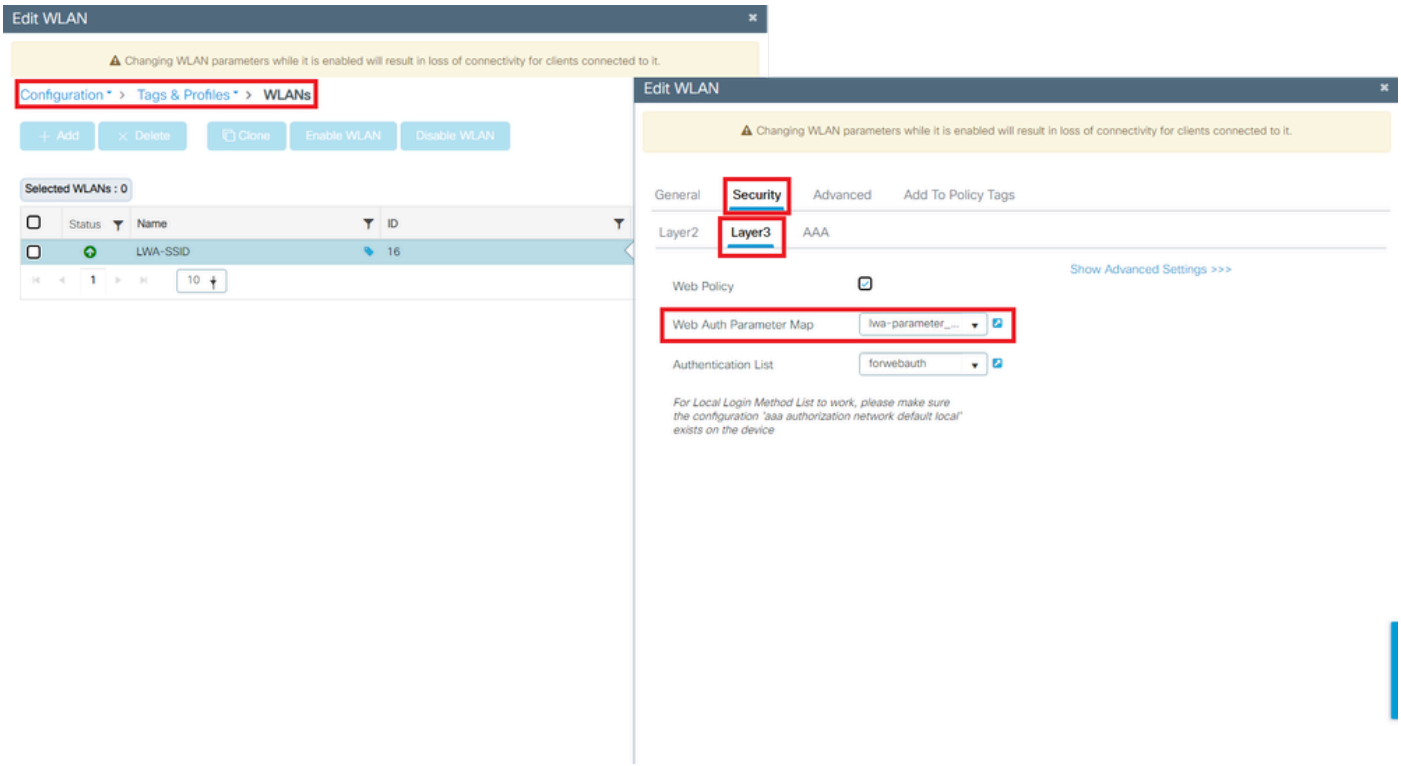
- WLC의 기본 포털이 표시됩니다.

권장 솔루션

첫 번째: WLAN이 사용자 지정된 웹 인증 매개변수 맵을 사용하고 있는지 확인합니다.

GUI에서 다음과 같이 표시되어야 합니다.

1. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs로 이동합니다.
2. 목록에서 WLAN을 선택합니다.
3. Security(보안) > Layer 3로 이동합니다.
4. 사용자 지정 웹 인증 매개변수 맵을 선택합니다.



