複数のワイヤレスLANコントローラをインポートするためのCMXの設定

内容

はじめに

このドキュメントでは、カンマ区切り値(CSV)ファイルを使用して、ワイヤレスLANコントローラ(WLC)をコネクテッドモバイルエクスペリエンス(CMX)にインポートする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- AireOS WLCの概念と設定
- 9800 WLCの概念と設定
- CMXの概念と設定
- Simple Network Management Protocol(SNMP)の概念と設定
- Network Mobility Services Protocol(NMSP)の概念と設定

使用するコンポーネント

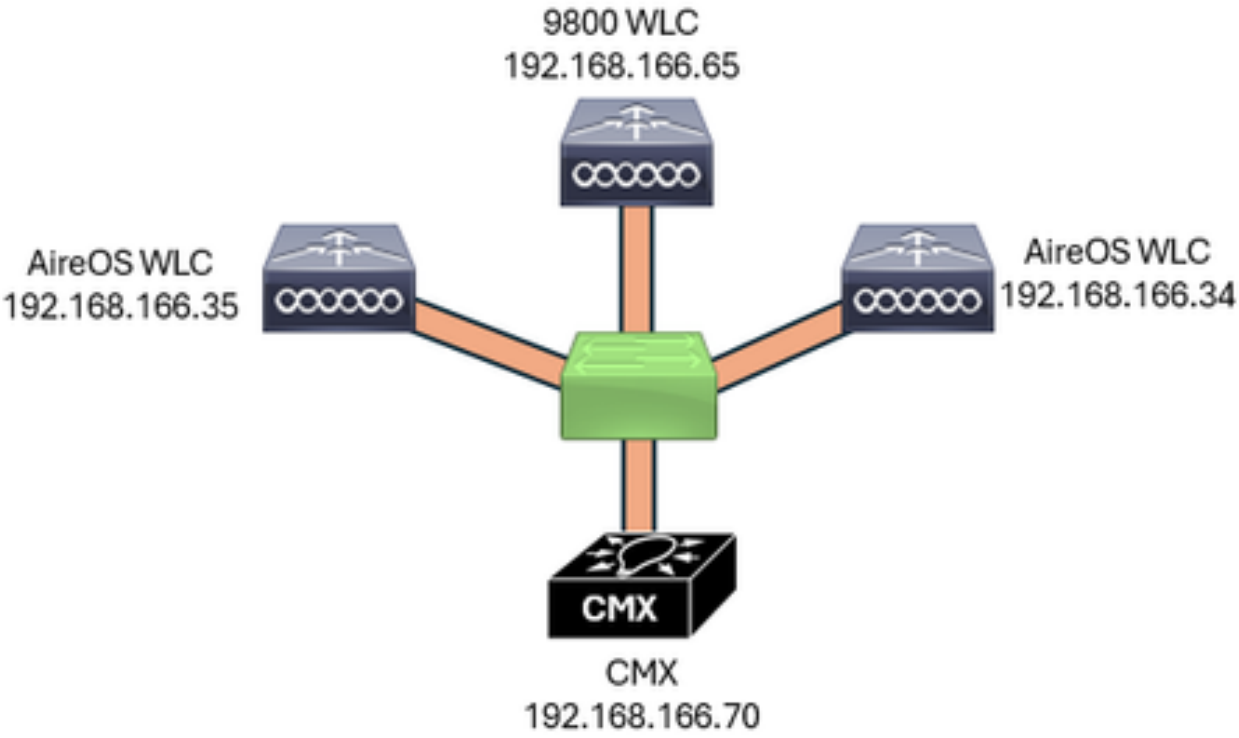
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Catalyst 9800ワイヤレスコントローラシリーズ(Catalyst 9800-CL)、Cisco IOS® XE Cuppertino 17.9.4
- AIR-CTVMワイヤレスコントローラシリーズ（AireOSクラウド）、バージョン8.10.196
- CMX、バージョン10.6.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図



