게스트 앵커 설정에서 중앙 웹 인증(CWA) 이해 및 문제 해결

목차

소개

이 문서에서는 중앙 웹 인증이 게스트 앵커 설정에서 작동하는 방식 및 프로덕션 네트워크에서 나타나는 몇 가지 일반적인 문제 및 이를 어떻게 해결할 수 있는지 설명합니다.

사전 요구 사항

요구 사항

Cisco는 WLC(Wireless LAN Controller)에서 중앙 웹 인증을 구성하는 방법에 대해 알고 있는 것을 권장합니다.

이 문서에서는 중앙 웹 인증 구성에 대한 단계를 제공합니다.
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

사용되는 구성 요소

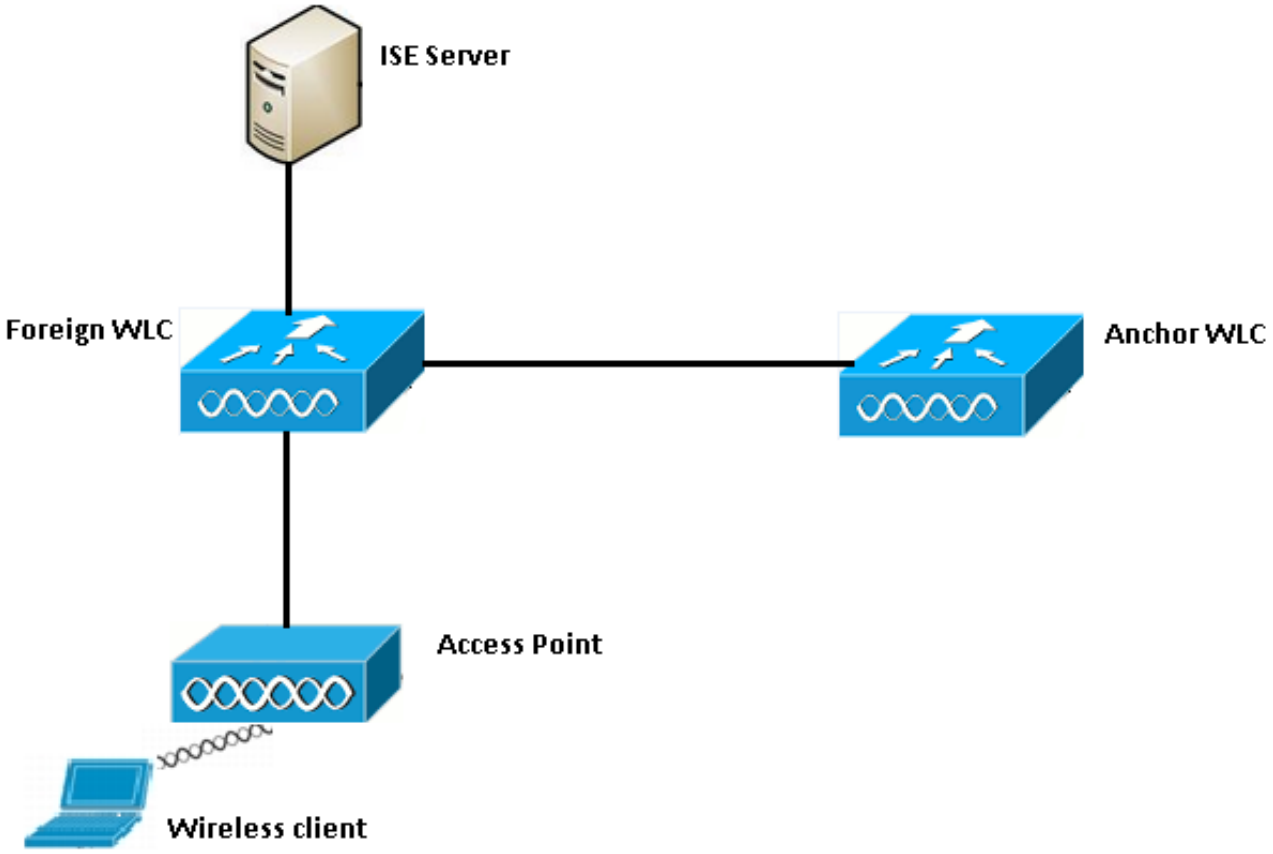
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 7.6을 실행하는 WLC 5508
- 버전 1.4를 실행하는 ISE(Identity Services Engine)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우, 모든 명령의 잠재적인 영향을 이해해야 합니다.