사용자 지정 매개 변수 맵 선택됨

CLI에서:

<#root>

```
WLC# show wlan name LWA-SSID
WLAN Profile Name : LWA-SSID
================================================
[...]
Security:
     Webauth Parameter Map :
```

<parameter-map>

```
WLC# configure terminal
WLC(config)# wlan
```

<wlan>

```
WLC(config-wlan)# security web-auth parameter-map
```

<parameter-map>

둘째, Cisco.com 웹 포털에서 다운로드한 사용자 지정은 매우 견고하고 복잡한 프로그래밍 인터페이스에서는 작동하지 않습니다. 일반적으로 CSS 수준에서만 변경하고 이미지를 추가하거나 제거하는 것이 좋습니다. 애플릿, PHP, 변수 수정, React.js 등은 지원되지 않습니다. 사용자 지정 포털이 클라이언트에 표시되지 않으면 기본 WLC 페이지를 사용하여 문제를 복제할 수 있는지 확인하십시오. 포털이 성공적으로 표시되면 사용자 지정된 페이지에서 지원되지 않는 항목이 사용됩니다.

셋째: EWC(Embedded Wireless Controller)를 사용하는 경우 CLI를 사용하여 사용자 정의된 페이지가 올바르게 표시되는지 확인하는 것이 좋습니다.

<#root>

```
EWC# configure terminal
EWC(config)# parameter-map type
```

<parameter-map>

```
EWC(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
EWC(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html
EWC(config-params-parameter-map)# custom-page failure device flash:loginfail.html
EWC(config-params-parameter-map)# custom-page success device flash:loginsucess.html
EWC(config-params-parameter-map)# end
```

최종 클라이언트에 사용자 지정 포털이 올바르게 표시되지 않음

최종 클라이언트에서 발생할 수 있는 동작

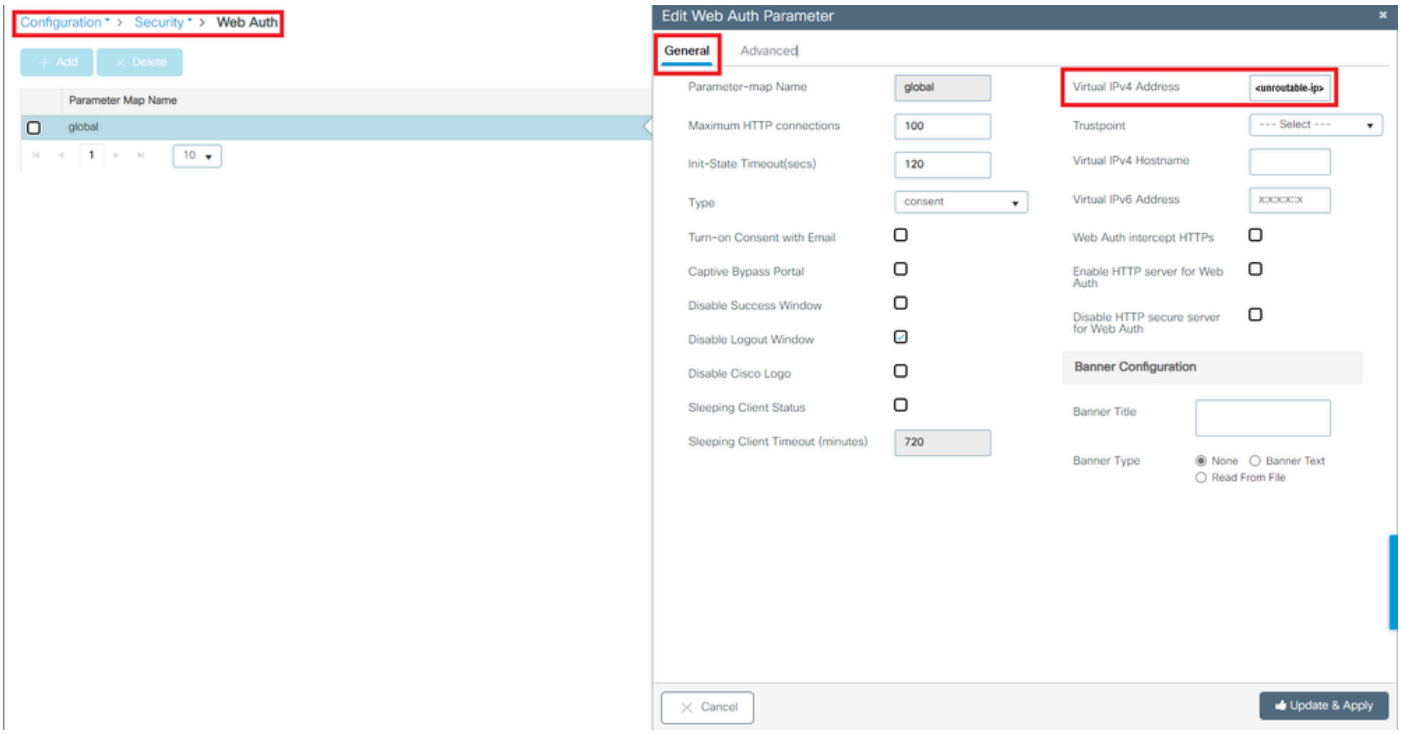
- 사용자 지정 포털이 올바르게 렌더링되지 않습니다(즉, 이미지가 표시되지 않음).