ネットワーク図

コンフィギュレーション

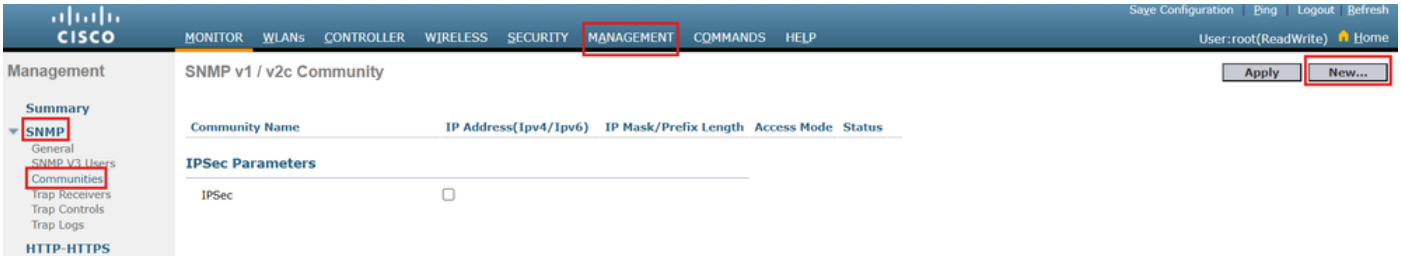
AireOS WLCでのSNMPの設定

CMXはSNMPを介してWLCと通信し、WLCの詳細と情報を収集します。したがって、WLCはSNMPを使用して設定する必要があります。

SNMP バージョン 2

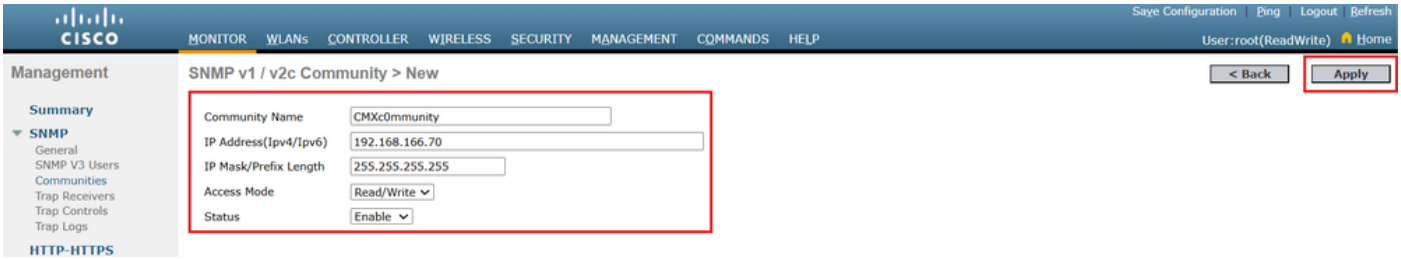
WLC GUI :

