# 使用行動化服務引擎(MSE)和身分識別服務引擎(ISE)ISE 2.0進行基於位置的授權

## 目錄



## 簡介

本文將演示如何將MSE（移動服務引擎）與身份服務引擎(ISE)整合以實現基於位置的授權。目的是根據無線裝置的物理位置允許或拒絕其訪問。

## 必要條件

### 解決方案的要求和拓撲

雖然MSE配置不在本文檔的討論範圍之內，但此解決方案具有以下一般概念：

-MSE由Prime Infrastructure（前身為NCS）管理，用於配置、對映建立和WLC分配

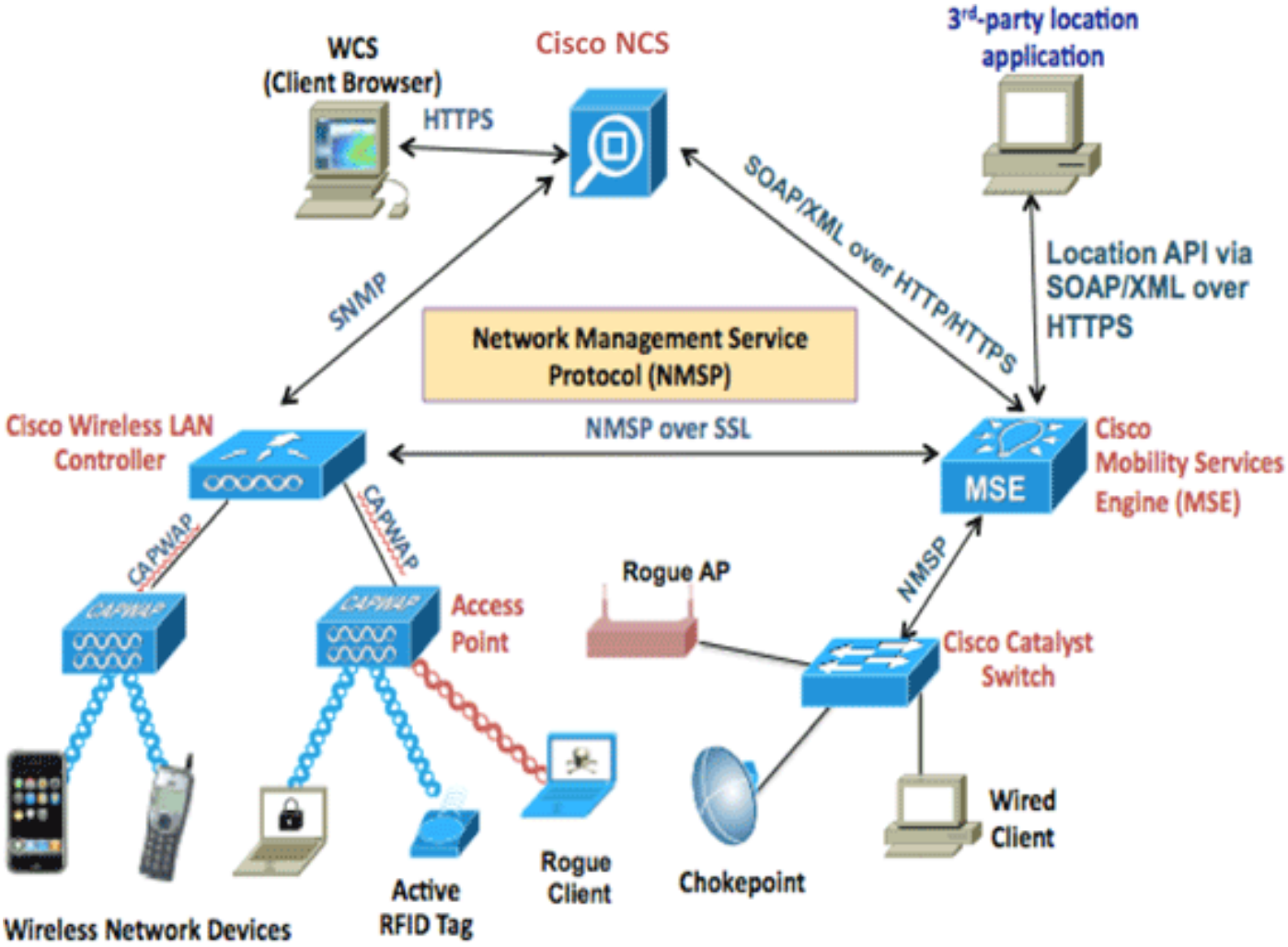
-MSE使用NMSP協定與無線LAN控制器(WLC)（由Prime分配後）通訊。這主要提供有關連線的客戶端的每個AP接收的接收訊號強度(RSSI)的資訊，這允許MSE計算它們的位置。