권장 솔루션

전역 매개변수 맵에 가상 IP 주소가 할당되어 있는지 확인합니다.

GUI에서 다음과 같이 표시되어야 합니다.

1. Configuration(컨피그레이션) > Security(보안) > Web Auth(웹 인증)로 이동합니다.
2. 목록에서 전역 매개변수 맵을 선택합니다.
3. 라우팅 불가 가상 IP 주소를 추가합니다.



전역 매개변수 맵의 가상 IP 주소가 라우팅 불가 IP 주소로 설정됨

CLI에서:

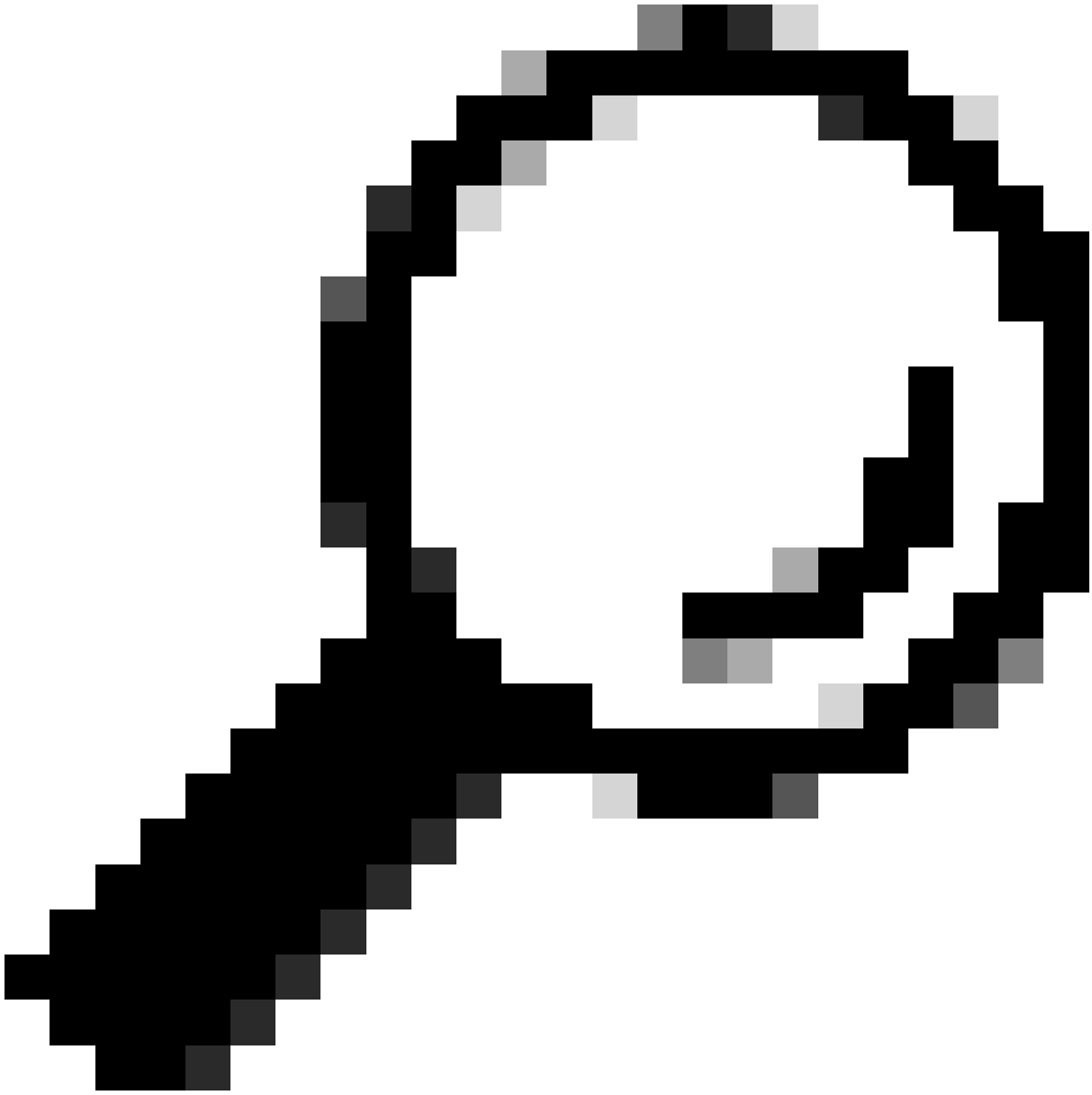
<#root>

```
WLC# show parameter-map type webauth global
Parameter Map Name : global
[...]
Virtual-ipv4 :
```

