

Locatiegebaseerde autorisatie met Mobility Services Engine (MSE) en Identity Services Engine (ISE) ISE 2.0

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Eisen en topologie van de oplossing](#)

[Gebruikte componenten](#)

[MSE integreren met ISE](#)

[Invoervergunning instellen](#)

[Probleemoplossing](#)

[Gerelateerde Cisco Support Community-discussies](#)

Inleiding

Dit artikel zal demonstreren hoe MSE (Mobility Services Engine) te integreren met Identity Services Engine (ISE) voor een locatiegebaseerde autorisatie. Het doel is toegang tot draadloze apparatuur te verlenen of te weigeren op basis van hun fysieke locatie.

Voorwaarden

Eisen en topologie van de oplossing

Hoewel de MSE-configuratie niet binnen het bereik van dit document valt, is hier een algemeen concept van de oplossing:

-MSE wordt beheerd door Prime Infrastructure (voorheen NCS) voor configuratie, plattegronden en WLC toewijzing

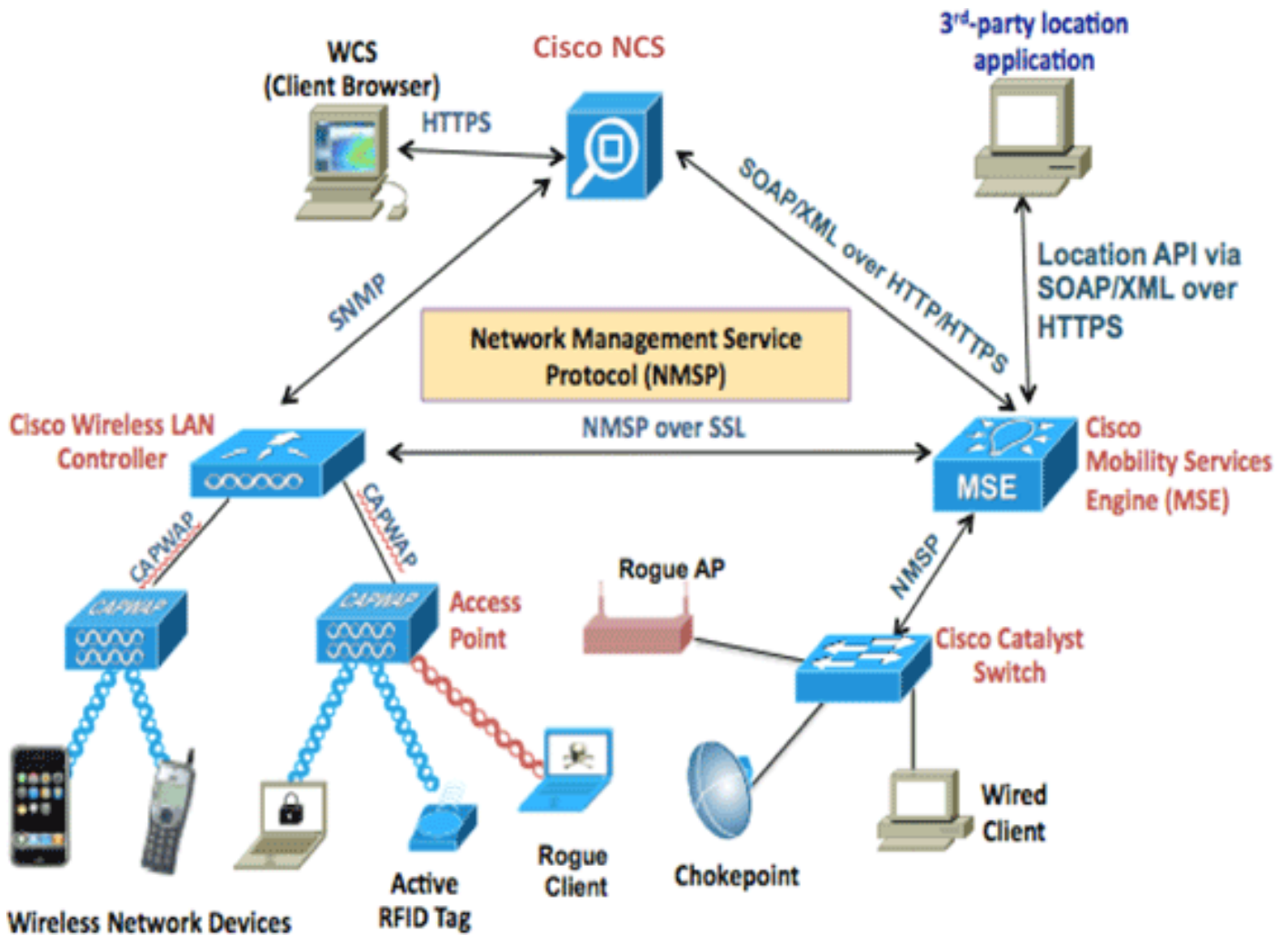
-MSE communiceert met de Wireless LAN Controller (WLC) (nadat deze door Prime) toegewezen is geweest met behulp van NMSP-protocol. Dit geeft in principe informatie over de Ontvangen Signal Sterkte (RSSI) ontvangen per APs voor verbonden cliënten, wat MSE in staat stelt om hun plaats te berekenen.