基本操作步驟：

首先，必須在Prime基礎設施(PI)上定義對映，在此對映上設定覆蓋區域並放置AP。

將MSE新增到prime時，請選擇CAS服務。

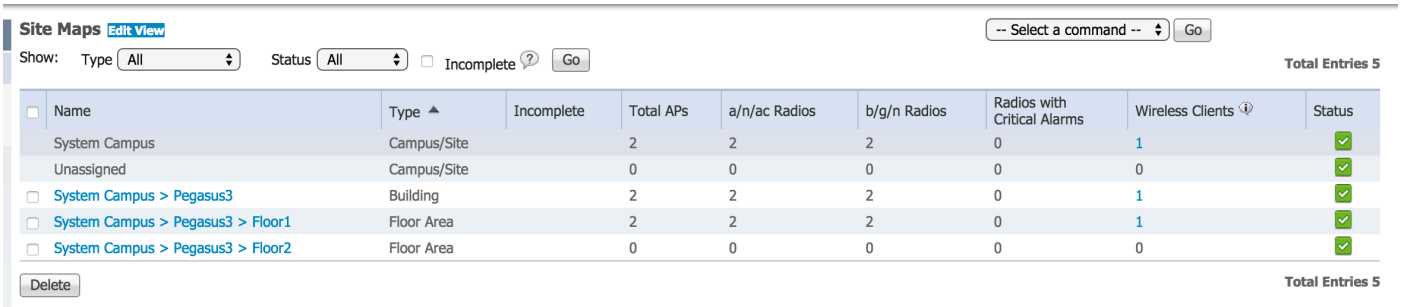
新增MSE後，在prime中，選擇同步服務，然後檢查WLC/和對映以將它們分配給MSE。




在將MSE與ISE整合之前，MSE必須啟動並運行，這意味著：

1. 需要將MSE新增到Prime基礎設施，並且同步服務
2. 需要啟用CAS服務並且需要啟用無線客戶端跟蹤
3. 必須在Prime中配置對映
4. MSP在MSE和WLC之間應該成功（WLC命令列上的「show nmsp status」）

