Mobility Services Engine（MSE）および Identity Services Engine（ISE）ISE 2.0 の場所に基づく認証

目次

概要

この記事では、ロケーション ベースの認証を実行するための Identity Services Engine（ISE）との MSE（モビリティ・ サービス・ エンジン）の統合方法について説明します。 目的は、物理的な場所に基づいてワイヤレス デバイスへのアクセスを許可または拒否できるようにすることです。

前提条件

ソリューションの要件とトポロジ

MSE の設定は本書で扱う範囲ではありませんが、ソリューションの一般概念を次に示します。

- MSE は Prime Infrastructure（以前の NCS）により設定、マップの作成、および WLC の割り当てが管理されています。

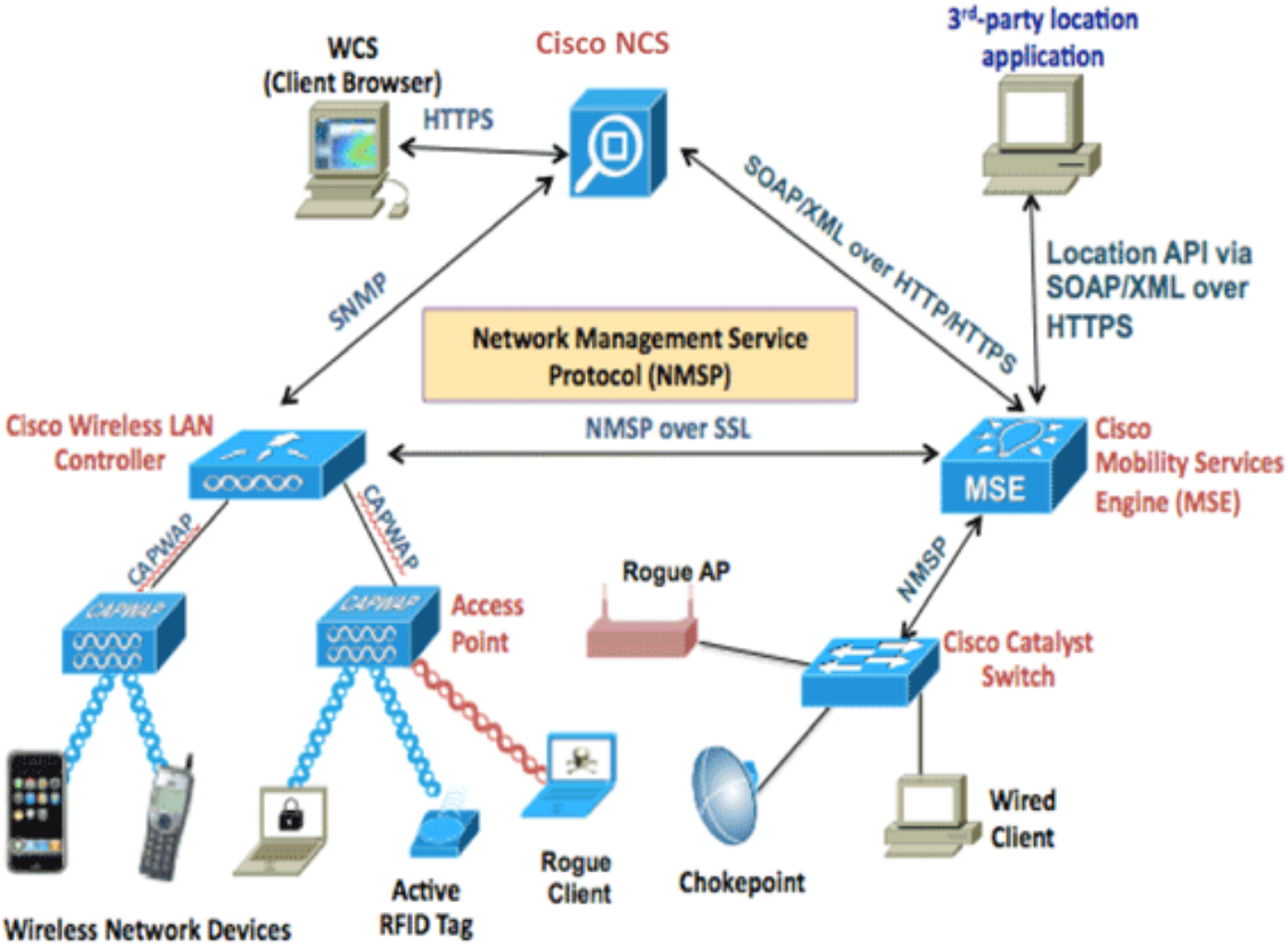
- MSE は NMSP プロトコルを使用して（Prime によって割り当てられた後）ワイヤレス LAN コントローラ（WLC）と通信します。 これは基本的に、接続されたクライアントについて AP ごとに受信した受信信号強度（RSSI）に関する情報を提供して、MSE が場所を計算できるようにしています。