기본 흐름

이 섹션에서는 이미지에 표시된 대로 게스트 앵커 설정에서 중앙 웹 인증서의 기본 워크플로를 보여줍니다.



1단계. 클라이언트는 연결 요청을 보낼 때 연결을 시작합니다.

2단계. WLC는 구성된 ISE 서버로 인증 요청을 보낼 때 MAC 인증 프로세스를 시작합니다.

3단계. ISE에 구성된 권한 부여 정책에 따라, Access-Accept 메시지가 리디렉션 URL을 사용하여 WLC로 다시 전송되고 ACL(Access Control List) 항목을 리디렉션합니다.

4단계. 외부 WLC가 클라이언트에 연결 응답을 보냅니다.

5단계. 이 정보는 외부 WLC가 모빌리티 핸드오프 메시지의 앵커 WLC에 전달합니다. 앵커 및 외부 WLC 모두에서 리디렉션 ACL이 구성되었는지 확인해야 합니다.

6단계. 이 단계에서는 클라이언트가 외부 WLC에서 Run(실행) 상태로 이동합니다.

7단계. 클라이언트가 브라우저에서 URL로 웹 인증을 시작하면 앵커는 리디렉션 프로세스를 시작합니다.

8단계. 클라이언트가 성공적으로 인증되면 클라이언트는 앵커 WLC에서 **RUN** 상태로 이동합니다.

성공적인 클라이언트 연결 시도를 위한 중앙 웹 인증 흐름

이제 디버그를 거칠 때 위에서 설명한 기본 흐름을 자세히 분석할 수 있습니다. 이러한 디버그는 분석에 도움이 되도록 앵커와 외부 WLC에서 모두 수집되었습니다.

```
debug client 00:17:7c:2f:b8:6e
debug aaa detail enable
debug mobility handoff enable
debug web-auth redirect enable mac 00:17:7c:2f:b8:6e
```

이러한 세부 정보는 여기에서 사용됩니다.

```
WLAN name: CWA
WLAN ID: 5
IP address of anchor WLC: 10.105.132.141
IP address of foreign WLC: 10.105.132.160
Redirect ACL used: REDIRECT
Client MAC address: 00:17:7c:2f:b8:6e
New mobility architecture disabled
```

1단계. 클라이언트는 연결 요청을 보낼 때 연결 프로세스를 시작합니다. 이는 외부 컨트롤러에서 볼 수 있습니다.

```
*apfMsConnTask_6: May 08 12:10:35.897: 00:17:7c:2f:b8:6e Association received from mobile on
BSSID dc:a5:f4:ec:df:34
```

2단계. WLC는 MAC 인증을 위해 무선 LAN(WLAN)이 매핑되어 있음을 확인하고 클라이언트를 **AAA 보류** 상태로 이동합니다. 또한 ISE에 인증 요청을 보낼 때 인증 프로세스를 시작합니다.