図に示すように、Management > SNMP > Communities > Newの順に移動します。

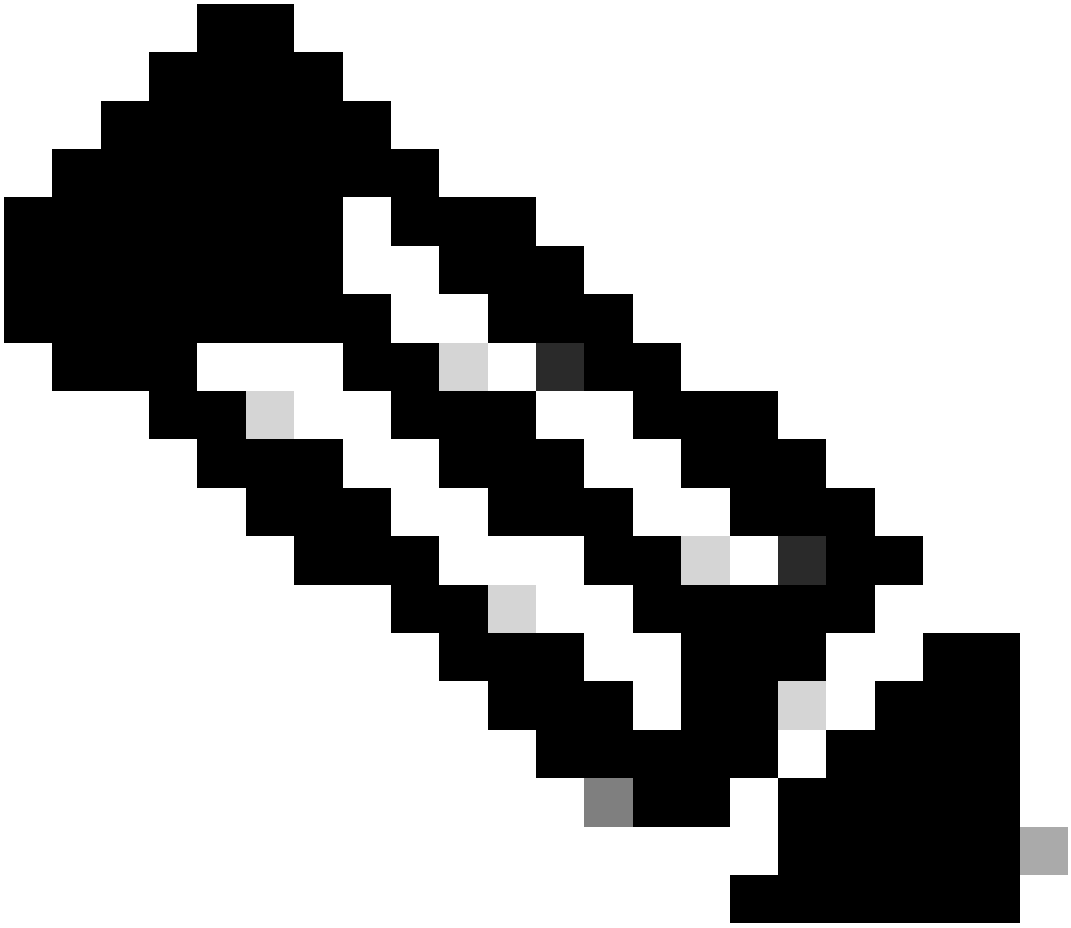


SNMPバージョン2の設定

SNMPの詳細を入力します。



SNMPバージョン2の設定の詳細



注:SNMPアクセスモードはRead/Writeとして設定する必要があります。SNMP Statusを Enableに設定する必要があります。

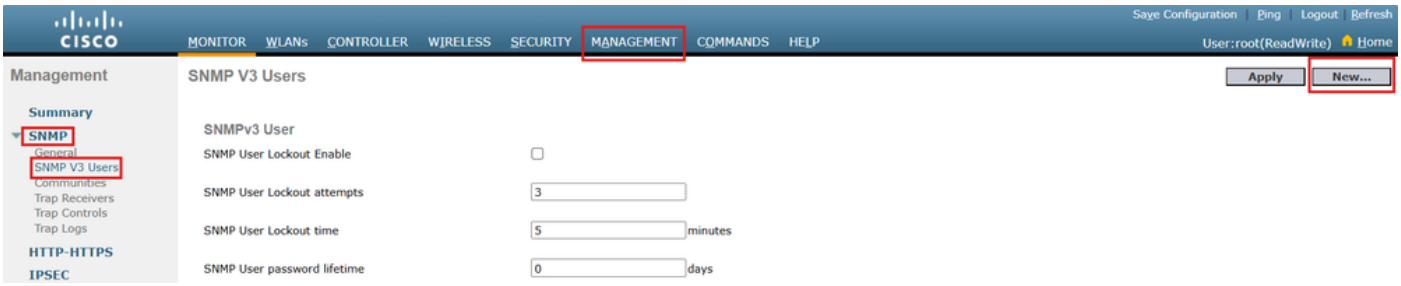
WLC CLI:

```
(Cisco Controller) >config snmp community create CMXcOmmunity
(Cisco Controller) >config snmp community ipaddr 192.168.166.70 255.255.255.255 CMXcOmmunity
(Cisco Controller) >config snmp community accessmode rw CMXcOmmunity
(Cisco Controller) >config snmp community mode enable CMXcOmmunity
```

SNMP バージョン 3

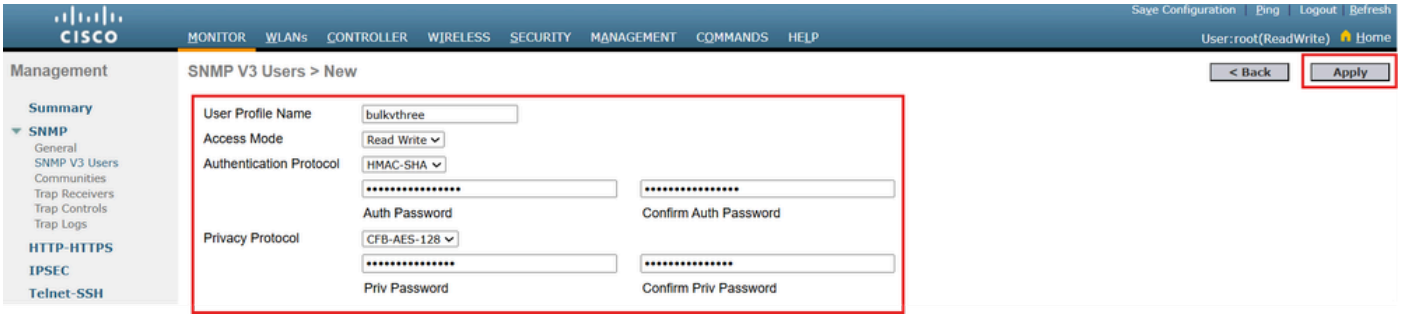
WLC GUI :

