ISE 게스트 임시 및 영구 액세스 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[구성](#)
[네트워크 다이어그램](#)
[영구 액세스](#)
[게스트 어카운트의 엔드포인트 비우기](#)
[임시 액세스](#)
[WLC 연결 끊기 동작](#)
[다음을 확인합니다.](#)
[영구 액세스](#)
[임시 액세스](#)
[버그](#)
[참조](#)
[관련 Cisco 지원 커뮤니티 토론](#)

소개

이 문서에서는 ISE(Identity Services Engine) 게스트 액세스 컨피그레이션에 대한 다양한 방법에 대해 설명합니다.권한 부여 규칙의 다른 조건에 따라 다음을 수행합니다.

- 네트워크에 대한 영구 액세스를 제공할 수 있음(후속 인증을 위한 필요 없음)
- 네트워크에 대한 임시 액세스를 제공할 수 있습니다(세션 만료 후 게스트 인증 필요).

또한 세션 제거를 위한 특정 WLC(Wireless LAN Controller) 동작은 임시 액세스 시나리오에 미치는 영향을 나타냅니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE 구축 및 게스트 플로우
- WLC(Wireless LAN Controller) 구성

사용되는 구성 요소

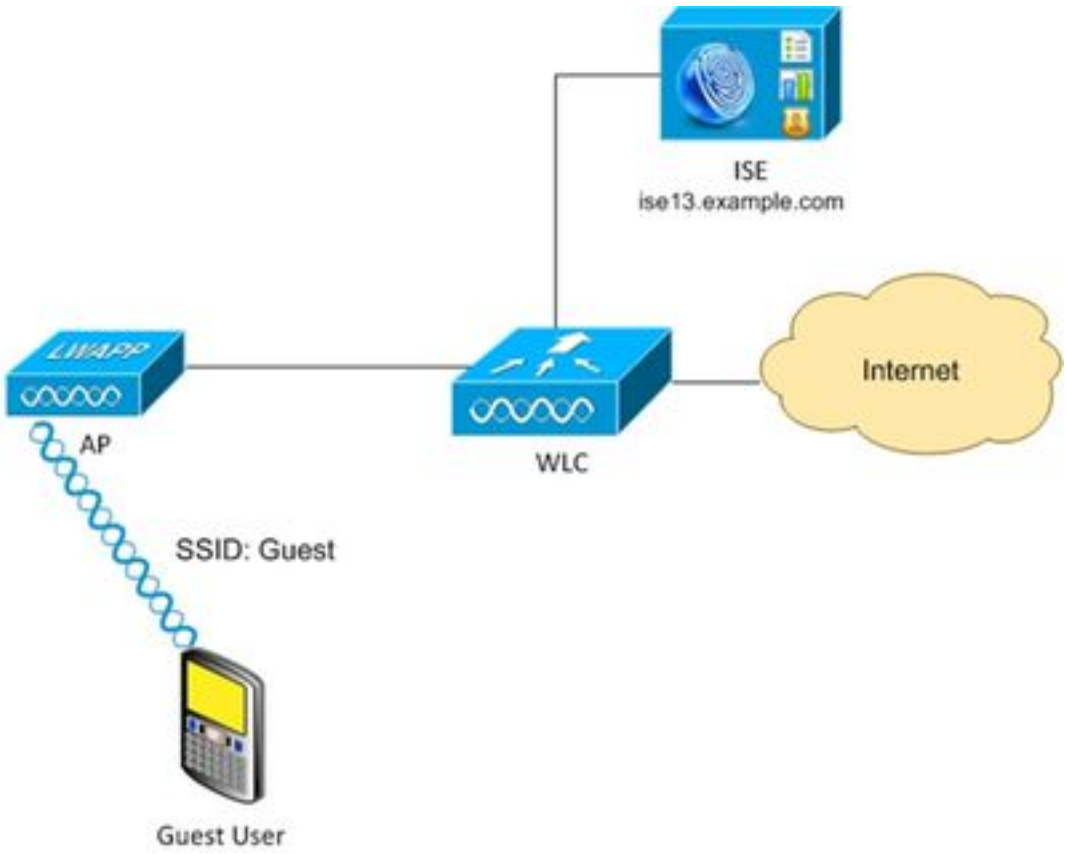
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Windows 7
- Cisco WLC 버전 7.6 이상
- ISE 소프트웨어, 버전 1.3 이상

구성

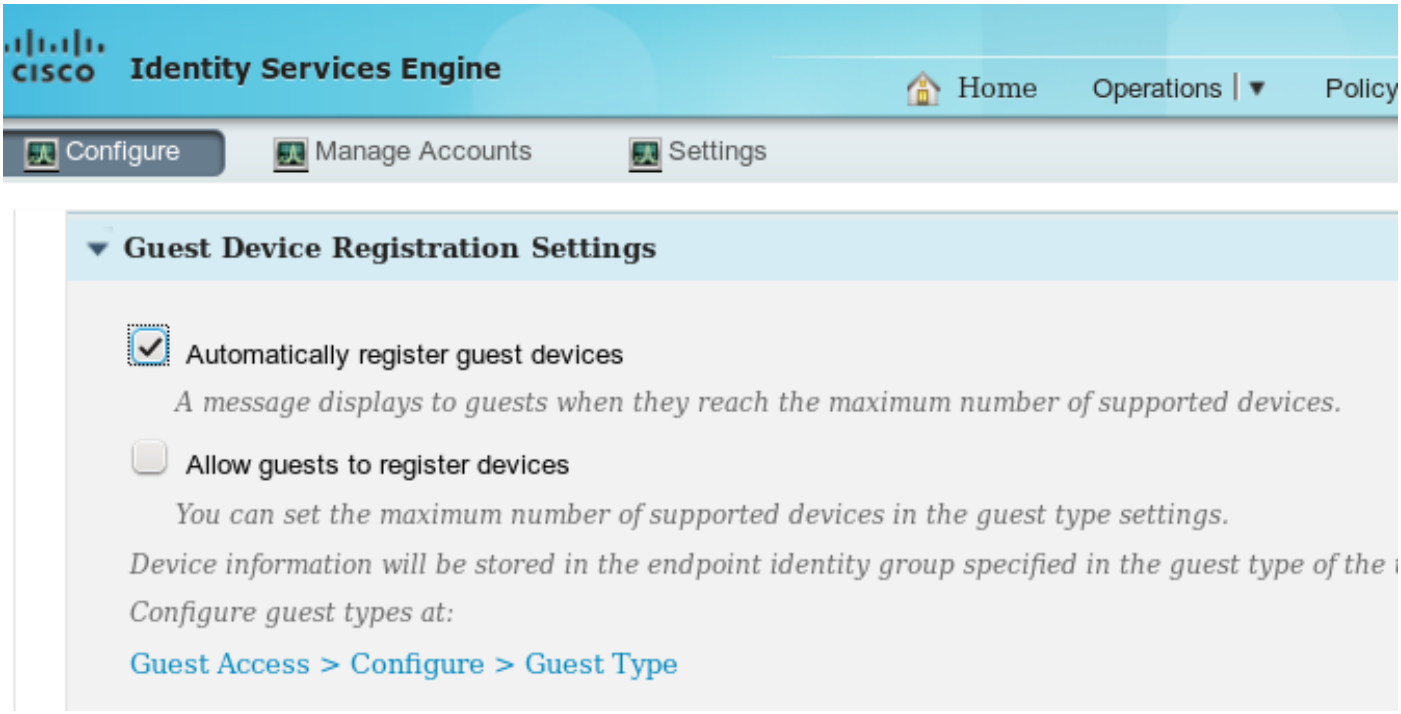
기본 게스트 액세스 컨피그레이션의 경우 컨피그레이션 예와 함께 참조를 확인하십시오.이 문서에서는 권한 부여 규칙 컨피그레이션 및 권한 부여 조건의 차이점을 중점적으로 다룹니다.