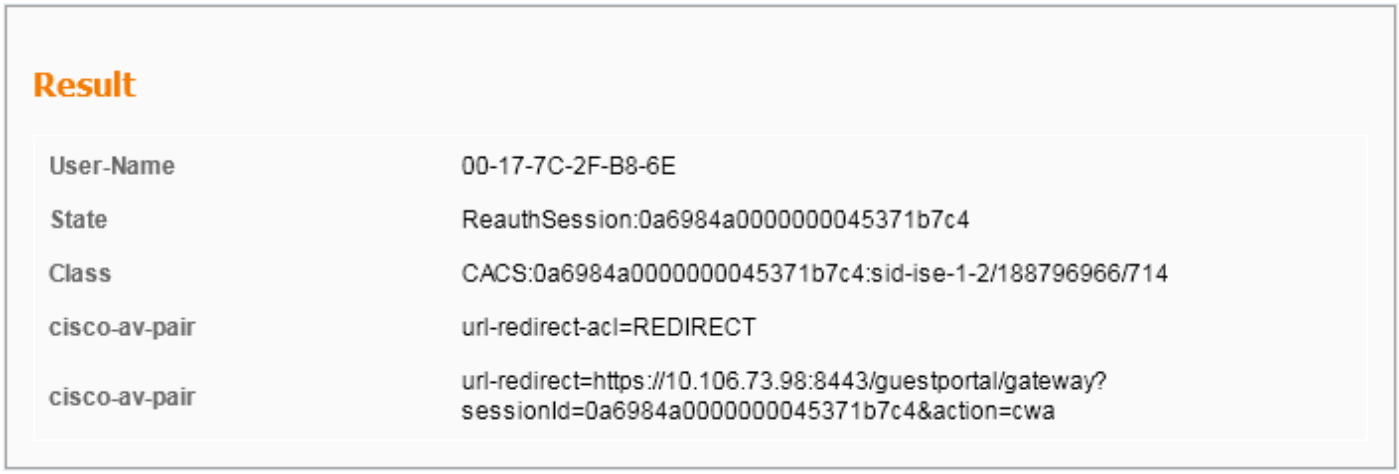
```
*apfMsConnTask_6: May 08 12:10:35.898: 00:17:7c:2f:b8:6e apfProcessAssocReq (apf_80211.c:8221)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Idle to AAA Pending
*aaaQueueReader: May 08 12:10:35.898: AuthenticationRequest: 0x2b6bf574

*aaaQueueReader: May 08 12:10:35.898: Callback.....................................0x10166e78
*aaaQueueReader: May 08 12:10:35.898: protocolType.................................0x40000001
*aaaQueueReader: May 08 12:10:35.898:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
```

3단계. ISE에서 MAC 인증 우회가 구성되고 MAC 인증 후 리디렉션 URL 및 ACL을 반환합니다. 권한 부여 응답에서 전송된 다음 매개변수를 볼 수 있습니다.

```
*radiusTransportThread: May 08 12:10:35.920: AuthorizationResponse: 0x14c47c58
*radiusTransportThread: May 08 12:10:35.920: structureSize..............................320
*radiusTransportThread: May 08 12:10:35.920: resultCode.................................0
*radiusTransportThread: May 08 12:10:35.920:
protocolUsed.................................0x00000001
*radiusTransportThread: May 08 12:10:35.920:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
*radiusTransportThread: May 08 12:10:35.920: Packet contains 5 AVPs:
*radiusTransportThread: May 08 12:10:35.920: AVP[01] User-
Name.............................00-17-7C-2F-B8-6E (17 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[02]
State.....................................ReauthSession:0a6984a00000004c536bac7b (38 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[03]
Class.....................................CACS:0a6984a00000004c536bac7b:sid-ise-1-2/188796966/38
(54 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[04] Cisco / Url-Redirect-
Acl.................REDIRECT (8 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[05] Cisco / Url-
```

```
Redirect.....................DATA (91 bytes)
```

ISE 로그 아래에서 동일한 정보를 볼 수 있습니다. Operations(운영) **>Authentications(인증)로** 이동하고 이미지에 표시된 대로 **Client session details(클라이언트 세션 세부사항)를** 클릭합니다.



4단계. 외부 WLC가 상태를 L2 인증 완료 상태로 변경하고 연결 응답을 클라이언트에 보냅니다.

참고: MAC 인증이 활성화된 경우 연결 응답은 이 작업이 완료될 때까지 전송되지 않습니다.

```
*apfReceiveTask: May 08 12:10:35.921: 00:17:7c:2f:b8:6e 0.0.0.0 AUTHCHECK (2) Change state to
L2AUTHCOMPLETE (4)
*apfReceiveTask: May 08 12:10:35.922: 00:17:7c:2f:b8:6e Sending Assoc Response to station on
BSSID dc:a5:f4:ec:df:34 (status 0) ApVapId 5 Slot 0
```

5단계: 그런 다음 foreign은 앵커에 대한 전달 프로세스를 시작합니다. 다음은 디버그 모빌리티 핸드오프 출력입니다.

```
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Attempting anchor export for mobile
00:17:7c:2f:b8:6e
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Anchor Export:
Client IP: 0.0.0.0, Anchor IP: 10.105.132.141
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e mmAnchorExportSend: Building
UrlRedirectPayload
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Anchor Export: Sending url redirect acl
REDIRECT
```

