

AireOS 및 차세대 WLC를 사용하여 ISE 무선 CWA 및 핫스팟 플로우 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[Unified 5508 WLC 구성](#)

[전역 컨피그레이션](#)

[게스트의 SSID\(Service Set Identifier\)를 구성합니다.](#)

[리디렉션 ACL 구성](#)

[HTTPS 리디렉션](#)

[적극적인 장애 조치](#)

[종속 바이패스](#)

[Converged 3850 NGWC 구성](#)

[전역 컨피그레이션](#)

[SSID 컨피그레이션](#)

[ACL 구성 리디렉션](#)

[CLI\(Command-Line Interface\) 컨피그레이션](#)

[ISE 구성](#)

[일반적인 ISE 컨피그레이션 작업](#)

[활용 사례 1: 모든 사용자 연결에서 게스트 인증이 포함된 CWA](#)

[활용 사례 2: CWA with Device Registration에서는 하루에 한 번 게스트 인증을 적용합니다.](#)

[활용 사례 3: HostSpot 포털](#)

[다음을 확인합니다.](#)

[활용 사례 1](#)

[활용 사례 2](#)

[활용 사례 3](#)

[AireOS의 FlexConnect 로컬 스위칭](#)

[외부 앵커 시나리오](#)

[문제 해결](#)

[AireOS 및 Converged Access WLC에서 공통적으로 손상된 상태](#)

[아이레OS WLC](#)

[NGWC](#)

[ISE](#)

[관련 정보](#)

소개

이 문서에서는 Identity Services Engine에서 Cisco AireOS 및 Next Generation Wireless LAN Controller를 사용하여 게스트 케이스 3개를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Wireless LAN Controller(통합 및 통합 액세스)
- Identity Services Engine(ISE)

사용되는 구성 요소

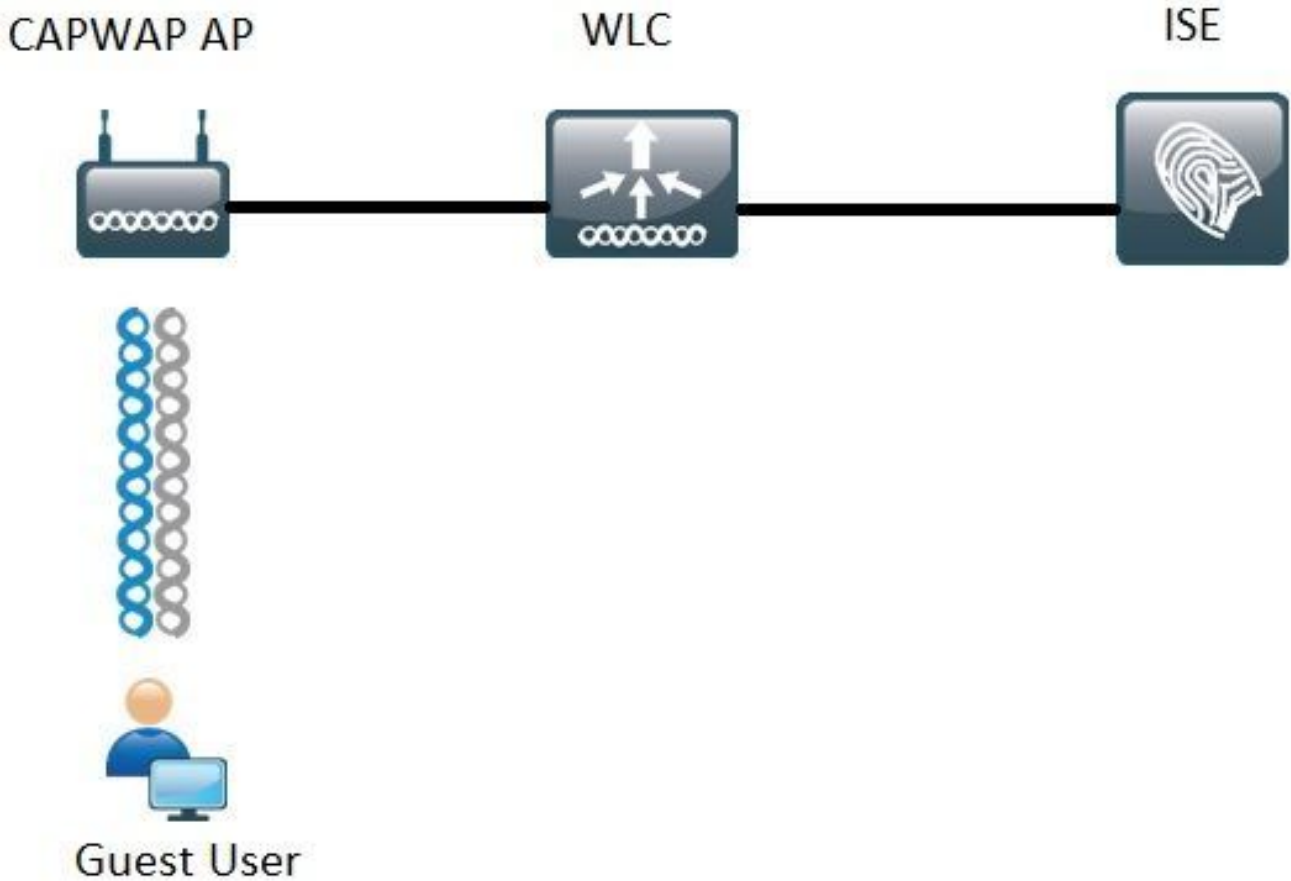
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Services Engine 버전 2.1
- Cisco Wireless LAN Controller 5508 및 8.0.121.0
- NGWC(Next Generation Wireless Controller) catalyst 3850(WS-C3850-24P) with 03.06.04.E

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.

구성

네트워크 다이어그램



이 문서에서 설명하는 단계는 ISE를 통한 모든 게스트 플로우를 지원하기 위한 Unified Access WLC 및 Converged Access WLC의 일반적인 컨피그레이션에 대해 설명합니다.

Unified 5508 WLC 구성

ISE에 구성된 활용 사례에 관계없이 WLC 관점에서는 모두 ISE를 인증 및 계정 관리 서버로 가리키는 MAC 필터링이 활성화된 Open SSID(AAA 재정의 및 RADIUS NAC 포함)에 연결하는 무선 엔드 포인트로 시작합니다. 이렇게 하면 ISE가 ISE의 게스트 포털에 리디렉션을 성공적으로 시행하기 위해 필요한 특성을 WLC에 동적으로 푸시할 수 있습니다.

전역 컨피그레이션

1. 인증 및 계정 관리 서버로 ISE를 전체적으로 추가합니다.

- Security(보안) > AAA > Authentication(인증)으로 이동하고 New(새로 만들기)를 클릭합니다



- ISE 서버 IP 및 공유 암호 입력
- 서버 상태 및 RFC 3676 지원(권한 부여 변경 또는 CoA 지원)이 모두 활성화됨으로 설정되어 있는지 확인합니다.
- 기본적으로 서버 시간 초과에서 AireOS WLC는 2초를 가집니다. 네트워크 특성(다른 위치의 레이턴시, ISE 및 WLC)에 따라 서버 시간 제한을 5초 이상으로 늘려 불필요한 장애 조치 이벤트를 방지하는 것이 유익할 수 있습니다.
- Apply를 클릭합니다.
- 구성할 PSN(Policy Services Node)이 여러 개인 경우 계속해서 추가 서버 항목을 생성합니다.

참고: 이 특정 컨피그레이션 예에는 2개의 ISE 인스턴스가 포함됩니다

- Security(보안) > AAA > RADIUS > Accounting(어카운팅)으로 이동하고 New(새로 만들기)를 클릭합니다.
- ISE 서버 IP 및 공유 암호 입력
- Server Status(서버 상태)가 Enabled(활성화됨)로 설정되어 있는지 확인합니다
- 필요한 경우 서버 시간 제한을 늘립니다(기본값은 2초).

2. 폴백 구성

통합 환경에서 서버 시간 초과가 트리거되면 WLC는 구성된 다음 서버로 이동합니다. WLAN에서 다음 줄을 클릭합니다. 사용 가능한 다른 서버가 없으면 WLC는 전역 서버 목록에서 다음 서버를 선택합니다. 페일오버가 발생한 후 SSID(기본, 보조)에 여러 서버가 구성된 경우, 기본 서버가 다시 온라인 상태가 된 경우에도 WLC는 기본적으로 인증 및(또는) 어카운팅 트래픽을 보조 인스턴스로 영구적으로 계속 전송합니다.

이 동작을 완화하려면 대안을 활성화합니다. Security(보안) > AAA > RADIUS > Fallback(대체)으로 이동합니다. 기본 동작은 off입니다. 서버 다운 이벤트에서 복구할 수 있는 유일한 방법은 관리자 작업(서버의 관리자 상태를 전역적으로 반송)이 필요합니다.

폴백을 활성화하려면 두 가지 옵션이 있습니다.

- **Passive(수동)** - 패시브 모드에서 서버가 WLC 인증 요청에 응답하지 않으면 WLC는 서버를 비활성 대기열로 이동하고 타이머(Interval in Sec 옵션)를 설정합니다. 타이머가 만료되면 WLC는 서버의 실제 상태와 상관없이 서버를 활성 대기열로 이동합니다. 인증 요청으로 시간

초과 이벤트가 발생하면(서버가 다운된 상태임) 서버 항목이 다시 비활성 대기열로 이동되고 타이머가 다시 시작됩니다. 서버가 성공적으로 응답하면 활성 대기열에 남아 있습니다. 여기서 구성 가능한 값은 180~3600초입니다.

- **Active(활성)** - 활성 모드에서 서버가 WLC 인증 요청에 응답하지 않으면 WLC는 서버를 Dead로 표시한 다음 서버를 비활성 서버 풀로 이동하고 서버가 응답할 때까지 주기적으로 프로브 메시지 전송을 시작합니다. 서버가 응답하면 WLC는 데드 서버를 액티브 풀로 이동하고 프로브 메시지 전송을 중지합니다.

이 모드에서는 WLC에서 사용자 이름 및 프로브 간격(초)을 입력해야 합니다(180~3600).

참고: WLC 프로브에는 성공적인 인증이 필요하지 않습니다. 어떤 방식으로든 성공 또는 실패한 인증은 서버를 활성 대기열로 승격하기에 충분한 서버 응답으로 간주됩니다.

게스트의 SSID(Service Set Identifier)를 구성합니다.

- WLANs(WLAN) 탭으로 이동하고 Create New(새로 만들기) 옵션에서 Go(이동)를 클릭합니다.



- 프로파일 이름 및 SSID 이름을 입력합니다. Apply를 클릭합니다.
- General(일반) 탭에서 사용할 인터페이스 또는 인터페이스 그룹(게스트 VLAN)을 선택합니다.



- Security(보안) > Layer 2(레이어 2) > Layer 2 Security(레이어 2 보안)에서 None(없음)을 선택하고 Mac Filtering(Mac 필터링) 확인란을 활성화합니다.



- **AAA Servers(AAA 서버)** 탭 아래에서 Authentication and Accounting servers(인증 및 어카운팅 서버)를 enabled(활성화)로 설정하고 기본 및 보조 서버를 선택합니다.



- **Interim Update**(중간 업데이트): 이 플로우에 혜택을 추가하지 않는 선택적 컨피그레이션입니다. 이를 활성화하려면 WLC i에서 8.x 이상의 코드를 실행해야 합니다.

Disabled(비활성화됨): 기능이 완전히 비활성화되었습니다.

0 간격으로 사용: 클라이언트의 MSCB(Mobile Station Control Block) 항목이 변경될 때마다 WLC가 ISE에 어카운팅 업데이트를 전송합니다(예: IPv4 또는 IPv6 주소 할당 또는 변경, 클라이언트 로밍 이벤트) 추가적인 정기 업데이트는 전송되지 않습니다.

구성된 Interim Interval(중간 간격)으로 활성화됨: 이 모드에서 WLC는 클라이언트의 MSCB 항목이 변경되면 ISE에 알림을 전송하고, 구성된 간격에 추가 정기 어카운팅 알림을 보냅니다(변경 사항과 무관).

- **Advanced**(고급) 탭에서 **Allow AAA Override(AAA 재정의 허용)**를 활성화하고 **NAC State(NAC 상태)**에서 **RADIUS NAC(RADIUS NAC)**를 선택합니다. 이렇게 하면 WLC가 ISE에서 오는 모든 특성 값 쌍(AVP)을 적용합니다.
- **SSID general(SSID 일반)** 탭으로 이동하고 **SSID 상태**를 **Enabled(활성화됨)**로 설정합니다

WLANs > Edit 'Guest'



- 변경 사항을 적용합니다.