네트워크 다이어그램

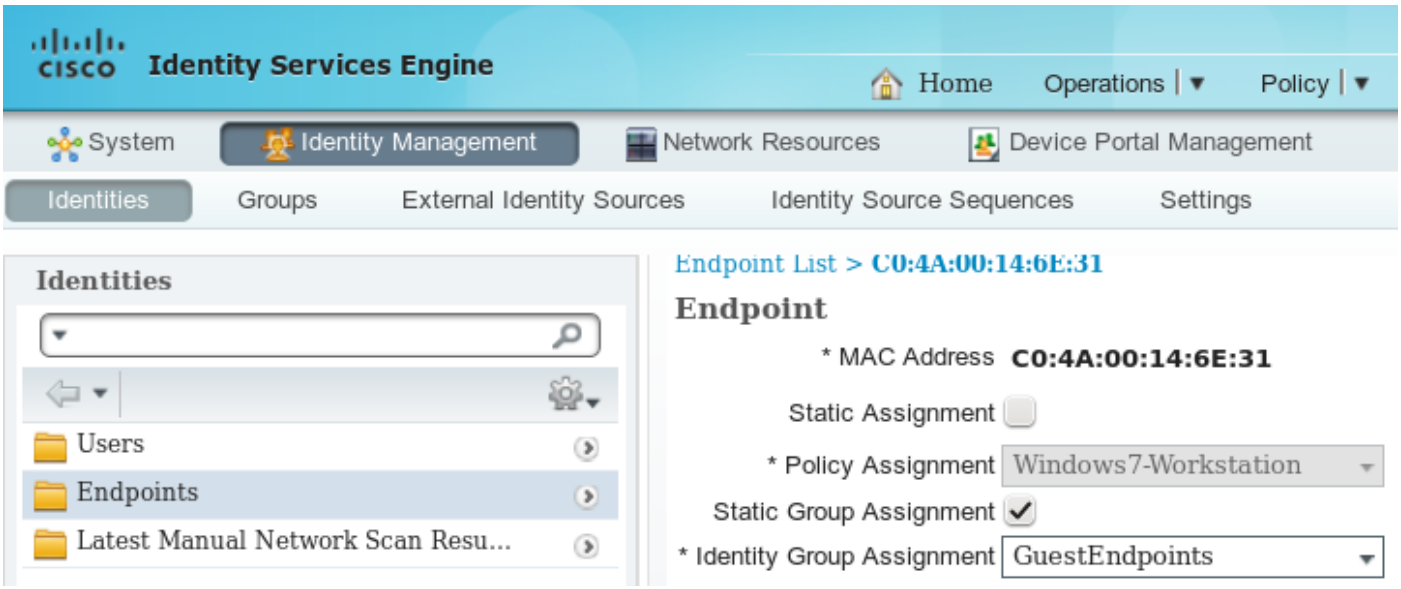


영구 액세스

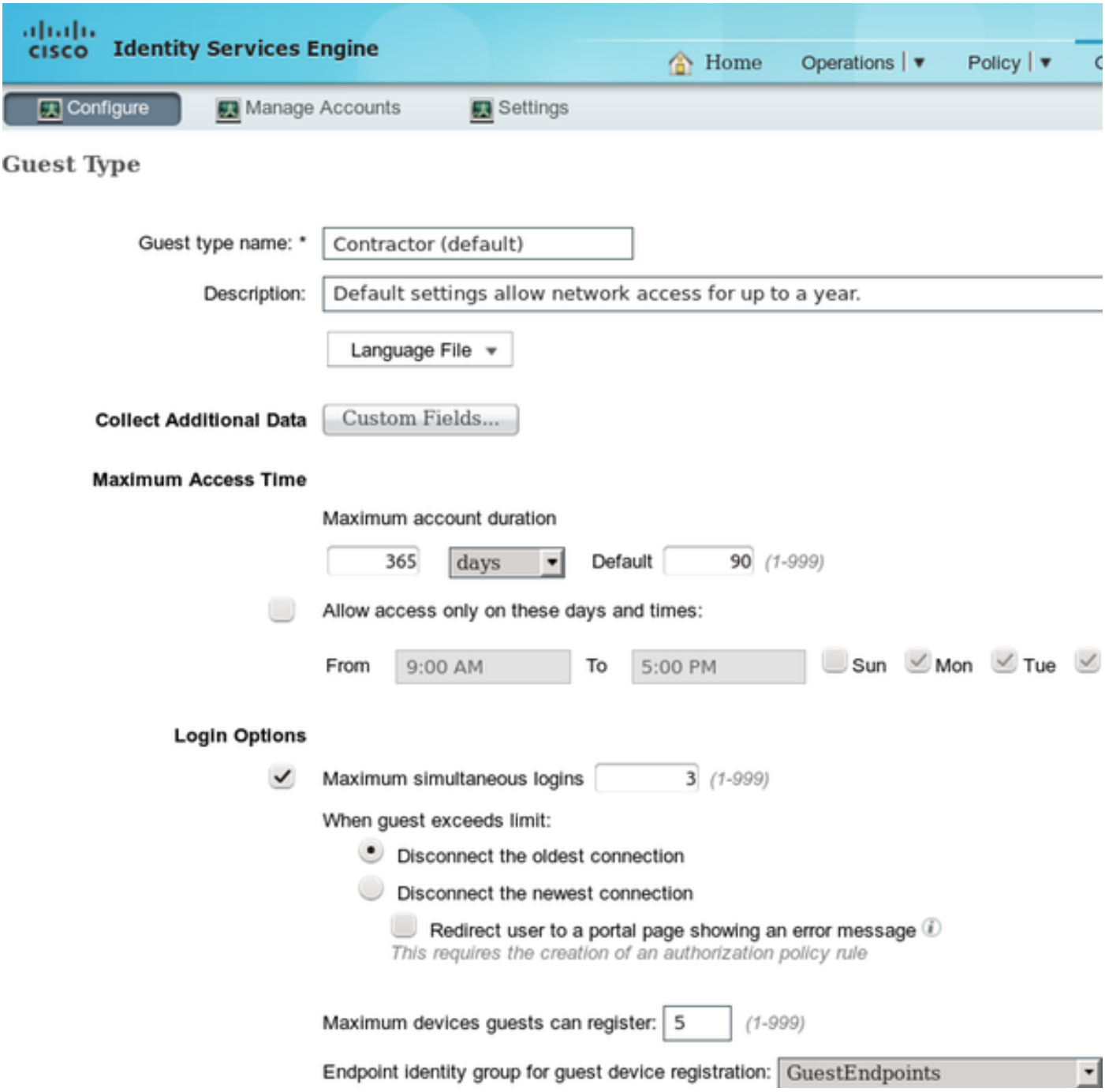
디바이스 등록이 활성화된 게스트 포털에서 인증 성공 후 ISE 버전 1.3 이상



