# WLC を使用した CMX 接続のトラブルシューティング

## 目次



## 概要

この資料は接続されたモービル エクスペリエンスでワイヤレス LAN コントローラ（WLC 統一され、コンバージする）の接続上の問題を、解決するために方式を記述したものです（CMX）。

## 前提条件

### 要件

Cisco はコンフィギュレーションプロセスおよび配置ガイドのナレッジがあることを推奨します。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- CMX 10.2.3-34
- WLC 2504/8.2.141.0
- バーチャル WLC 8.3.102.0
- コンバージしたアクセス WLC C3650-24TS/03.06.05E

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

# 背景説明

この技術情報は WLC が CMX に出て来ます状況に追加される、または WLC は無効か非アクティブように失敗するか焦点を合わせ。 基本的にはネットワーク モビリティ サービス プロトコル（NMSP）トンネルが起動しないまたは NMSP 通信非アクティブようにとき現れます。

WLC と CMX 間の通信は NMSP の使用と起こります。

NMSP は TCPポート 16113 で WLC の方のおよび基づいてモビリティ サービス エンジン（MSE）/CMX とコントローラ間の証明書（キー ハッシュ）交換を必要とする TLS に動作します。 WLC と CMX 間の Transport Layer Security/Secure Sockets Layer（TLS/SSL）トンネルはコントローラによって開始されます。

# 可能性のある 障害シナリオのトラブルシューティング

開始するべき最初の場所はこのコマンド 出力とあります。

CMX コマンド・ラインにログイン し、コマンド **cmxctl 構成コントローラを示します**実行して下さい。

```
** To troubleshoot INACTIVE/INVALID controllers verify that:
the controller is reachable
the controller's time is same or ahead of MSE time
the SNMP port(161) is open on the controller
the NMSP port(16113) is open on the controller
the controller version is correct
the correct key hash is pushed across to the controller by referring the following:
+------------------+--------------------------------------------------------------------------+
| MAC Address      | 00:50:56:99:47:61                                                        |
|
+------------------+--------------------------------------------------------------------------+
| SHA1 Key         | f216b284ba16ac827313ea2aa5f4dec1817f1069                                 |
+------------------+--------------------------------------------------------------------------+
| SHA2 Key         | 2e359bd5e83f32c230b03ed8172b33652ce96c978e2733a742aaa3d47a653a02         |
+------------------+--------------------------------------------------------------------------+
```

また、CMX MAC アドレスおよびハッシュ キーは出力から見つけることができます:

非アクティブ少なくとも 1 あるとき出力はチェックリストを示したものです:

1. 到達可能性
2. 時刻
3. 簡易ネットワーク管理プロトコル（SNMP） 161 ポート
4. NMSP 16113 ポート
5. バージョン
6. コントローラで押される正しいハッシュ

## 到達可能性を確認して下さい

到達可能性をコントローラにチェックするために、WLC に ping をから CMX 実行して下さい。

## 時刻の同期

最良の方法は同じ Network Time Protocol （NTP）サーバを両方の CMX および WLC を指すことです。

統一された WLC （AireOS）では、これはコマンドで設定されます:

```
config time ntp server <index> <IP address of NTP>
```

コンバージしたアクセス IOS XE では、コマンドを実行して下さい:

```
(config)#ntp server <IP address of NTP>
```

NTP サーバの IP アドレスをの変更するため CMX:

ステップ 1.コマンド・ラインに **cmxadmin** としてログイン して下さい、ルート ユーザ **<su root>** に切り替えて下さい。

ステップ 2.コマンド **cmxctl 停止**とのすべての CMX サービスを**- a** 停止して下さい。

ステップ 3.コマンド **サービス ntpd 停止**が付いている NTP deamon を停止して下さい。

ステップ 4 すべてのプロセスが停止したら、コマンド **VI /etc/ntp.conf を**実行して下さい。 挿入モード**に切り替え、ESC を**クリックし、入力するために IP アドレスを変更するためにそして『i』 をクリック して下さい**:** 設定を保存する **wq**。

ステップ 5 パラメータが変更されたらコマンド **サービス ntpd 開始を**実行して下さい。

ステップ 6 NTP サーバがコマンド **ntpdate** と到達可能**- d < NTP server> の IP アドレス**であるかどうか確認して下さい。