図に示すように、Management > SNMP > SNMP V3 Users > Newの順に移動します。

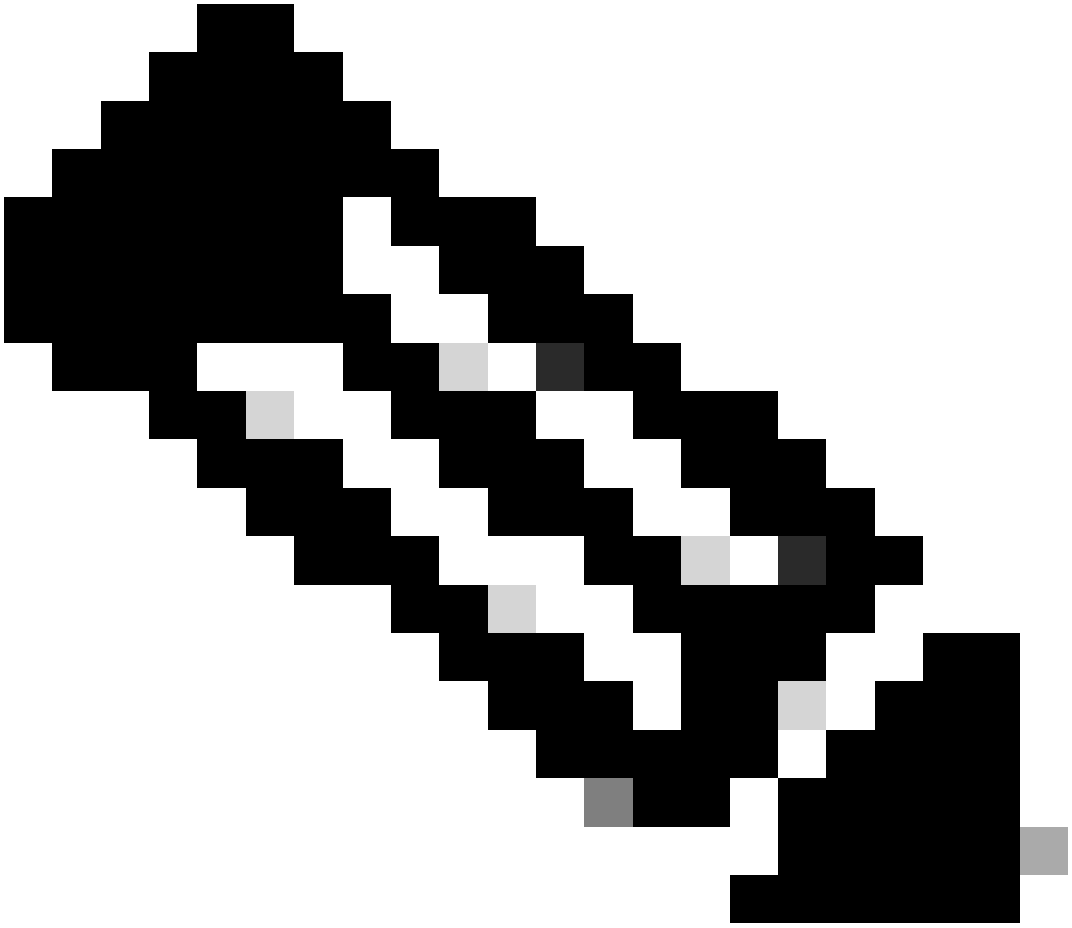


SNMPバージョン3の設定

SNMPの詳細を入力します。



SNMPバージョン3の設定の詳細



注:SNMPアクセスモードはRead/Writeとして設定する必要があります。SNMP認証プロトコルはSHAまたはMD5です。SNMPプライバシープロトコルはAESまたはDESです。

WLC CLI:

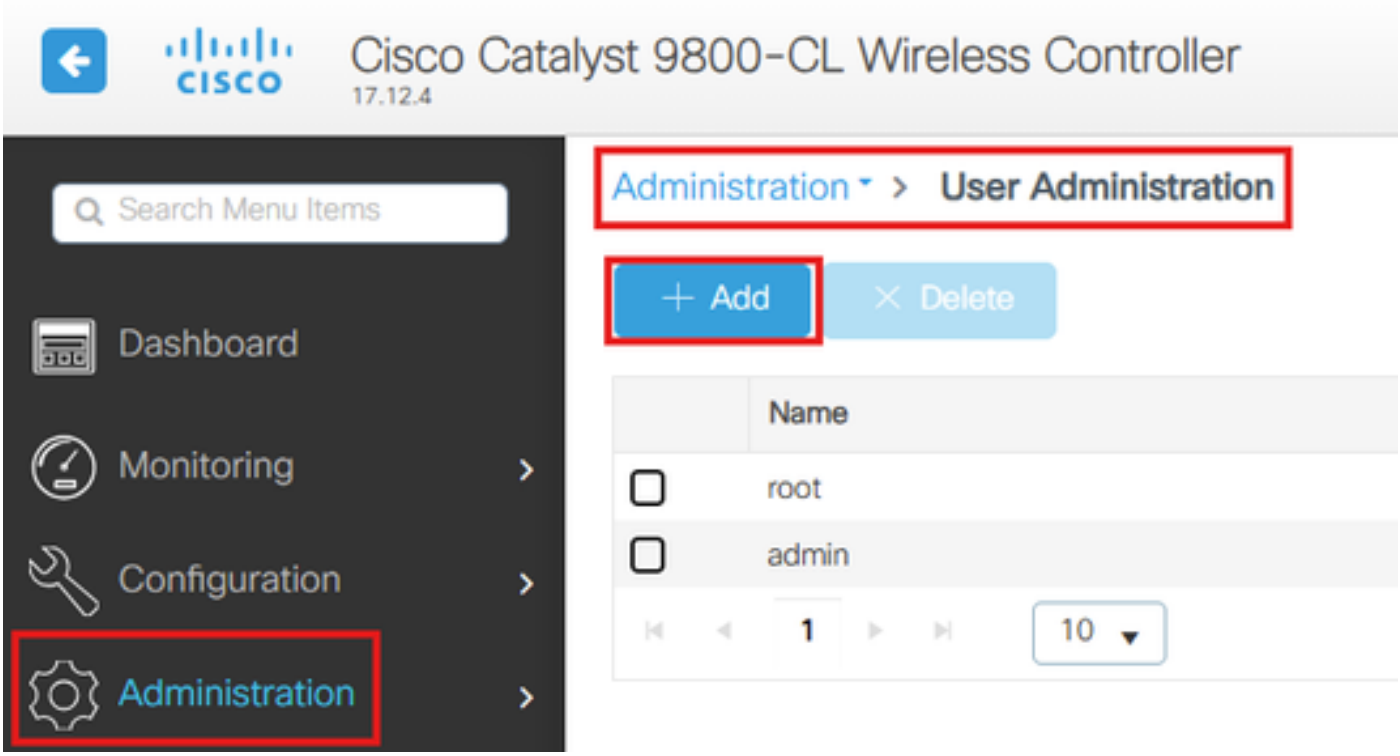
```
(Cisco Controller) >config snmp v3user create bulkvthree rw hmacsha aescfb128 makEsnmpw0rkbulk version3
```