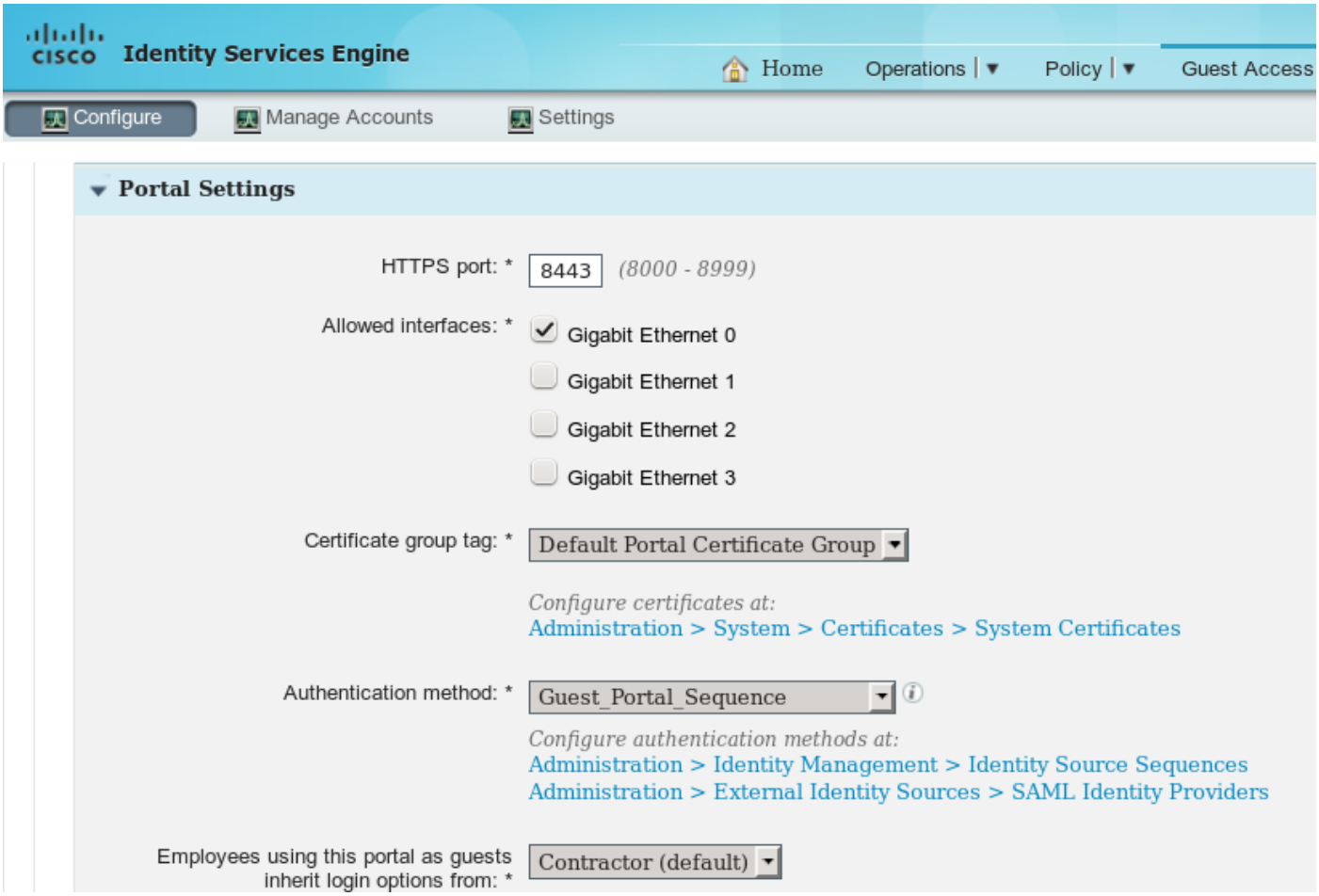
엔드포인트 디바이스(mac 주소)는 특정 엔드포인트 그룹(이 예에서는 GuestEndpoints)에 정적으로 등록됩니다.



해당 그룹은 이 이미지에 표시된 대로 사용자의 게스트 유형에서 파생됩니다.



