격리된 게스트 네트워크에 대한 고정 리디렉션이 있는 ISE 컨피그레이션 예

목차

소개

이 문서에서는 이중화를 유지하기 위해 격리 게스트 네트워크에 대해 고정 리디렉션을 사용하여 Cisco ISE(Identity Services Engine)를 구성하는 방법에 대해 설명합니다.또한 클라이언트가 확인할 수 없는 인증서 경고와 함께 프롬프트를 표시하지 않도록 정책 노드를 구성하는 방법에 대해서도 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE CWA(Central Web Authentication) 및 모든 관련 구성 요소
- 브라우저 인증서 유효성 확인
- Cisco ISE 버전 1.2.0.899 이상
- Cisco WLC(Wireless LAN Controller) 버전 7.2.110.0 이상(버전 7.4.100.0 이상이 기본)

참고:CWA는 WLC [및 ISE 컨피그레이션 예시](#) *Cisco* 문서[의 중앙 웹 인증](#)에 설명되어 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 버전 1.2.0.899
- Cisco vWLC(Virtual WLC) 버전 7.4.110.0
- Cisco ASA(Adaptive Security Appliance)) 버전 8.2.5

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

배경 정보

많은 BYOD(Bring Your Own Device) 환경에서 게스트 네트워크는 DMZ(De-Modified Zone)의 내부 네트워크로부터 완전히 격리됩니다. 게스트 DMZ의 DHCP는 인터넷 액세스만 제공되므로 게스트 사용자에게 공용 DNS(Domain Name System) 서버를 제공하는 경우가 많습니다.

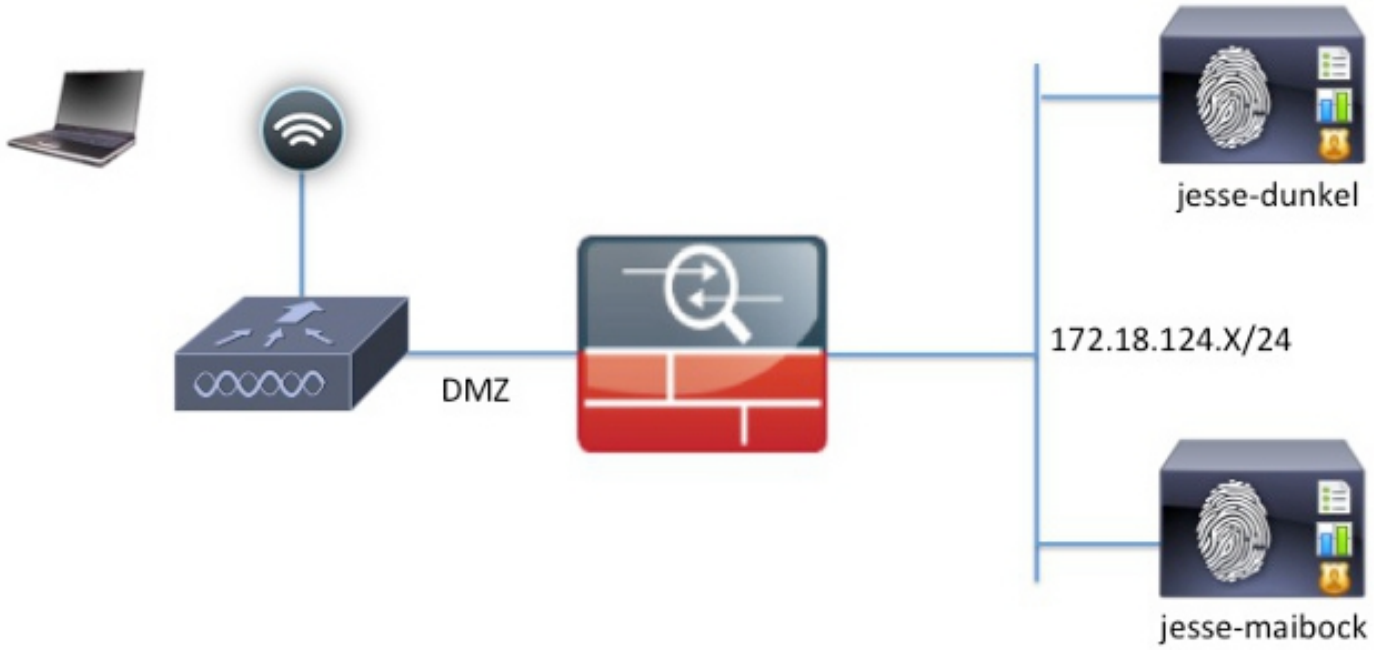
ISE는 웹 인증을 위해 클라이언트를 FQDN(Fully Qualified Domain Name)으로 리디렉션하기 때문에 버전 1.2 이전 ISE에서 게스트 리디렉션을 어렵게 합니다.그러나 ISE 버전 1.2 이상에서는 관리자가 게스트 사용자를 고정 IP 주소 또는 호스트 이름으로 리디렉션할 수 있습니다.

