Contents

Introduction

This article will demonstrate how to integrate MSE (Mobility Service Engine) with Identity Services Engine (ISE) for Location based authorization. The purpose is to allow or deny access to wireless device based on their physical location.

Prerequisites

Requirements and topology of solution

While MSE Configuraiton is out of the scope of this document, here is general concept of the solution:

-MSE is managed by Prime Infrastructure (formerly NCS) for configuration, maps creation, and WLC assignment

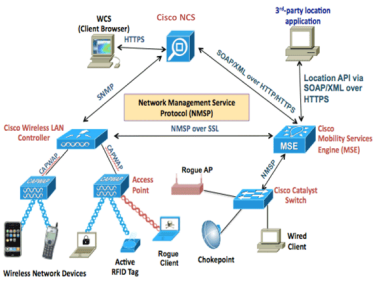
-MSE communicates with the Wireless LAN Controller (WLC) (after being assigned to it by Prime) using NMSP Protocol. This basically gives information about Received Signal Strength (RSSI) received per APs for connected clients, which allows MSE to calcultate their location.

Basic steps to do that:

First you have to define a map on Prime Infrastructure (PI), set coverage area on this map, and place the APs.

When you add MSE to prime, choose CAS service.

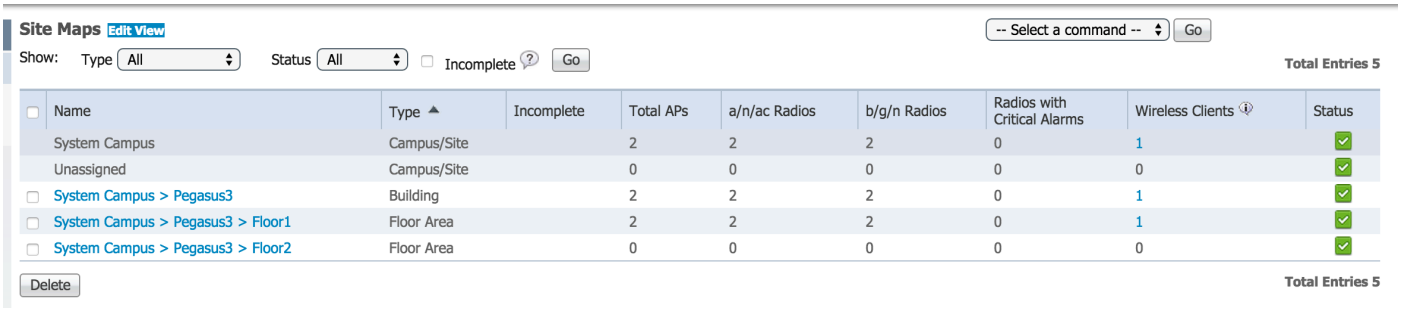
Once MSE is added, in prime, choose sync services, and check your WLC / and maps to assign them to the MSE.



Prior to integrate MSE with ISE, MSE has to be up and running, that means:

1. MSE needs to be added to Prime Infrastructure, and services synchronized
2. CAS Service needs to be enabled and Wireless client tracking needs to be enabled
3. Maps have to be configured in Prime
4. NMSP Should be successful between MSE and WLCs ("show nmsp status" on the WLC command line)

In this setup, there will be only one Building with 2 floors:



