MSE(Mobility Services Engine) 및 ISE(Identity Services Engine) ISE 2.0을 통한 위치 기반 권한 부여

목차

소개

이 문서에서는 위치 기반 권한 부여를 위해 MSE(Mobility Service Engine)와 ISE(Identity Services Engine)를 통합하는 방법을 시연합니다.그 목적은 물리적 위치에 따라 무선 장치에 대한 액세스를 허용하거나 거부하는 것입니다.

사전 요구 사항

솔루션의 요구 사항 및 토폴로지

MSE 컨피그레이션은 이 문서의 범위를 벗어났지만, 솔루션의 일반적인 개념은 다음과 같습니다.

-MSE는 구성, 맵 생성 및 WLC 할당을 위해 Prime Infrastructure(이전의 NCS)에서 관리됨

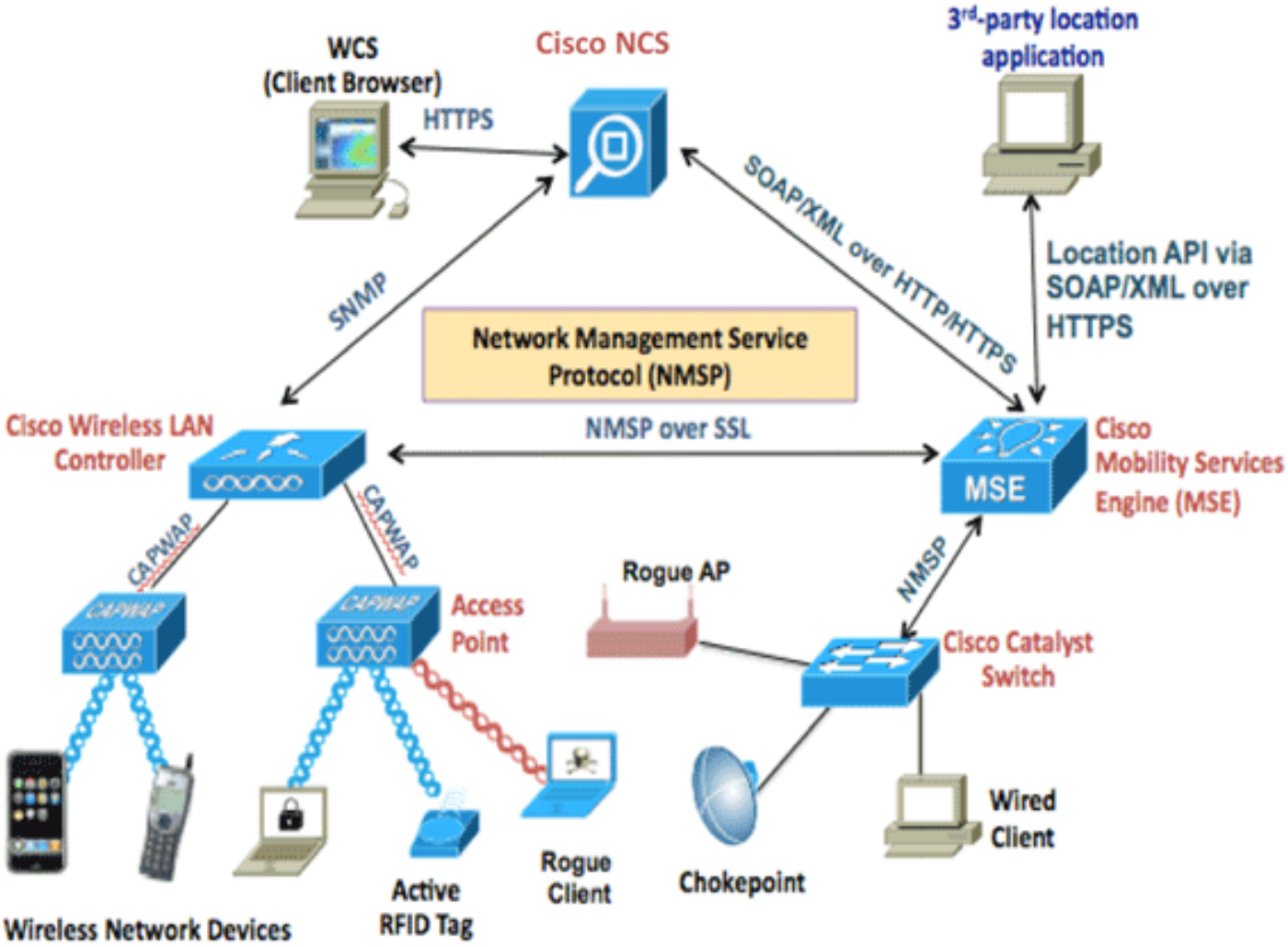
-MSE는 NMSP 프로토콜을 사용하여 WLC(Wireless LAN Controller)와 통신합니다(Prime이 할당한 후).이는 기본적으로 연결된 클라이언트의 AP당 수신되는 RSSI(Received Signal Strength)에 대한 정보를 제공하며, MSE가 위치를 계산할 수 있도록 합니다.