在此設定中，將僅有一個樓層2層：



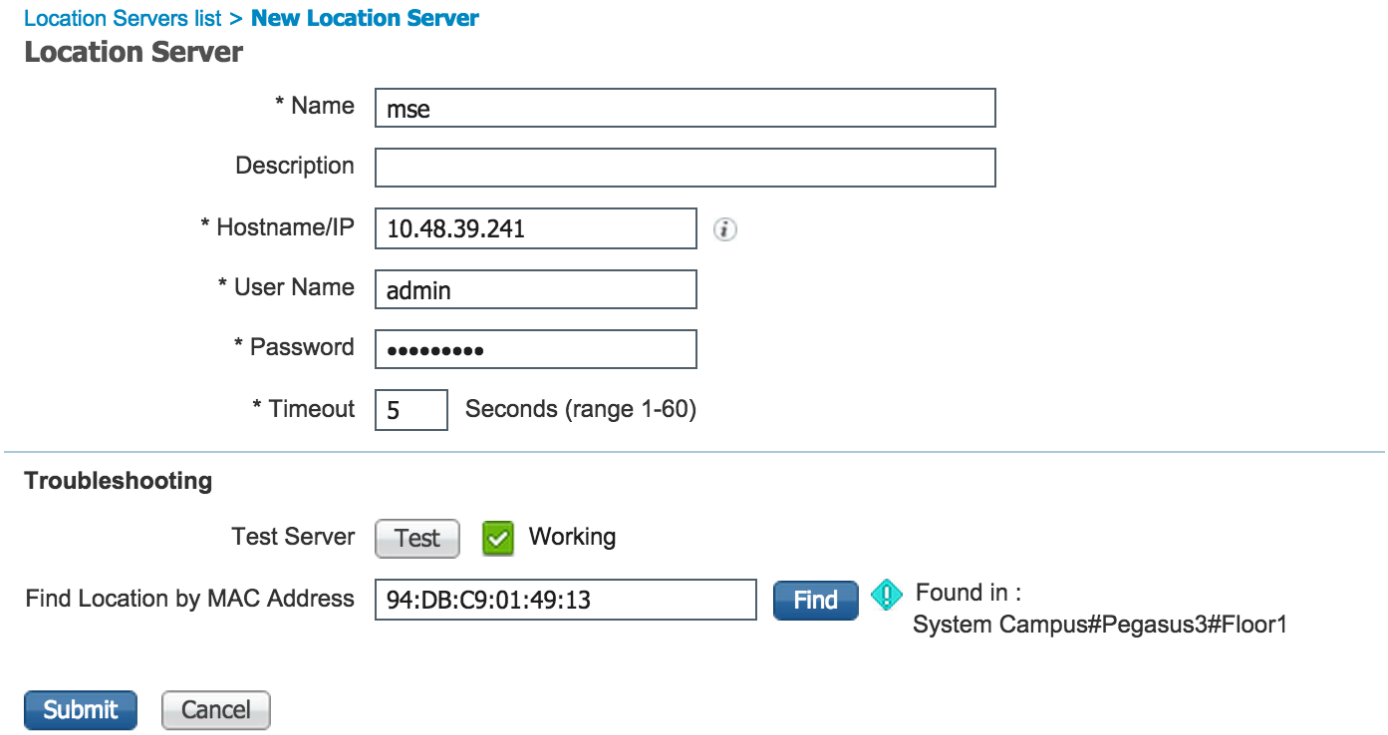

## 採用元件

- MSE版本8.0.110
- ISE版本2.0

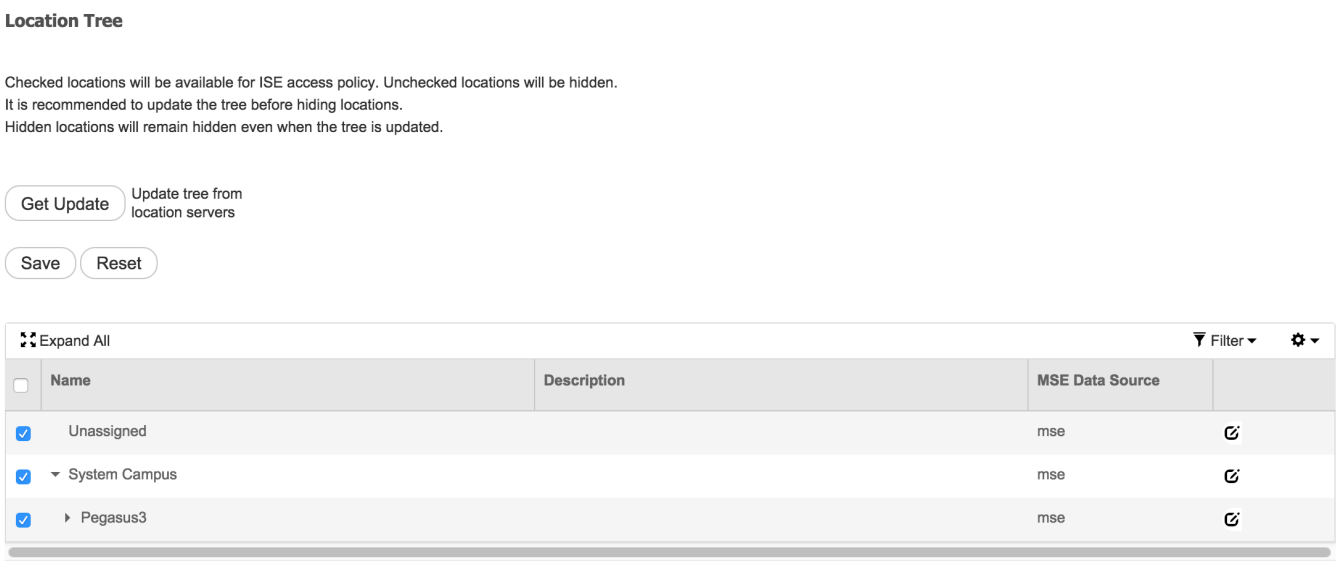
# 將MSE與ISE整合

轉至Network Resources， Location Services，然後點選add以新增MSE。

這些引數是不言自明的，您可以測試連線，還可以通過mac地址查詢客戶端位置：




下一步是轉到「位置」樹，然後按一下「獲取更新」。這將允許ISE從MSE獲取建築和樓層，並使其在ISE中可用，類似於新增AD組時。




# 設定授權

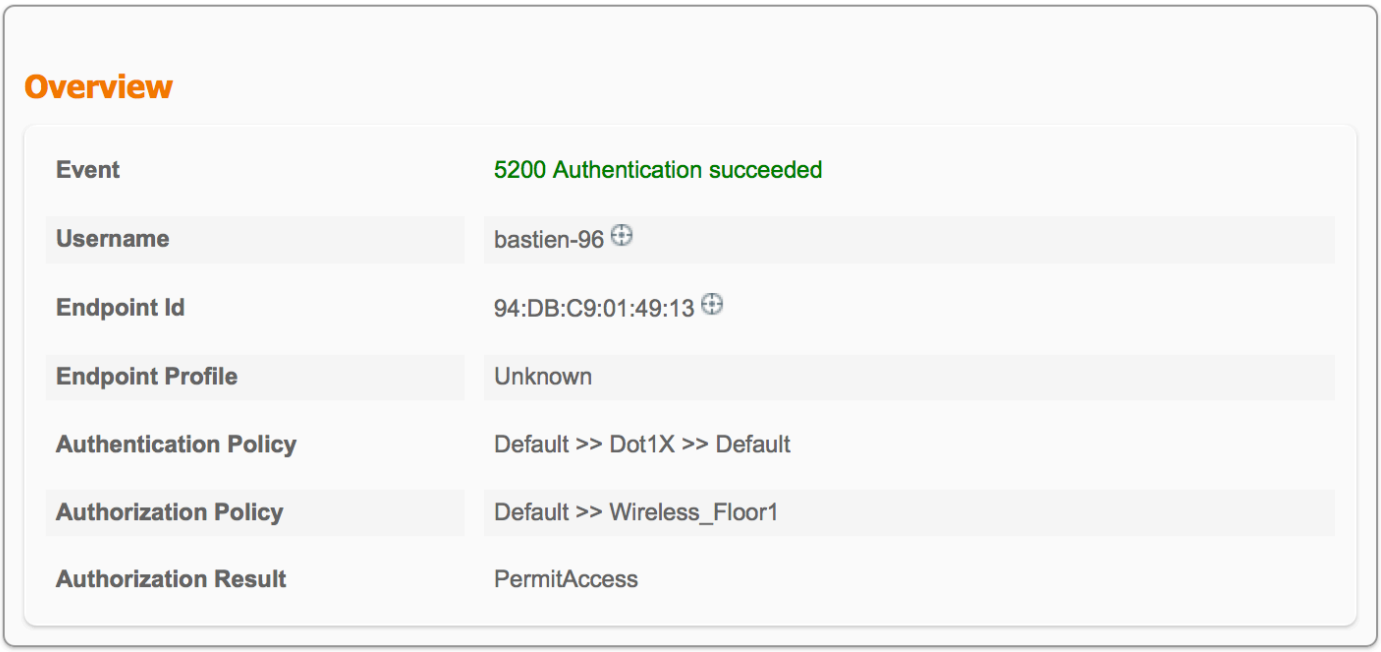
屬性MSE:Map Location現在可用於授權策略。

配置以下兩個規則：

| Status | Rule Name | Conditions (identity groups and other conditions) | Permissions |
|---|---|---|---|
| ✓ | Wireless_Floor1 | if (Wireless_802.1X AND MSE:MapLocation EQUALS System Campus#Pegasus3#Floor1) | then PermitAccess Edit \| |
| ✓ | Wireless | if Wireless_802.1X | then DenyAccess Edit \| |

