

# Autorizzazione basata sulla posizione con Mobility Services Engine (MSE) e Identity Services Engine (ISE) ISE 2.0

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti e topologia della soluzione](#)

[Componenti usati](#)

[Integrazione di MSE con ISE](#)

[Impostazione dell'autorizzazione](#)

[Risoluzione dei problemi](#)

[Discussioni correlate nella Cisco Support Community](#)

## Introduzione

In questo articolo verrà illustrato come integrare MSE (Mobility Service Engine) con Identity Services Engine (ISE) per l'autorizzazione basata sulla posizione. Lo scopo è quello di consentire o negare l'accesso ai dispositivi wireless in base alla loro posizione fisica.

## Prerequisiti

### Requisiti e topologia della soluzione

Sebbene la configurazione MSE non rientri nell'ambito di questo documento, di seguito viene illustrato il concetto generale della soluzione:

-MSE è gestito da Prime Infrastructure (in precedenza NCS) per la configurazione, la creazione di mappe e l'assegnazione WLC

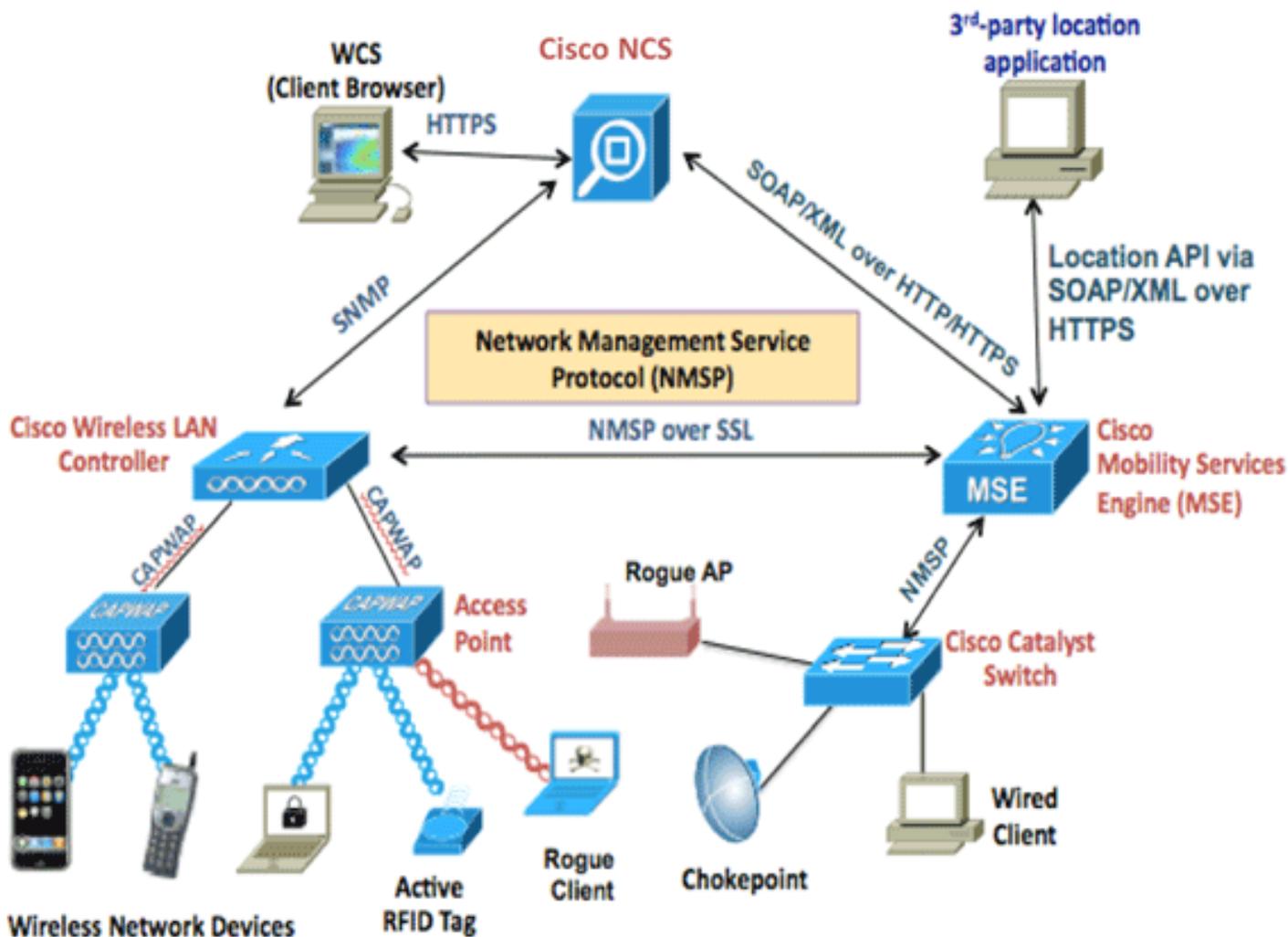
-MSE comunica con il controller WLC (Wireless LAN Controller) (dopo essere stato assegnato da Prime) utilizzando il protocollo NMSP. In questo modo vengono fornite informazioni sull'RSSI (Received Signal Strength) ricevuto per access point per i client connessi, che consente a MSE di calcolare la propria posizione.