이를 위한 기본 단계:

먼저 Prime Infrastructure(PI)에서 맵을 정의하고 이 맵에 적용 범위 영역을 설정하고 AP를 배치해야 합니다.

MSE를 Prime에 추가할 때 CAS 서비스를 선택합니다.

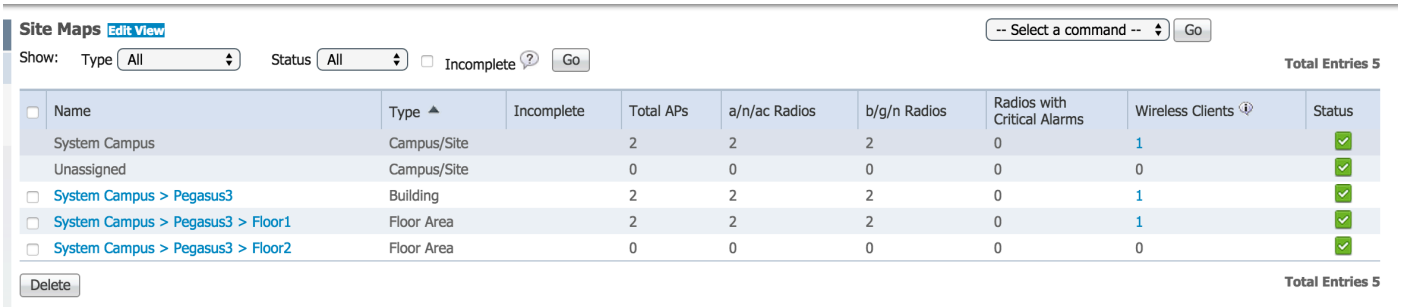
MSE가 추가되면 prime에서 동기화 서비스를 선택하고 WLC/를 확인하고 MSE에 할당할 맵을 선택합니다.



MSE를 ISE와 통합하기 전에 MSE가 실행 중이어야 합니다. 즉, 다음과 같습니다.

1. MSE를 Prime Infrastructure에 추가하고 서비스를 동기화해야 합니다.
2. CAS 서비스를 활성화해야 하며 무선 클라이언트 추적을 활성화해야 합니다.
3. Prime에서 맵을 구성해야 함
4. NMSP가 MSE와 WLC 사이에 성공해야 합니다(WLC 명령행에서 "show nmsp status").

이 설정에는 2개의 층으로 구성된 하나의 빌딩만 있습니다.