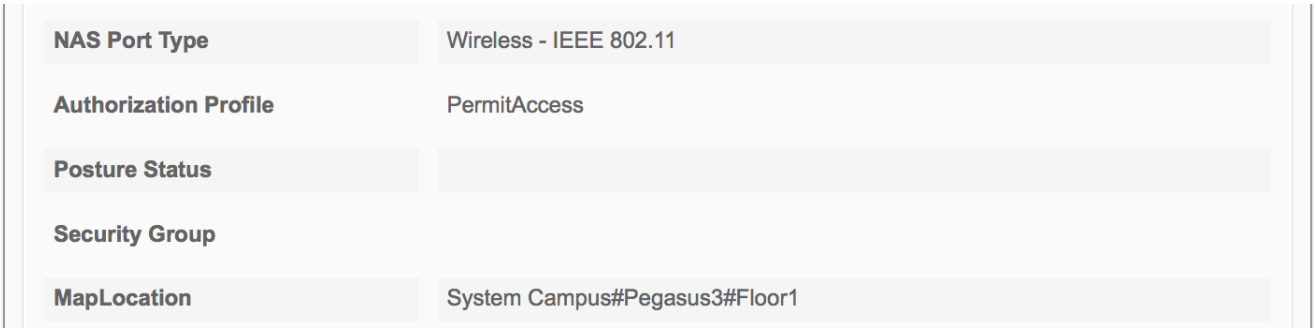
Floor1中的使用者應該能夠進行身份驗證。

我們在身份驗證詳細資訊中看到正確的配置檔案以及MAP Location屬性



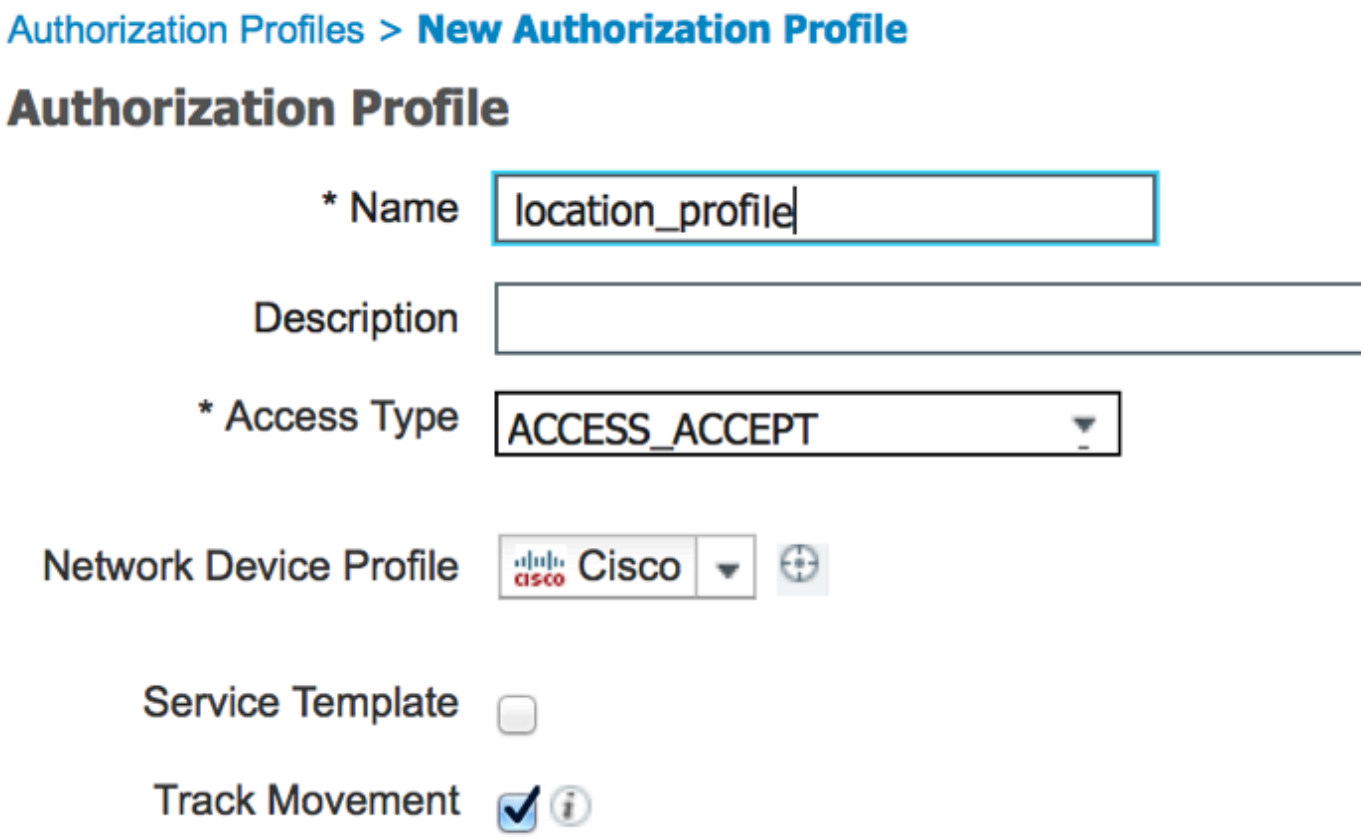
**Overview**

| | |
|---|---|
| **Event** | 5200 Authentication succeeded |
| **Username** | bastien-96 |
| **Endpoint Id** | 94:DB:C9:01:49:13 |
| **Endpoint Profile** | Unknown |
| **Authentication Policy** | Default >> Dot1X >> Default |
| **Authorization Policy** | Default >> Wireless_Floor1 |
| **Authorization Result** | PermitAccess |



| | |
|---|---|
| **NAS Port Type** | Wireless - IEEE 802.11 |
| **Authorization Profile** | PermitAccess |
| **Posture Status** | |
| **Security Group** | |
| **MapLocation** | System Campus#Pegasus3#Floor1 |

使用上述配置時，如果終端從一個區域移動到另一個區域，則不會取消其身份驗證。如果要跟蹤使用者移動，並在授權更改時傳送CoA，您可以在授權配置檔案中啟用跟蹤選項，該選項將每5分鐘檢查一次位置更改。 請注意，這可能干擾正常的快速漫遊操作。




## 疑難排解

對於此功能，ISE配置非常簡單，但是，如果MSE無法找到裝置，可能會出現大多數問題。

要檢查MSE設定是否正確的一些事項：

1 — 確保使用者連線的WLC與MSE ISE整合了有效的NMSP連線：

```
(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
```

如果沒有，本文檔將有所幫助

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

2 — 檢查MSE是否能夠跟蹤裝置

```
[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