

Standortbasierte Autorisierung mit Mobility Services Engine (MSE) und Identity Services Engine (ISE) ISE 2.0

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen und Topologie der Lösung](#)

[Verwendete Komponenten](#)

[Integration von MSE mit ISE](#)

[Einrichten der Autorisierung](#)

[Fehlerbehebung](#)

[Ähnliche Diskussionen in der Cisco Support Community](#)

Einführung

In diesem Artikel wird die Integration von MSE (Mobility Service Engine) in Identity Services Engine (ISE) für die standortbasierte Autorisierung erläutert. Der Zweck besteht darin, den Zugriff auf Wireless-Geräte basierend auf ihrem physischen Standort zu gestatten oder zu verweigern.

Voraussetzungen

Anforderungen und Topologie der Lösung

Obwohl die MSE-Konfiguration nicht in den Anwendungsbereich dieses Dokuments fällt, folgt das allgemeine Konzept der Lösung:

- MSE wird von der Prime-Infrastruktur (ehemals NCS) für die Konfiguration, die Erstellung von Karten und die WLC-Zuweisung verwaltet.

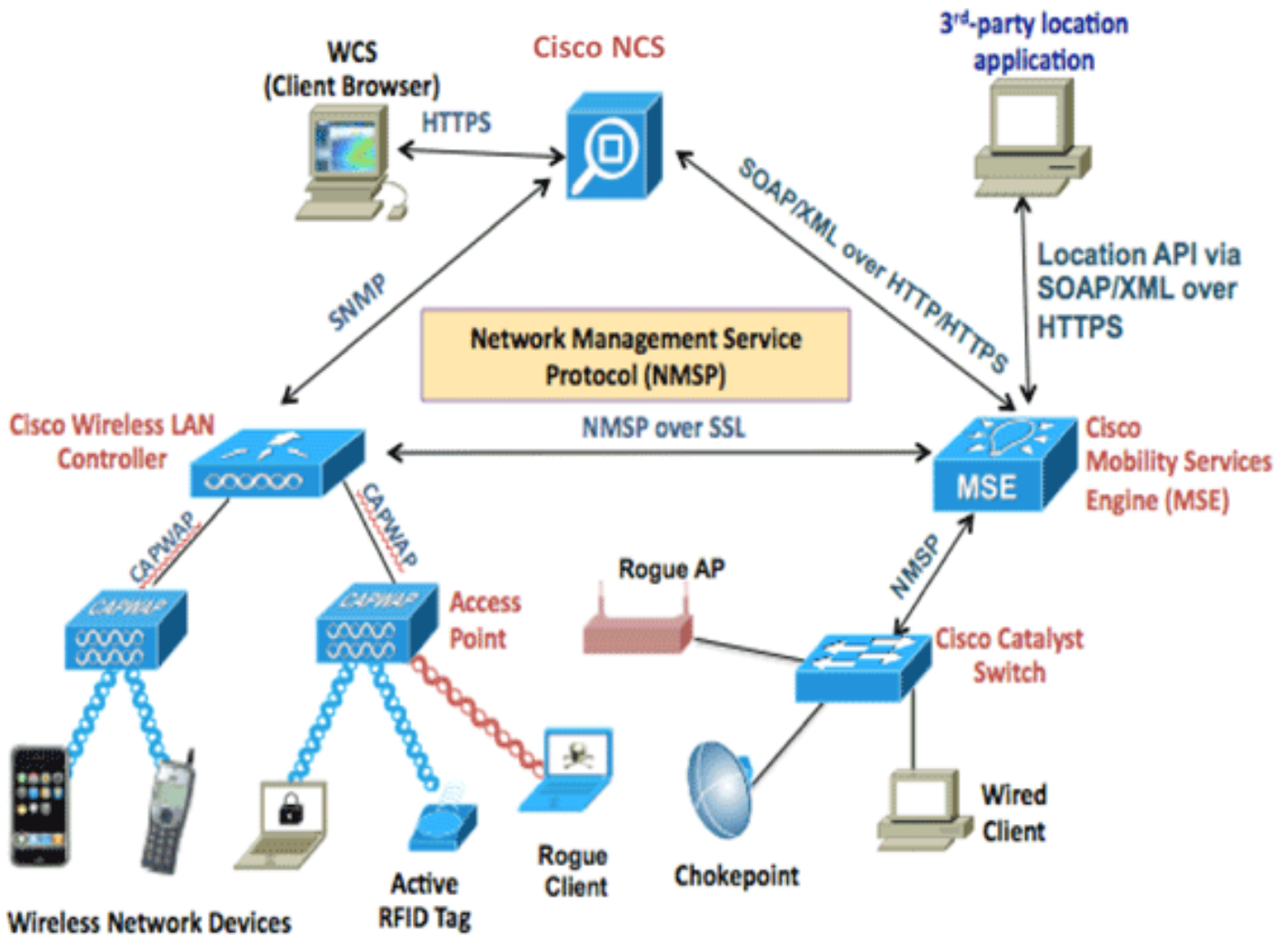
-MSE kommuniziert mithilfe des NMSP-Protokolls mit dem Wireless LAN Controller (WLC) (nachdem ihm dieser durch Prime zugewiesen wurde). Dies gibt im Wesentlichen Informationen über die empfangene Signalstärke (Received Signal Strength, RSSI) an, die pro APs für verbundene Clients empfangen wird, sodass die MSE ihren Standort berechnen kann.