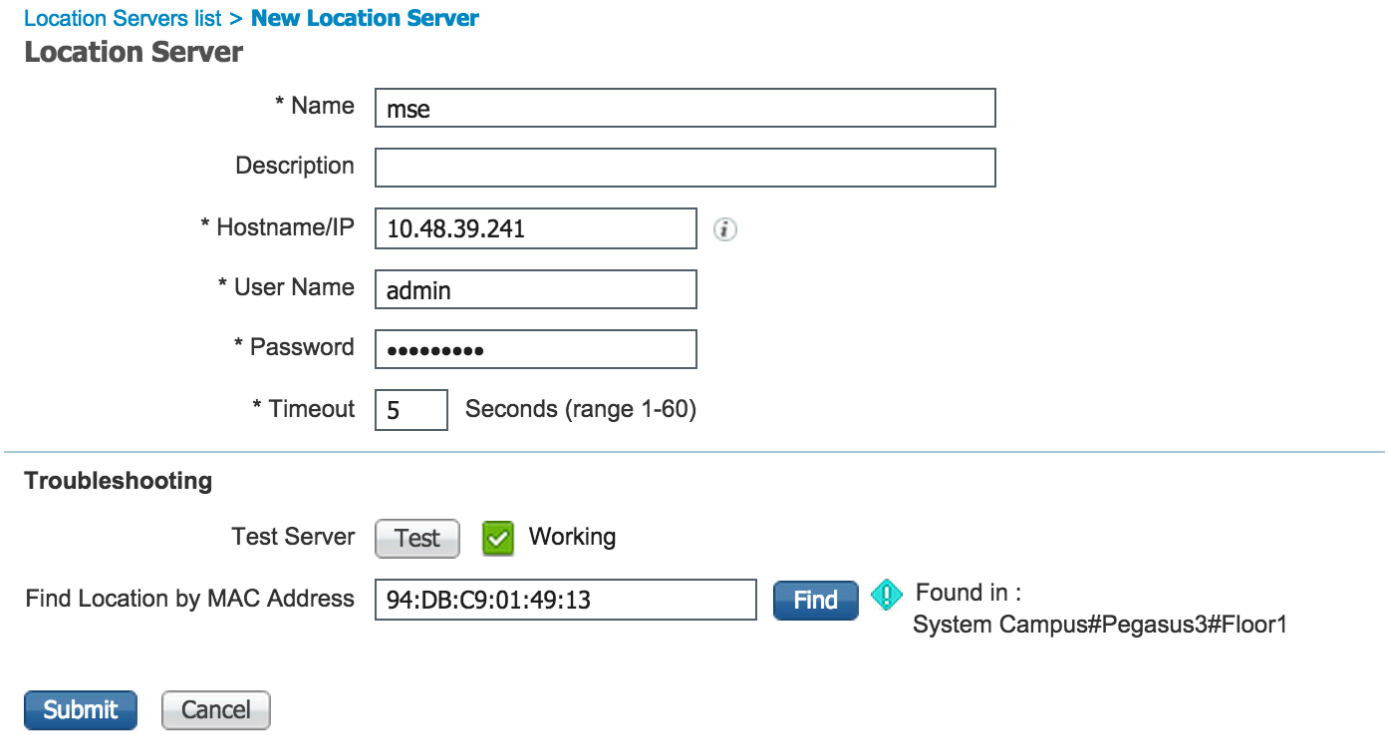
사용된 구성 요소

- MSE 버전 8.0.110
- ISE 버전 2.0

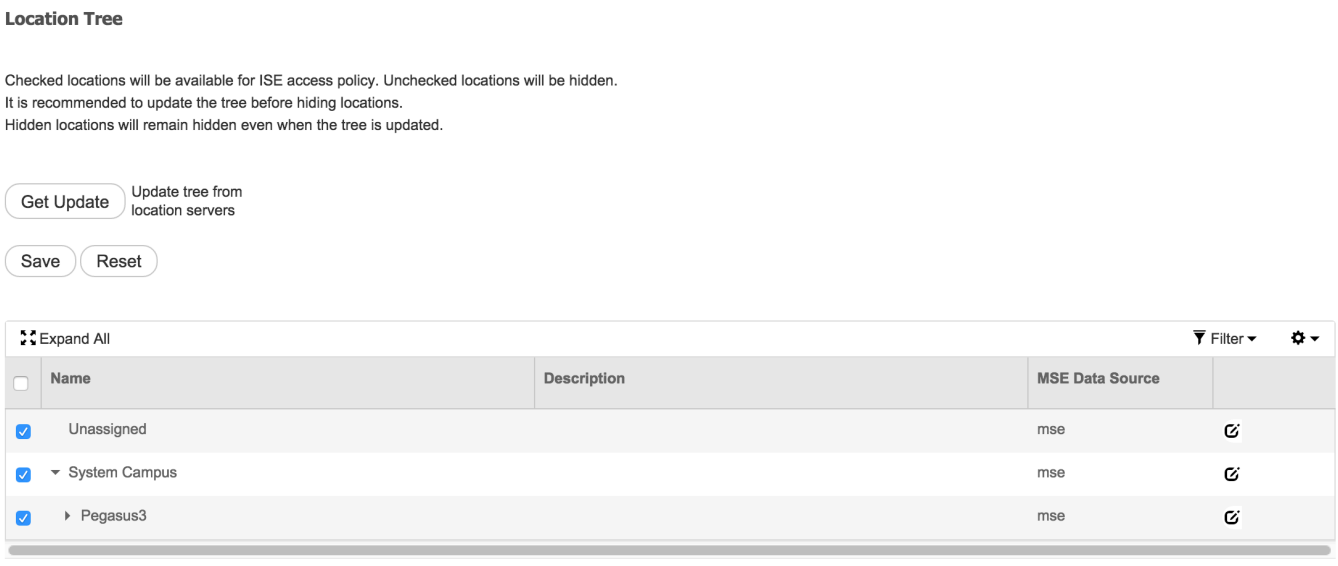
MSE와 ISE 통합

네트워크 리소스, 위치 서비스로 이동하고 추가를 클릭하여 MSE를 추가합니다.

매개변수는 자동으로 설명되며, 연결을 테스트하고 MAC 주소별로 클라이언트 위치를 조회할 수도 있습니다.



다음으로 할 일은 위치 트리로 이동하여 업데이트 가져오기를 클릭하는 것입니다.이렇게 하면 ISE가 MSE에서 건물 및 층을 가져오고 AD 그룹을 추가할 때와 비슷하게 ISE에서 사용할 수 있습니다.