<unroutable-ip>

```
[...]

WLC# configure terminal
WLC(config)# parameter-map type webauth global
WLC(config-params-parameter-map)# virtual-ip ipv4
```

<unroutable-ip>



팁: 가상 IP 주소는 웹 인증 로그인 페이지의 리디렉션 주소 역할을 합니다. 네트워크의 다른 디바이스에는 동일한 IP가 없어야 하며, 물리적 포트에 매핑되거나 라우팅 테이블에 존재하지 않아야 합니다. 따라서 가상 IP를 라우팅 불가 IP 주소로 구성하는 것이 좋습니다. RFC5737에 있는 주소만 사용할 수 있습니다.

포털에서 "연결이 보안/서명 확인 실패"라고 합니다.

최종 클라이언트에서 발생할 수 있는 동작

- 포털을 열면 연결이 안전하지 않다는 오류가 표시됩니다.
- 포털에서 인증서를 사용해야 합니다.

알아야 할 사항

포털이 HTTPS로 표시될 것으로 예상되면 SSL(Secure Socket Layer) 인증서를 사용해야 합니다. 해당 인증서는 타사 CA(Certificate Authority)에서 발급하여 도메인이 실제 도메인인지 검증해야 하며, 자격 증명을 입력하거나 포털을 볼 때 최종 클라이언트에 신뢰를 제공해야 합니다. WLC에 인증서를 업로드하려면 이 문서를 참조하십시오.

권장 솔루션

첫 번째: 원하는 HTTP/HTTPS 서비스를 다시 시작합니다. 이제 어떤 HTTP/HTTPS 서버를 활성화하여 네트워크 요구 사항에 완벽하게 적응할 수 있어야 할지를 더 효과적으로 제어할 수 있습니다. 웹 인증을 위한 HTTP 및 HTTPS 요청 구성에 대한 자세한 내용은 이 링크를 참조하십시오.