6단계. 클라이언트가 외부 WLC에서 RUN 상태로 전환되는 것을 확인할 수 있습니다. 이제 클라이언트의 올바른 상태는 앵커에서만 볼 수 있습니다. 다음은 외래 정보에서 수집된 show client detail 출력입니다(관련 정보만 표시됨).

```
Client MAC Address.............................. 00:17:7c:2f:b8:6e
Client Username ................................ 00-17-7C-2F-B8-6E
AP MAC Address.................................. dc:a5:f4:ec:df:30
BSSID........................................... dc:a5:f4:ec:df:34
IP Address...................................... Unknown
Gateway Address................................. Unknown
Netmask......................................... Unknown
Mobility State.................................. Export Foreign
Mobility Anchor IP Address...................... 10.105.132.141
Policy Manager State............................ RUN
Policy Manager Rule Created..................... Yes
AAA Override ACL Name........................... REDIRECT
```

```
AAA URL
redirect.............................https://10.106.73.98:8443/guestportal/gatewaysessionId=
0a6984a00000004c536bac7b&action=cwa
```

7단계. 외부 컨트롤러는 앵커와 핸드오프 요청을 시작합니다. 이제 핸드오프 메시지가 아래에 표시됩니다.

```
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e Received Anchor Export request: from Switch
IP: 10.105.132.160
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e Adding mobile on Remote AP
00:00:00:00:00:00(0)
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv:, Mobility role is Unassoc
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv Ssid=cwa Security
Policy=0x42000
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv vapId= 5, Ssid=cwa
AnchorLocal=0x0
*mmListen: May 08 05:52:50.588: 00:17:7c:2f:b8:6e mmAnchorExportRcv:Url redirect
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa
*mmListen: May 08 05:52:50.588: 00:17:7c:2f:b8:6e Url redirect ACL REDIRECT

A handoff acknowledgement message is also sent to the foreign and can be seen in the debugs on
foreign:
*mmListen: May 08 12:10:38.802: 00:17:7c:2f:b8:6e Received Anchor Export Ack for client from
Switch IP: 10.105.132.141
*mmListen: May 08 12:10:38.802: 00:17:7c:2f:b8:6e Anchor Mac: d0:c2:82:e2:91:60, Old Foreign
Mac: 30:e4:db:1b:e0:a0 New Foreign Mac: 30:e4:db:1b:e0:a0
```

8단계. 그런 다음 앵커 컨트롤러가 클라이언트를 DHCP 필수 상태로 이동합니다. 클라이언트가 IP 주소를 가져오면 컨트롤러는 계속해서 클라이언트를 처리하고 중앙 웹 인증 필수 상태로 이동합니다. 앵커에 수집된 show client detail 출력에서도 동일한 항목을 볼 수 있습니다.

```
Client MAC Address.............................. 00:17:7c:2f:b8:6e
AP MAC Address.................................. 00:00:00:00:00:00
Client State.................................... Associated
Wireless LAN Id................................. 5
IP Address...................................... 10.105.132.254
Mobility State.................................. Export Anchor
Mobility Foreign IP Address..................... 10.105.132.160
Policy Manager State............................ CENTRAL_WEB_AUTH
AAA Override ACL Name........................... REDIRECT
AAA URL redirect.............................
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa
```

9단계. 외부 WLC는 클라이언트를 실행 상태로 전환하면 동시에 회계 프로세스를 시작합니다. ISE에 어카운팅 시작 메시지를 전송합니다.

```
*aaaQueueReader: May 08 12:10:38.803: AccountingMessage Accounting Start: 0x2b6c0a78
*aaaQueueReader: May 08 12:10:38.803: Packet contains 16 AVPs:
*aaaQueueReader: May 08 12:10:38.803: AVP[01] User-Name.............................00-17-7C-
2F-B8-6E (17 bytes)
```

참고: 어카운팅은 외부 WLC에서만 구성해야 합니다.