구성

네트워크 다이어그램

논리적 다이어그램입니다.

> **참고:**실제로 내부 네트워크에 무선 컨트롤러가 있고, 액세스 포인트(AP)가 내부 네트워크에 있으며, SSID(Service Set Identification)가 DMZ 컨트롤러에 고정되어 있습니다.자세한 내용은 Cisco WLC의 설명서를 참조하십시오.



구성

WLC의 컨피그레이션은 일반 CWA 컨피그레이션과 변경되지 않습니다.SSID는 RADIUS 인증을 사용하는 MAC 필터링을 허용하도록 구성되며 RADIUS 어카운팅은 둘 이상의 ISE 정책 노드를 가리킵니다.

이 문서에서는 ISE 컨피그레이션에 대해 중점적으로 설명합니다.

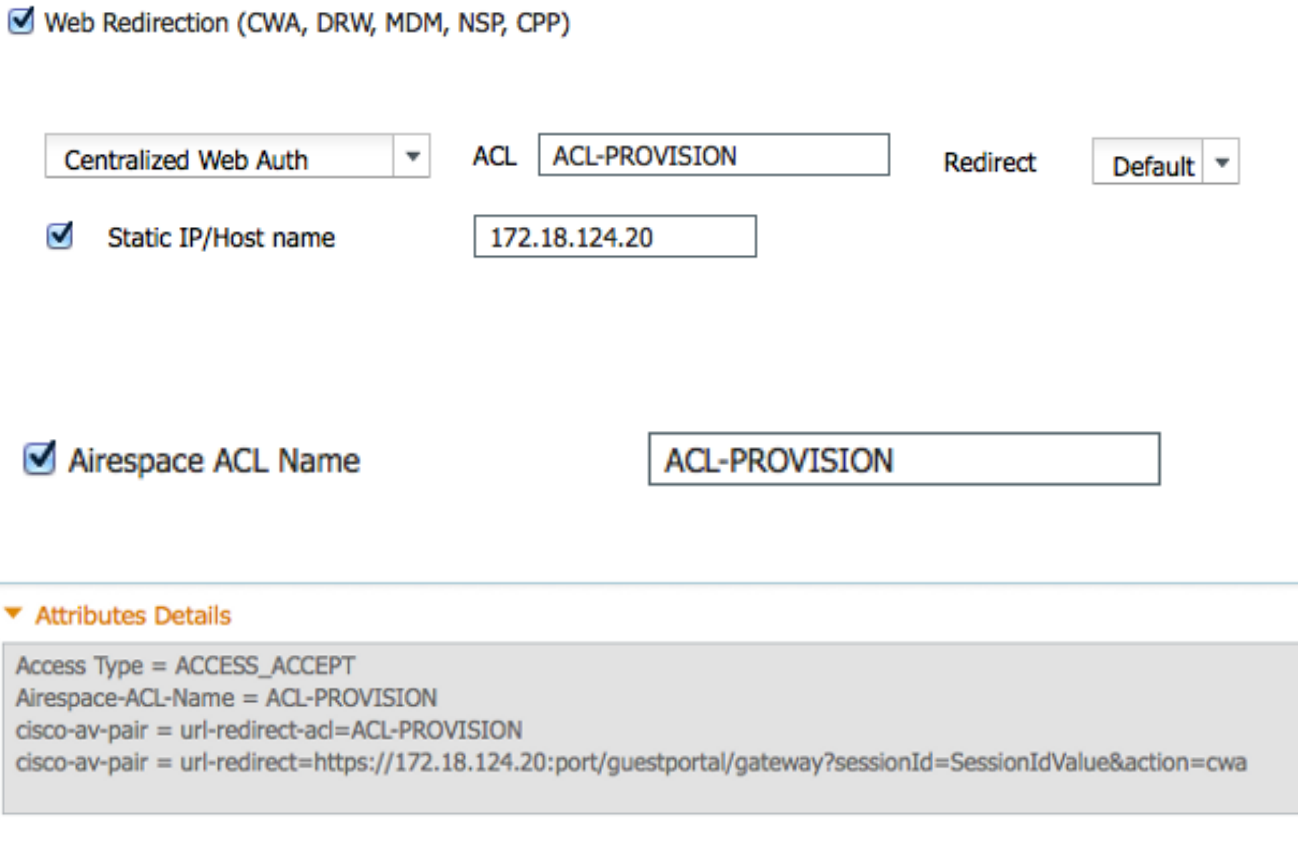
> **참고:**이 컨피그레이션 예에서 정책 노드는 **jesse-dunkel**(172.18.124.20) 및 **jesse-maibock**(172.18.124.21)입니다.