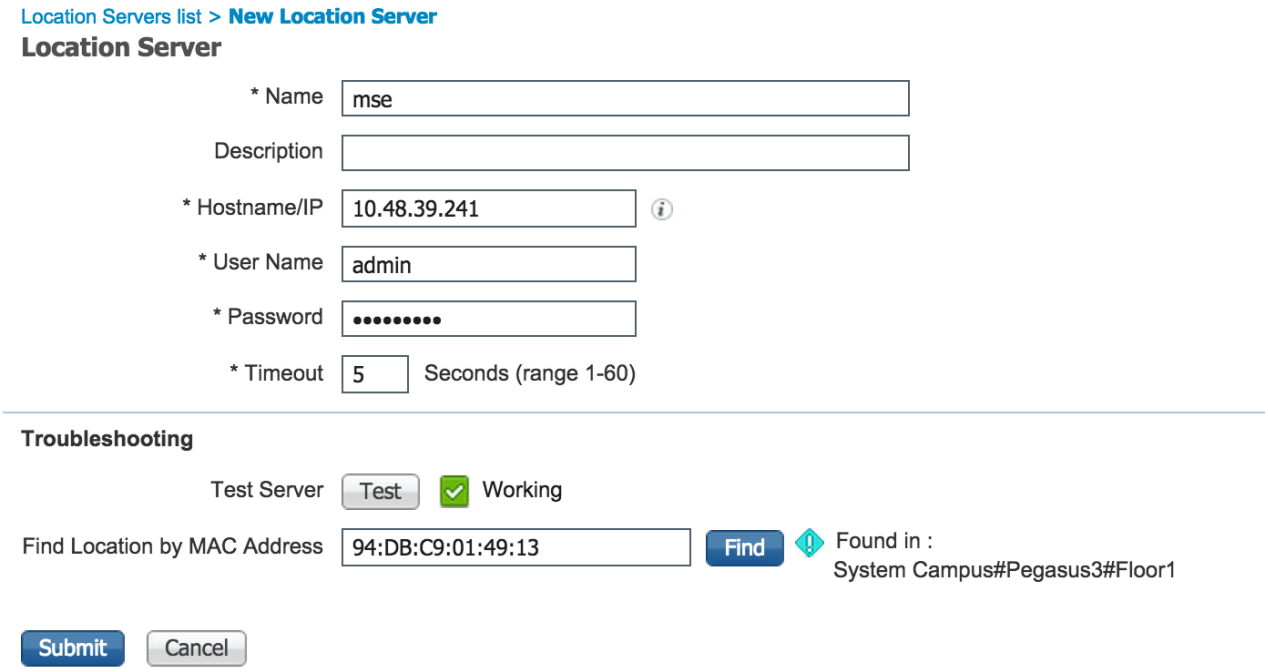
Components used

- MSE version 8.0.110
- ISE version 2.0

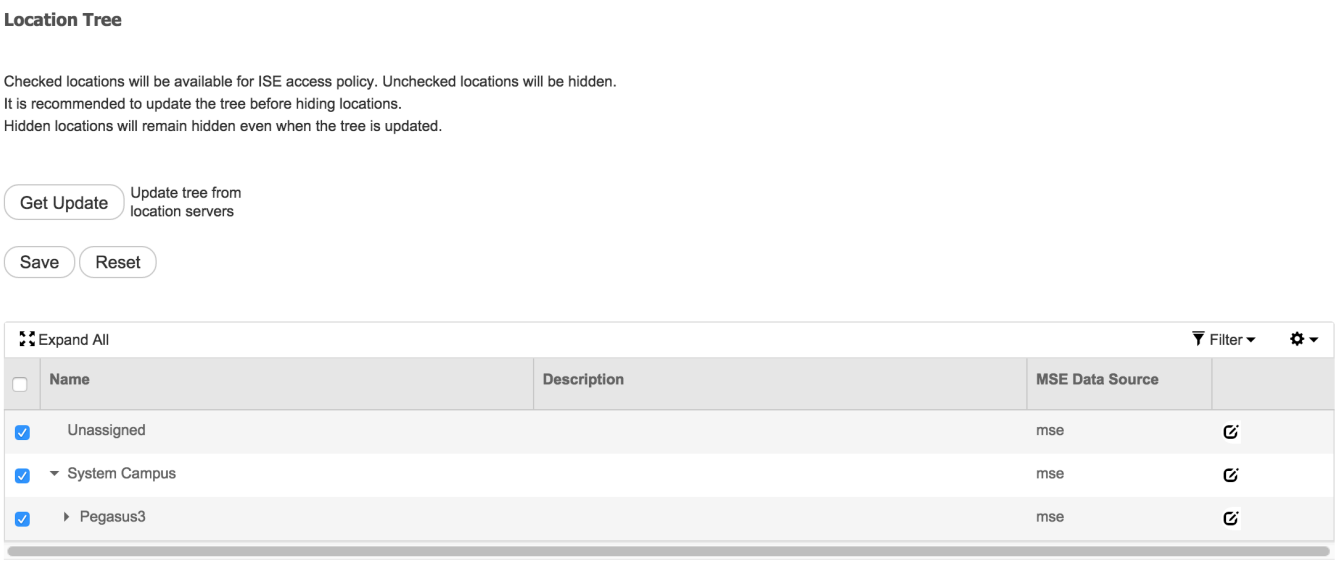
Integrating MSE with ISE

Go to Network Resources, Location Services, and click add to add MSE.

Parameters are self explanatory, and you can test connection, and also client location lookup by mac address:



Next thing to do, is to go to Location tree, and click Get Update. This will allow ISE to fetch Buildings and Floor from MSE, and make them available in ISE, Similar to when you add AD Groups.



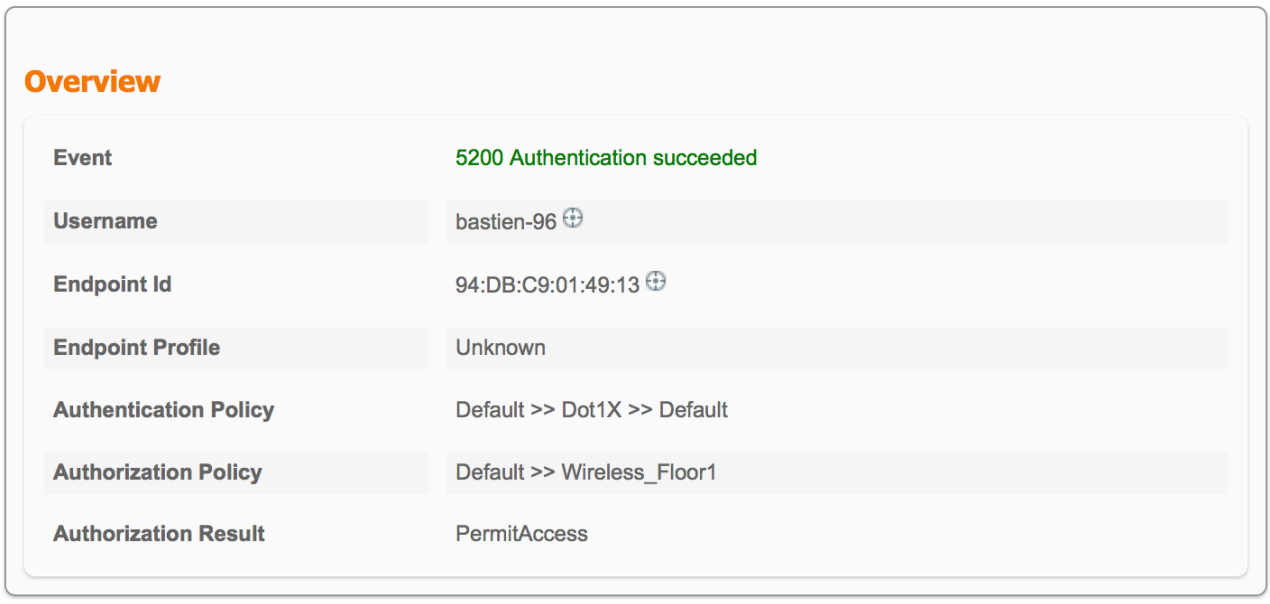
Setting Up Authorization

The attributes MSE:Map Location can now be used in authorization policies.