리디렉션 ACL 구성

이 ACL은 ISE에서 참조되며 리디렉션되는 트래픽과 허용되는 트래픽을 결정합니다.

- Security Tab(보안 탭) > Access Control Lists(액세스 제어 목록)로 이동하여 New(새로 만들기)를 클릭합니다.
- 다음은 ACL의 예입니다

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	157.210 / 255.255.255.255	TCP	Any	8443	Any	Any	0
4	Permit	157.210 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	157.21 / 255.255.255.255	TCP	Any	8443	Any	Any	0
6	Permit	157.21 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0

이 ACL은 TCP 포트 8443을 통한 DNS 서비스 및 ISE 노드 간 액세스를 허용해야 합니다. 하단에 암시적 거부가 있습니다. 즉 나머지 트래픽이 ISE의 게스트 포털 URL로 리디렉션됩니다.

HTTPS 리디렉션

이 기능은 AireOS 버전 8.0.x 이상에서 지원되지만 기본적으로 꺼져 있습니다. HTTPS 지원을 활성화하려면 WLC Management(WLC 관리) > HTTP-HTTPS > HTTPS Redirection(HTTPS 리디렉션)으로 이동하여 Enabled(활성화됨)로 설정하거나 CLI에서 다음 명령을 적용합니다.

```
(Cisco Controller) >config network web-auth https-redirect enable
```

HTTPS 리디렉션이 활성화된 후 인증서 경고

https-redirect가 활성화된 후 사용자는 리디렉션 중에 인증서 신뢰 문제를 경험할 수 있습니다. 이는 컨트롤러에 유효한 체인 인증서가 있고 이 인증서가 서드파티 신뢰할 수 있는 인증 기관에서 서명한 경우에도 나타납니다. 그 이유는 WLC에 설치된 인증서가 가상 인터페이스 호스트 이름 또는 IP 주소로 발급되기 때문입니다. 클라이언트가 <https://cisco.com>를 시도할 때, 브라우저는 인증서가 cisco.com에 발급되기를 기대합니다. 그러나 WLC가 클라이언트에서 발급한 GET을 가로챌 수 없으려면 먼저 SSL 핸드셰이크 단계 중에 WLC가 가상 인터페이스 인증서를 제시하는 HTTPS 세션을 설정해야 합니다. 이렇게 하면 클라이언트가 액세스하려는 원래 웹 사이트(예: WLC의 가상 인터페이스 호스트 이름이 아닌 cisco.com)에 SSL 핸드셰이크 중에 제공된 인증서가 발행되지 않았으므로 브라우저에서 경고가 표시됩니다. 브라우저마다 다른 인증서 오류 메시지를 볼 수 있지만 모두 동일한 문제와 관련이 있습니다.

적극적인 장애 조치

이 기능은 AireOS WLC에서 기본적으로 활성화되어 있습니다. 적극적인 장애 조치가 활성화된 경우 WLC는 AAA 서버를 응답하지 않는 것으로 표시하고 RADIUS 시간 초과 이벤트가 한 클라이언트에 영향을 준 다음 구성된 AAA 서버로 이동합니다.

이 기능이 비활성화되면 RADIUS 시간 초과 이벤트가 최소 3개의 클라이언트 세션에서 발생한 경우에만 WLC가 다음 서버로 장애 조치됩니다. 이 기능은 이 명령으로 비활성화할 수 있습니다(이 명령에 대한 재부팅 필요 없음).

```
(Cisco Controller) >config radius aggressive-failover disable
```

기능의 현재 상태를 확인하려면

```
(Cisco Controller) >show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Acct Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
```

종속 바이패스

종속 포털을 검색하고 로그인 페이지를 자동 시작하는 CNA(Captive Network Assistant) 메커니즘을 지원하는 엔드포인트는 대개 제어된 창에서 의사 브라우저를 통해 이 작업을 수행하는 반면 다른 엔드포인트는 완전히 작동하는 브라우저를 실행하여 이 작업을 트리거합니다. CNA가 의사(pseudo) 브라우저를 실행하는 엔드포인트의 경우 흐름이 끊어질 수 있습니다 ISE 종속 포털로 리디렉션되는 경우 이는 일반적으로 Apple IOS 디바이스에 영향을 미치며, 특히 디바이스 등록, VLAN DHCP-Release, 규정 준수 확인이 필요한 플로우에 부정적인 영향을 미칩니다.

사용 중인 흐름의 복잡성에 따라 종속 우회를 활성화하는 것이 좋습니다. 이러한 시나리오에서 WLC는 CNA 포털 검색 메커니즘을 무시하며 클라이언트는 브라우저를 열어 리디렉션 프로세스를 시작해야 합니다.

기능의 상태를 확인합니다.

```
(Cisco Controller) >show network summary
```

```
Web Auth CMCC Support ..... Disabled
Web Auth Redirect Ports ..... 80,3128
Web Auth Proxy Redirect ..... Disable
Web Auth Captive-Bypass ..... Disabled
Web Auth Secure Web ..... Enable
Web Auth Secure Redirection ..... Enable
```

이 기능을 활성화하려면 다음 명령을 입력합니다.

```
(Cisco Controller) >config network web-auth captive-bypass enable
```

Web-auth support for Captive-Bypass will be enabled.

You must reset system for this setting to take effect.

WLC는 사용자에게 변경 사항을 적용하려면 재설정 시스템(재시작)이 필요함을 알립니다.

이 시점에서 **show network 요약**은 기능이 활성화된 것으로 표시되지만, 변경 사항을 적용하려면 WLC를 다시 시작해야 합니다.

Converged 3850 NGWC 구성

전역 컨피그레이션

1. 인증 및 계정 관리 서버로 ISE를 전체적으로 추가

- Configuration(컨피그레이션) > Security(보안) > RADIUS > Servers(서버)로 이동하고 New(새로 만들기)를 클릭합니다.
- ISE 서버 IP 주소, 공유 암호, 서버 시간 초과 및 재시도 횟수를 환경 조건을 반영합니다.
- RFC 3570(CoA 지원)에 대한 지원이 활성화되었는지 확인합니다.
- 이 과정을 반복하여 보조 서버 항목을 추가합니다.

RADIUS Servers
Radius Servers > New

Server Name	ISE1
Server IP Address	██████████.157.210
Shared Secret
Confirm Shared Secret
Auth Port (0-65535)	1812
Acct Port (0-65535)	1813
Server Timeout (1-1000)secs	5
Retry Count (0-100)	2
Support for RFC 3576	Enable ▾

2. ISE의 서버 그룹 생성

- Configuration(컨피그레이션) > Security(보안) > Server Groups(서버 그룹)로 이동하고 New(새로 만들기)를 클릭합니다.
- 그룹에 이름을 지정하고 분 단위로 **Dead-time** 값을 입력합니다. 컨트롤러가 활성 서버 목록으로 다시 프로모션되기 전에 서버를 비활성 대기열에 유지하는 시간입니다.
- Available Servers(사용 가능한 서버) 목록에서 Assigned Servers(할당된 서버) 열에 추가합니다.

Radius Server Group
Radius Server Group > New

Name: ISE_Group

MAC-delimiter: colon

MAC-filtering: none

Dead-time (0-1440) in minutes: 10

Group Type: radius

Servers In This Group

Available Servers

Assigned Servers: ISE2, ISE1

3. Dot1x를 전역적으로 사용하도록 설정합니다.

- Configuration(컨피그레이션) > AAA > Method Lists(메소드 목록) > General(일반)로 이동하고 Dot1x system Auth Control을 활성화합니다

General

Dot1x System Auth Control

Local Authentication: None

Local Authorization: None

4. 방법 목록 구성

- Configuration(컨피그레이션) > AAA > Method Lists(방법 목록) > Authentication(인증)으로 이동하여 새 방법 목록을 생성합니다. 이 경우 유형 Dot1x 및 그룹 ISE_Group(이전 단계에서 생성된 그룹)입니다. 그런 다음 Apply를 누릅니다

Authentication
Authentication > New

Method List Name: ISE_Method

Type: dot1x login

Group Type: group local

Fallback to local:

Groups In This Method

Available Server Groups

Assigned Server Groups: ISE_Group

- 어카운팅(Configuration(컨피그레이션) > AAA > Method Lists(메소드 목록) > accounting(어카운팅)) 및 Authorization(Configuration(컨피그레이션) > AAA > Method Lists(메소드 목록) > Authorization(권한 부여)에 대해서도 동일한 작업을 수행합니다. 이렇게 생겼나 보군요

5. 권한 부여 MAC 필터 방법을 생성합니다.

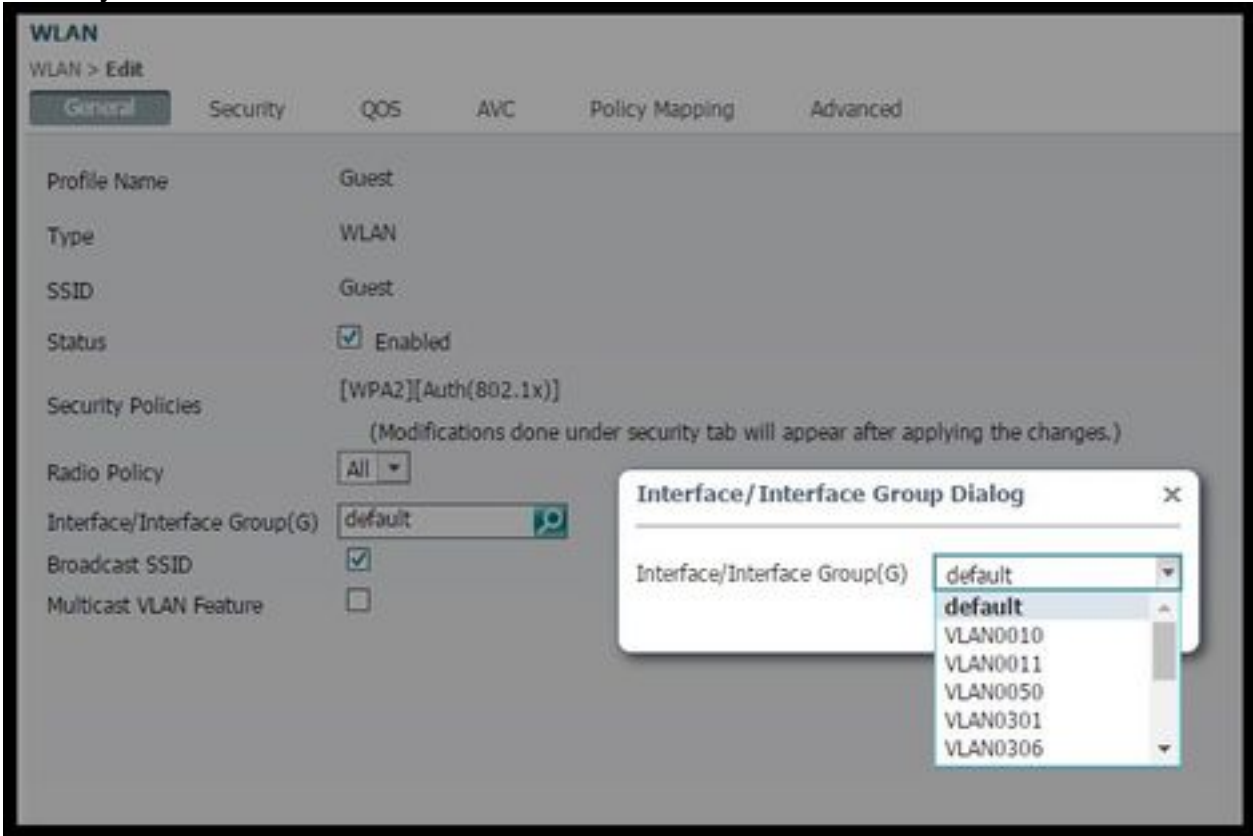
이는 나중에 SSID 설정에서 호출됩니다.

- Configuration(컨피그레이션) > AAA > Method Lists(메소드 목록) > Authorization(권한 부여)으로 이동하고 **New(새로 만들기)**를 클릭합니다.
- 메소드 목록 이름을 입력합니다. Type(유형) = Network(네트워크) 및 Group Type Group(그룹 유형 그룹)을 선택합니다.
- Assigned Server Groups(할당된 서버 그룹) 필드에 ISE_Group을 추가합니다.