CWA 흐름은 WLC가 ISE에 RADIUS MAB(MAC Authentication Bypass) 요청을 전송할 때 시작됩니다.ISE는 HTTP 트래픽을 ISE로 리디렉션하기 위해 컨트롤러에 리디렉션 URL로 응답합니다.세션이 단일 PSN에서 유지 관리되므로 RADIUS 및 HTTP 트래픽이 동일한 PSN(Policy Services Node)으로 이동하는 것이 중요합니다.이 작업은 일반적으로 단일 규칙으로 수행되며 PSN은 CWA URL에 자체 호스트 이름을 삽입합니다.그러나 고정 리디렉션을 사용하여 RADIUS 및 HTTP 트래픽이 동일한 PSN으로 전송되도록 하려면 각 PSN에 대한 규칙을 생성해야 합니다.

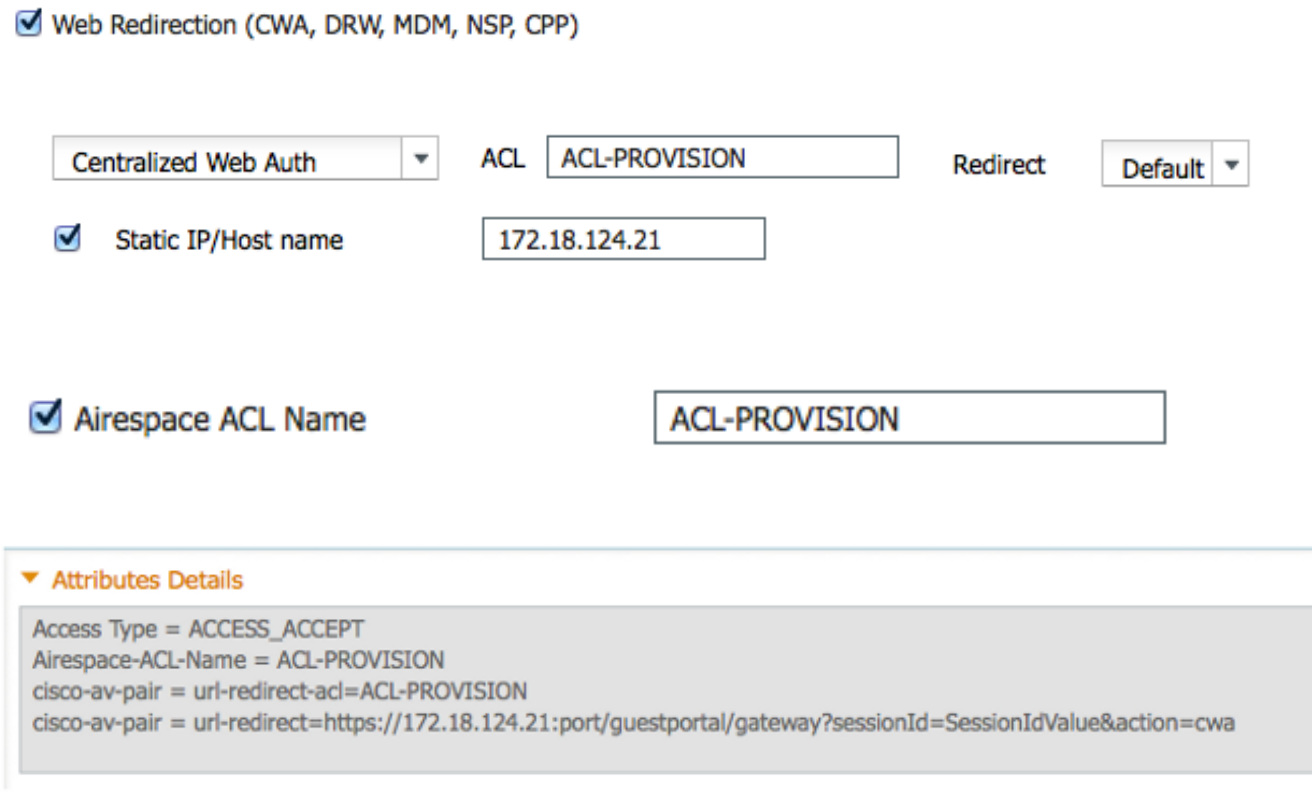
ISE를 구성하려면 다음 단계를 완료합니다.

1. 클라이언트를 PSN IP 주소로 리디렉션하려면 두 가지 규칙을 설정합니다.Policy(**정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)로 이동합니다**.

   다음 그림에서는 프로파일 이름 DunkelGuestWireless에 대한 정보를 **보여줍니다**.

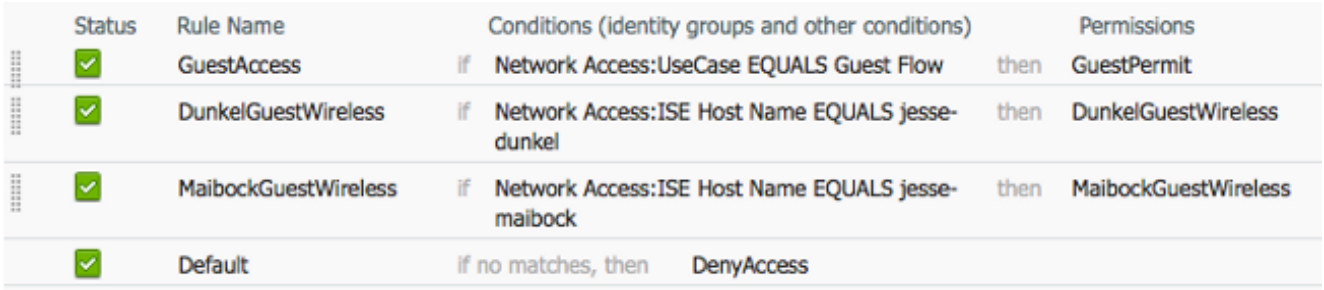


   다음 그림에서는 프로파일 이름 MaibockGuestWireless에 대한 정보를 **보여줍니다**.