これを実行するための基本的なステップは次のとおりです。

まず、Prime Infrastructure（PI）にマップを定義し、このマップのカバレッジ エリアを設定して AP を配置する必要があります。

Prime に MSE を追加する場合は CAS サービスを選択します。

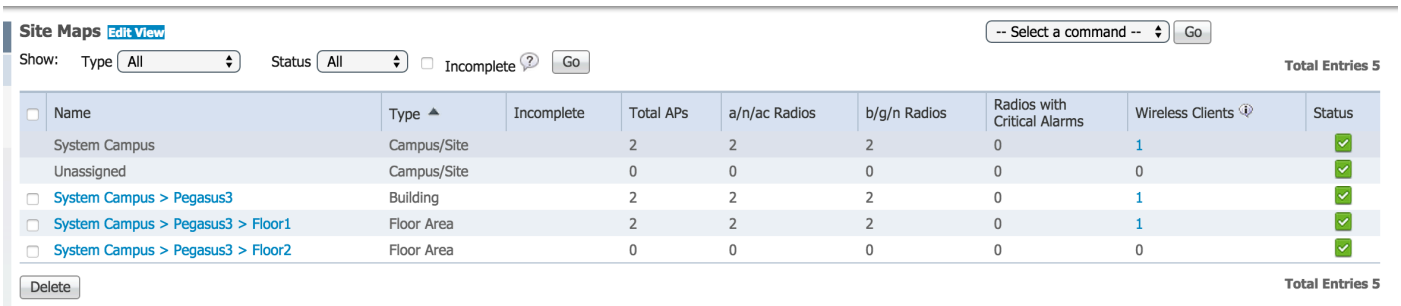
MSE が Prime に追加されたら、同期サービスを選択し、WLC とマップを確認して MSE にそれらを割り当てます。



ISE と MSE を統合する前に、MSE は起動し、実行している必要があります。つまり、次のことが必要です。

1. MSE が Prime Infrastructure に追加され、サービスが同期されている必要があります。
2. CAS サービスが有効になっている必要があり、また、ワイヤレス クライアントのトラッキングが有効になっている必要があります。
3. マップが Prime で設定されている必要があります。
4. NMSP が MSE と WLC 間で正常に動作している必要があります（WLC コマンド ラインで「show nmsp status」により確認できます）。