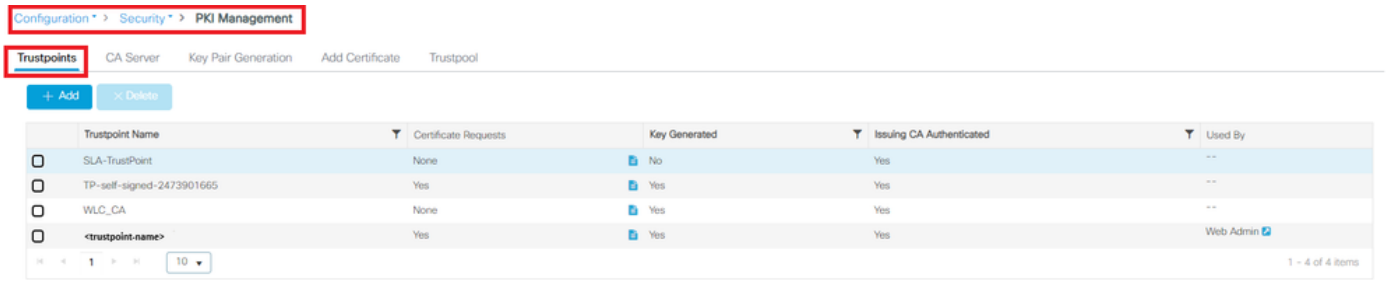
CLI에서:

```
WLC# configure terminal
WLC(config)# no ip http server
WLC(config)# no ip http secure-server
WLC(config)# ip http server
WLC(config)# ip http secure-server
```

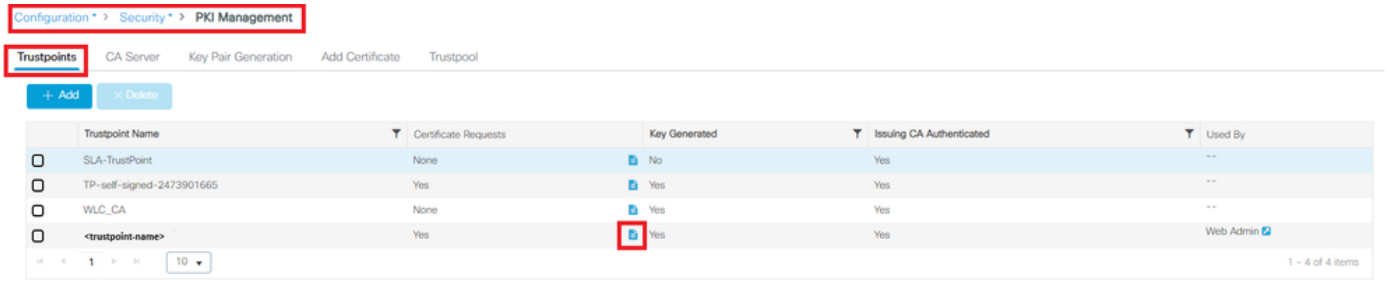
둘째: 인증서가 WLC에 올바르게 업로드되고 유효 날짜가 올바른지 확인하십시오.

GUI에서 다음과 같이 표시되어야 합니다.

1. Configuration(컨피그레이션) > Security(보안) > PKI Management(PKI 관리)로 이동합니다.
2. 목록에서 신뢰 지점 검색
3. 세부 정보 확인



신뢰 지점 존재 확인신뢰 지점



세부사항 확인

신뢰 지점 유효성 확인

CLI에서:

<#root>

```
WLC# show crypto pki certificate
```

[<certificate>]

```
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=<Common Name>
    o=<Organizational Unit>
  Subject:
    cn=<Common Name>
    o=<Organizational Unit>
  Validity Date:
```