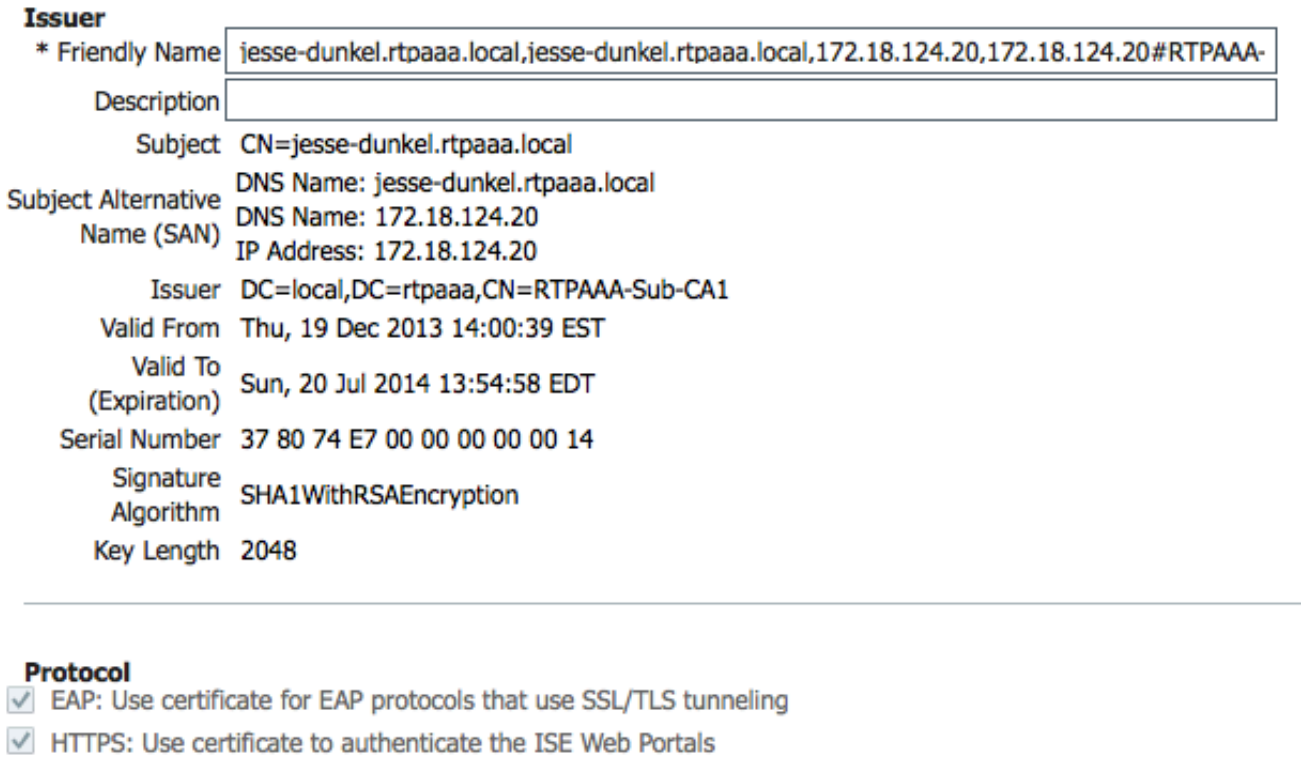


참고:ACL-**PROVISION**은 클라이언트가 인증 시 ISE와 통신할 수 있도록 WLC에 구성된 로컬 ACL(Access Control List)입니다.자세한 내용은 WLC 및 ISE 구성 예 Cisco 문서의 중앙 웹 인증을 참조하십시오.

2. **Network Access:**ISE Host Name 특성에서 일치되도록 권한 부여 정책을 구성하고 적절한 권한 부여 프로파일을 제공합니다.



이제 클라이언트가 IP 주소로 리디렉션되므로 사용자는 URL이 인증서의 정보와 일치하지 않기 때문에 인증서 경고를 받습니다.예를 들어, 인증서의 FQDN은 **jesse-dunkel.rtpaa.local**이지만 URL은 **172.18.124.20입니다**. 다음은 브라우저가 IP 주소로 인증서를 검증할 수 있는 인증서 예입니다.