SSID 컨피그레이션

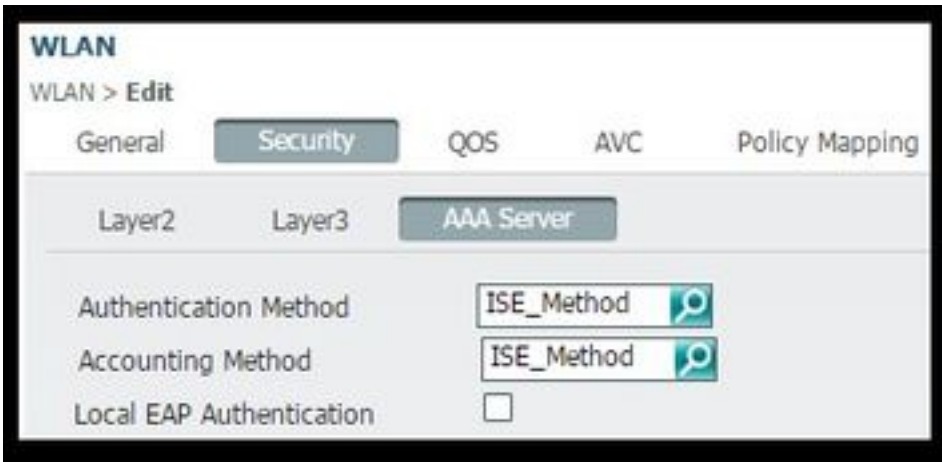
1. 게스트 SSID 생성

- Configuration(컨피그레이션) > **Wireless(무선)** > **WLANs(WLAN)**로 이동하고 New(새로 만들기)를 클릭합니다
- WLAN ID, SSID 및 Profile Name(프로파일 이름)을 입력하고 Apply(적용)를 클릭합니다.
- Interface/Interface Group(인터페이스/인터페이스 그룹) 아래의 SSID 설정에서 Guest VLAN Layer 3 인터페이스를 선택합니다.

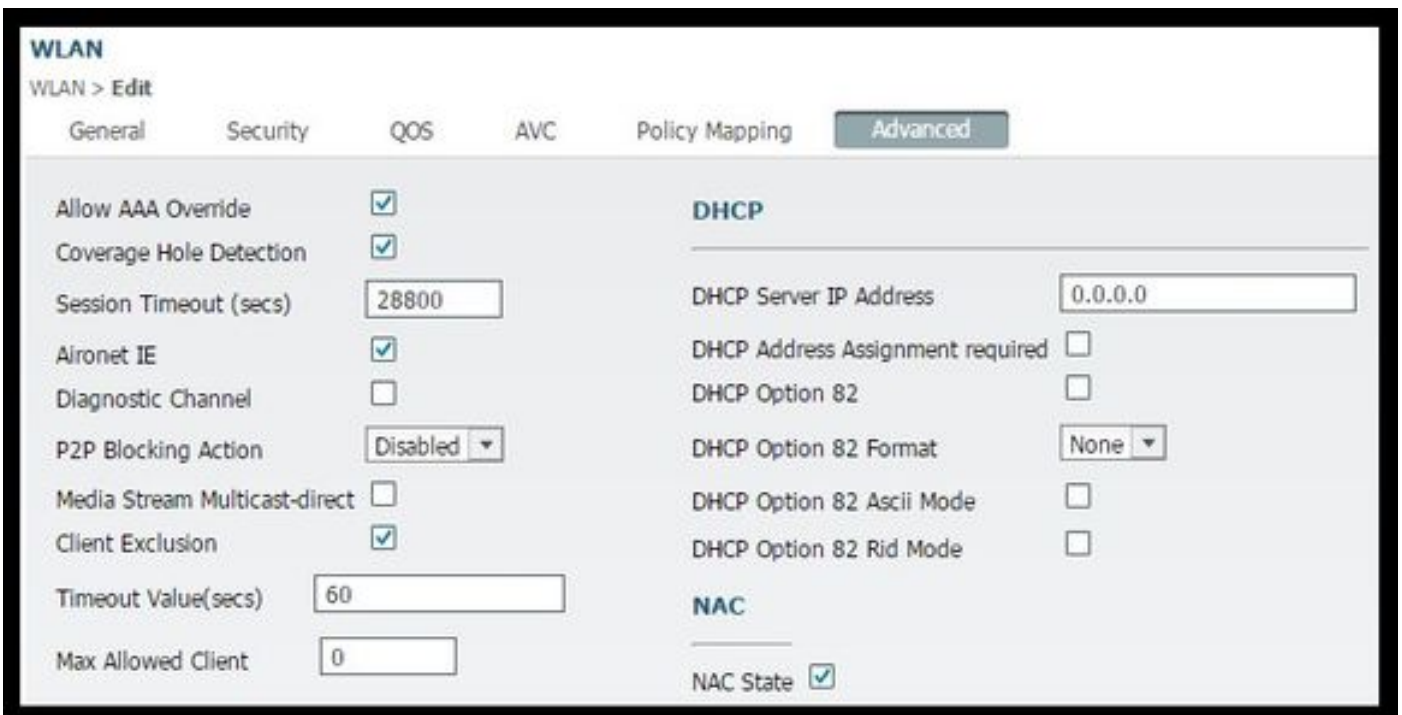


- Security(보안) > Layer 2(레이어 2)에서 None(없음)을 선택하고 Mac Filtering(Mac 필터링) 옆에 이전에 구성한 Mac Filter Method List Name(MacFilterMethod)을 입력합니다.
- Security(보안) > AAA Server(AAA 서버) 탭에서 적절한 Authentication and Accounting methods(인증 및 계정 관리 방법) 목록(ISE_Method)을 선택합니다.





- Advanced(고급) 탭에서 Allow AAA Override and NAC state(AAA 재정의 및 NAC 상태 허용)를 활성화합니다. 나머지 설정은 각 구축 요구 사항(세션 시간 초과, 클라이언트 제외, Aironet Extensions 지원)에 따라 조정해야 합니다.



- General(일반) 탭으로 이동하여 Status(상태)를 Enabled(활성화됨)로 설정합니다. 그런 다음 Apply를 누릅니다.

ACL 구성 리디렉션

이 ACL은 초기 MAB 요청에 대한 응답으로 나중에 access-accept에서 ISE에 의해 참조됩니다. NGWC는 이를 사용하여 리디렉션할 트래픽과 허용해야 할 트래픽을 결정합니다.

- configuration(컨피그레이션) > security(보안) > ACL > Access Control Lists(액세스 제어 목록)로 이동하고 Add New(새로 추가)를 클릭합니다.
- Extended(확장)를 선택하고 ACL Name(ACL 이름)을 입력합니다.
- 이 그림에서는 일반적인 리디렉션 ACL의 예를 보여줍니다.

Access Control Lists
ACLs > ACL detail

Details :

Name: **Guest_Redirect**
Type: **IPv4 Extended**

Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port
<input type="radio"/> 10	deny	icmp	any	any	-	-
<input type="radio"/> 20	deny	udp	any	any	-	eq 67
<input type="radio"/> 30	deny	udp	any	any	-	eq 68
<input type="radio"/> 40	deny	udp	any	any	-	eq 53
<input type="radio"/> 50	deny	tcp	any	157.210	-	eq 8443
<input type="radio"/> 60	deny	tcp	any	157.21	-	eq 8443
<input type="radio"/> 70	permit	tcp	any	any	-	eq 80
<input type="radio"/> 80	permit	tcp	any	any	-	eq 443

참고: 행 10은 선택 사항입니다. 이는 일반적으로 문제 해결 제안을 위해 추가됩니다. 이 ACL은 DHCP, DNS 서비스 및 ISE 서버 포트 TCP 8443(ACE 거부)에 대한 액세스를 허용해야 합니다. HTTP 및 HTTPS 트래픽이 리디렉션됩니다(ACE 허용).

CLI(Command-Line Interface) 컨피그레이션

이전 단계에서 설명한 모든 컨피그레이션은 CLI를 통해서도 적용할 수 있습니다.

802.1x 전역적으로 활성화됨

```
dot1x system-auth-control
```

전역 AAA 컨피그레이션

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa authorization network MacFilterMethod group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
  client 172.16.157.210 server-key *****
  client 172.16.157.21 server-key *****
  auth-type any
!
radius server ISE1
  address ipv4 172.16.157.210 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
radius server ISE2
  address ipv4 172.16.157.21 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
```

```
!  
!  
aaa group server radius ISE_Group  
server name ISE2  
server name ISE1  
deadtime 10  
mac-delimiter colon  
!
```

WLAN 구성

```
wlan Guest 1 Guest  
aaa-override  
accounting-list ISE_Method  
client vlan VLAN0301  
mac-filtering MacFilterMethod  
nac  
no security wpa  
no security wpa akm dot1x  
no security wpa wpa2  
no security wpa wpa2 ciphers aes  
security dot1x authentication-list ISE_Method  
no security ft over-the-ds  
session-timeout 28800  
no shutdown
```

리디렉션 ACL 예

```
3850#show ip access-lists Guest_Redirect  
Extended IP access list Guest_Redirect  
10 deny icmp any any  
20 deny udp any any eq bootps  
30 deny udp any any eq bootpc  
40 deny udp any any eq domain  
50 deny tcp any host 172.16.157.210 eq 8443  
60 deny tcp any host 172.16.157.21 eq 8443  
70 permit tcp any any eq www  
80 permit tcp any any eq 443
```

HTTP 및 HTTPS 지원