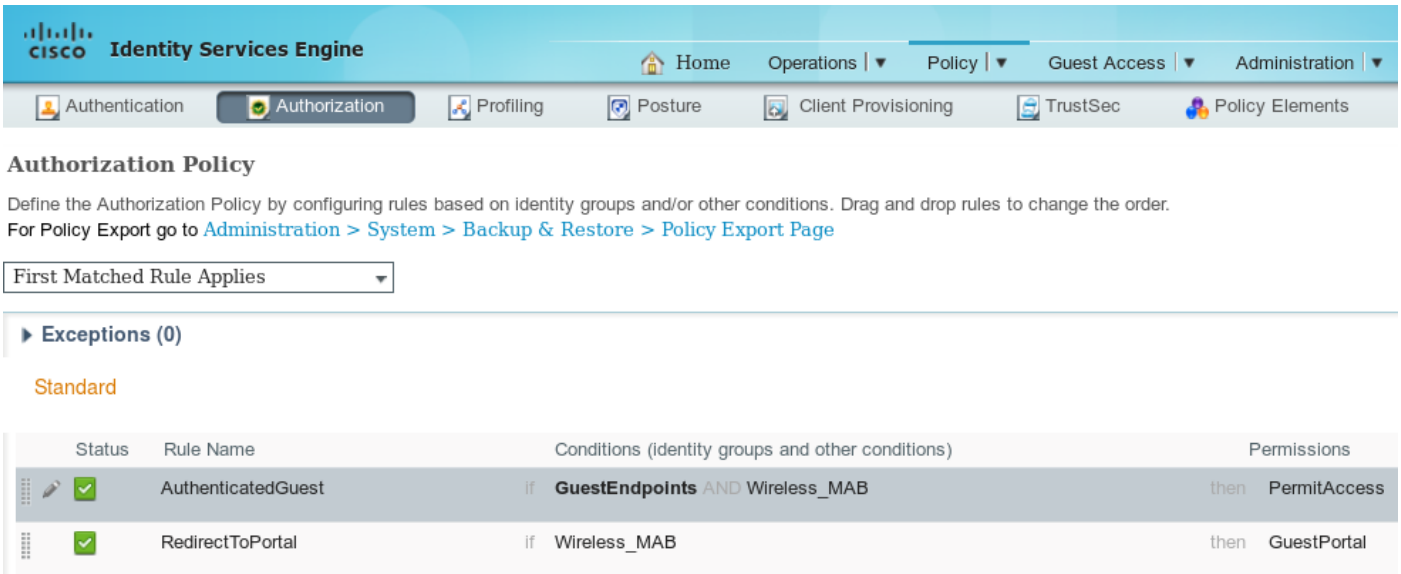
회사 사용자(게스트 이외의 ID 저장소)인 경우 포털 설정에서 해당 설정이 파생됩니다.



결과적으로 게스트와 연결된 mac 주소는 항상 특정 ID 그룹에 속합니다.이는 자동으로 변경할 수 없습니다(예: 프로 파 일러 서비스).

참고:프로파일러 결과를 적용하려면 EndPointPolicy 권한 부여 조건을 사용할 수 있습니다.

디바이스가 항상 특정 엔드포인트 ID 그룹에 속한다는 사실을 알고 있으면 이 이미지에 표시된 대로 이를 기반으로 권한 부여 규칙을 작성할 수 있습니다.

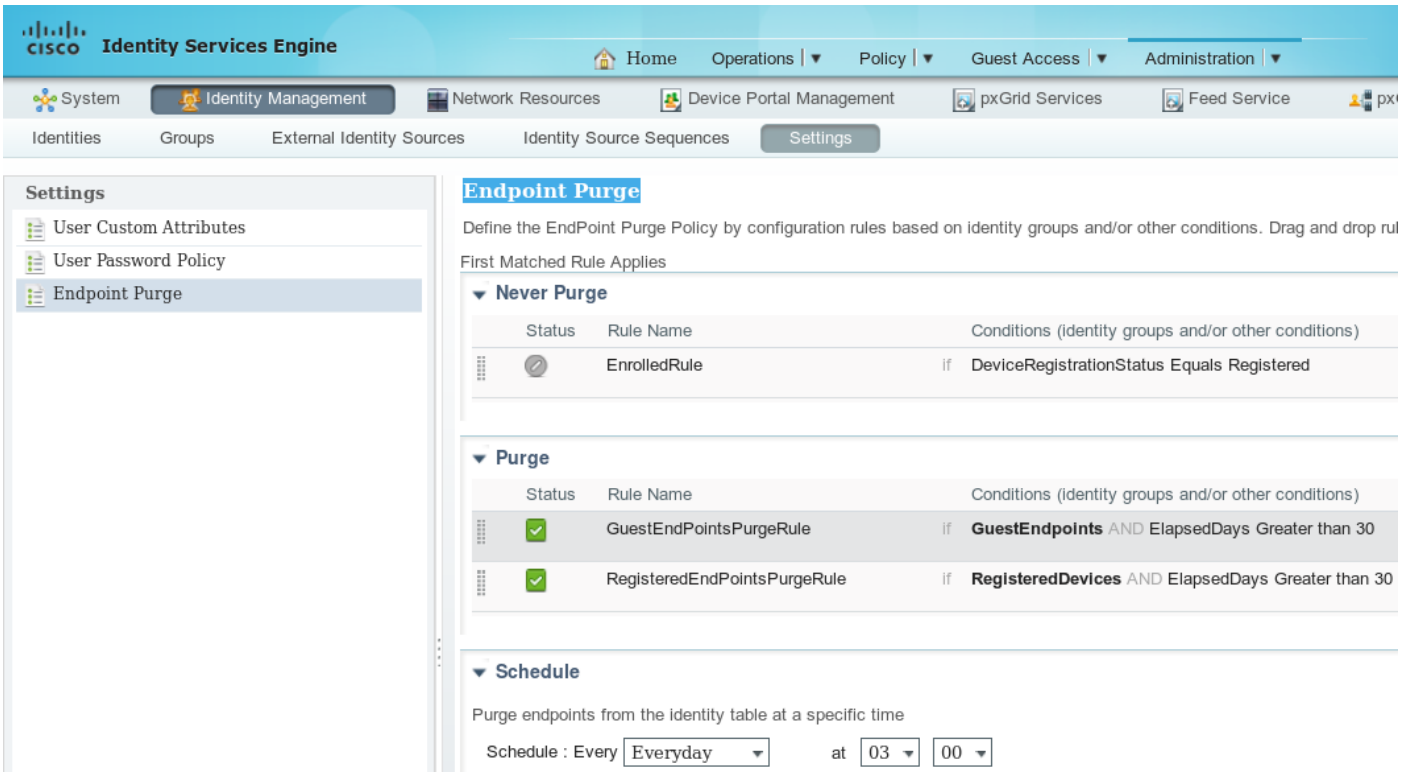


사용자가 인증되지 않으면 권한 부여가 일반 규칙 RedirectToPortal과 일치합니다.게스트 포털 및 인증으로 리디렉션한 후 엔드포인트는 특정 엔드포인트 ID 그룹에 배치됩니다.이는 보다 구체적인 첫 번째 조건에 사용됩니다.해당 엔드포인트의 모든 후속 인증은 첫 번째 권한 부여 규칙에 도달하

고 사용자는 게스트 포털에서 재인증할 필요 없이 전체 네트워크 액세스를 제공합니다.

