

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования и топология решения](#)

[Используемые компоненты](#)

[Интеграция MSE с ISE](#)

[Устанавливание авторизации](#)

[Устранение неисправностей](#)

[Связанные обсуждения Сообщества Cisco Support](#)

Введение

Эта статья продемонстрирует, как интегрировать MSE (Механизм Сервиса мобильности) с платформой Identity Services Engine (ISE) для Основанной на местоположении авторизации. Цель состоит в том, чтобы позволить или запретить доступ к беспроводному устройству на основе их физического размещения.

Предварительные условия

Требования и топология решения

В то время как MSE Configuraiton вне области этого документа, вот общее представление решения:

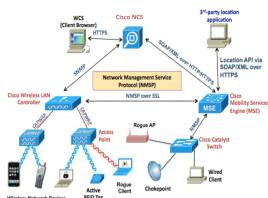
- MSE управляет Главная Инфраструктура (раньше NCS) для конфигурации, создания карт и присвоения WLC
- MSE связывается с Контроллером беспроводной локальной сети (WLC) (после того, чтобы быть назначенным на него Главным) использующий Протокол NMSP. Это в основном дает информацию о Силе Полученного сигнала (RSSI), полученный на AP для подключенных клиентов, который позволяет MSE calculate их местоположение.

Основные шаги, чтобы сделать это:

Сначала необходимо определить карту на Главной инфраструктуре (PI), установить зону уверенного приема на этой карте и разместить AP.

Когда вы добавляете MSE к началу, выбираете сервис CAS.

Как только MSE добавлен в начале, выберите синхронизирующие сервисы и проверьте свой WLC / и карты для присвоения их на MSE.



До интегрируют MSE с ISE, MSE должен быть в порядке, который означает:

1. MSE должен быть добавлен к Главной Инфраструктуре, и сервисы синхронизировались
2. Сервис CAS должен быть включен и Беспроводной клиент, отслеживающий потребности, которые будут включены
3. Карты должны быть настроены в Главном
4. NMSP Должен быть успешным между MSE и WLC ("show nmosp status" на командной строке WLC)

В этой настройке будет только одно Здание с 2 этажами:

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

Используемые компоненты

- Версия 8.0.110 MSE
- Версия 2.0 ISE

Интеграция MSE с ISE

Перейдите к Сетевым ресурсам, Службам определения местоположения, и щелчок добавляет для добавления MSE.

Параметры сам объяснительные, и вы можете тестовое подключение, и также клиентский поиск местоположения мак адресом:

[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

Следующая вещь сделать, состоит в том, чтобы перейти к дереву Местоположения и нажать Get Update. Это позволит ISE выбирать Здания и Пол от MSE, и делать их доступными в ISE, Подобном тому, когда вы добавите AD Groups.

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.

[Get Update](#) Update tree from location servers

[Save](#) [Reset](#)

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

Установка авторизации

Атрибуты Местоположение MSE:Map могут теперь использоваться в политике авторизации.

Настройте 2 ниже правил:

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	Edit
<input checked="" type="checkbox"/>	Wireless	if Wireless_802.1X	then DenyAccess	Edit

Пользователи в Floor1 должны быть в состоянии аутентифицироваться.

Мы видим в подробных данных аутентификации корректный профиль, а также атрибут Местоположения MAP

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

С вышеупомянутой конфигурацией, если оконечная точка перемещается от одной зоны до

другого, это не будет deauthenticated. Если вы хотите отследить пользовательское перемещение и передать CoA, если изменение Авторизации, можно включить опцию отслеживания в профиле авторизации, который проверит для местоположения, изменяющегося каждые 5 минут. Обратите внимание на то, что это может иметь отрицательные последствия для обычных быстрых операций роуминга.

Authorization Profiles > New Authorization Profile




Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Устранение неисправностей

Для этой функции конфигурация ISE является прямой, однако, большинство проблем могло бы произойти, если MSE не в состоянии определить местоположение устройства.

Несколькими вещами проверить для проверки MSE является настройка должным образом:

1-Удостоверяются, что с WLC, где у связанного пользователя есть допустимое соединение NMSP с ISE MSE, интегрируют:

В противном случае этот документ поможет

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

2-Проверок, если MSE в состоянии отследить устройства