9800 WLC上のSSHアクセス設定

CMXがWLCへのアクセスに使用できるユーザ管理の設定

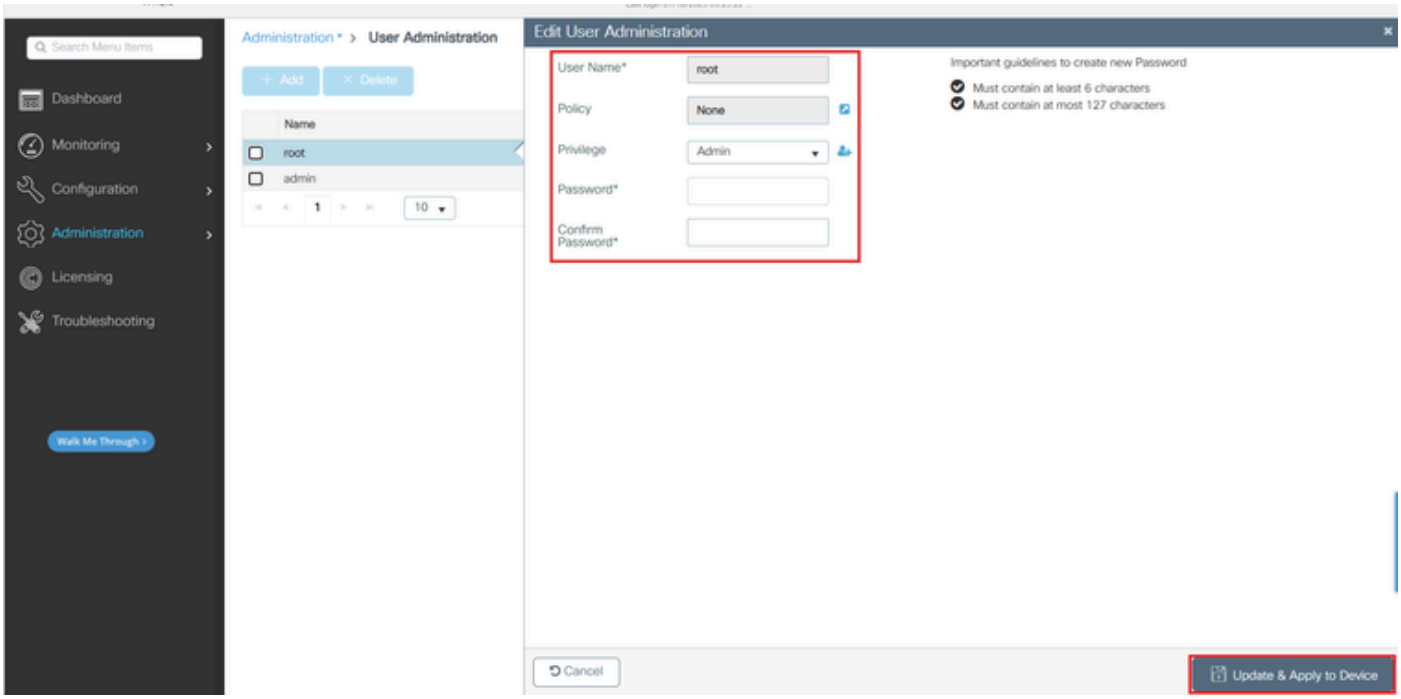
WLC GUI :

図に示すように、Administration > User Administration > Addの順に移動します。



WLCユーザ設定

ユーザの詳細を入力し、Update & Apply to Deviceをクリックします。



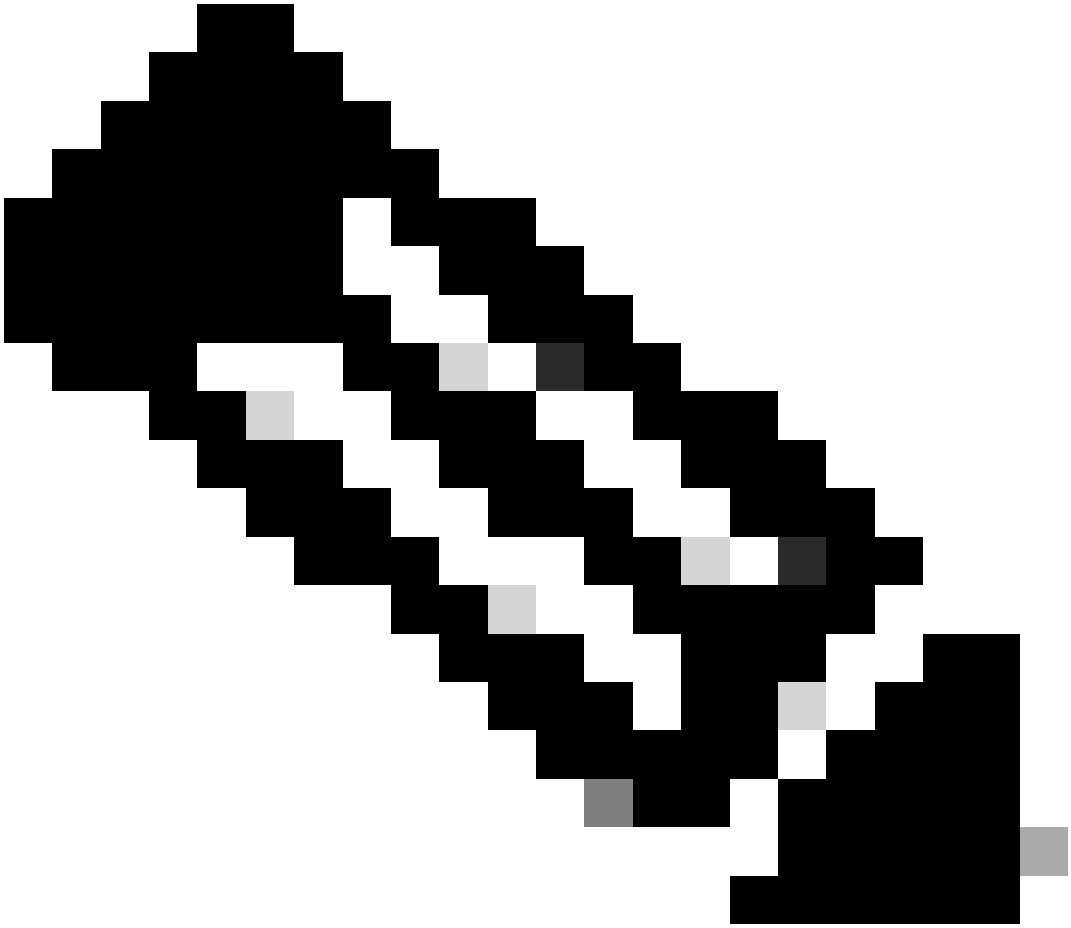
WLCユーザ情報の設定

WLC CLI:

```
#conf t
(config)#username root privilege 15 password 0 RtpW2121!
(config)#end
```