この設定では、2 階建ての建物 1 棟のみとなります。



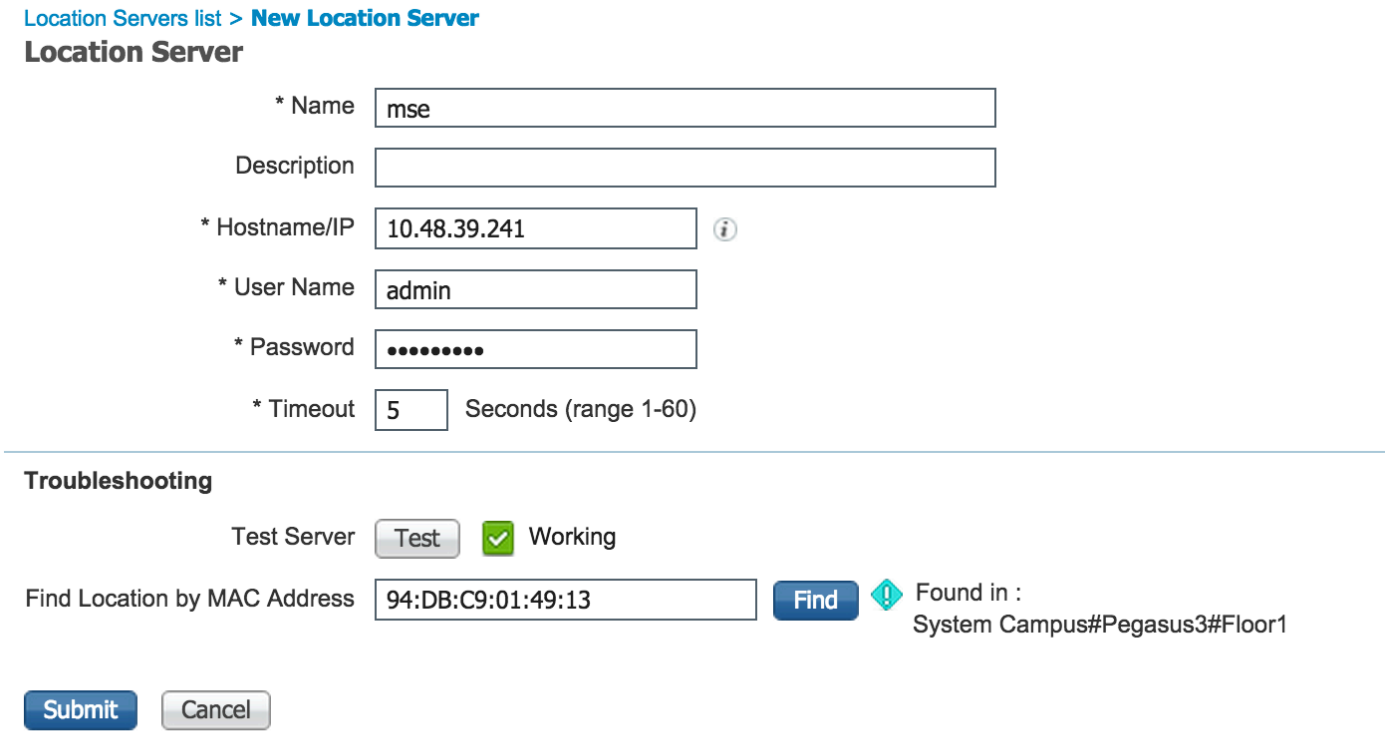
使用されているコンポーネント

- MSE バージョン 8.0.110
- ISE バージョン 2.0

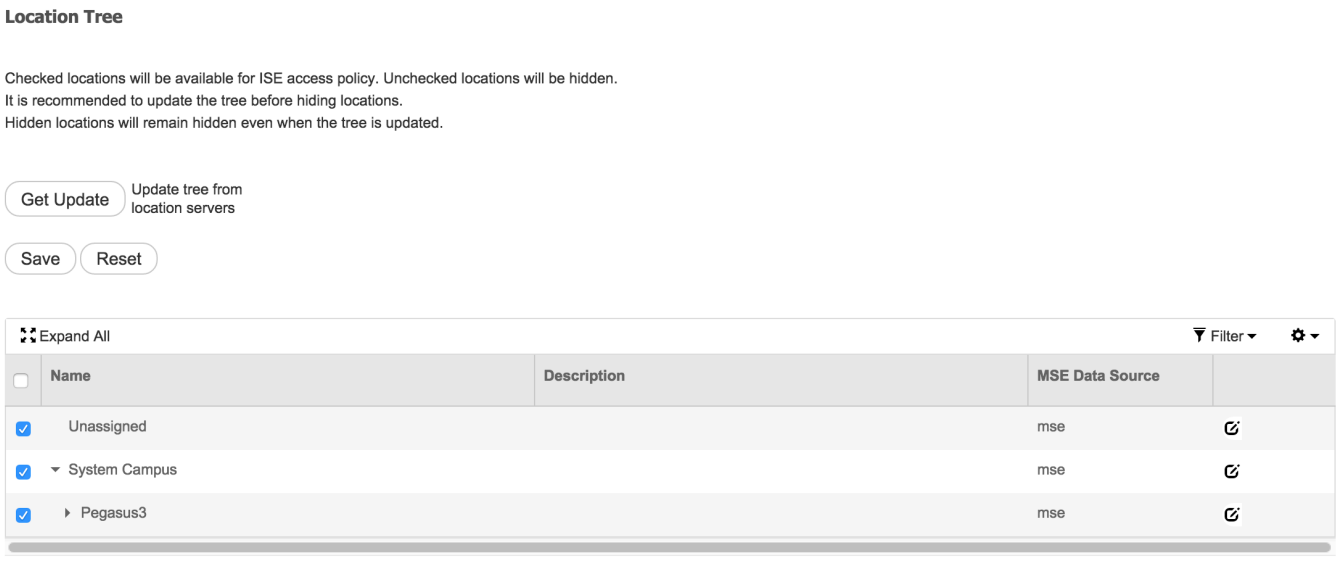
ISE との MSE の統合

[Network Resources] > [Location Services] に移動し、[Add] をクリックして MSE を追加します。

パラメータは一目瞭然であるため説明する必要はありません。また、接続のテストや、MAC アドレスを使用したクライアント ロケーションのルックアップを行うことができます。



次に、[Location] ツリーに移動し、[Get Update] をクリックする必要があります。 これにより、ISE は MSE から建物と階を取得し、それらを ISE で使用できるようにします。これは AD グループを追加する場合と似ています。