Configure the 2 below rules:

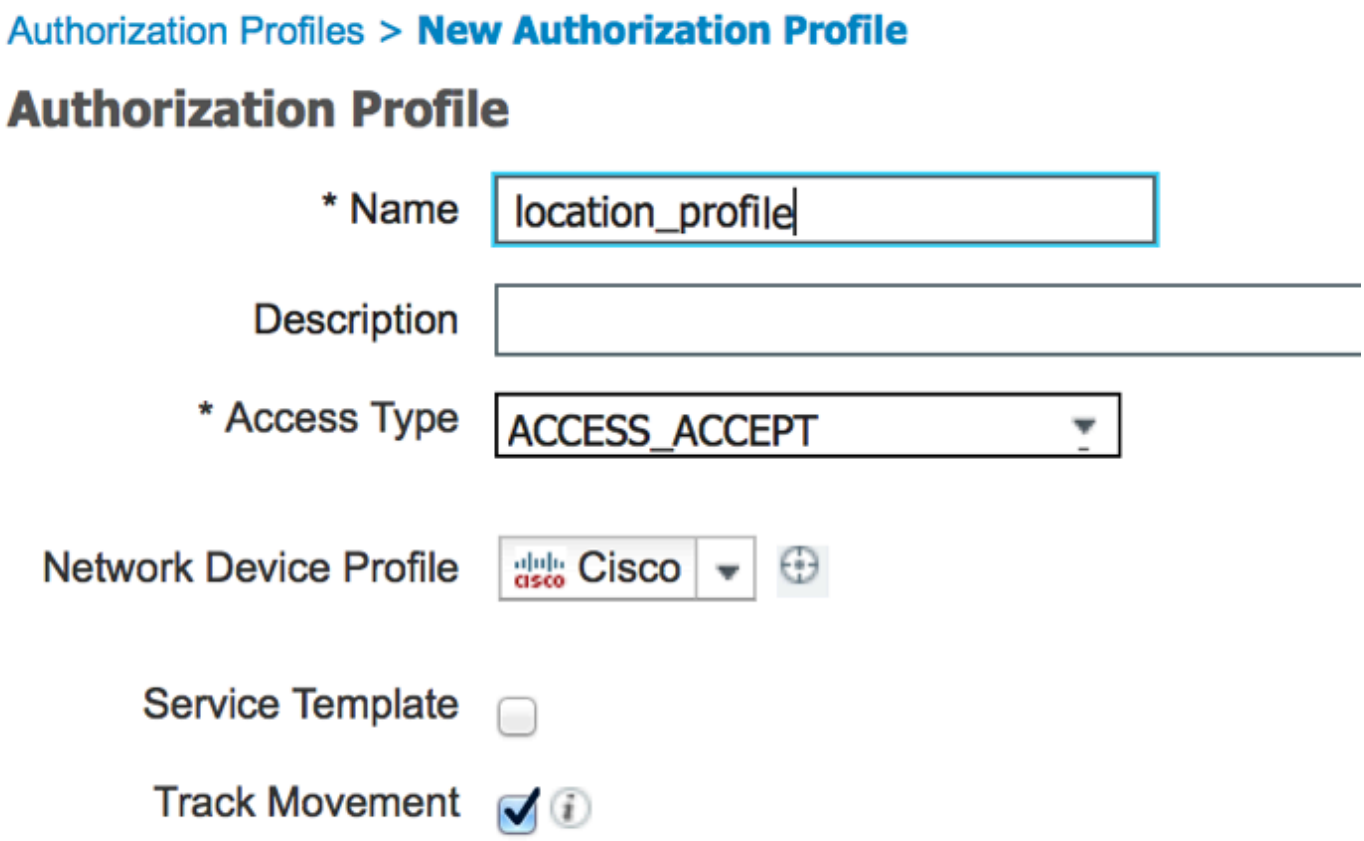
Users in Floor1 should be able to authenticate.

We see in the authentication details the correct profile, as well as MAP Location attribute



With the above configuration, if the endpoint is moving from one zone to another, it will not be

deauthenticated. If you want to track user movement, and send a CoA if Authorization change, you can enable the tracking option in the authorization profile, which will check for location changing every 5 minutes. Note that this can be disruptive to normal fast roaming operations.



Troubleshooting

For this feature, ISE configuration is straightforward, however, most issues might happen if MSE is not able to locate the device.

A few things to check to make sure MSE is setup properly:

1- Make sure that the WLC where user connected has valid NMSP connection to the MSE ISE is integrated with:

If not, this document will help

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

2- Check if MSE is able to track devices