CMXがアクセスに使用できるパスワードを使用して、WLCへの特権アクセスを設定します。この設定は、次のようにCLIを介してのみ実行できます。

```
#conf t
(config)#enable password 0 RtpW2121!
(config)#end
```



注：任意のパスワードのセキュリティレベルを設定します。

TXT工ディタでWLC情報を入力します

CSVファイルはExcelシートで直接作成できますが、ほとんどのネットワーク管理者はメモ帳++またはテキスト工ディタで快適に作業できます。このドキュメントでは、最初にメモ帳++でWLCエントリの作成が行われ、作成されたドキュメントはCSVファイルとして保存されます。

テキストエディタに追加する情報は、WLCのタイプによって異なります。次に例を示します。

AireOS:

- WLC、WLC IPアドレス、WLCバージョン、SNMPバージョン、SNMP情報

SNMP のバージョン:

- SNMP バージョン 2
  - WLC、WLC IPアドレス、WLCバージョン、SNMPバージョン、コミュニティ名
- SNMP バージョン 3
  - WLC、WLC IPアドレス、WLCバージョン、SNMPバージョン、SNMPユーザ名、SNMP認証プロトコル、SNMP認証パスワード、SNMPプライバシープロトコル、SNMPプライバシーパスワード

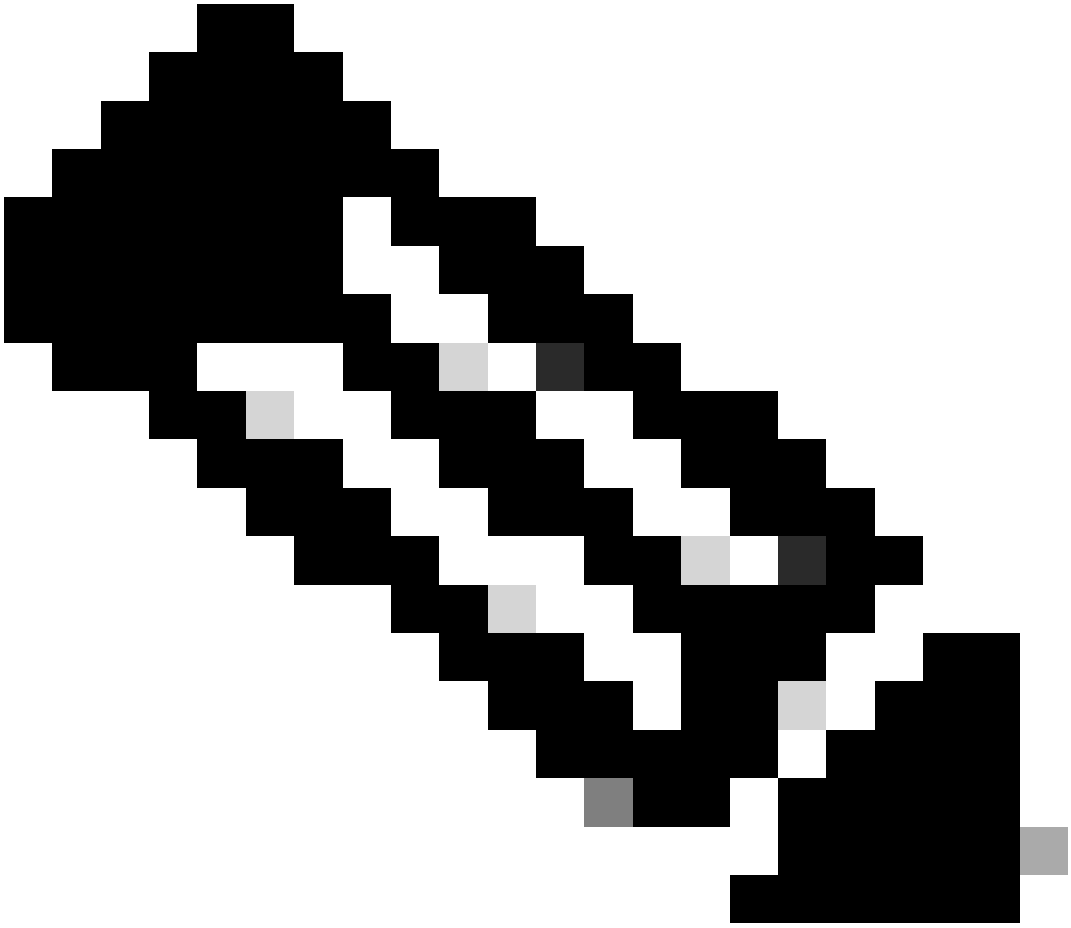
9800 WLC:

- Catalyst(IOS XE)WLC、WLC IPアドレス、WLCバージョン、SSHユーザ名、SSHパスワード、イネーブルパスワード

前述の情報に基づき、このドキュメントでは3台のWLCを使用して、AireOS SNMPバージョン2、SNMPバージョン3、および9800 WLCの設定を例示し、このプロセスで可能なすべての設定を網羅しています。このドキュメントで使用するWLCの設定は次のとおりです。

AireOS:

- SNMP バージョン 2
  - WLC、192.168.166.33、8.10.196.0、v2c、CMXc0mmunity
- SNMP バージョン 3
  - WLC、192.168.166.34、8.10.196.0、v3、bulkvthree、hmacsha、makEsnmpw0rkbulk、aescfb128、version3workinG



注：サポートされる認証タイプはhmacmd5またはhmacshaです。サポートされるプライベートタイプはdesまたはaescfb128です。これらのパラメータでは大文字と小文字が区別されます。

9800 WLC:

- Catalyst(IOS XE)WLC、192.168.166.65、17.09.04、root、RtpW2121!、RtpW2121!

CSVエントリの最初の列では、CMXはWLCタイプがAireOSか9800 WLCかを認識できます。最初の列にWLCと表示されている場合、CMXはそのWLCがAireOSであることを認識しますが、最初の列にCatalyst(IOS XE)と表示されている場合、CMXはそのWLCが9800 WLCであることを認識します。

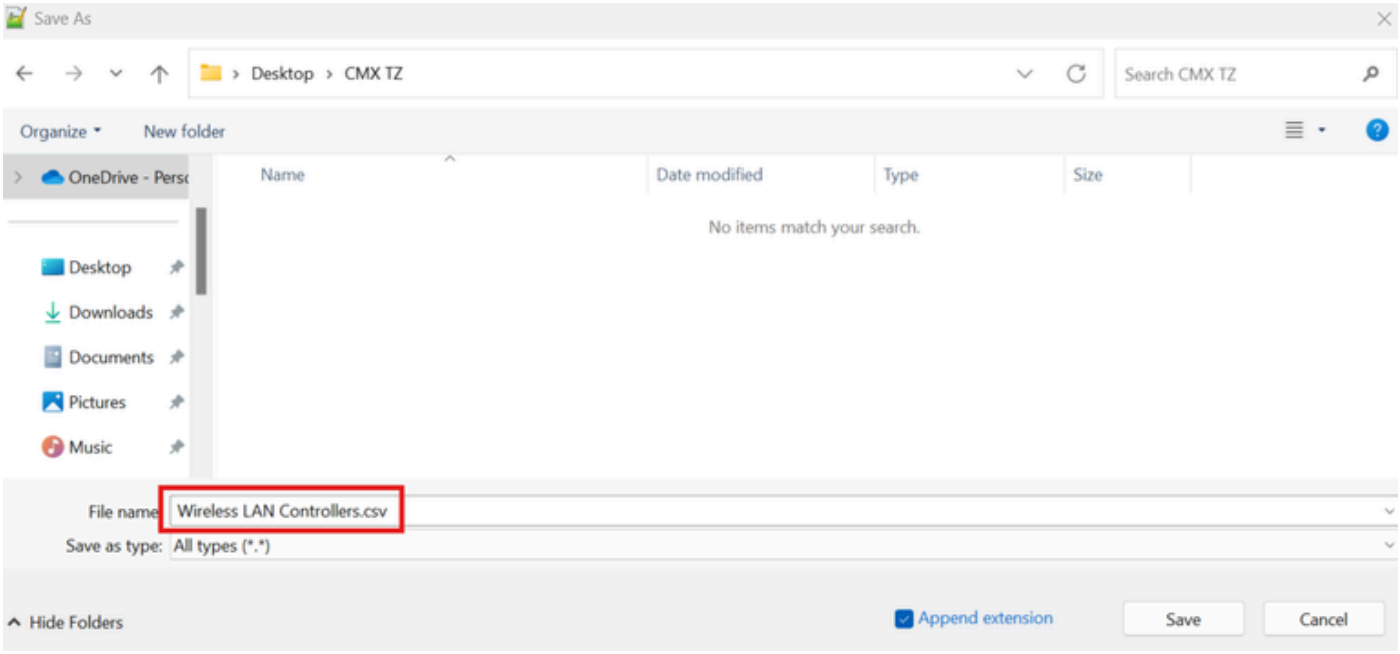
メモ帳++の設定：

Wireless LAN Controllers.txt

```
1  WLC,192.168.166.33,8.10.196.0,v2c,CMXc0mmunity
2  WLC,192.168.166.34,8.10.196.0,v3,bulkvthree,hmacsha,makEsnmpw0rkbulk,aescfb128,version3workinG
3  Catalyst (IOS-XE) WLC,192.168.166.65,17.09.04,root,RtpW2121!,RtpW2121!
```