게스트 어카운트의 엔드포인트 비우기

이 상황은 영원히 지속될 수 있다.그러나 ISE 1.3 엔드포인트 제거 기능이 도입되었습니다.기본 컨피그레이션을 사용합니다.



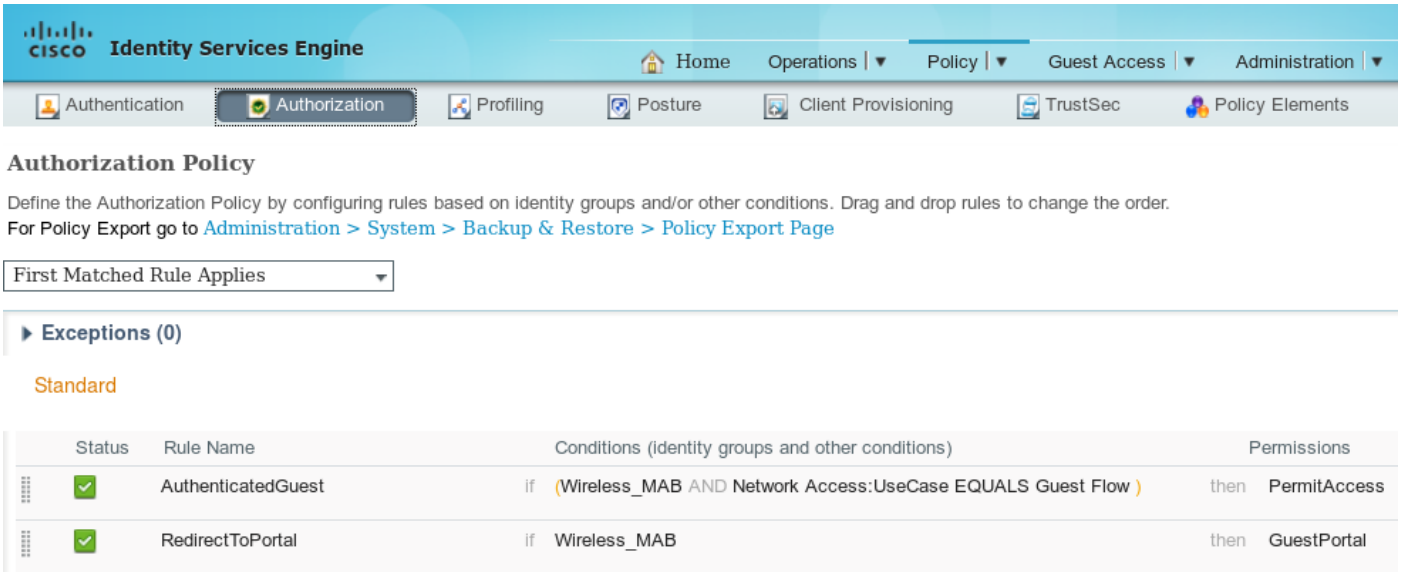
게스트 인증에 사용되는 모든 엔드포인트는 엔드포인트 생성에서 30일 후에 제거됩니다. 따라서 보통 30일 후 네트워크 액세스를 시도하는 게스트 사용자가 RedirectToPortal 권한 부여 규칙을 적중하고 인증을 위해 리디렉션됩니다.

> **참고:**엔드포인트 비우기 기능은 게스트 어카운트 비우기 정책 및 게스트 어카운트 만료와 독립적입니다.

> **참고:**ISE 1.2 엔드포인트는 내부 프로파일러 큐 제한을 누를 때만 자동으로 제거할 수 있습니다.그리고 최근에 사용한 엔드포인트가 제거됩니다.

임시 액세스

게스트 액세스를 위한 또 다른 방법은 게스트 플로우 조건을 사용하는 것입니다.



해당 조건은 ISE에서 활성 세션을 확인하고 있으며 해당 특성을 확인합니다.해당 세션에 이전 게스트 사용자가 성공적으로 인증한 조건이 일치함을 나타내는 특성이 있는 경우.ISE가 NAD(Network Access Device)에서 RADIUS 계정 관리 중지 메시지를 받으면 세션이 종료되고 나중에 제거됩니다.이 단계에서 Network Access:UseCase = Guest Flow is not satisfaction anymore threat(네트워크 액세스:UseCase = 게스트 흐름)가 더 이상 충족되지 않습니다.결과적으로 해당 엔드포인트의 모든 후속 인증은 게스트 인증을 위한 일반 규칙 리디렉션에 도달합니다.

> **참고:**사용자가 HotSpot 포털을 통해 인증되는 경우 게스트 플로우가 지원되지 않습니다.이러한 시나리오에서 UseCase 특성은 Guest Flow 대신 Host Lookup으로 설정됩니다.

WLC 연결 끊기 동작

클라이언트가 무선 네트워크에서 연결을 끊은 후(예: Windows에서 연결 끊기 단추 사용) 인증 해제 프레임을 보냅니다.그러나 이는 WLC에서 생략되며 "debug client xxxx"를 사용하여 확인할 수 있습니다. WLC는 클라이언트가 WLAN에서 연결을 끊을 때 디버그를 표시하지 않습니다.Windows 클라이언트의 결과:

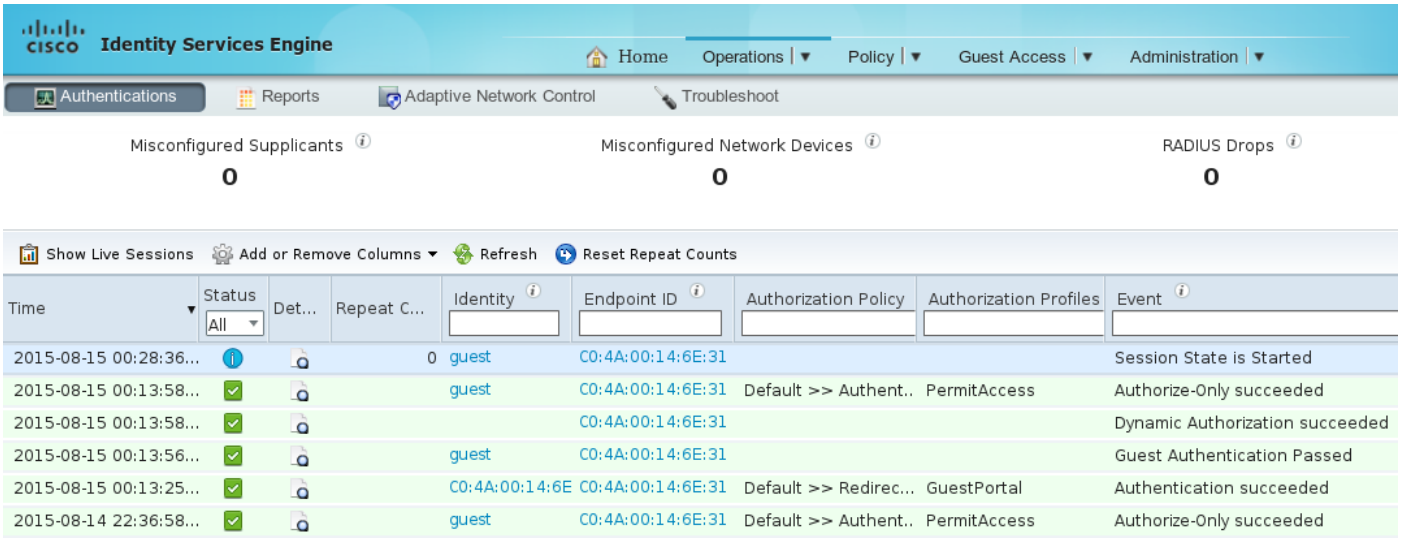
- ip 주소가 인터페이스에서 제거됩니다.
- 인터페이스 상태:미디어 연결 끊김

그러나 WLC에서는 상태가 변경되지 않습니다(클라이언트는 여전히 RUN 상태에 있음).

이는 WLC를 위한 계획된 설계이며,

- 사용자 유휴 시간 제한 횟수
- 세션 시간 초과 적중
- L2 암호화를 사용하는 경우 그룹 키 회전 간격이 적중할 때
- 다른 이유로 AP/WLC가 클라이언트를 꺼냅니다(예: AP 무선 재설정, WLAN 종료 등).

WLC가 WLAN 세션을 지운 적이 없으며 Radius 계정 관리 중지를 보낸 적이 없기 때문에 사용자가 WLAN 세션에서 연결을 끊은 후 이러한 동작 및 임시 액세스 컨피그레이션이 ISE에서 제거되지 않습니다. 세션이 제거되지 않은 경우 ISE는 여전히 이전 세션을 기억하며 게스트 플로우 조건이 충족됩니다.연결을 해제하고 다시 연결한 후에는 다시 인증할 필요 없이 전체 네트워크 액세스가 가능합니다.



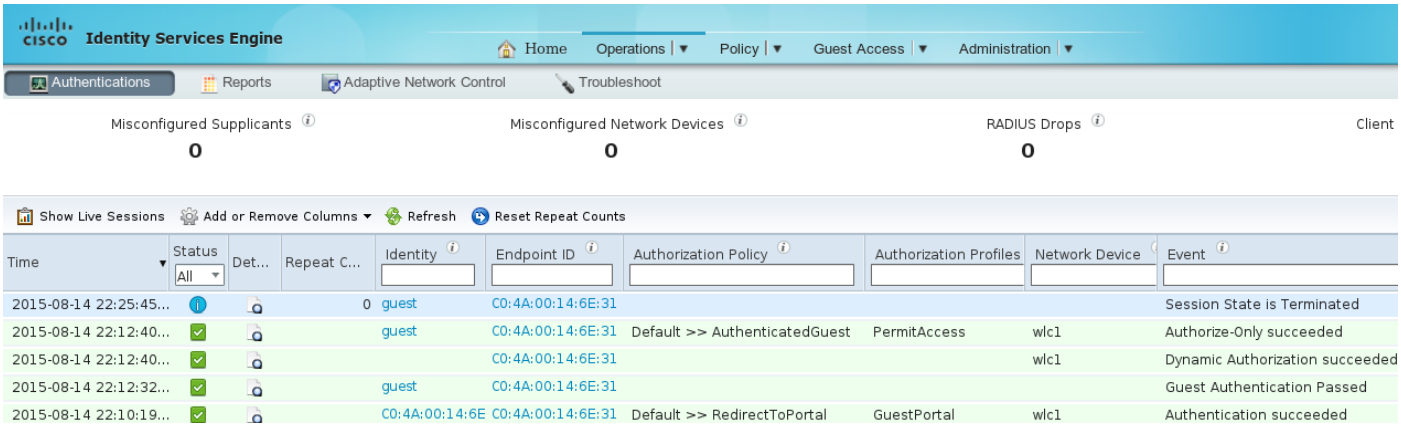
그러나 연결 해제 후 사용자가 다른 WLAN에 연결되면 WLC는 이전 세션을 지워야 합니다.Radius 계정 관리 중지 가 전송 되고 ISE가 세션을 제거 합니다.클라이언트가 원래 WLAN Guest Flow(WLAN 게스트 플로우) 조건에 연결하려고 시도하는 경우, 충족되지 않고 사용자가 인증을 위해 리디렉션됩니다.

> **참고:**MFP(Management Frame Protection)로 구성된 WLC는 CCXv5 MFP 클라이언트의 암호화된 디인증 프레임을 수락합니다.