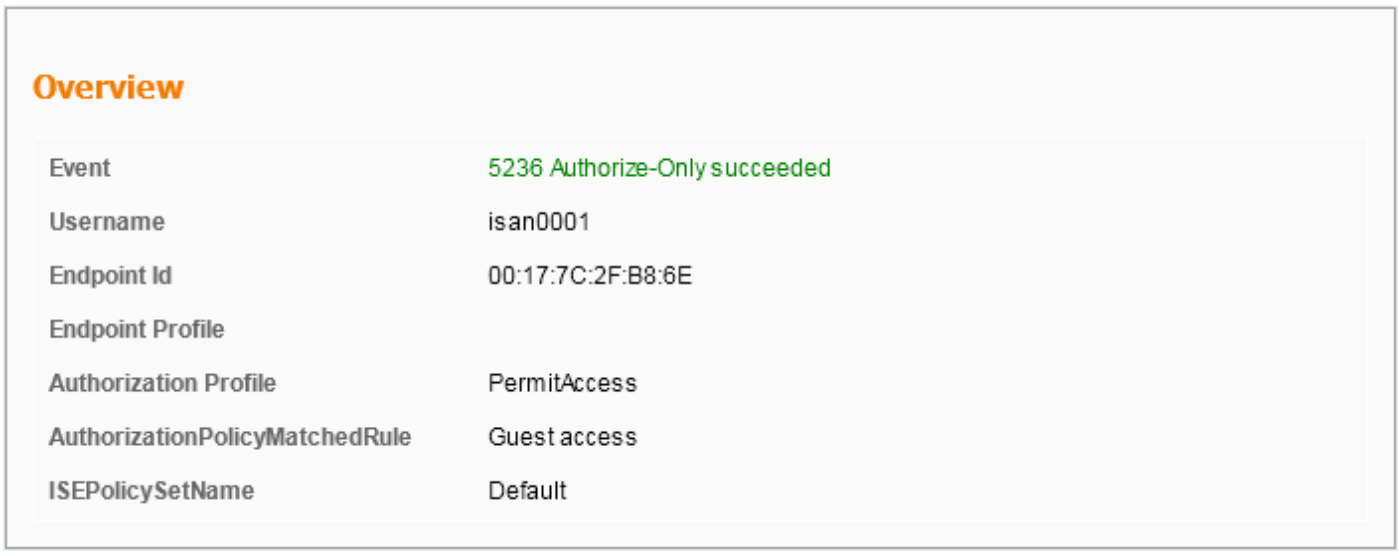
10단계. 사용자는 브라우저에 URL을 입력하여 웹 인증 리디렉션 프로세스를 시작합니다. 앵커 컨트롤러에서 관련 디버그를 볼 수 있습니다.

```
*webauthRedirect: May 08 05:53:05.927: 0:17:7c:2f:b8:6e- received connection
*webauthRedirect: May 08 05:53:05.928: captive-bypass detection disabled, Not checking for wispr
in HTTP GET, client mac=0:17:7c:2f:b8:6e
*webauthRedirect: May 08 05:53:05.928: 0:17:7c:2f:b8:6e- Preparing redirect URL according to
configured Web-Auth type
*webauthRedirect: May 08 05:53:05.928: 0:17:7c:2f:b8:6e: Client configured with AAA overridden
redirect URL
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa
```

11단계. 웹 인증 프로세스의 인증 부분이 앵커 위치가 아니라 외부 WLC에서 처리된다는 것도 확인할 수 있습니다. 해외의 디버그 AAA 출력에서도 동일한 항목을 볼 수 있습니다.

```
*aaaQueueReader: May 08 12:11:11.537: AuthenticationRequest: 0x2b6c0a78
*aaaQueueReader: May 08 12:11:11.537: Callback.....................................0x10166e78
*aaaQueueReader: May 08 12:11:11.537: protocolType.................................0x40000001
*aaaQueueReader: May 08 12:11:11.537:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
*aaaQueueReader: May 08 12:11:11.537: Packet contains 12 AVPs (not shown)
Authorization response from ISE:
*radiusTransportThread: May 08 12:11:11.552: AuthorizationResponse: 0x14c47c58
*radiusTransportThread: May 08 12:11:11.552: structureSize..............................252
*radiusTransportThread: May 08 12:11:11.552: resultCode.................................0
*radiusTransportThread: May 08 12:11:11.552:
protocolUsed.................................0x00000001
*radiusTransportThread: May 08 12:11:11.552:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
*radiusTransportThread: May 08 12:11:11.552: Packet contains 6 AVPs:
*radiusTransportThread: May 08 12:11:11.552: AVP[01] User-
Name.............................isan0001 (8 bytes) -----> (Username used for web
authentication)
*radiusTransportThread: May 08 12:11:11.552: AVP[02]
State.....................................ReauthSession:0a6984a00000004c536bac7b (38 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[03]
Class.....................................CACS:0a6984a00000004c536bac7b:sid-ise-1-2/188796966/40
(54 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[04] Session-
Timeout.........................0x00006e28 (28200) (4 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[05] Termination-
Action.....................0x00000000 (0) (4 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[06] Message-
Authenticator...................DATA (16 bytes)
```

ISE에서 이미지에 표시된 것과 동일한 것을 확인할 수 있습니다.