Basisstappen om dat te doen:

Eerst moet u een kaart definiëren op Prime Infrastructure (PI), het dekkingsgebied op deze kaart instellen en de APs plaatsen.

Wanneer u MSE aan priemgetal toevoegt, kiest u CAS-service.

Als MSE is toegevoegd, kiest u in eerste instantie de sync-services en controleert u de WLC / en de kaarten om ze aan de MSE toe te wijzen.



Voordat MSE met ISE wordt geïntegreerd, moet MSE actief zijn, dat wil zeggen:

1. MSE moet worden toegevoegd aan Prime-infrastructuur en services zijn gesynchroniseerd
2. CAS-service moet worden ingeschakeld en draadloze client-tracking moet worden ingeschakeld
3. De kaarten moeten in de machine worden geconfigureerd
4. NMSP zou tussen MSE en WLCs succesvol moeten zijn (toon nmstp status" op de WLC opdrachtregel)

Bij deze installatie is er slechts één gebouw met 2 verdiepingen:

Site Maps [Edit View](#) -- Select a command -- Go

Show: Type Status Incomplete [?](#) Total Entries 5

<input type="checkbox"/>	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 checked="" type="checkbox"/>
<input type="checkbox"/>	Unassigned	Campus/Site		0	0	0	0	0	<input checked="" type="checkbox"/>
<input type="checkbox"/>	System Campus > Pegasus3	Building		2	2	2	0	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	System Campus > Pegasus3 > Floor1	Floor Area		2	2	2	0	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	System Campus > Pegasus3 > Floor2	Floor Area		0	0	0	0	0	<input checked="" type="checkbox"/>

Total Entries 5

Gebuurte componenten

- MSE versie 8.0.110
- ISE versie 2.0

MSE integreren met ISE

Ga naar netwerkbronnen, locatieservices en klik op Toevoegen om MSE toe te voegen.

De parameters zijn zelf-verklarend, en je kunt verbinding testen, en ook cliënt locatie raadpleging door mac adres:

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

Location Server

* Name	<input type="text" value="mse"/>
Description	<input type="text"/>
* Hostname/IP	<input type="text" value="10.48.39.241"/> ⓘ
* User Name	<input type="text" value="admin"/>
* Password	<input type="password" value="••••••••"/>
* Timeout	<input type="text" value="5"/> Seconds (range 1-60)

Troubleshooting

Test Server Working

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

Daarna moet je naar de Location boom gaan en op Get Update klikken. Dit stelt ISE in staat om gebouwen en vloeren van MSE te halen en maakt ze beschikbaar in ISE, vergelijkbaar met wanneer u AD groepen toevoegt.

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

Invoervergunning instellen

De eigenschappen MSE:Map Locatie kunnen nu in autorisatiebeleid gebruikt worden.

Configureer de 2 onderstaande regels:

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 ▾

Gebruikers in Floor1 moeten dit kunnen authenticeren.

We zien in de authenticatie details het juiste profiel evenals MAP Locatie attributie

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



Als het eindpunt van de ene zone naar de andere overgaat, wordt de configuratie niet gedecodeerd. Als u de beweging van de gebruiker wilt volgen en een CoA wilt verzenden als de vergunningsverandering, kunt u de volgoptie in het vergunningprofiel inschakelen, dat om de 5 minuten zal controleren op de plaats die verandert. Merk op dat dit versturend kan werken voor normale snelle roamingoperaties.

Authorization Profile

* Name

Description

* Access Type

Network Device Profile  

Service Template

Track Movement 

Probleemoplossing

Voor deze optie is de ISE-configuratie eenvoudig. De meeste problemen kunnen echter optreden als MSE het apparaat niet kan vinden.

Een paar dingen om te controleren of MSE goed is ingesteld:

1- Zorg dat de WLC waar de gebruiker aangesloten is, een geldige NMSP verbinding met MSE ISE heeft geïntegreerd met:

```
(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
```

Als dit niet het geval is, helpt dit document

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

2- Controleer of MSE in staat is om apparaten te volgen

```
[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