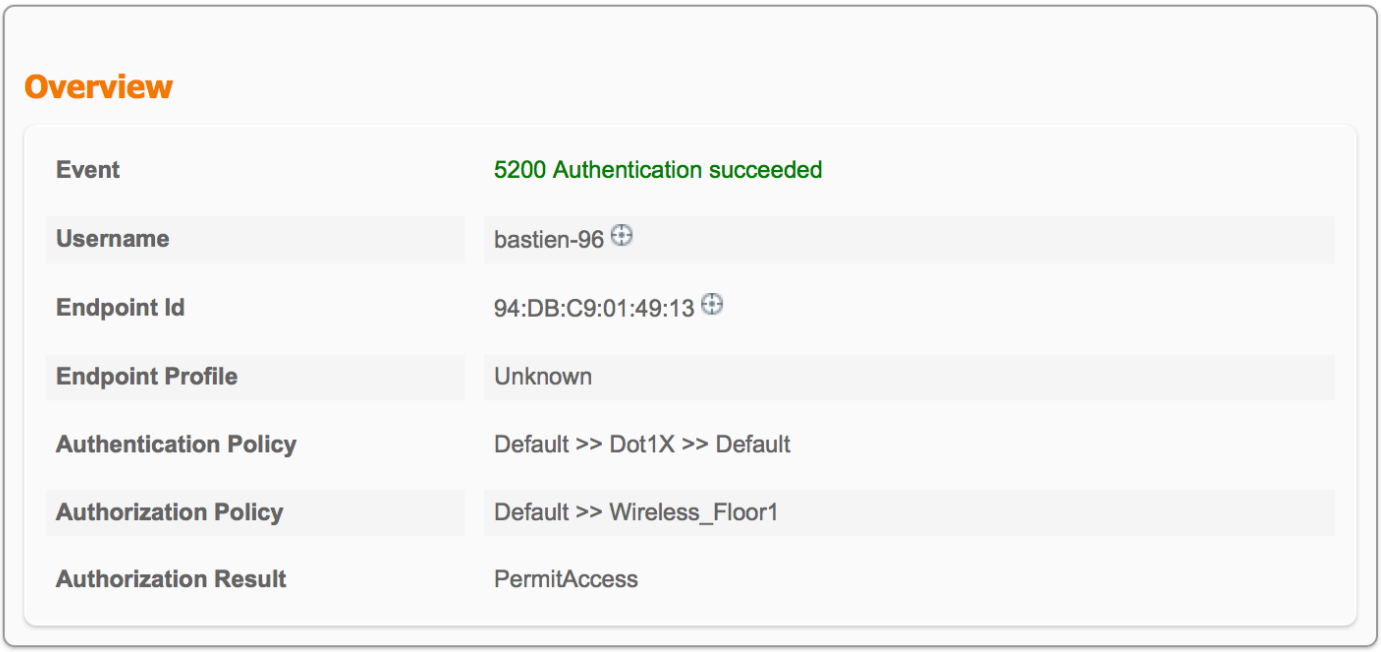
認証の設定

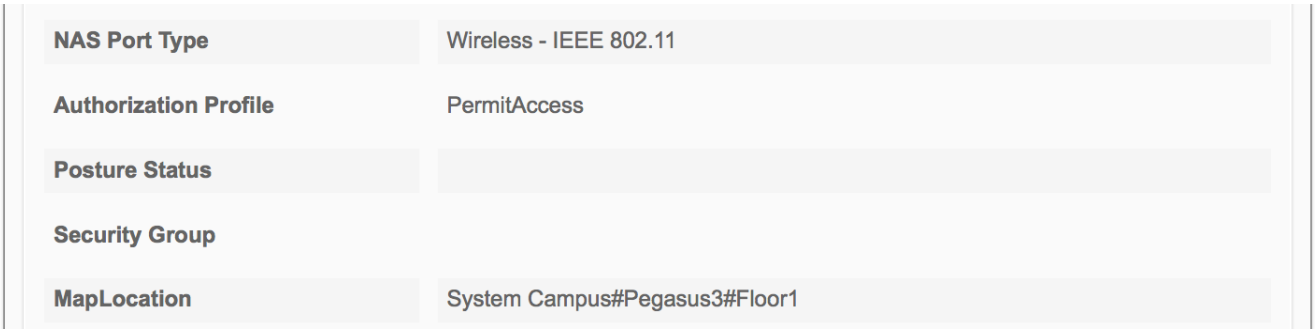
属性 MSE： 認証ポリシーにマップ ロケーションを使用できるようになりました。