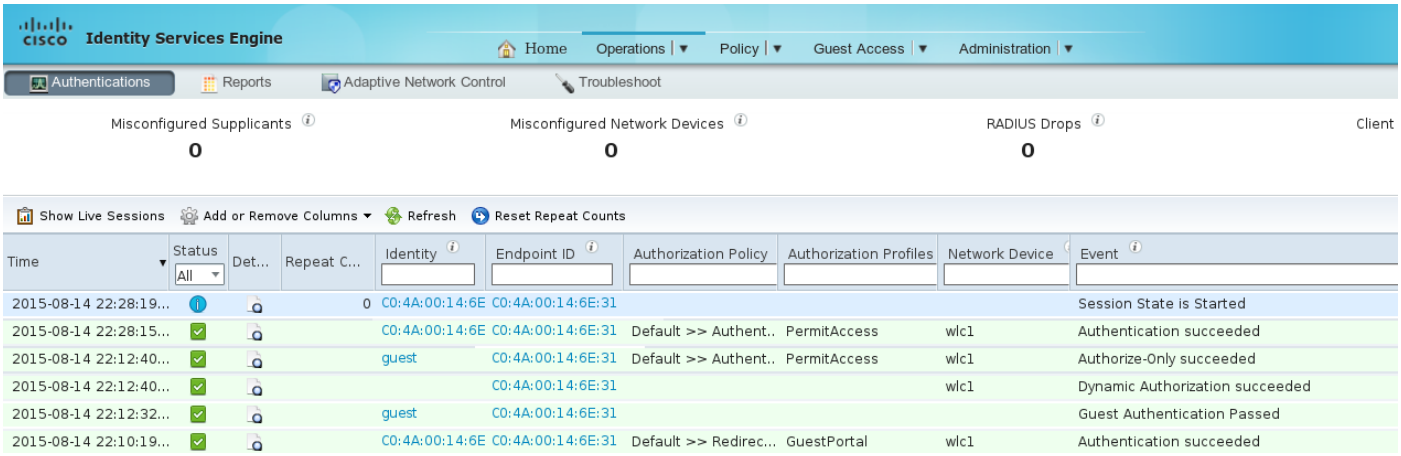
다음을 확인합니다.

영구 액세스

게스트 포털에 리디렉션되고 성공적인 인증 ISE는 재인증을 트리거하기 위해 CoA(Change of Authorization)를 전송합니다.따라서 새로운 MAB(MAC Authentication Bypass) 세션이 구축됩니다.이 시간 엔드포인트는 GuestEndpoints ID 그룹에 속하며 전체 액세스를 제공하는 규칙을 확인합니다.

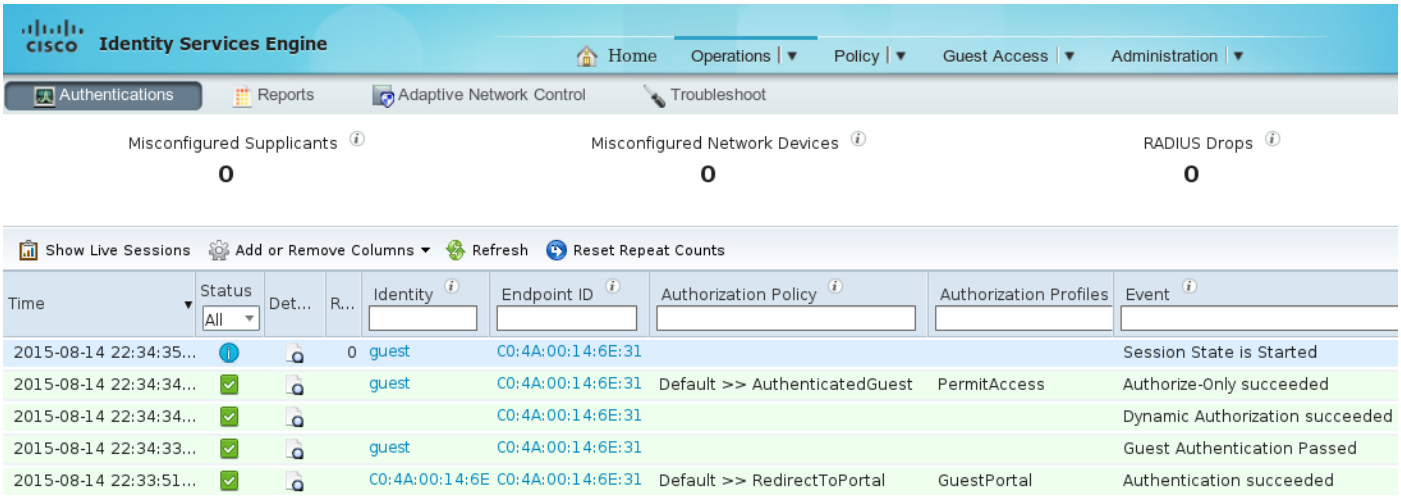


이 단계에서 무선 사용자는 연결을 끊고 다른 WLAN에 연결한 다음 다시 연결할 수 있습니다.모든 후속 인증에서는 mac 주소를 기반으로 ID를 사용하지만 특정 ID 그룹에 속한 엔드포인트 때문에 첫 번째 규칙에 도달합니다.게스트 인증 없이 전체 네트워크 액세스가 제공됩니다.