SAN(Subject Alternative Name) 항목을 사용하면 브라우저에서 IP 주소 **172.18.124.20**이 포함된 URL을 검증할 수 있습니다. 다양한 클라이언트 비호환성을 해결하려면 3개의 SAN 항목을 생성해야 합니다.

3. DNS 이름에 대한 SAN 항목을 생성하고 Subject(주체) 필드의 **CN=** 항목과 일치하는지 확인합니다.

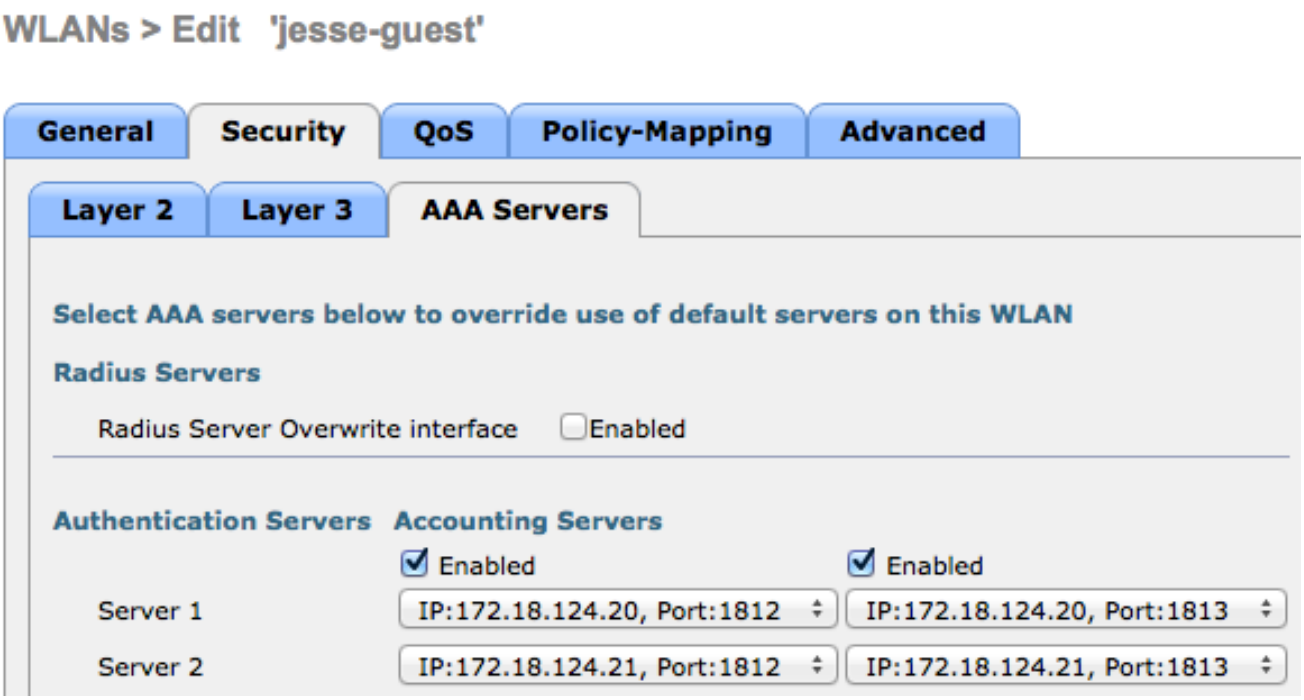
4. 클라이언트가 IP 주소를 검증할 수 있도록 두 개의 항목을 생성합니다.이는 IP 주소의 DNS 이름 및 IP Address 특성에 나타나는 IP 주소에 대한 것입니다.일부 클라이언트는 DNS 이름만 참조합니다.다른 사용자는 DNS Name 특성에서 IP 주소를 수락하지 않고 대신 IP Address 특성을 참조합니다.

   참고:인증서 생성에 대한 자세한 내용은 **Cisco Identity Services Engine 하드웨어 설치 가이드, 릴리스 1.2를** 참조하십시오.