start date: <start-date>

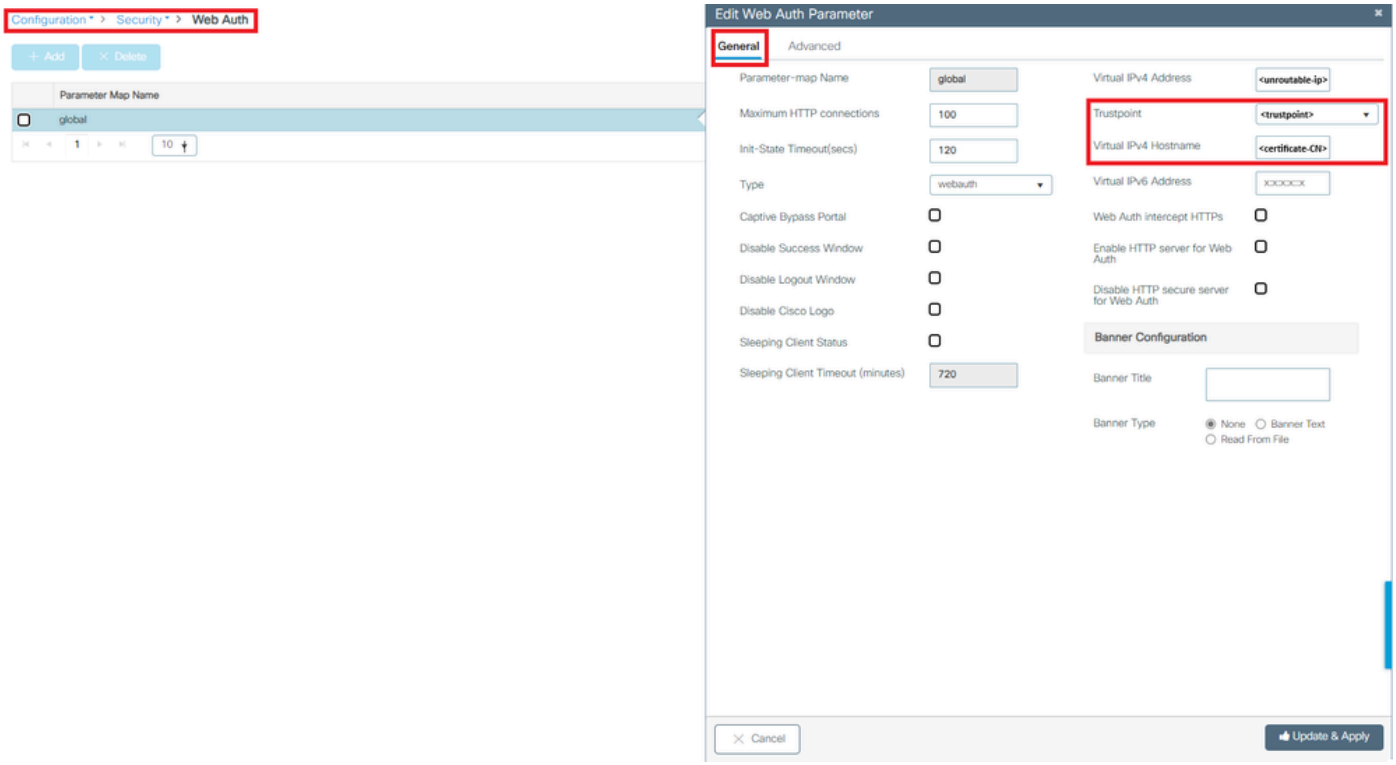
end date: <end-date>

Associated Trustpoints: <trustpoint>

셋째: WebAuth 매개변수 맵에서 사용하기 위해 선택한 인증서가 올바른지, 그리고 가상 IPv4 호스트 이름이 인증서의 CN(Common Name)과 일치하는지 확인하십시오.

GUI에서 다음과 같이 표시되어야 합니다.

1. Configuration(컨피그레이션) > Security(보안) > Web Auth(웹 인증)로 이동합니다.
2. 목록에서 사용된 매개변수 맵을 선택합니다.
3. 신뢰 지점 및 가상 IPv4 호스트 이름이 올바른지 확인합니다.



신뢰 지점 및 가상 IPv4 호스트 이름 확인

CLI에서:

<#root>

```
WLC# show run | section paramter-map type
```

<type> <name>

```
parameter-map type
```

<type> <name>

```
[...]
virtual-ip ipv4
```

<unroutable-ip> <certificate-common-name>

```
trustpoint
```

<trustpoint>

관련 정보

- 로컬 웹 인증 구성

- 웹 기반 인증(EWC)
- Catalyst 9800 WLC에서 웹 인증 포털 사용자 지정
- Catalyst 9800 WLC에서 CSR 인증서 생성 및 다운로드
- 가상 인터페이스 구성

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.