```
3850#show run | inc http  
ip http server  
ip http secure-server
```

참고: HTTP를 통한 WLC에 대한 액세스를 제한하기 위해 ACL을 적용할 경우 리디렉션에 영향을 줍니다.

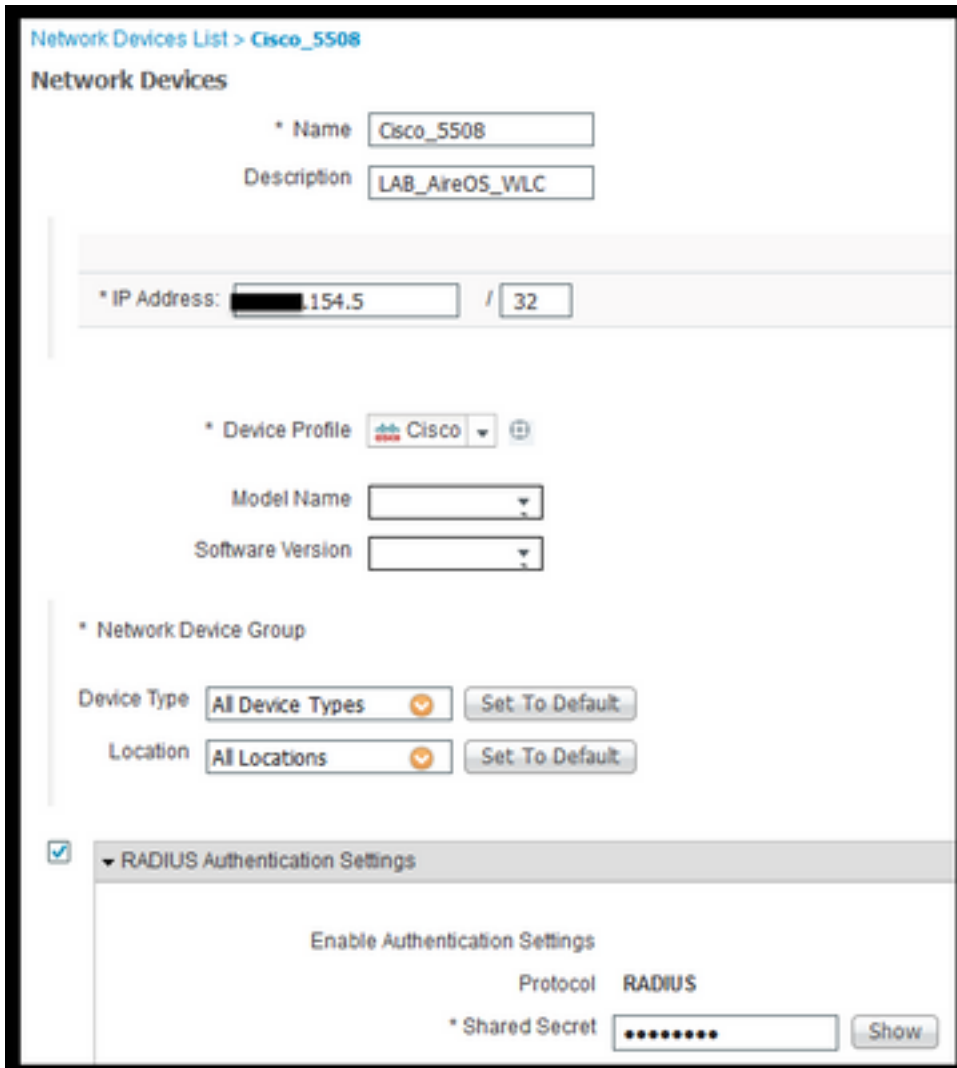
ISE 구성

이 섹션에서는 이 문서에서 설명하는 모든 사용 사례를 지원하는 데 필요한 ISE의 컨피그레이션에

대해 설명합니다.

일반적인 ISE 컨피그레이션 작업

1. ISE에 로그인하고 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동하고 Add(추가)를 클릭합니다.
2. WLC에 연결된 이름 및 디바이스 IP 주소를 입력합니다.
3. RADIUS 인증 설정 상자를 선택하고 WLC 측에 구성된 공유 암호를 입력합니다. 그런 다음 Submit(제출)을 클릭합니다.



The screenshot displays the configuration page for a network device in Cisco ISE. The breadcrumb trail is "Network Devices List > Cisco_5508". The main heading is "Network Devices".

Fields and values shown:

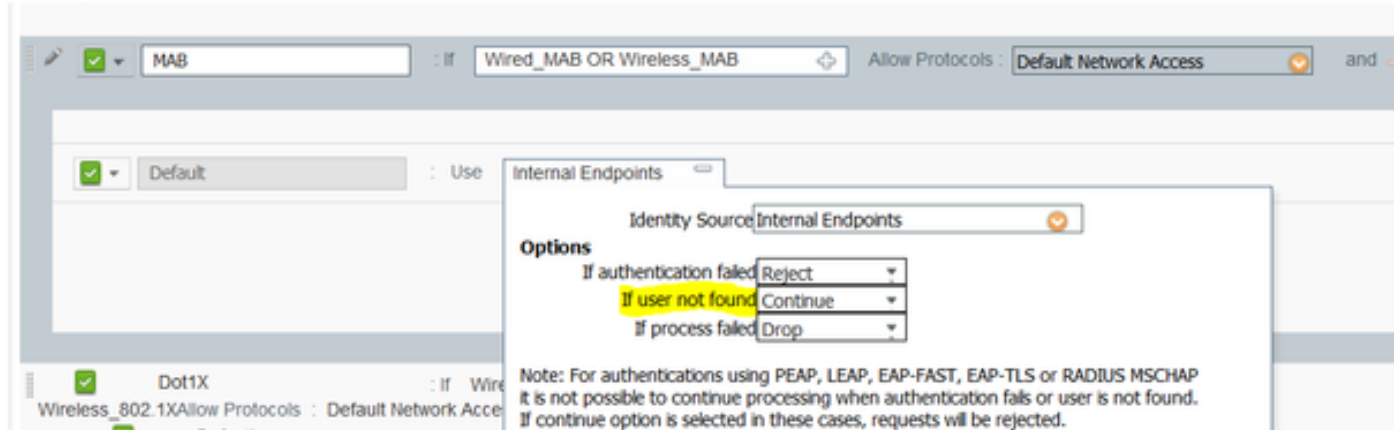
- Name: Cisco_5508
- Description: LAB_AireOS_WLC
- IP Address: [redacted].154.5 / 32
- Device Profile: Cisco
- Model Name: [empty]
- Software Version: [empty]
- Network Device Group: All Device Types (Set To Default), All Locations (Set To Default)
- RADIUS Authentication Settings: Enable Authentication Settings, Protocol: RADIUS, Shared Secret: [masked] (Show button)

4. Policy(정책) > Authentication(인증)으로 이동하고 MAB에서 Edit(편집)를 클릭하고 Use(사용): Internal Endpoints(내부 엔드포인트) 아래에서 If user is not found(사용자를 찾을 수 없는 경우) 옵션이 Continue(계속)로 설정되었는지 확인합니다(기본적으로 있어야 함).

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Policy Type Simple Rule-Based



활용 사례 1: 모든 사용자 연결에서 게스트 인증이 포함된 CWA

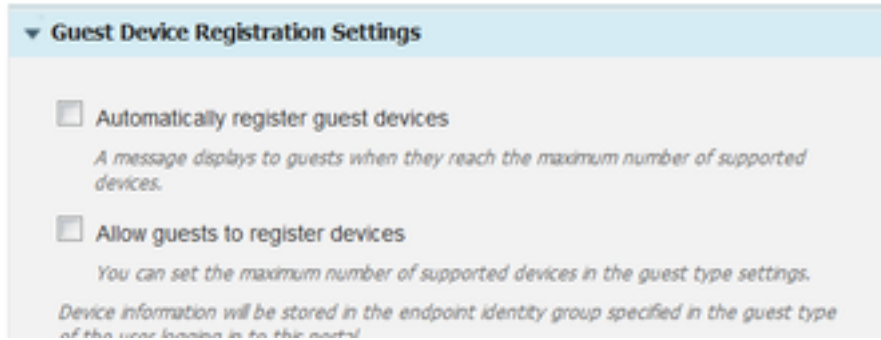
플로우 개요

1. 무선 사용자가 게스트 SSID에 연결합니다.
2. WLC는 ISE의 MAC 주소를 기반으로 AAA 서버로 엔드포인트를 인증합니다.
3. ISE는 두 개의 AVP(Attribute Value Pair)를 사용하여 다시 액세스 및 accept를 반환합니다. url-redirect 및 url-redirect-acl. WLC가 엔드포인트 세션에 이 AVP를 적용하면 스테이션은 DHCP-Required로 전환되고 IP 주소를 가져오면 CENTRAL_WEB_AUTH에 유지됩니다. 이 단계에서 WLC는 클라이언트의 http/https 트래픽 리디렉션을 시작할 준비가 되었습니다.
4. 최종 사용자가 웹 브라우저를 열고 HTTP 또는 HTTPS 트래픽이 생성되면 WLC가 사용자를 ISE 게스트 포털로 리디렉션합니다.
5. 사용자가 게스트 포털에 도착 하면 게스트 자격 증명을 입력 하라는 메시지가 표시 됩니다 (이 경우 후원자 생성).
6. 자격 증명 검증 시 ISE는 AUP 페이지를 표시하고 클라이언트가 수락하면 동적 CoA 유형 재인증이 WLC로 전송됩니다.
7. WLC는 이동 스테이션에 인증 해제를 발행하지 않고 MAC 필터링 인증을 재처리합니다. 엔드포인트와 원활하게 연결되어야 합니다.
8. 재인증 이벤트가 발생하면 ISE는 권한 부여 정책을 재평가하고 이전에 성공한 게스트 인증 이벤트가 있으므로 엔드포인트에 Permit(허용) 액세스 권한이 부여됩니다.

이 프로세스는 사용자가 SSID에 연결할 때마다 반복됩니다.

설정

1. ISE로 이동하고 **Work Centers(작업 센터) > Guest Access(게스트 액세스) > Configure(구성) > Guest Portals(게스트 포털) > Select Sponsored Guest Portal(스폰서 게스트 포털 선택)**(또는 새 포털 유형 Sponsored-Guest 생성)로 이동합니다.
2. **Guest Device Registration settings(게스트 디바이스 등록 설정)**에서 모든 옵션의 선택을 취소하고 **Save(저장)**를 클릭합니다.



3. 정책 > 정책 요소 > 결과 > 권한 부여 > 권한 부여 프로파일로 이동합니다. Add(추가)를 클릭합니다.

4. 이 프로파일은 초기 MAB(Mac authentication bypass) 요청에 대한 응답으로 Redirect-URL 및 Redirect-URL-ACL의 WLC로 푸시됩니다.

- 웹 리디렉션(CWA, MDM, NSP, CPP)을 선택한 후 Select Centralized Web Auth(중앙 집중식 웹 인증 선택), Type the Redirect ACL name under ACL field(ACL 필드 아래에 리디렉션 ACL 이름을 입력하고 Value(값) 아래에서 Sponsored Guest Portal(기본값)(또는 이전 단계에서 생성한 다른 특정 포털)을 선택합니다.

프로필은 이 그림과 비슷해야 합니다. 그런 다음 Save를 클릭합니다.

Authorization Profiles > CWA_Redirect

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP) (i)

ACL Value

Display Certificates Renewal Message

Static IP/Host name/FQDN

페이지 하단의 특성 세부사항: VAP(Attribute Value Pairs)가 WLC로 푸시될 때 이를 설정합니다.

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=Guest_Redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a65b8890-2230-11e6-99ab-005056bf55e0&daysToExpiry=value&action=cwa
```

5. Policy(정책) > Authorization(권한 부여)으로 이동하여 새 규칙을 삽입합니다. 이 규칙은 WLC의 초기 MAC 인증 요청에 대한 응답으로 리디렉션 프로세스를 트리거하는 규칙입니다(이 경우 Wireless_Guest_Redirect라고 함).

6. 조건 아래에서 라이브러리에서 기존 조건 선택을 선택한 다음 조건 이름 아래에서 복합 조건을 선택합니다. Wireless_MAB라는 미리 정의된 복합 조건을 선택합니다.

참고: 이 조건은 WLC에서 시작되는 액세스 요청에 필요한 2개의 Radius 특성으로 구성됩니다(NAS-Port-Type= IEEE 802.11 <모든 무선 요청에 존재> 및 Service-Type = Call Check< mac 인증 우회에 대한 특정 요청을 참조>).

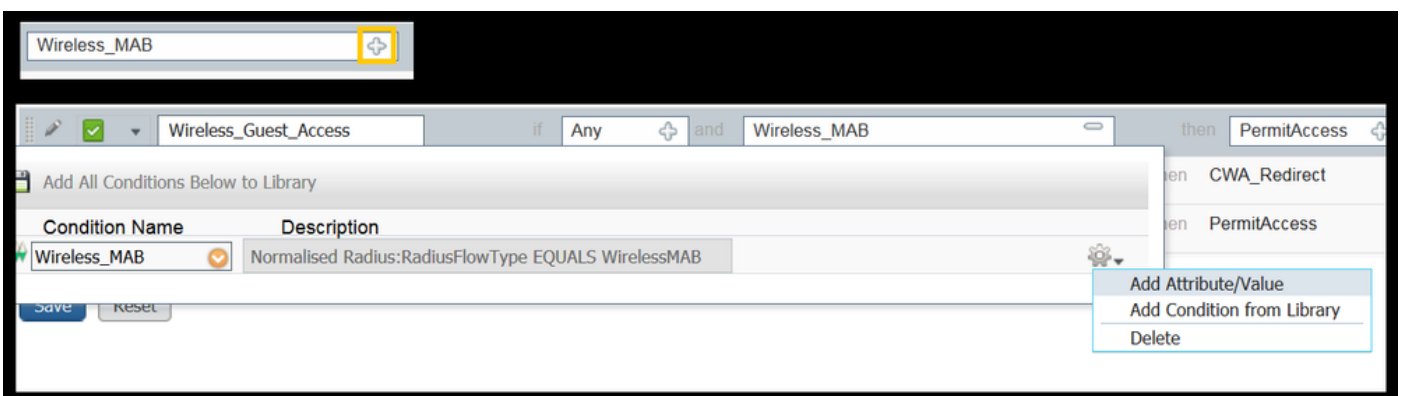
7. 결과에서 Standard > CWA_Redirect(이전 단계에서 생성한 권한 부여 프로파일)를 선택합니다. 그런 다음 Done(완료)을 클릭하고 Save(저장)를 클릭합니다

Wireless_Guest_Redirect if Wireless_MAB then CWA_Redirect Edit

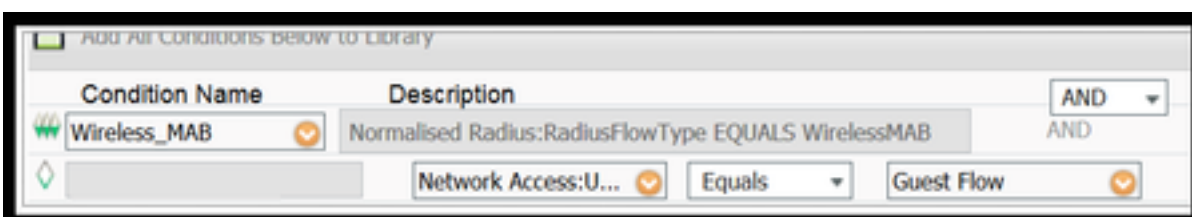
8. CWA_Redirect 규칙 끝으로 이동하고 Edit 옆의 화살표를 클릭합니다. 그런 다음 위에서 중복을 선택합니다.