ステップ 7.少なくとも 5 分、なぜなら NTP サービスがコマンド **ntpstat** と再起動し、確認するようにして下さい。

ステップ 8 NTP サーバが CMX と同期されたら、CMX サービスを再開し、**cmxadmin** ユーザに戻って切り替えるためにコマンド **cmxctl 再起動を**実行して下さい。

## SNMP 到達可能性

CMX が WLC に SNMP にアクセスできるかどうか確認するためにコマンドをの CMX 実行して下さい:

```
Snmpwalk -c <name of community> -v 2c <IP address of WLC>.
```

このコマンドは WLC がデフォルト SNMP バージョン 2 を実行することを仮定します。 バージョン 3 では、コマンド一見のような:

```
snmpwalk -v3  -l authPriv -u <snmpadmin> -a SHA -A <password>  -x AES -X <PRIvPassWord>
127.0.0.1:161 system
```

SNMP がイネーブルになっているでなければ、またはコミュニティ名間違っていますがありま

タイムアウトがあります。 それが正常である場合、WLC の全 SNMP データベース内容を見ます。

## NMSP 到達可能性

CMX が WLC に NMSP にアクセスできるかどうか確認するためにコマンドを実行して下さい:

CMX:

```
 netstat -a | grep 16113
```

WLC:

```
show nmsp status
show nmsp subscription summary
```

## バージョン互換性

最新の資料とバージョン互換性をチェックして下さい。

http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html#pgfId-229490

## コントローラで押される正しいハッシュ

### コントローラ側 AireOS のハッシュ

通常、wlc は自動的に sha2 およびユーザ名を追加します。 キーはコマンドで**示します auth リストを**確認することができます。

```
(Cisco Controller) >show auth-list

Authorize MIC APs against Auth-list or AAA ..... disabled
Authorize LSC APs against Auth-List ..... disabled
APs Allowed to Join
 AP with Manufacturing Installed Certificate.... yes
 AP with Self-Signed Certificate..... no
 AP with Locally Significant Certificate..... no

Mac Addr                  Cert Type    Key Hash
-----------------------   ----------   ----------------------------------------
00:50:56:99:6a:32     LBS-SSC-SHA256
7aa0d8facc0aa4a5a65b374f7d16972d142f4bb4823d91b7bc143811c7534e32
```

CMX のハッシュ キーおよび MAC アドレスが表にない場合、WLC で手動で付け加えることは可能性のあるです:

```
config auth-list add sha256-lbs-ssc <mac addr of CMX> <sha2key>
```

### コントローラ側 IOS XE のハッシュはアクセス コンバージしました

NGWC コントローラでは、次の通りコマンドを手動で実行する必要があります:

```
nmsp enable
username<cmx mac-addr> mac aaa attribute list <list name>
aaa attribute list CMX
attribute type password <CMX sha2 key >
```

**注:** cmx MAC Addr は句読点コロンなしで追加する必要があります ( : )

ハッシュ キーを解決するため:

```
 Switch#show trace messages nmsp connection

[12/19/16 14:57:50.389 UTC 4dd 8729] sslConnectionInit: SSL_do_handshake for conn ssl 587c85e0,
conn state: INIT, SSL state: HANDSHAKING
[12/19/16 14:57:50.395 UTC 4de 8729] Peer certificate Validation Done for conn ssl 587c85e0,
calling authlist..
[12/19/16 14:57:50.396 UTC 4df 8729] Client Cert Hash Key
[2e359bd5e83f32c230b03ed8172b33652ce96c978e2733a742aaa3d47a653a02]
[12/19/16 14:57:50.397 UTC 4e0 8729] Authlist authentication failed for conn ssl 587c85e0
[12/19/16 14:57:51.396 UTC 4e1 8729] Peer Not Validated against the AuthList
```

それでも問題に直面する場合、ヘルプのための Ciscoサポート フォーラムを参照して下さい。 この技術情報で述べられる出力およびチェックリストは確定的にフォーラムの問題を狭めるのを助けることができますまたは TACサポート要求を開くことができます。