12단계. 이 정보는 앵커 WLC에 전달됩니다. 이 핸드셰이크는 디버그에 명확하게 표시되지 않으며 다음과 같이 전달 후 정책을 적용하는 앵커를 통해 확인할 수 있습니다.

```
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Received Anchor Export policy update, valid
mask 0x900:
Qos Level: 0, DSCP: 0, dot1p: 0 Interface Name: , IPv4 ACL Name:
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Applying post-handoff policy for station
00:17:7c:2f:b8:6e - valid mask 0x900
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e QOS Level: -1, DSCP: -1, dot1p: -1,
Data Avg: -1, realtime Avg: -1, Data Burst -1, Realtime Burst -1
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Session: 0, User session: 28200, User elapsed
1
Interface: N/A, IPv4 ACL: N/A, IPv6 ACL: N/A.
```

인증이 완료되었는지 확인하는 가장 좋은 방법은 ISE에서 전달된 로그를 확인하고 컨트롤러에서 show client detail의 출력을 수집하는 것입니다. 이 출력은 클라이언트가 **RUN** 상태로 표시되어야 합니다.

```
Client MAC Address.............................. 00:17:7c:2f:b8:6e
Client State.................................... Associated
Client NAC OOB State............................ Access
Wireless LAN Id................................. 5
IP Address...................................... 10.105.132.254
Mobility State.................................. Export Anchor
Mobility Foreign IP Address..................... 10.105.132.160
Policy Manager State............................ RUN
```

또 다른 중요한 확인 사항은 앵커가 성공적인 인증 후 무상 ARP(Address Resolution Protocol)를 전송한다는 사실입니다.

```
*pemReceiveTask: May 08 05:53:23.343: 00:17:7c:2f:b8:6e Sending a gratuitous ARP for
10.105.132.254, VLAN Id 20480
```

여기서 클라이언트는 앵커 컨트롤러에서 전달하는 모든 유형의 트래픽을 보낼 수 있습니다.

클라이언트 연결이 끊길 때 중앙 Webauth 흐름

세션/유휴 시간 제한으로 인해 또는 WLC에서 클라이언트를 수동으로 제거할 때 다음 단계가 수행됩니다.

외부 WLC는 클라이언트에 인증 취소 메시지를 전송하고 삭제 일정을 잡습니다.

```
*apfReceiveTask: May 08 12:19:21.199: 00:17:7c:2f:b8:6e apfMsExpireMobileStation (apf_ms.c:6634)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Associated to
Disassociated
*apfReceiveTask: May 08 12:19:21.199: 00:17:7c:2f:b8:6e Sent Deauthenticate to mobile on BSSID
dc:a5:f4:ec:df:30 slot 0(caller apf_ms.c:6728
```

그런 다음 ISE 서버에 클라이언트 인증 세션이 종료되었음을 알리기 위해 radius 중지 계정 관리 메시지를 보냅니다.

```
*aaaQueueReader: May 08 12:19:21.199: AccountingMessage Accounting Stop: 0x2b6d5684
*aaaQueueReader: May 08 12:19:21.199: Packet contains 24 AVPs:
*aaaQueueReader: May 08 12:19:21.199: AVP[01] User-Name.............................00-17-7C-
```

```
2F-B8-6E (17 bytes)
```