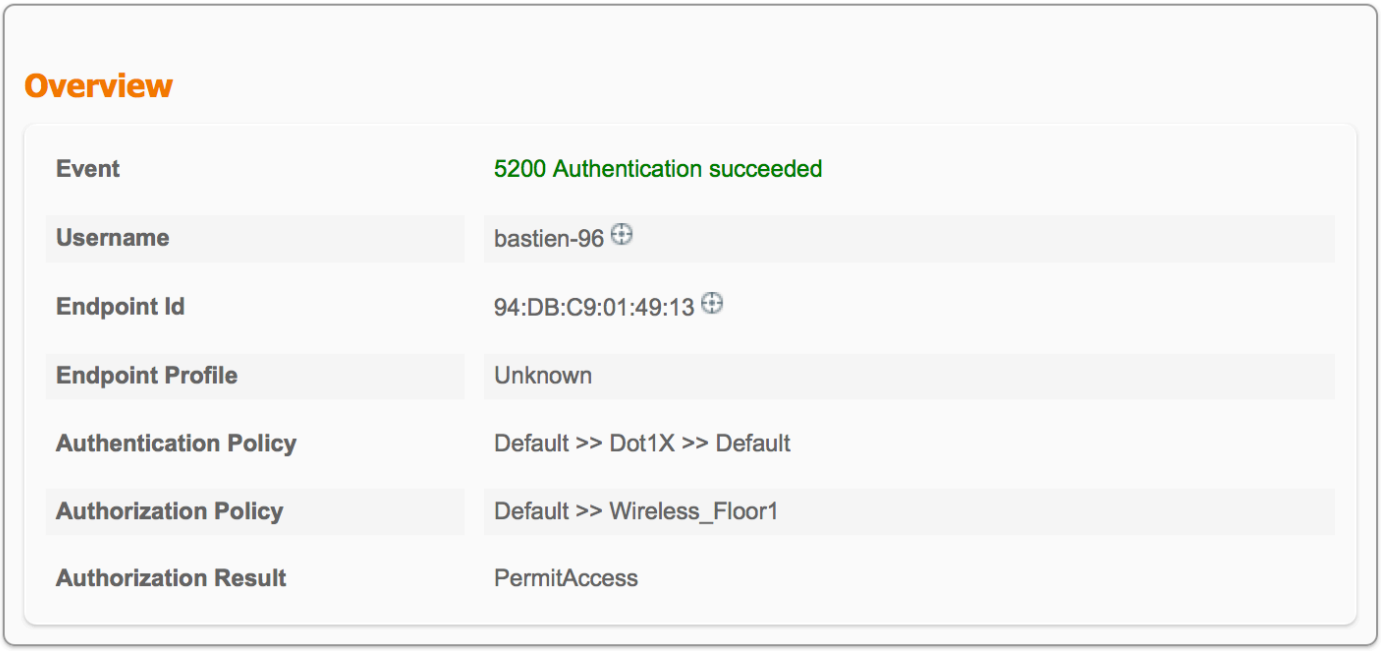
권한 부여 설정

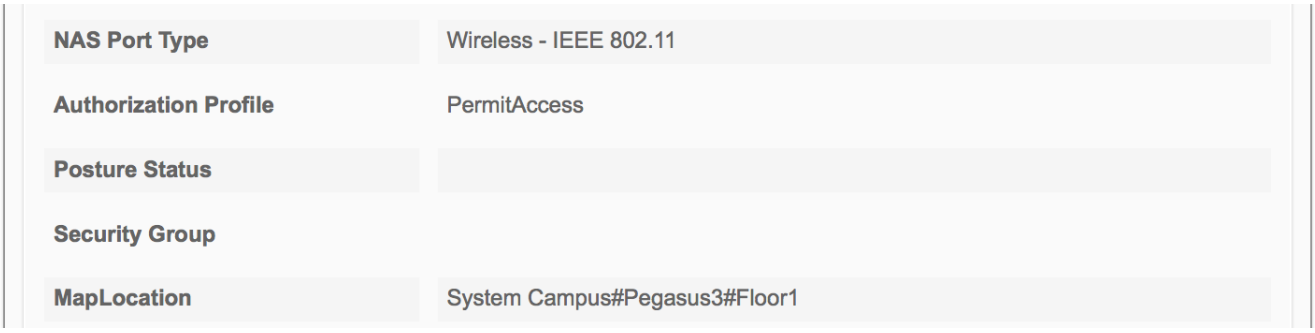
이제 권한 부여 정책에서 MSE:Map Location 특성을 사용할 수 있습니다.

아래 규칙 2개를 구성합니다.