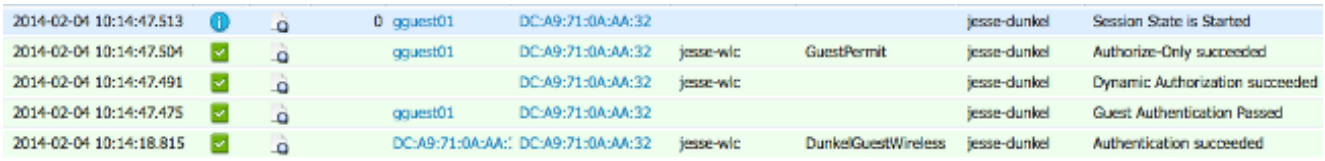
다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 다음 단계를 완료하십시오.

1. 두 규칙이 모두 작동하는지 확인하려면 WLAN에 구성된 ISE PSN의 순서를 수동으로 설정합니다.



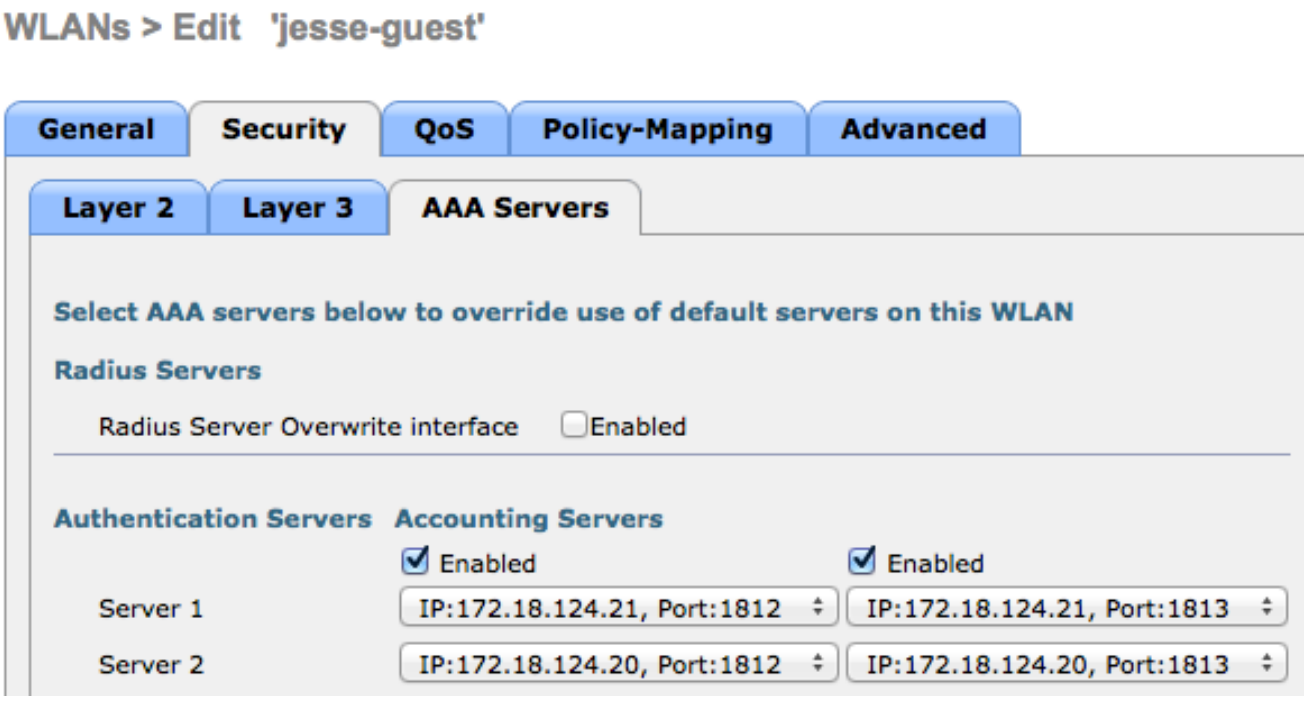
2. 게스트 SSID에 로그인하고 Operation(작업) **> Authentications** in the ISE(ISE에서 인증)로 이동하고 올바른 권한 부여 규칙이 적중되었는지 확인합니다.