9. 세션이 ISE의 CoA(이 경우 Wireless_Guest_Access)에서 재인증되면 엔드포인트가 매칭하는 정책이므로 이름을 수정합니다.

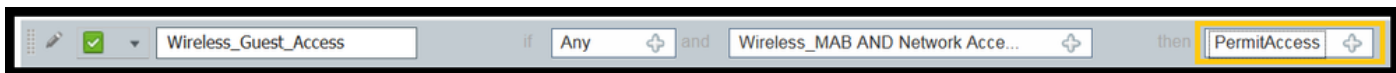
10. Wireless_MAB 복합 조건 옆에서 + 기호를 클릭하여 조건을 확장하고 Wireless_MAB 조건 끝까지 Add Attribute/Value를 클릭합니다.



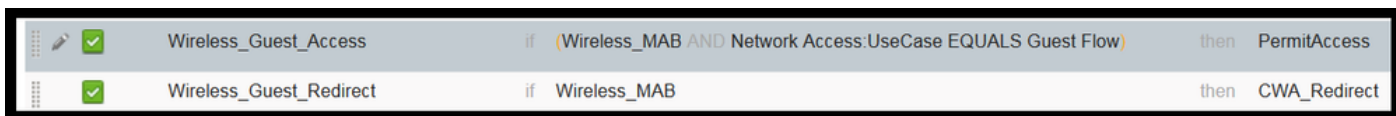
11. "Select Attribute(특성 선택)"에서 Network Access(네트워크 액세스) > UseCase Equals Guest flow(UseCase Equals 게스트 플로우)를 선택합니다.



12. Permissions(권한)에서 PermitAccess(액세스 허용)를 선택합니다. 그런 다음 Done(완료)을 클릭하고 Save(저장)를 클릭합니다



두 정책은 다음과 유사해야 합니다.



활용 사례 2: CWA with Device Registration에서는 하루에 한 번 게스트 인증을 적용합니다.

플로우 개요

1. 무선 사용자가 게스트 SSID에 연결합니다.
2. WLC는 ISE의 MAC 주소를 기반으로 AAA 서버로 엔드포인트를 인증합니다.
3. ISE는 두 개의 AVP(Attribute Value Pairs)(url-redirect 및 url-redirect-acl)를 사용하여 반환 및 액세스 승인을 반환합니다.
4. WLC가 엔드포인트 세션에 이 AVP를 적용하면 스테이션은 DHCP-Required로 전환되고 IP 주소를 가져오면 CENTRAL_WEB_AUTH에 유지됩니다. 이 단계에서 WLC는 클라이언트의 http/https 트래픽 리디렉션을 시작할 준비가 되었습니다.
5. 최종 사용자가 웹 브라우저를 열고 HTTP 또는 HTTPS 트래픽이 생성되면 WLC가 사용자를 ISE 게스트 포털로 리디렉션합니다.
6. 사용자가 게스트 포털에 도착하면 스폰서가 생성한 자격 증명을 입력하라는 프롬프트가 표시됩니다.
7. 자격 증명 검증 시 ISE는 이 엔드포인트를 특정(사전 구성된) 엔드포인트 ID 그룹(디바이스 등록)에 추가합니다.
8. AUP 페이지가 표시되고 클라이언트가 수락하면 Dynamic CoA type Re-authenticate가 표시됩니다. WLC로 전송됩니다.
9. WLC는 이동 스테이션에 인증 해제를 실행하지 않고 MAC 필터링 인증을 재처리합니다. 엔드포인트와 원활하게 연결되어야 합니다.
10. 재인증 이벤트가 발생하면 ISE는 권한 부여 정책을 재평가합니다. 엔드포인트가 올바른 엔드포인트 ID 그룹 ISE의 멤버이므로 이번에는 제한 없이 액세스 승인을 반환합니다.
11. 엔드포인트는 6단계에서 등록되었으므로 사용자가 돌아올 때마다 ISE에서 수동으로 제거될 때까지 네트워크에서 허용되거나, 엔드포인트 비우기 정책이 실행되어 기준을 충족하는 엔드포인트를 플래시합니다.

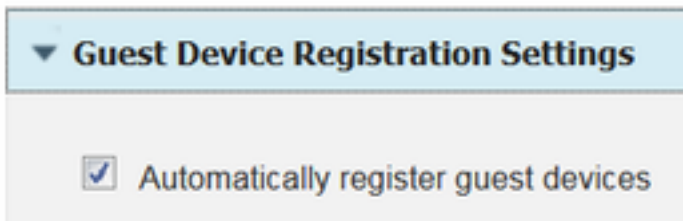
이 Lab 시나리오에서는 하루에 한 번 인증이 시행됩니다. 재인증 트리거는 엔드 포인트 ID 그룹의 모든 엔드 포인트를 매일 제거 하는 엔드 포인트 비우기 정책 입니다.

참고: 마지막 AUP 수락 이후 경과 시간을 기준으로 게스트 인증 이벤트를 적용할 수 있습니다 . 게스트 로그인을 하루에 한 번 더 자주 적용해야 하는 경우(예: 4시간마다) 이 옵션을 선택할 수 있습니다.

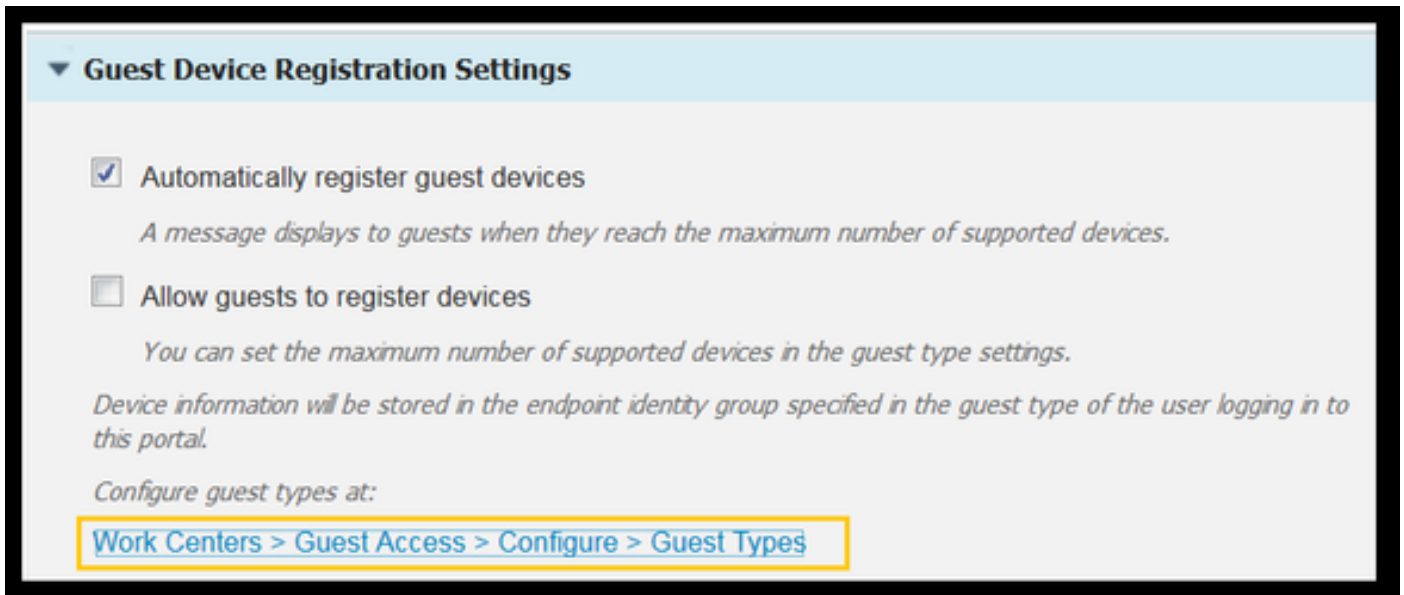
설정

1. ISE에서 **Work Centers(작업 센터) > Guest Access(게스트 액세스) > Configure(구성) > Guest Portals(게스트 포털) > Select Sponsored Guest Portal(스폰서 게스트 포털 선택)**(또는 새 포털 유형 Sponsored-Guest 생성)로 이동합니다.
2. **Guest Device Registration settings(게스트 디바이스 등록 설정)**에서 **Automatically register guest devices(게스트 디바이스 자동 등록)** 옵션이 선택되어 있는지 확인합니다. 저장을 클릭

합니다.



3. Work center(작업 센터) > Guest Access(게스트 액세스) > Configure(구성) > Guest Types(게스트 유형)로 이동하거나 포털의 Guest Device Registration Settings(게스트 디바이스 등록 설정)에서 지정된 바로 가기를 클릭합니다.



4. 스폰서 사용자가 게스트 계정을 생성할 때 게스트 유형을 할당합니다. 각 개별 게스트 유형에는 다른 엔드포인트 ID 그룹에 속하는 등록된 엔드포인트가 있을 수 있습니다. 디바이스를 추가해야 하는 엔드포인트 ID 그룹을 할당하려면 스폰서가 이러한 게스트 사용자에게 대해 사용하는 게스트 유형을 선택합니다(이 활용 사례는 매주(기본값) 기준).

5. 게스트 유형에서 로그인 옵션 아래의 드롭다운 메뉴에서 게스트 디바이스 등록을 위한 엔드포인트 ID 그룹을 선택합니다

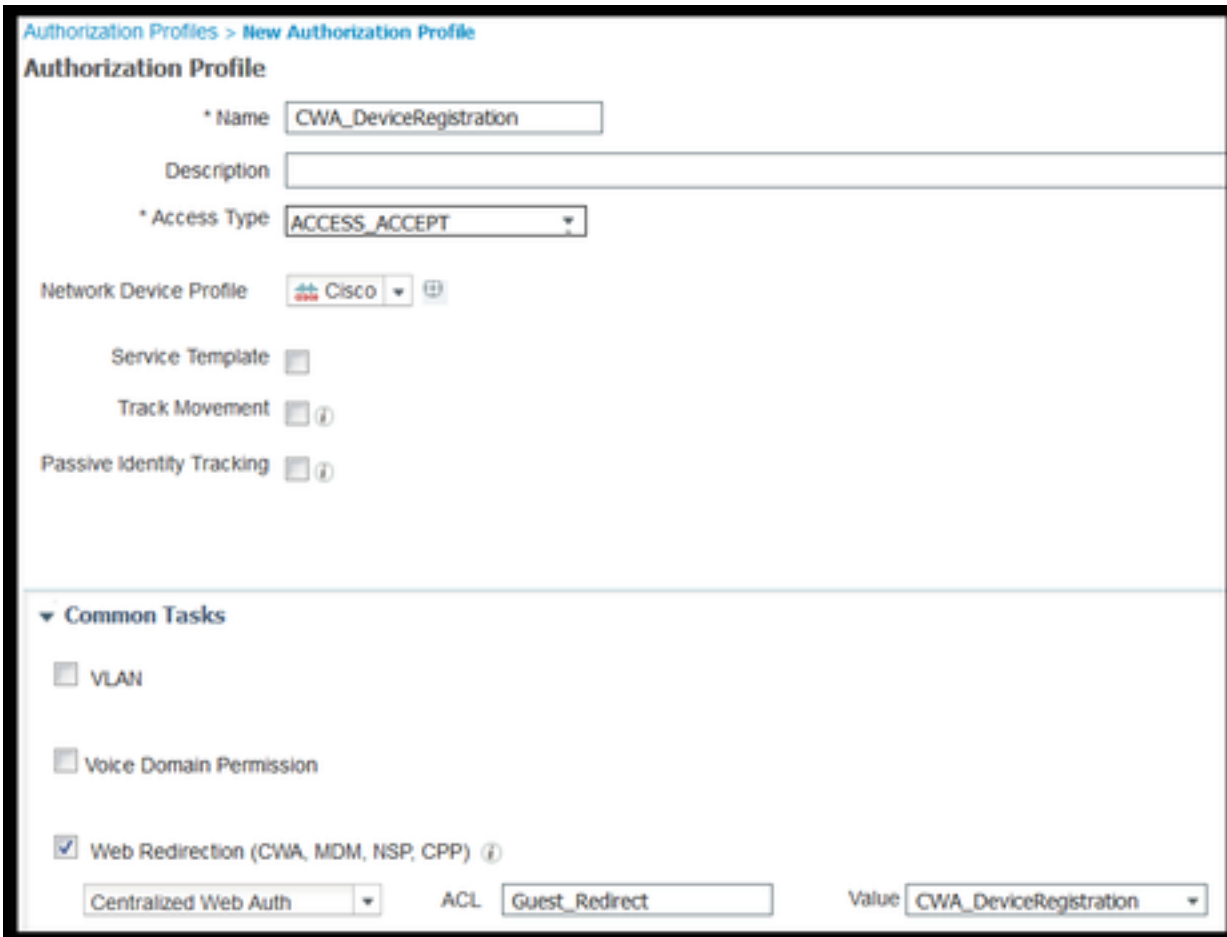
Maximum devices guests can register: (1-999)

Endpoint identity group for guest device registration: ⓘ

6. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)로 이동합니다. Add(추가)를 클릭합니다.