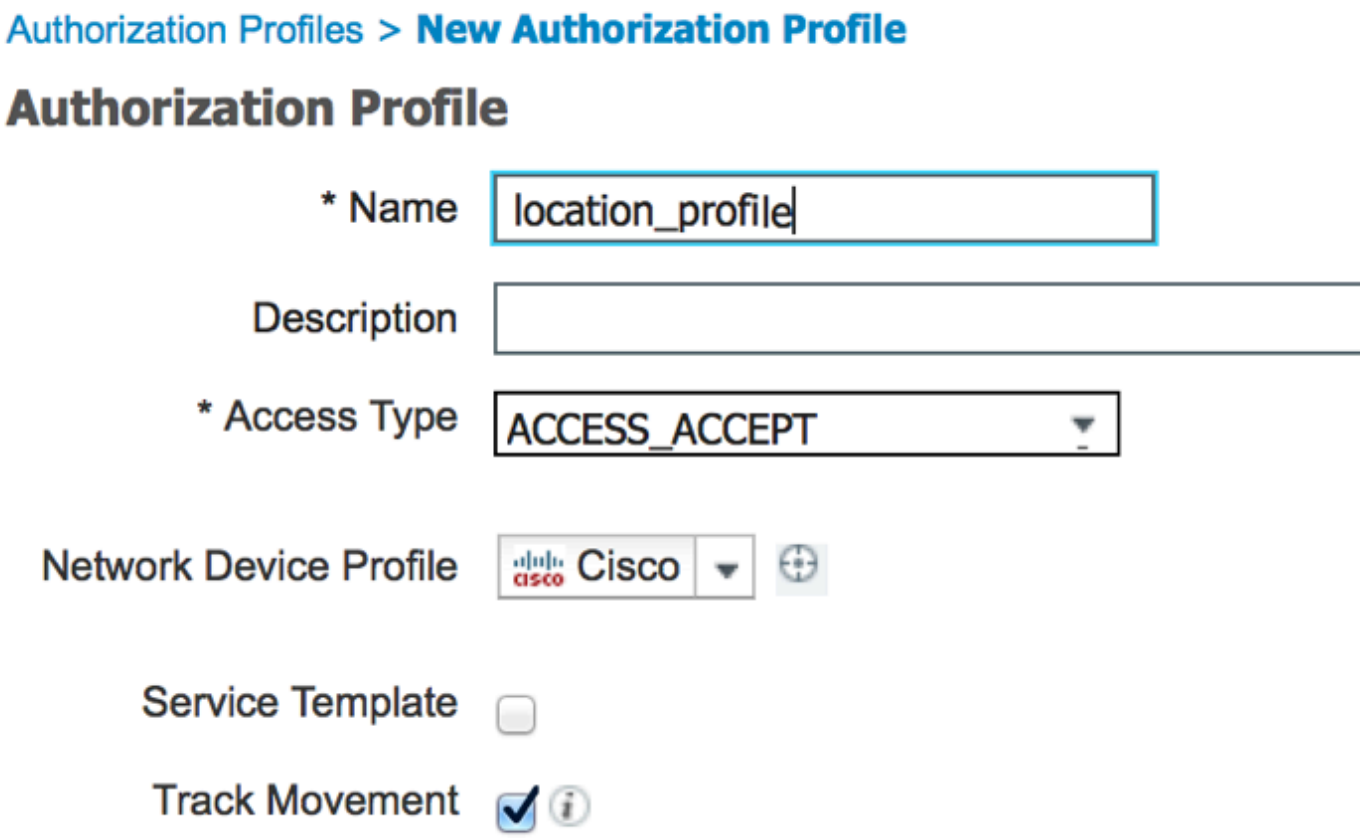
Floor1의 사용자는 인증할 수 있어야 합니다.

인증 세부 정보에서 올바른 프로필과 MAP Location 특성을 확인할 수 있습니다





위의 컨피그레이션을 사용하면 엔드포인트가 한 영역에서 다른 영역으로 이동할 경우 디인증되지 않습니다.사용자 이동을 추적하고 CoA if Authorization(권한 부여 시 변경)을 보내려면 권한 부여 프로파일에서 추적 옵션을 활성화할 수 있습니다. 그러면 5분마다 위치가 변경되는지 확인할 수 있습니다. 이는 정상적인 빠른 로밍 작업에 지장을 줄 수 있습니다.



문제 해결

이 기능의 경우 ISE 컨피그레이션은 간단하지만 MSE가 디바이스를 찾을 수 없는 경우 대부분의 문제가 발생할 수 있습니다.

MSE가 올바르게 설정되었는지 확인할 몇 가지 사항은 다음과 같습니다.

1- 사용자가 연결된 WLC에 MSE ISE에 대한 유효한 NMSP 연결이 다음과 통합되어 있는지 확인합니다.

```
(b2504) >show nmsp status
MSE IP Address            Tx Echo Resp    Rx Echo Req    Tx Data    Rx Data
--------------            ------------    -----------    -------    -------
10.48.39.241         3711            3711           15481      7
```

그렇지 않은 경우 이 문서는

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/CMX/CMX_Troubleshooting.pdf

2- MSE에서 디바이스를 추적할 수 있는지 확인

```
[root@loc-server ~]# service msed status
...
-------------
```

Context Aware Service

Total Active Elements(Wireless Clients, Tags, Rogue APs, Rogue Clients, Interferers, Wired Clients): 29
Active Wireless Clients: 29
Active Tags: 0
Active Rogue APs: 0
Active Rogue Clients: 0