Grundlegende Schritte hierfür:

Zuerst müssen Sie eine Karte für die Prime-Infrastruktur (PI) definieren, den Abdeckungsbereich auf dieser Karte festlegen und die APs platzieren.

Wenn Sie MSE zu prime hinzufügen, wählen Sie CAS-Service aus.

Wenn MSE hinzugefügt wurde, wählen Sie im Prime Sync Services aus, prüfen Sie Ihren WLC/und weisen Sie diese der MSE zu.



Vor der Integration von MSE in die ISE muss die MSE betriebsbereit sein, d. h.:

1. MSE muss der Prime-Infrastruktur hinzugefügt und Services synchronisiert werden
2. Der CAS-Dienst muss aktiviert und die Wireless-Client-Verfolgung aktiviert werden.
3. Karten müssen in Prime konfiguriert werden.
4. NMSP sollte zwischen MSE und WLCs erfolgreich sein ("show nmosp status" in der WLC-Befehlszeile).

In dieser Konfiguration gibt es nur ein Gebäude mit zwei Stockwerken:

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	✓

Verwendete Komponenten

- MSE Version 8.0.110
- ISE Version 2.0

Integration von MSE mit ISE

Gehen Sie zu Netzwerkressourcen, Standortdienste, und klicken Sie auf Hinzufügen, um MSE hinzuzufügen.

Die Parameter sind selbsterklärend, und Sie können die Verbindung testen und auch die Suche nach dem Clientstandort anhand der MAC-Adresse durchführen:

[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

Als Nächstes gehen Sie zur Verzeichnisstruktur und klicken auf Update abrufen. Auf diese Weise kann die ISE Gebäude und Stockwerke von der MSE abrufen und diese in der ISE bereitstellen, ähnlich wie beim Hinzufügen von AD-Gruppen.

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	🔗

Einrichten der Autorisierung

Die Attribute MSE:Map Location können jetzt in Autorisierungsrichtlinien verwendet werden.

Konfigurieren Sie die beiden folgenden Regeln:

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

Benutzer in Floor1 sollten sich authentifizieren können.

In den Authentifizierungsdetails sehen wir das richtige Profil sowie das MAP Location-Attribut.

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

Wenn der Endpunkt mit der oben beschriebenen Konfiguration von einer Zone in eine andere verschoben wird, wird er nicht deauthentifiziert. Wenn Sie die Benutzerbewegung nachverfolgen und eine CoA senden möchten, wenn sich die Autorisierung ändert, können Sie die Verfolgungsoption im Autorisierungsprofil aktivieren. Das Autorisierungsprofil überprüft alle 5 Minuten, ob sich der Standort ändert. Beachten Sie, dass dies den normalen schnellen Roaming-Betrieb stören kann.

Authorization Profile


* Name

Description

* Access Type

Network Device Profile  

Service Template

Track Movement 

Fehlerbehebung

Für diese Funktion ist die ISE-Konfiguration einfach. Die meisten Probleme können jedoch auftreten, wenn die MSE das Gerät nicht finden kann.

Es müssen einige Punkte überprüft werden, um sicherzustellen, dass die MSE korrekt eingerichtet ist:

1- Vergewissern Sie sich, dass der WLC, an den der Benutzer angeschlossen ist, über eine gültige NMSP-Verbindung zur MSE ISE verfügt, in Folgendes integriert ist:

```
(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
```

Falls nicht, hilft Ihnen dieses Dokument

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

2 - Überprüfen, ob die MSE Geräte verfolgen kann

```
[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