또한 모빌리티 핸드오프 메시지를 앵커 WLC에 보내 클라이언트 세션을 종료하도록 알립니다. 이는 앵커 WLC의 모빌리티 디버그에서 확인할 수 있습니다.

```
*mmListen: May 08 06:01:32.907: 00:17:7c:2f:b8:6e Received Handoff End request for client from
Switch IP: 10.105.132.160
*apfReceiveTask: May 08 06:01:32.907: 00:17:7c:2f:b8:6e apfMmProcessResponse: Handoff end rcvd
for mobile 00:17:7c:2f:b8:6e, delete mobile. reason code = 0
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e 10.105.132.254 RUN (20) mobility role
update request from Export Anchor to Handoff
Peer = 10.105.132.160, Old Anchor = 10.105.132.141, New Anchor = 0.0.0.0
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e apfMmProcessCloseResponse (apf_mm.c:647)
Expiring Mobile!
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e Mobility Response: IP 0.0.0.0 code
Anchor Close (5), reason Normal disconnect (0), PEM State DHCP_REQD, Role Handoff(6)
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e Deleting mobile on AP
00:00:00:00:00:00(0)
```

ISE에서 클라이언트 계정 일시 중단

ISE는 WLC가 클라이언트 세션을 종료하도록 알리는 게스트 사용자 계정을 일시 중단할 수 있습니다. 이 기능은 클라이언트가 연결된 WLC를 확인할 필요가 없는 관리자에게 유용하며 간단히 세션을 종료합니다. 이제 ISE에서 게스트 사용자 계정이 일시 중단/만료될 때 어떤 일이 발생하는지 확인할 수 있습니다.

ISE 서버는 클라이언트 연결을 제거해야 함을 나타내는 Change of Authorization 메시지를 외부 컨트롤러로 보냅니다. 디버그 출력에서 확인할 수 있습니다.

```
*radiusCoASupportTransportThread: May 13 02:01:53.446: 00:17:7c:2f:b8 :6e apfMsDeleteByMscb
Scheduling mobile for deletion with deleteReason 6, reason Code 252
*radiusCoASupportTransportThread: May 13 02:01:53.446: 00:17:7c:2f:b8:6e Schedul ing deletion of
Mobile Station: (callerId: 30) in 1 seconds
```

외부 WLC가 클라이언트에 인증 취소 메시지를 보냅니다.

```
*apfReceiveTask: May 13 02:01:54.303: 00:17:7c:2f:b8:6e Sent Deauthenticate to mobile on BSSID
dc:a5:f4:ec:df:30 slot 0(caller apf_ms.c:5921)
```

또한 어카운팅 중지 메시지를 어카운팅 서버에 전송하여 클라이언트 인증 세션을 종료합니다.

```
*aaaQueueReader: May 13 02:01:54.303: AccountingMessage Accounting Stop: 0x2b6d2 c7c
*aaaQueueReader: May 13 02:01:54.303: Packet contains 23 AVPs:
*aaaQueueReader: May 13 02:01:54.303: AVP[01] User-Name.....................
.............00177c2fb86e (12 bytes)
```

전달 메시지는 또한 클라이언트 세션을 종료하기 위해 앵커 WLC에 전송됩니다. 앵커 WLC에서 확인할 수 있습니다.

```
*mmListen: May 12 19:42:52.871: 00:17:7c:2f:b8:6e Received Handoff End request for client from
Switch IP: 10.105.132.160
*apfReceiveTask: May 12 19:42:52.872: 00:17:7c:2f:b8:6e apfMmProcessResponse: Handoff end rcvd
for mobile 00:17:7c:2f:b8:6e, delete mobile. reason code = 0
```

게스트 앵커 설정에서 중앙 웹 인증 문제 해결

이제 CWA를 사용할 때 나타나는 몇 가지 일반적인 문제와 이를 해결하기 위해 수행할 수 있는 작업을 살펴보겠습니다.

시나리오 1. 클라이언트가 START 상태로 중단되어 IP 주소를 가져오지 않음

MAC 인증이 활성화된 이후 중앙 웹 인증 시나리오에서 MAC 인증이 완료된 후 연결 응답이 전송됩니다. 이 경우 WLC와 RADIUS 서버 간에 통신 장애가 있거나 RADIUS 서버에 컨피그레이션이 잘못되어 액세스 거부를 전송하게 되면 연결 루프에서 반복적으로 연결 거부를 가져오는 클라이언트를 볼 수 있습니다. 클라이언트 제외가 활성화된 경우에도 클라이언트가 제외될 수 있습니다.

코드 8.2 이상에서 사용 가능한 **test aaa radius** 명령을 사용하여 radius 서버 연결을 확인할 수 있습니다.

아래 참조 링크는 이 기능을 사용하는 방법을 보여줍니다.
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html

시나리오 2. 클라이언트가 IP 주소를 가져올 수 없습니다.