次の 2 つのルールを設定します。

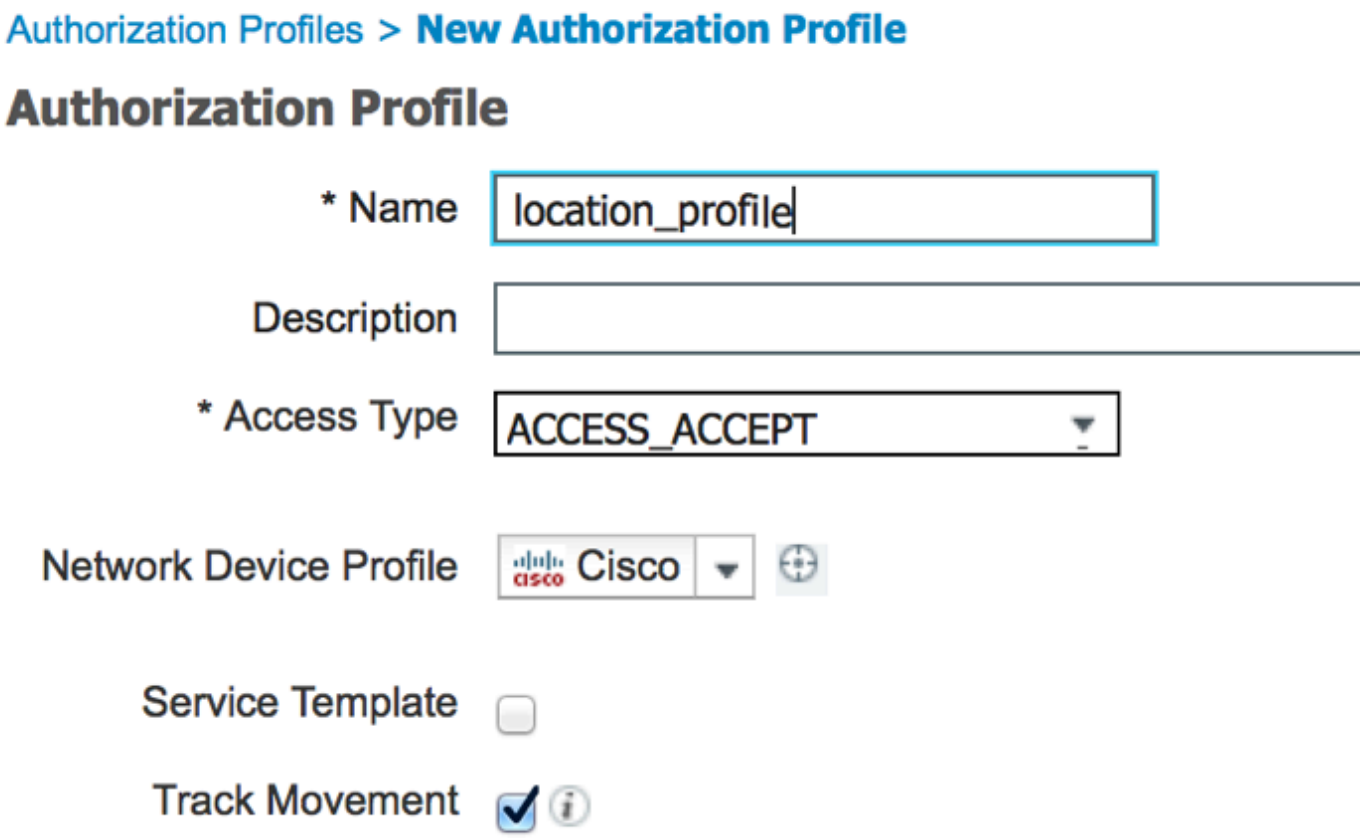
Floor1 のユーザは認証を実行できる必要があります。

認証の詳細には、[MAP Location] の属性とともに正しいプロファイルが表示されます。





上記の設定では、エンドポイントがあるゾーンから別のゾーンに移動した場合、認証は解除されません。 ユーザの移動を追跡し、認証が変更された場合に CoA を送信する場合は、認証プロファイルでトラッキング オプションを有効にすると、5 分おきにロケーションの変化を確認します。 これは、通常の高速ローミング操作に悪影響を及ぼす可能性があります。



トラブルシューティング

この機能の場合、ISE の設定は簡単ですが、問題のほとんどは MSE でデバイスを見つけられない場合に発生しているようです。

MSE が正しく設定されていることを確認するため、いくつかのことをチェックします。

1- ISE と統合されている MSE への有効な NMSP 接続が ユーザが接続されている WLC にあることを確認します。

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

そうでない場合は、次のドキュメントを参照してください。

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

2- MSE がデバイスを追跡できるかどうかを確認します。

```
[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