Operazioni di base:

Innanzitutto è necessario definire una mappa su Prime Infrastructure (PI), impostare l'area di copertura su questa mappa e posizionare gli access point.

Quando si aggiunge MSE a prime, scegliere il servizio CAS.

Una volta aggiunto MSE, in prime, scegliere i servizi di sincronizzazione e controllare il WLC / e le mappe per assegnarli al MSE.



Prima di integrare MSE con ISE, MSE deve essere operativo:

1. È necessario aggiungere MSE a Prime Infrastructure e sincronizzare i servizi
2. Il servizio CAS deve essere abilitato e deve essere abilitato il monitoraggio dei client wireless
3. Le mappe devono essere configurate in Prime
4. L'NMSMP deve avere esito positivo tra MSE e WLC ("show nmsmp status" sulla riga di comando del WLC)

In questa struttura, ci sarà un solo edificio con 2 piani:

Name	Type	Incomplete	Total APs	a/n/ac Radios	b/g/n Radios	Radios with Critical Alarms	Wireless Clients	Status
<input type="checkbox"/> System Campus	Campus/Site		2	2	2	0	1	✓
<input type="checkbox"/> Unassigned	Campus/Site		0	0	0	0	0	✓
<input type="checkbox"/> System Campus > Pegasus3	Building		2	2	2	0	1	✓
<input type="checkbox"/> System Campus > Pegasus3 > Floor1	Floor Area		2	2	2	0	1	✓
<input type="checkbox"/> System Campus > Pegasus3 > Floor2	Floor Area		0	0	0	0	0	✓

## Componenti usati

- MSE versione 8.0.110
- ISE versione 2.0

## Integrazione di MSE con ISE

Andare a Risorse di rete, Servizi percorso e fare clic su Aggiungi per aggiungere MSE.

I parametri sono di immediata comprensione ed è possibile testare la connessione e anche la ricerca della posizione del client per indirizzo MAC:

[Location Servers list](#) > **New Location Server**

### Location Server

\* Name

Description

\* Hostname/IP  ⓘ

\* User Name

\* Password

\* Timeout  Seconds (range 1-60)

### Troubleshooting

Test Server   Working

Find Location by MAC Address   ⓘ Found in :  
System Campus#Pegasus3#Floor1

Passare alla struttura ad albero Posizione e fare clic su Recupera aggiornamento. Ciò consentirà ad ISE di recuperare gli edifici e il pavimento da MSE e di renderli disponibili in ISE, come quando si aggiungono gruppi AD.

### Location Tree

Checked locations will be available for ISE access policy. Unchecked locations will be hidden.  
It is recommended to update the tree before hiding locations.  
Hidden locations will remain hidden even when the tree is updated.

Update tree from location servers

Expand All		Filter	⚙
<input type="checkbox"/>	Name	Description	MSE Data Source
<input checked="" type="checkbox"/>	Unassigned		mse
<input checked="" type="checkbox"/>	System Campus		mse
<input checked="" type="checkbox"/>	Pegasus3		mse

## Impostazione dell'autorizzazione

È ora possibile utilizzare gli attributi MSE:Map Location nei criteri di autorizzazione.

Configurare le due regole seguenti:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless_Floor1	if (Wireless_802.1X AND MSE:MapLocation EQUALS System Campus#Pegasus3#Floor1)	then PermitAccess <a href="#">Edit</a>
<input checked="" type="checkbox"/>	Wireless	if Wireless_802.1X	then DenyAccess <a href="#">Edit</a>

Gli utenti di Floor1 devono essere in grado di eseguire l'autenticazione.

Nei dettagli di autenticazione vengono visualizzati il profilo corretto e l'attributo di posizione MAP

### Overview

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

<b>NAS Port Type</b>	Wireless - IEEE 802.11
<b>Authorization Profile</b>	PermitAccess
<b>Posture Status</b>	
<b>Security Group</b>	
<b>MapLocation</b>	System Campus#Pegasus3#Floor1

Con la configurazione precedente, se l'endpoint si sposta da una zona all'altra, non verrà deautenticato. Se si desidera tenere traccia dei movimenti degli utenti e inviare un CoA se l'autorizzazione viene modificata, è possibile attivare l'opzione di verifica nel profilo di autorizzazione, che verificherà la modifica della posizione ogni 5 minuti. Si noti che ciò può causare interruzioni delle normali operazioni di roaming veloce.

## Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement

## Risoluzione dei problemi

Per questa funzione, la configurazione ISE è semplice, tuttavia la maggior parte dei problemi potrebbe verificarsi se MSE non è in grado di individuare il dispositivo.

Verificare che MSE sia configurato correttamente:

1- Verificare che il WLC a cui l'utente ha connesso la connessione NMSP valida al MSE ISE sia integrato con:

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

In caso contrario, questo documento

[http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless\\_Networks/Unified\\_Access/CMX/CMX\\_Troubleshooting.pdf](http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/CMX/CMX_Troubleshooting.pdf)

2- Verificare se MSE è in grado di rilevare le periferiche

```
[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