7. 이 프로파일은 초기 MAB(Mac authentication bypass) 요청에 대한 응답으로 Redirect-URL 및 Redirect-URL-ACL의 WLC로 푸시됩니다.

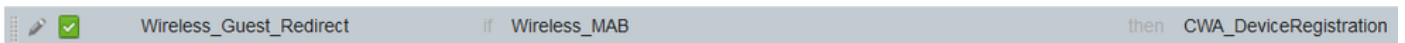
- 웹 리디렉션(CWA, MDM, NSP, CPP)을 선택한 후 Centralized Web Auth를 선택한 다음 ACL 필드 아래에 리디렉션 ACL 이름을 입력하고 Value(값) 아래에서 이 플로우에 대해 생성된 포털(CWA_DeviceRegistration)을 선택합니다.



8. Policy(정책) > Authorization(권한 부여)으로 이동하여 새 규칙을 삽입합니다. 이 규칙은 WLC의 초기 MAC 인증 요청에 대한 응답으로 리디렉션 프로세스를 트리거하는 규칙입니다(이 경우 Wireless_Guest_Redirect라고 함).

9. 조건에서 라이브러리에서 기존 조건 선택을 선택한 다음 조건 이름에서 복합 조건을 선택합니다. Wireless_MAB라는 미리 정의된 복합 조건을 선택합니다.

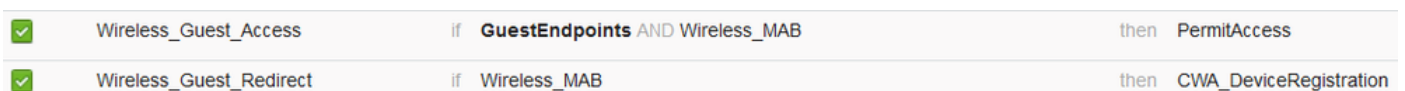
10. 결과 아래에서 Standard > CWA_DeviceRegistration(이전 단계에서 생성한 권한 부여 프로파일)을 선택합니다. 그런 다음 Done(완료)을 클릭하고 Save(저장)를 클릭합니다



11. 위의 정책을 복제하고, 엔드포인트가 재인증 이벤트(Wireless_Guest_Access라고 함)에서 반환된 후 발견한 정책이므로 이름을 수정합니다.

12. Identity Group Details(ID 그룹 세부 정보) 상자에서 Endpoint Identity Group(엔드포인트 ID 그룹)을 선택하고 Guest Type(GuestEndpoints) 아래에서 참조하는 그룹을 선택합니다.

13. Results(결과)에서 PermitAccess(액세스 허용)를 선택합니다. Done(완료)을 클릭하고 변경 사항을 저장합니다.



14. 매일 GuestEndpoint 그룹을 지우는 엔드포인트 비우기 정책을 생성하고 생성합니다.

- Administration(관리) > Identity management(ID 관리)> Settings(설정) > Endpoint Purge(엔드

포인트 제거)로 이동합니다

- Purge 규칙에서 Elapsed Time이 30일을 초과하는 경우 기본적으로 GuestEndpoints 삭제를 트리거하는 하나가 있어야 합니다.
- GuestEndpoints에 대한 기존 정책을 수정하거나 새 정책을 만듭니다(기본값이 제거된 경우). 비우기 정책은 정의된 시간에 매일 실행됩니다.


이 경우 조건은 GuestEndpoints의 Members with Elapsed Days less than 1 day(경과된 일이 1일 미만인 게스트 엔드포인트의 멤버)입니다

활용 사례 3: HostSpot 포털

플로우 개요

1. 무선 사용자가 게스트 SSID에 연결합니다.
2. WLC는 ISE를 AAA 서버로 사용하여 MAC 주소를 기반으로 엔드포인트를 인증합니다.
3. ISE는 두 개의 AVP(Attribute Value Pair)가 포함된 access-accept를 반환합니다. url-redirect 및 url-redirect-acl.
4. WLC가 엔드포인트 세션에 이 AVP를 적용하면 스테이션은 DHCP-Required로 전환되고 IP 주소를 가져오면 CENTRAL_WEB_AUTH에 유지됩니다. 이 단계에서 WLC는 클라이언트의 http/https 트래픽을 리디렉션할 준비가 되었습니다.
5. 최종 사용자가 웹 브라우저를 열고 HTTP 또는 HTTPS 트래픽이 생성되면 WLC는 사용자를 ISE HotSpot 포털로 리디렉션합니다.
6. 포털에서 사용자는 Acceptable Use Policy(사용 제한 정책)를 수락하라는 프롬프트가 표시됩니다.
7. ISE는 엔드포인트 MAC 주소(엔드포인트 ID)를 구성된 엔드포인트 ID 그룹에 추가합니다.
8. 요청을 처리하는 PSN(Policy Services Node)에서 WLC에 Dynamic CoA type **Admin-Reset**을 실행합니다.
9. WLC가 수신 CoA 처리를 완료하면 클라이언트에 대해 인증 해제를 실행합니다(클라이언트가 돌아오는 데 걸리는 시간에 대한 연결이 끊어짐).
10. 클라이언트가 다시 연결되면 새 세션이 생성되므로 ISE 측에서 세션 연속성이 없습니다. 이는 인증이 새 스레드로 처리됨을 의미합니다.
11. 엔드포인트가 구성된 엔드포인트 ID 그룹에 추가되고, 엔드포인트가 해당 그룹의 일부인지 확인하는 권한 부여 정책이 있으므로 새 인증은 이 정책과 일치합니다. 그 결과 게스트 네트워크에 대한 전체 액세스 권한을 갖게 됩니다.
12. 엔드포인트 ID 개체가 엔드포인트 제거 정책의 결과로 ISE 데이터베이스에서 삭제되지 않는 한 사용자는 AUP를 다시 수락할 필요가 없습니다.

설정

1. 등록 시 이러한 디바이스를 이동할 새 엔드포인트 ID 그룹을 생성합니다. Work Centers(작업 센터) > Guest Access(게스트 액세스) > Identity Groups(ID 그룹) > Endpoint Identity Groups(엔드포인트 ID 그룹)로 이동하고  .
- 그룹 이름(이 예에서는 HotSpot_Endpoints)을 입력합니다. 설명을 추가하고 상위 그룹이 필요하지 않습니다.

Endpoint Identity Group List > HotSpot_Endpoints

Endpoint Identity Group

* Name

Description

Parent Group

2. Work Centers(작업 센터) > Guest Access(게스트 액세스) > Configure(구성) > Guest Portals(게스트 포털)로 이동하고 Hotspot Portal(핫스팟 포털)을 선택합니다(기본값).

3. Portal Settings(포털 설정)를 확장하고 Endpoint Identity Group(엔드포인트 ID 그룹)에서 Endpoint Identity Group(엔드포인트 ID 그룹) 아래의 HostSpot_Endpoints group(호스트 스팟_엔드포인트 그룹)을 선택합니다. 이렇게 하면 등록된 디바이스가 지정된 그룹에 전송됩니다.

Endpoint

Identity *Configure endpoint identity groups at:*
group: * [Work Centers](#) > [Guest Access](#) > [Identity Groups](#)

4. 변경사항을 저장합니다.

5. WLC에서 시작한 MAB 인증 시 HotSpot 포털을 호출하는 권한 부여 프로파일을 생성합니다.

- Policy(정책) > Policy elements(정책 요소) > Results(결과) > authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)로 이동하고 하나(HotSpotRedirect)를 생성합니다.
- 웹 리디렉션(CWA, MDM, NSP, CPP)을 선택한 후 Hot Spot(핫 스팟)을 선택하고 ACL 필드 (Guest_Redirect)에 리디렉션 ACL 이름을 입력한 다음 Value(값)로 올바른 포털(핫스팟 포털(기본값))을 선택합니다.

Add New Standard Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

▼ Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Hot Spot ACL Value

Static IP/Host name/FQDN

▼ Attributes Details

Access Type = ACCESS_ACCEPT
 cisco-av-pair = url-redirect-ad=Guest_Redirect
 cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a60e04d0-2230-11e6-99ab-005056bf55e0&action=cwa&type=drw

6. WLC의 초기 MAB 요청 시 HotSpotRedirect 결과를 트리거하는 권한 부여 정책을 생성합니다.

- Policy(정책) > Authorization(권한 부여)으로 이동하고 새 규칙을 삽입합니다. 이 규칙은 WLC의 초기 MAC 인증 요청에 대한 응답으로 리디렉션 프로세스를 트리거하는 규칙입니다(이 경우 **Wireless_HotSpot_Redirect**라고 함).
- Conditions(조건) 아래에서 **Select Existing Condition from Library**(라이브러리에서 기존 조건 선택)를 선택한 다음 조건 이름 아래에서 **Compound condition**(복합 조건)을 선택합니다
- 결과 아래에서 **Standard > HotSpotRedirect**(이전 단계에서 생성한 권한 부여 프로파일)를 선택합니다. 그런 다음 **Done**(완료)을 클릭하고 **Save**(저장)를 클릭합니다

7. 두 번째 권한 부여 정책을 생성합니다.

- 위의 정책을 복제하고, 엔드포인트가 재인증 이벤트(Wireless_HotSpot_Access라고 함)에서 반환된 후 적용하는 정책이므로 이름을 수정합니다.
- Identity Group Details(ID 그룹 세부 정보) 상자에서 **Endpoint Identity Group**(엔드포인트 ID 그룹)을 선택한 다음 이전에 생성한 그룹(HotSpot_Endpoints)을 선택합니다.
- 결과 아래에서 허용 액세스를 선택합니다. **Done**(완료)을 클릭하고 변경 사항을 저장합니다.

Wireless_HotSpot_Access	if HotSpot_Endpoints AND Wireless_MAB	then PermitAccess
Wireless_HotSpot_Redirect	if Wireless_MAB	then HotSpotRedirect

8. 5일보다 긴 경과 시간으로 끝점을 지우는 비우기 정책을 구성합니다.

- Administration(관리) > Identity Management(ID 관리) > Settings(설정) > Endpoint Purge(엔드포인트 제거)로 이동하고 Purge rules(제거 규칙)에서 새 ID를 생성합니다.
- Identity Group Details(ID 그룹 세부사항) 상자에서 **Endpoint Identity Group**(엔드포인트 ID 그룹) > **HotSpot_Endpoints**를 선택합니다
- 조건에서 **Create New Condition (Advanced Option)**을 클릭합니다.
- Select Attribute(특성 선택)에서 **ENDPOINTPURGE : ElapsedDays GREATER THAN 5**일을 선택합니다.

HotSpot_Endpoints_PurgeRule	if HotSpot_Endpoints AND ENDPOINTPURGE:ElapsedDays GREATER THAN 5
-----------------------------	---

다음을 확인합니다.

활용 사례 1

1. 사용자가 게스트 SSID에 연결합니다.
2. 브라우저를 열고 HTTP 트래픽이 생성되는 즉시 게스트 포털이 표시됩니다.
3. 게스트 사용자가 AUP를 인증하고 수락하면 성공 페이지가 표시됩니다.
4. 재인증 CoA가 전송됩니다(클라이언트에 투명).
5. 엔드포인트 세션은 네트워크에 대한 전체 액세스 권한으로 재인증됩니다.
6. 모든 후속 게스트 연결은 네트워크에 액세스하기 전에 게스트 인증을 통과해야 합니다.



Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

Password:

Sign On

[Don't have an account?](#)



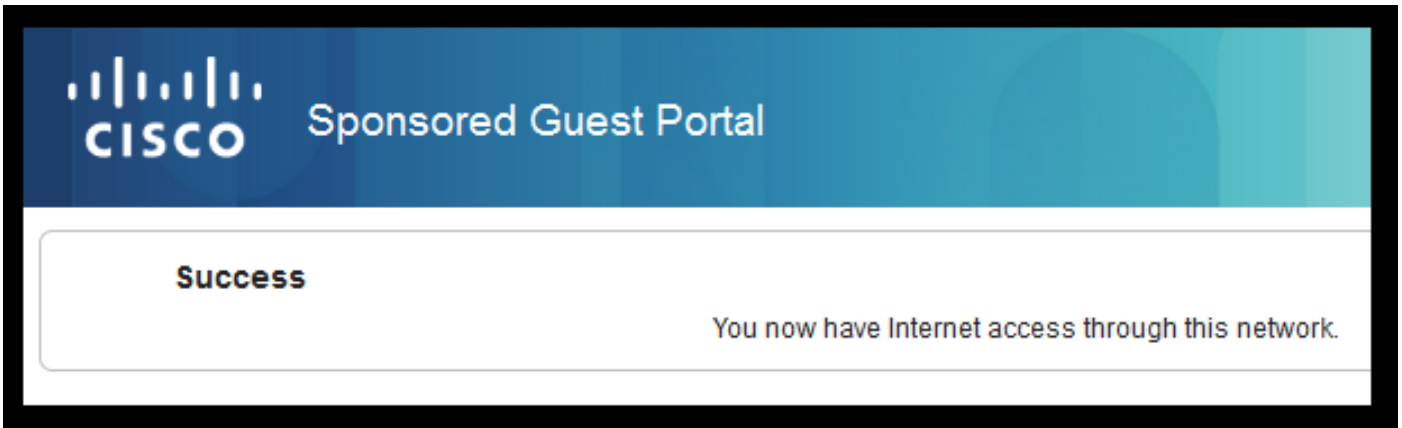
Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline

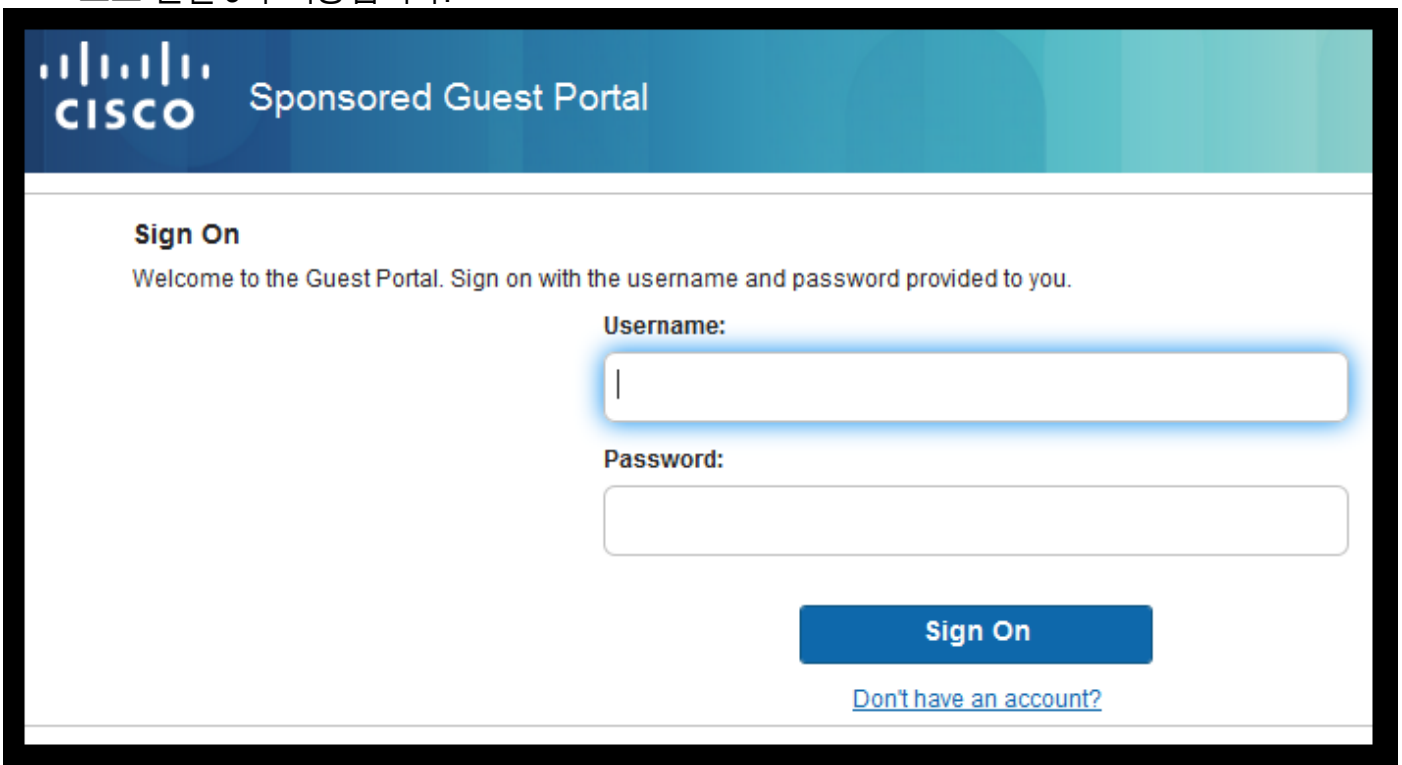


ISE RADIUS 라이브 로그에서 플로우:

1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Accounting Start
1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Re-Authentication Event
	68:7F:74:72:18:2E					← CoA Event
1001	68:7F:74:72:18:2E					← Guest Authentication Event
68:7F:74:72:18:2E	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MA...	Default >> Wir...	CWA_Redirect	← Initial MAB request

활용 사례 2

1. 사용자가 게스트 SSID에 연결합니다.
2. 브라우저를 열고 HTTP 트래픽이 생성되는 즉시 게스트 포털이 표시됩니다.
3. 게스트 사용자가 AUP를 인증하고 수락하면 디바이스가 등록됩니다.
4. 성공 페이지가 표시되고 재인증 CoA가 전송됩니다(클라이언트에 투명).
5. 엔드포인트 세션은 네트워크에 대한 전체 액세스 권한으로 재인증됩니다.
6. 엔드포인트가 구성된 엔드포인트 ID 그룹에 있는 한 게스트 인증을 적용하지 않고 이후의 게스트 연결 9가 허용됩니다.





Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline



Welcome Message

Click **Continue** to connect to the network.

You're very close to gaining network access.

Continue



Sponsored Guest Portal

Success

You now have Internet access through this network.

ISE RADIUS 라이브 로그에서 플로우:

Status	Details	Identity	Endpoint ID	Authorization Profiles	Identity Group
●		68.7F:74.72:1...	68.7F:74.72:...	PermitAccess	
✓		68.7F:74.72:1...	68.7F:74.72:...	PermitAccess	GuestEndpoints
✓		hfr592	68.7F:74.72:...	PermitAccess	User Identity Groups:GuestType_Contractor (default)...
✓			68.7F:74.72:...		
✓		hfr592	68.7F:74.72:...		GuestType_Contractor (default)
✓		68.7F:74.72:1...	68.7F:74.72:...	CWA_DeviceRegistration	Profiled

Accounting Start
Subsequent MAB request(no redirect to guest portal)
Re-Authentication Event
CoA Reauth Event
Guest Authentication and Device Registration
Initial MAB request

활용 사례 3

1. 사용자가 게스트 SSID에 연결합니다.
2. 브라우저를 열고 HTTP 트래픽이 생성되는 즉시 AUP 페이지가 표시됩니다.
3. 게스트 사용자가 AUP를 수락하면 디바이스가 등록됩니다.
4. 성공 페이지가 표시되고 Admin-Reset CoA가 전송됩니다(클라이언트에 투명).
5. 엔드포인트가 네트워크에 대한 전체 액세스로 다시 연결됩니다.
6. 엔드포인트가 구성된 엔드포인트 ID 그룹에 남아 있는 한 AUP 수락을 적용하지 않고(달리 구성되지 않는 한) 후속 게스트 연결이 허용됩니다.



Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

Accept

Decline



Connection Successful

You have successfully connected to the network.

AireOS의 FlexConnect 로컬 스위칭

FlexConnect 로컬 스위칭이 구성된 경우 네트워크 관리자는 다음을 확인해야 합니다.

- 리디렉션 ACL은 FlexConnect ACL로 구성됩니다.
- 리디렉션 ACL은 FlexConnect Tab(FlexConnect 탭) > **External WebAuthentication ACLs(외부 웹 인증 ACL)** > Policies(정책) > Select Redirect ACL(리디렉션 ACL 선택)에서 AP 자체를 통해 어떤 방식으로든 정책으로 적용되었습니다.

All APs > Details for aaa-ap-3

General Credentials Interfaces High Availability Inventory **FlexConnect** Advanced

VLAN Support

Native VLAN ID 301 **VLAN Mappings**

FlexConnect Group Name Not Configured

PreAuthentication Access Control Lists

External WebAuthentication ACLs

Local Split ACLs

Central DHCP Processing

Layer2 ACLs

Policies

Policy ACL CWA_Redirect **Add**

Policy Access Control Lists

CWA_Redirect

또는 FlexConnect 그룹에 정책 ACL을 추가하여(Wireless > FlexConnect Groups > Select the correct group > ACL Mapping > Policies Redirect ACL을 선택하고 Add를 클릭합니다)

FlexConnect Groups > Edit 'test'

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP WLAN VLAN mapping

AAA VLAN-ACL mapping WLAN-ACL mapping **Policies**

Policies

Policy ACL CWA_Redirect **Add**

Policy Access Control Lists

CWA_Redirect

TOR_Redirect

정책 ACL을 추가하면 구성된 ACL을 FlexConnect 그룹의 AP 멤버로 푸시하도록 WLC가 트리거됩니다. 이 작업을 수행하지 않으면 웹 리디렉션 문제가 발생합니다.

외부 앵커 시나리오

자동 앵커(외부 앵커) 시나리오에서는 다음 사실을 강조하는 것이 중요합니다.

- 리디렉션 ACL은 외부 및 앵커 WLC에서 모두 정의되어야 합니다. 앵커에만 적용되는 경우에도 마찬가지입니다.
- 레이어 2 인증은 항상 외부 WLC에 의해 처리됩니다. 이는 모든 RADIUS 인증 및 어카운팅 트래픽이 ISE와 외부 WLC 간에 발생하므로 설계 단계(트러블슈팅도 수행)에서 중요합니다.
- 리디렉션 AVP가 클라이언트 세션에 적용되면 외부 WLC는 모빌리티 전달 메시지를 통해 앵커의 클라이언트 세션을 업데이트합니다.
- 이때 앵커 WLC는 미리 구성된 리디렉션 ACL을 사용하여 리디렉션을 적용하기 시작합니다.
- 앵커 및 외부 모두에서 오는 ISE(동일한 인증 이벤트 참조)에 대한 계정 업데이트를 방지하려면 앵커 WLC SSID에서 계정 관리를 완전히 해제해야 합니다.
- URL 기반 ACL은 외부 앵커 시나리오에서 지원되지 않습니다.

문제 해결

AireOS 및 Converged Access WLC에서 공통적으로 손상된 상태

1. 클라이언트가 게스트 SSID에 참가할 수 없습니다.

"show client detailed xx:xx:xx:xx:xx"를 입력하면 클라이언트가 START에 머물러 있음을 알 수 있습니다. 일반적으로 이는 WLC가 AAA 서버가 반환하는 특성을 적용할 수 없음을 나타냅니다.

ISE에서 푸시한 리디렉션 ACL 이름이 WLC에 사전 정의된 ACL의 이름과 정확히 일치하는지 확인합니다.

ISE가 WLC(VLAN ID, 인터페이스 이름, Airespace-ACL)로 푸시다운하도록 구성한 다른 특성에도 동일한 원칙이 적용됩니다. 그런 다음 클라이언트는 DHCP로 전환한 다음 CENTRAL_WEB_AUTH로 전환해야 합니다.

2. 리디렉션 AVP는 클라이언트의 세션에 적용되지만 리디렉션이 작동하지 않음

클라이언트의 정책 관리자 상태가 SSID에 대해 구성된 동적 인터페이스에 정렬된 유효한 IP 주소를 사용하는 CENTRAL_WEB_AUTH인지 확인하고 Redirect ACL 및 URL-Redirect 특성이 클라이언트의 세션에 적용되는지 확인합니다.