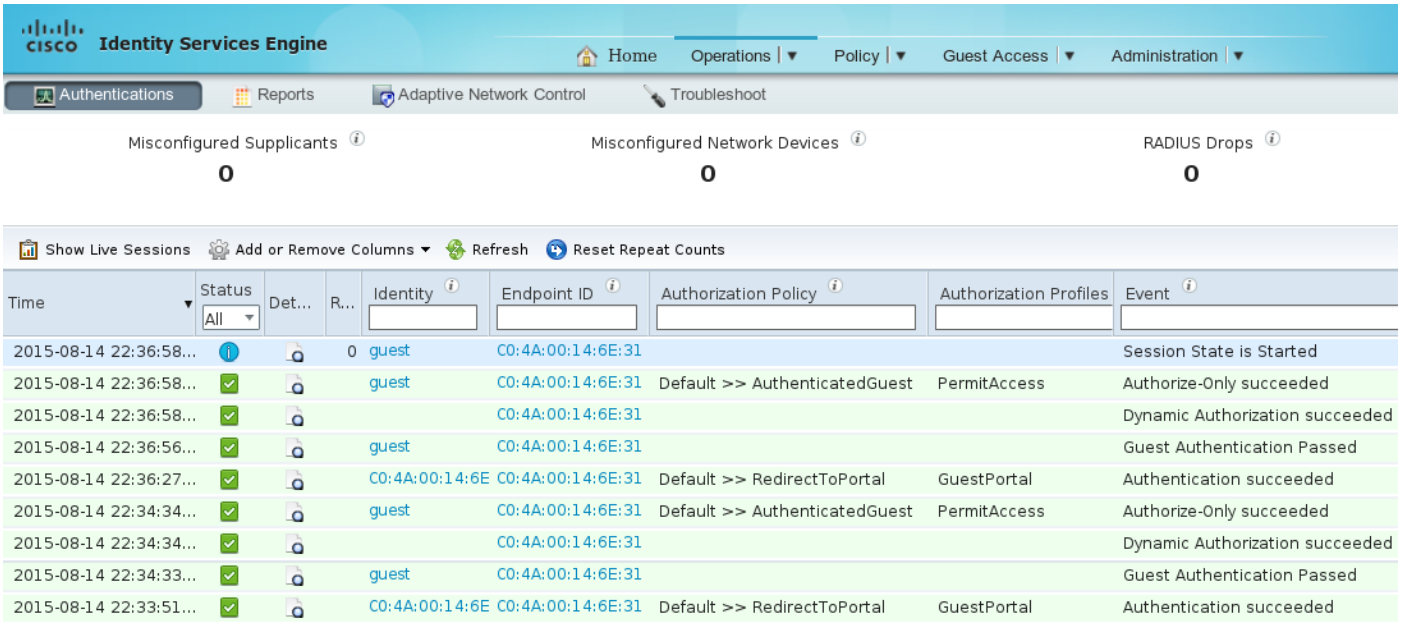


임시 액세스

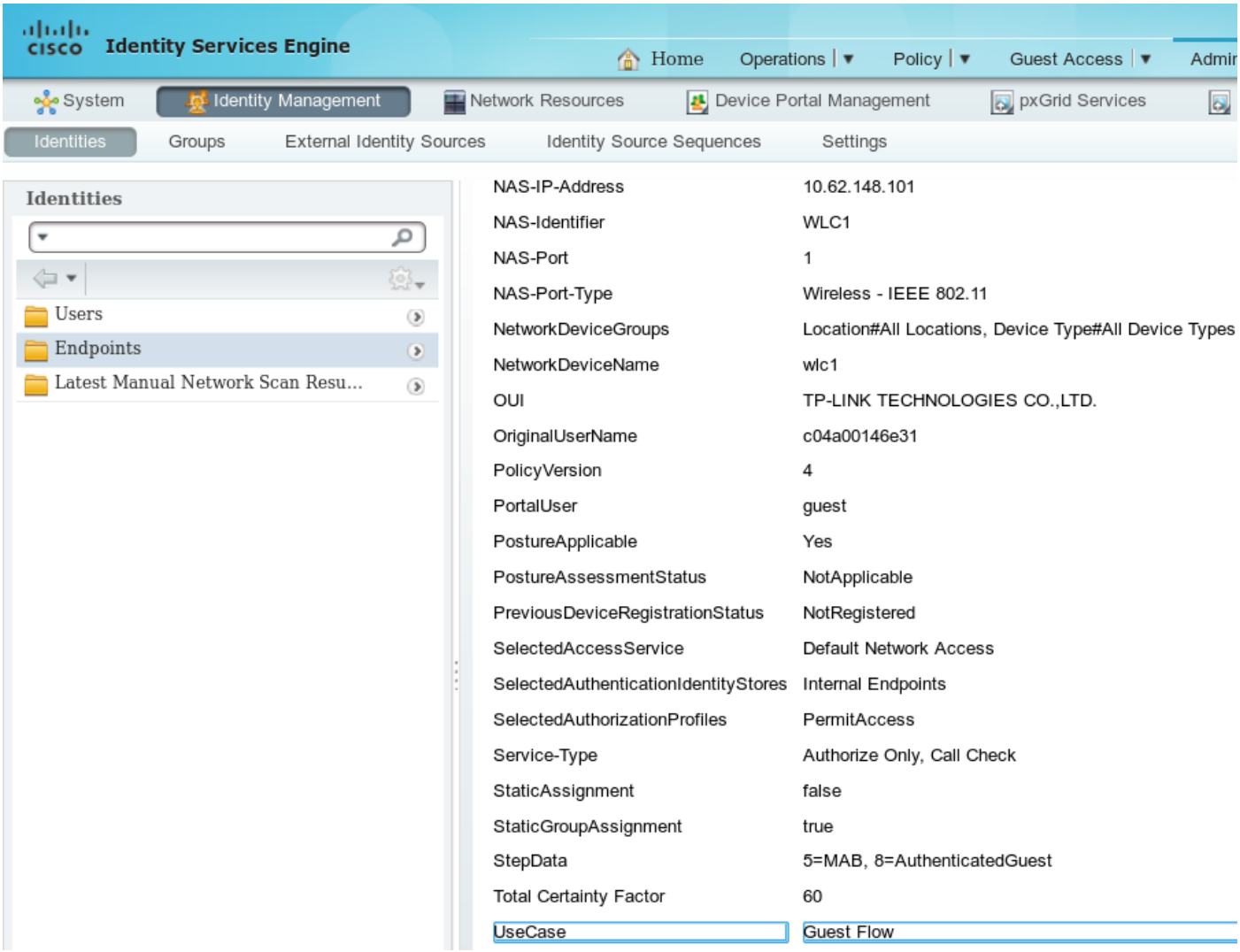
두 번째 시나리오의 경우(Guest Flow 기반 조건 포함) 시작이 동일합니다.



그러나 모든 후속 인증에 대해 세션이 제거된 후 게스트가 일반 규칙을 적중하고 다시 게스트 인증을 위해 리디렉션됩니다.



세션에 대한 올바른 특성이 있을 경우 게스트 플로우 조건이 충족됩니다.이는 엔드포인트 특성을 통해 확인할 수 있습니다.성공적인 게스트 인증 결과가 표시됩니다.




```
PortalUser guest
StepData 5=MAB, 8=AuthenticatedGuest
UseCase Guest Flow
```

버그

CSCuu41157 ISE ENH CoA는 게스트 계정 제거 또는 만료 시 전송 종료를 종료합니다.

(게스트 계정 제거 또는 만료 후 게스트 세션 종료 개선 요청)

참조

- Cisco ISE 1.3 관리자 가이드
- Cisco ISE 1.4 관리자 가이드
- ISE 버전 1.3 핫스팟 컨피그레이션 예
- ISE 버전 1.3 셀프 등록 게스트 포털 컨피그레이션 예
- WLC 및 ISE 컨피그레이션의 중앙 웹 인증 예
- ISE 컨피그레이션을 사용하는 WLC의 FlexConnect AP를 사용한 중앙 웹 인증 예
- 기술 지원 및 문서 – Cisco Systems