클라이언트가 CWA 게스트 앵커 설정에서 IP 주소를 가져오지 못하는 이유는 몇 가지가 있습니다.

- **앵커 및 외형의 SSID 컨피그레이션이 일치하지 않습니다.**

앵커와 외부 WLC 간에 SSID 컨피그레이션을 동일하게 유지하는 것이 좋습니다. 엄격한 검사가 수행되는 일부 측면은 L2/L3 보안 구성, DHCP 구성 및 AAA 재정의 매개변수입니다. 동일한 상태가 아닐 경우 앵커에 대한 전달이 실패하고 앵커 디버그에서 다음 메시지를 볼 수 있습니다.

```
DHCP dropping packet due to ongoing mobility handshake exchange, (siaddr 0.0.0.0, mobility state = 'apfMsMmAnchorExportRequested'
```

이를 완화하려면 SSID 컨피그레이션이 동일한 앵커 및 외래 상태인지 확인해야 합니다.

- **앵커와 외부 WLC 간의 모빌리티 터널이 다운/플랩 중입니다.**

모든 클라이언트 트래픽은 IP 프로토콜 97을 사용하는 모빌리티 데이터 터널에서 전송됩니다. 모빌리티 터널이 가동되지 않은 경우 전달이 완료되지 않고 클라이언트가 외부에서 RUN 상태로 이동하지 않음을 확인할 수 있습니다. 모빌리티 터널 상태는 **UP**로 표시되어야 하며 이미지에 표시된 대로 Controller(컨트롤러) **>Mobility Management(모빌리티 관리) >Mobility Groups(모빌리티 그룹)**에서 확인할 수 있습니다.

멤버로 매핑된 컨트롤러가 하나만 있는 경우(foriegn 또는 anchor) Monitor(모니터) > Statistics(통계) **> Mobility Statistics(모빌리티 통계)** 아래에서 전역 모빌리티 통계를 확인할 수도 있습니다.

- **앵커 또는 외부 컨트롤러에 구성되지 않은 리디렉션 ACL:**

radius 서버에서 보낸 리디렉션 ACL의 이름이 외부 WLC에 구성된 것과 일치하지 않는 경우, MAC 인증이 완료된 경우에도 클라이언트는 거부되며 DHCP를 수행하지 않습니다. 클라이언트 트래픽이 앵커에서 종료되므로 개별 ACL 규칙을 구성해야 하는 것은 아닙니다. 리디렉션 ACL과 동일한 이름으로 생성된 ACL이 있는 한 클라이언트는 앵커에게 전달됩니다. 클라이언트가 webauth 필수 상태로 이동하도록 앵커는 ACL 이름 및 규칙을 올바르게 구성해야 합니다.

시나리오 3. 클라이언트가 웹 페이지로 리디렉션되지 않음

웹 인증 페이지가 표시되지 않는 이유는 몇 가지가 있습니다. 일반적인 WLC 관련 문제는 다음과 같습니다.

- **DNS 서버 문제**

DNS 서버 연결성/구성 오류 문제는 클라이언트가 리디렉션되지 못하는 가장 일반적인 이유 중 하나입니다. 이는 WLC 로그나 디버그에 표시되지 않으므로 catch하기 어려울 수도 있습니다. 사용자는 DHCP 서버에서 푸시된 DNS 서버 컨피그레이션이 올바른지 그리고 무선 클라이언트에서 연결할 수 있는지 확인해야 합니다. 비작동 클라이언트의 간단한 DNS 조회가 가장 쉽게 확인할 수 있는 방법입니다.

- **앵커에서 내부 DHCP 서버를 사용하는 경우 기본 게이트웨이에 연결할 수 없습니다.**

내부 DHCP 서버를 사용하는 경우 기본 게이트웨이 컨피그레이션이 올바르고 앵커 WLC에 연결되는 스위치 포트에서 VLAN이 허용되는지 확인해야 합니다. 그렇지 않은 경우 클라이언트는 IP 주소를 얻지만 아무 것도 액세스할 수 없습니다. 클라이언트의 ARP 테이블에서 게이트웨이의 MAC 주소를 확인할 수 있습니다. 게이트웨이에 대한 L2 연결을 확인하고 연결할 수 있는지 신속하게 확인할 수 있습니다.