리디렉션 ACL

AireOS WLC에서 리디렉션 ACL은 양방향으로 TCP 포트 8443의 DNS 및 ISE와 같이 리디렉션하지 않아야 하는 트래픽을 명시적으로 허용해야 하며 암시적 거부 ip any는 나머지 트래픽을 리디렉션하도록 트리거합니다.

컨버지드 액세스에서는 논리가 정반대입니다. Deny ACE는 ACE가 리디렉션을 트리거하는 동안 리디렉션을 우회합니다. 따라서 TCP 포트 80 및 443을 명시적으로 허용하는 것이 좋습니다.

게스트 VLAN에서 포트 8443을 통해 ISE에 대한 액세스를 확인합니다. 컨피그레이션 측면에서 모든 것이 잘 보이는 경우 가장 쉽게 진행할 수 있는 방법은 클라이언트의 무선 어댑터 뒤에 있는 캡처를 수집하고 리디렉션이 중단된 위치를 확인하는 것입니다.

- DNS 확인이 수행됩니까?
- 요청한 페이지에 대해 TCP 3 way 핸드셰이크가 완료되었습니까?
- 클라이언트가 GET을 시작한 후 WLC에서 리디렉션 작업을 반환합니까?

- 8443을 통한 ISE에 대한 TCP 3 way 핸드셰이크가 완료되었습니까?

3. ISE가 게스트 흐름의 끝에 VLAN 변경 사항을 푸시한 후 클라이언트가 네트워크에 액세스할 수 없습니다

클라이언트가 흐름의 시작 부분에서 IP 주소를 옮겨진 후(Pre Redirect 상태), 게스트 인증이 발생한 후(CoA 재인증 이후) VLAN 변경이 푸시다운되면(상태 에이전트 없이) 게스트 흐름에서 DHCP 릴리스/갱신을 강제하는 유일한 방법은 모바일 디바이스에서 작동하지 않는 Java 애플릿을 사용하는 것입니다.

그러면 클라이언트가 VLAN X에서 IP 주소가 VLAN Y인 블랙홀링됩니다. 이는 솔루션을 계획할 때 고려해야 합니다.

4. ISE는 리디렉션 중에 게스트 클라이언트의 브라우저에 "HTTP 500 내부 오류, Radius 세션을 찾을 수 없음" 메시지를 표시합니다

일반적으로 ISE의 세션 손실(세션이 종료됨)을 나타냅니다. 가장 일반적인 이유는 Foreign-Anchor가 구축된 경우 Anchor WLC에 구성된 어카운팅입니다. 이 문제를 해결하려면 앵커에서 어카운팅을 비활성화하고 외래 핸드 인증 및 어카운팅을 유지합니다.

5. 클라이언트는 ISE의 HotSpot 포털에서 AUP를 수락한 후 연결을 끊고 연결이 끊긴 상태로 유지되거나 다른 SSID에 연결됩니다.

이 흐름과 관련된 CoA(Dynamic Change of Authorization)로 인해(CoA Admin Reset) WLC에서 무선 스테이션에 대한 인증 해제를 실행하는 경우 핫스팟에서 이 문제가 발생할 수 있습니다. 대부분의 무선 엔드포인트는 인증 해제가 발생한 후 SSID로 돌아갈 때 문제가 발생하지 않지만, 경우에 따라 클라이언트는 인증 해제가 발생한 이벤트에 대한 응답으로 다른 기본 설정 SSID에 연결됩니다. ISE 또는 WLC에서는 원래 SSID에 고정하거나 사용 가능한 다른(기본 설정) SSID에 연결하는 무선 클라이언트에 따라 이를 방지하기 위해 아무것도 수행할 수 없습니다.

이 경우 무선 사용자는 HotSpot SSID에 수동으로 다시 연결해야 합니다.

아이레OS WLC

```
(Cisco Controller) >debug client
```

Debug client sets to DEBUG CLIENT STATE MACHINE(클라이언트 상태 머신 변경과 관련된 구성 요소 집합 디버그)를 설정합니다.

```
(Cisco Controller) >show debug
```

```
MAC Addr 1..... AA:AA:AA:AA:AA:AA
```

```
Debug Flags Enabled:  
dhcp packet enabled.  
dot11 mobile enabled.  
dot11 state enabled  
dot1x events enabled.  
dot1x states enabled.  
mobility client handoff enabled.
```

```
pem events enabled.
pem state enabled.
802.11r event debug enabled.
802.11w event debug enabled.
CCKM client debug enabled.
```

AAA 구성 요소 디버그

```
(Cisco Controller) >debug aaa {events, detail and packets} enable
```

이는 MAB 또는 Dot1X SSID를 통해 연결하는 사용자의 양에 따라 리소스에 영향을 줄 수 있습니다. DEBUG 레벨의 이러한 구성 요소는 WLC와 ISE 간의 AAA 트랜잭션을 기록하고 화면에 RADIUS 패킷을 인쇄합니다.

이는 ISE가 예상 특성을 제공할 수 없거나 WLC가 해당 특성을 올바르게 처리하지 못하는 경우에 중요합니다.

웹 인증 리디렉션

```
(Cisco Controller) >debug web-auth redirect enable mac aa:aa:aa:aa:aa:aa
```

이는 WLC가 리디렉션을 성공적으로 트리거하는지 확인하는 데 사용할 수 있습니다. 다음은 리디렉션이 디버그에서 어떻게 표시되는지 보여주는 예입니다.

```
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser host is 10.10.10.10
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser path is /
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- added redirect=, URL is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- str1 is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20c
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- clen string is Content-Length: 430

*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- Message to be sent is
HTTP/1.1 200 OK
Location:
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-0050
```

NGWC

Debug client sets to DEBUG CLIENT STATE MACHINE(클라이언트 상태 머신 변경과 관련된 구성 요소 집합 디버그)를 설정합니다.

```
3850#debug client mac-address <client MAC>
```

이 구성 요소는 화면에 RADIUS 패킷 (인증 및 계정 관리) 를 인쇄 합니다. 이는 ISE가 올바른 AVP를 제공하는지 확인하고 CoA가 올바르게 전송 및 처리되는지 확인해야 할 때 유용합니다.

```
3850#debug radius
```

그러면 무선 클라이언트가 관련된 모든 AAA 전환(인증, 권한 부여 및 계정 관리)이 수행됩니다. 이는 WLC가 AVP를 올바르게 구문 분석하고 이를 클라이언트 세션에 적용하는지 확인하는 데 중요합니다.

```
3850#debug aaa wireless all
```

이는 NGWC에서 리디렉션 문제가 의심되는 경우 활성화할 수 있습니다.

```
3850#debug epm plugin redirect all
```

```
3850#debug ip http transactions
```

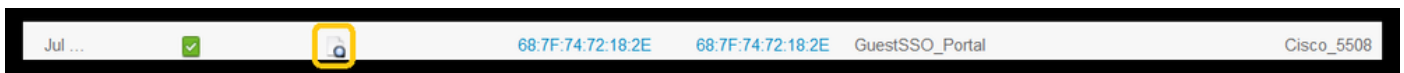
```
3850#debug ip http url
```

ISE

RADIUS 라이브 로그

초기 MAB 요청이 ISE에서 올바르게 처리되었으며 ISE가 예상 특성을 푸시하는지 확인합니다.

Operations(운영) > RADIUS > Live logs(라이브 로그)로 이동하고 Endpoint ID(엔드포인트 ID) 아래의 클라이언트 MAC을 사용하여 출력을 필터링합니다. 인증 이벤트가 발견되면 세부 정보를 클릭한 다음 수락의 일부로 푸시된 결과를 확인합니다.



TCPDump

이 기능은 ISE와 WLC 간의 RADIUS 패킷 교환을 자세히 살펴봐야 할 때 사용할 수 있습니다. 이렇게 하면 ISE가 WLC 측에서 디버그를 활성화할 필요 없이 access-accept에서 올바른 특성을 전송함을 증명할 수 있습니다. TCDDump를 사용하여 캡처를 시작하려면 Operations(운영) > Troubleshoot(문제 해결) > Diagnostic Tools(진단 도구) > General Tools(일반 도구) > TCPDump로 이동합니다.

다음은 TCPDump를 통해 캡처한 올바른 흐름의 예입니다

Source	Destination	Protocol	Length	Info
████████.154.5	████████.157.13	RADIUS	299	Access-Request(1) (id=0, l=257)
████████.157.13	████████.154.5	RADIUS	443	Access-Accept(2) (id=0, l=401)
████████.154.5	████████.157.13	RADIUS	340	Accounting-Request(4) (id=8, l=298)
████████.157.13	████████.154.5	RADIUS	62	Accounting-Response(5) (id=8, l=20)
████████.157.13	████████.154.5	RADIUS	244	CoA-Request(43) (id=1, l=202)
████████.154.5	████████.157.13	RADIUS	80	CoA-ACK(44) (id=1, l=38)
████████.154.5	████████.157.13	RADIUS	299	Access-Request(1) (id=1, l=257)
████████.157.13	████████.154.5	RADIUS	239	Access-Accept(2) (id=1, l=197)

여기에 초기 MAB 요청에 대한 응답으로 전송된 AVP가 있습니다(위의 스크린샷에서 두 번째 패킷).

RADIUS Protocol

```
Code: Access-Accept (2)
Packet identifier: 0x0 (0)
Length: 401
Authenticator: fleaaaffcfaa240270b885a9ba8ccd06d
[This is a response to a request in frame 1]
[Time from request: 0.214509000 seconds]
Attribute Value Pairs
  AVP: l=19 t=User-Name(1): 00-05-4E-41-19-FC
  AVP: l=40 t=State(24): 52656175746853657373696f6e3a30653234396130353030...
  AVP: l=55 t=Class(25): 434143533a30653234396130353030303030616130353536...
  AVP: l=37 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=31 t=Cisco-AVPair(1): url-redirect-acl=Gues_Redirect
  AVP: l=195 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=189 t=Cisco-AVPair(1): url-redirect=https://ise21a.rtpaaa.net:8443/portal/gateway?sessionId=0e249a0500000aa05565e1c9&portal=194a5780-5e4e-11e4-b905-005056bf2f0a&action=cwa&token=c6c8a6b0d683ea0c650282b4372a7622
  AVP: l=35 t=Vendor-Specific(26) v=ciscoSystems(9)
```

엔드포인트 디버깅:

정책 결정, 포털 선택, 게스트 인증과 관련된 ISE 프로세스에 대해 자세히 살펴보아야 하는 경우, CoA는 완전한 구성 요소를 디버그 레벨로 설정하는 대신 엔드포인트 디버깅을 활성화하는 것이 가장 쉬운 접근 방법입니다.

이를 활성화하려면 Operations(운영) > Troubleshooting(문제 해결) > DiagnosticTools(진단 도구) > General Tools(일반 도구) > EndPoint Debug(엔드포인트 디버깅)로 이동합니다.

Overview

Event	5200 Authentication succeeded
Username	00:24:97:BA:84:81
Endpoint Id	00:24:97:BA:84:81 ⓘ Endpoint Debug...
Endpoint Profile	Cisco-Device
Authentication Policy	Default >> MAB >> Default
Authorization Policy	Default >> Wireless_CWA_RedirectSSO
Authorization Result	GuestSSO_Portal

엔드포인트 디버그 페이지에서 엔드포인트 MAC 주소를 입력하고 문제를 다시 생성할 준비가 되면 시작 을 클릭합니다.

▼ General Tools

- RADIUS Authentication Trouble...
- Execute Network Device Com...
- Evaluate Configuration Validator
- Posture Troubleshooting
- EndPoint Debug
- TCP Dump

Endpoint Debug


Status: Stopped Start


MAC Address IP ⓘ


Automatic disable after Minutes ⓘ

디버그가 중지되면 디버그 출력을 다운로드할 엔드포인트 ID를 식별하는 링크를 클릭합니다.

Endpoint Debug

Status:  Processing ...

MAC Address IP 

Automatic disable after Minutes 

Selected 0 | Total 1

<input type="checkbox"/>	File Name	Host Name	Modified Date	Size (Bytes)
<input type="checkbox"/>	68-7f-74-72-18-2e	TORISE21A	Jul 8 12:06	1021448

관련 정보

[TAC 권장 AireOS 빌드](#)

[Cisco Wireless Controller 컨피그레이션 가이드, 릴리스 8.0.](#)

[Cisco Identity Services Engine 관리자 가이드, 릴리스 2.1](#)

[ISE\(Identity Services Engine\)를 통한 범용 NGWC 무선 컨피그레이션](#)

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.