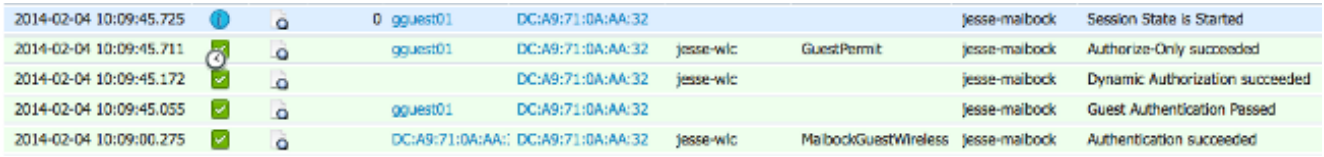
초기 MAB 인증은 DunkelGuestWireless **권한 부여** 프로파일**에** 제공됩니다.이는 첫 번째 ISE 노드인 **jesse-dunkel**으로 특별히 리디렉션하는 규칙입니다.gguest01 사용자**가** 로그인하면 GuestPermit의 올바른 최종 권한**이** 지정됩니다.

3. WLC에서 인증 세션을 지우려면 무선 네트워크에서 클라이언트 장치를 분리하고 WLC의 **모니터 > 클라이언트**로 이동한 다음 출력에서 세션을 삭제합니다. WLC는 기본적으로 5분 동안 유휴 세션을 보관하므로 유효한 테스트를 수행하려면 새로 시작해야 합니다.

4. 게스트 WLAN 컨피그레이션에서 ISE PSN의 순서를 반대로 합니다.



5. 게스트 SSID에 로그인하고 Operation(작업) **> Authentications** in the ISE(ISE에서 인증)로 이동하고 올바른 권한 부여 규칙이 적중되었는지 확인합니다.



두 번째 시도에서는 **MaibockGuestWireless** 권한 부여 프로파일이 초기 MAB 인증에 올바르게 적중됩니다.**jesse-dunkel**에 대한 첫 번째 시도(2단계)와 유사하게, **jesse-maibock에 대한** 인증은 최종 권한 부여에 대한 **GuestPermit**을 올바르게 적중합니다.GuestPermit 권한 부여 프로파일에 PSN 관련 정보가 없으므로 단일 규칙을 모든 PSN에 대한 인증에 사용할 수 있습니다.

문제 해결

Authentication Details(인증 세부사항) 창은 인증/권한 부여 프로세스의 모든 단계를 표시하는 강력한 보기입니다.액세스 하려면 Operations(운영) **> Authentications(인증)로** 이동하고 Details(세부사항) 열 아래의 돋보기 아이콘을 클릭 합니다.인증/권한 부여 규칙 조건이 올바르게 구성되었는지 확인하려면 이 창을 사용합니다.

이 경우 Policy Server(정책 서버) 필드가 주요 포커스 영역입니다.이 필드는 인증이 서비스되는 ISE PSN의 호스트 이름을 포함합니다.

Overview

Event	5200 Authentication succeeded
Username	DC:A9:71:0A:AA:32
Endpoint Id	DC:A9:71:0A:AA:32
Endpoint Profile	
Authorization Profile	DunkelGuestWireless
AuthorizationPolicyMatchedRule	DunkelGuestWireless
ISEPolicySetName	GuestWireless
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-02-04 10:14:18.79
Received Timestamp	2014-02-04 10:14:18.815
Policy Server	jesse-dunkel
Event	5200 Authentication succeeded

정책 서버 항목을 규칙 조건과 비교하고 두 개의 일치(이 값은 대/소문자 구분)를 확인합니다.

DunkelGuestWireless	if	Network Access:ISE Host Name EQUALS jesse-dunkel

참고:테스트 사이에 SSID에서 연결을 끊고 WLC에서 클라이언트 항목을 지워야 합니다.