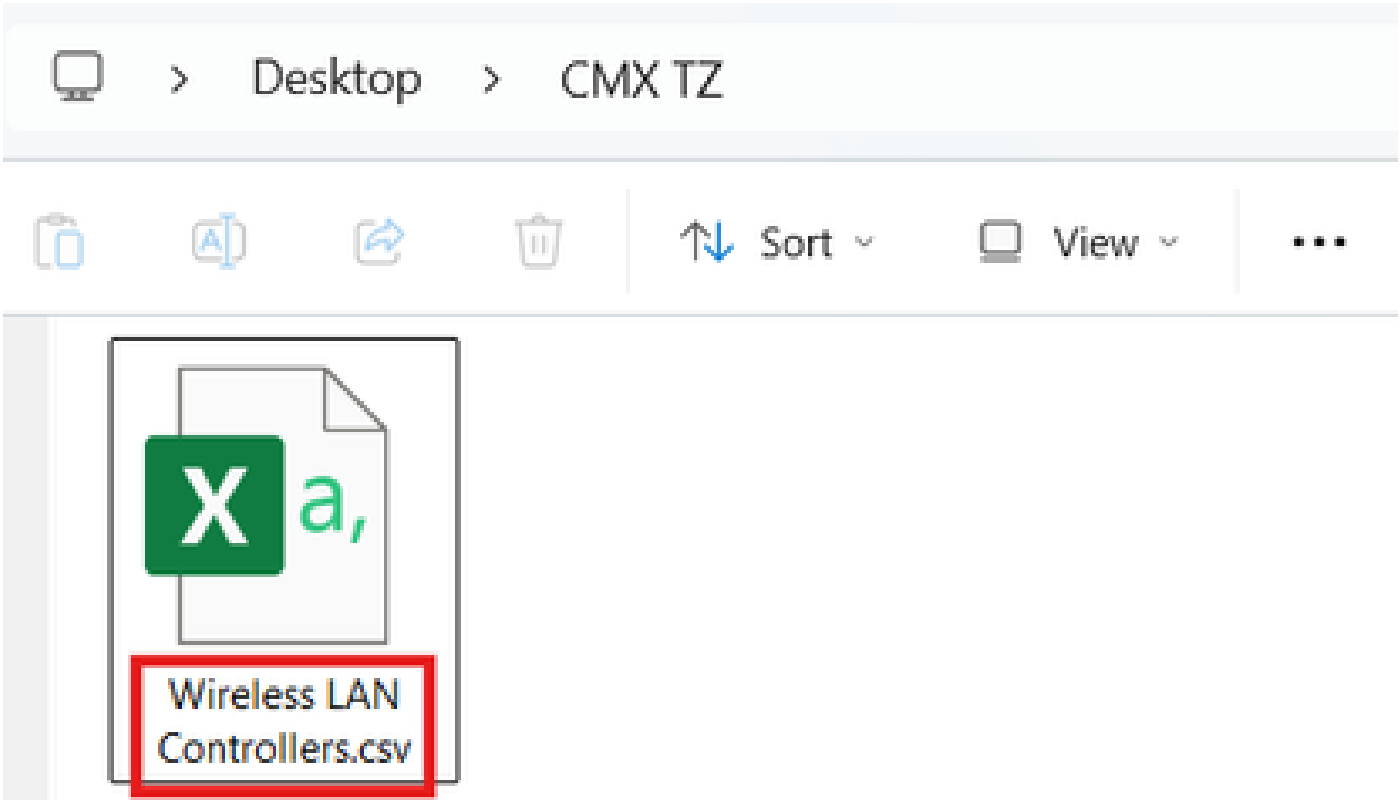
ファイルをCSV形式で保存

ファイルの拡張子が.csvであることを確認します。こうすることで、ファイルはtxtとして保存されず、CMXがサポートする正しい拡張子が付けられます。



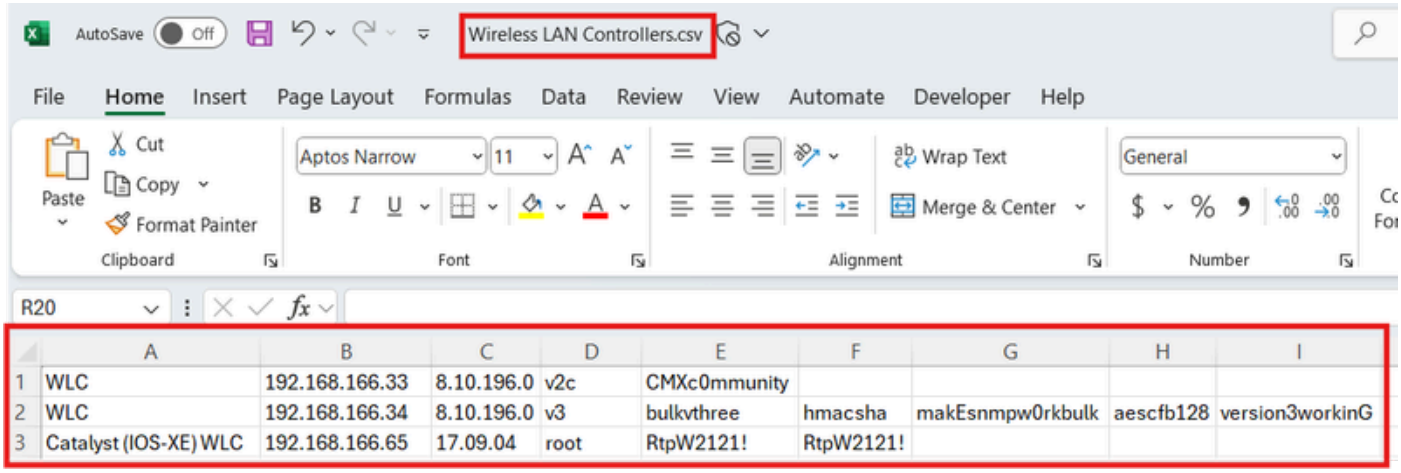
ファイルをCSVとして保存

ファイルはCSVファイルとして保存されているを示します。



CSV形式で保存されたファイルの表示

ファイルが開いている場合は、適切な情報が表示されます。



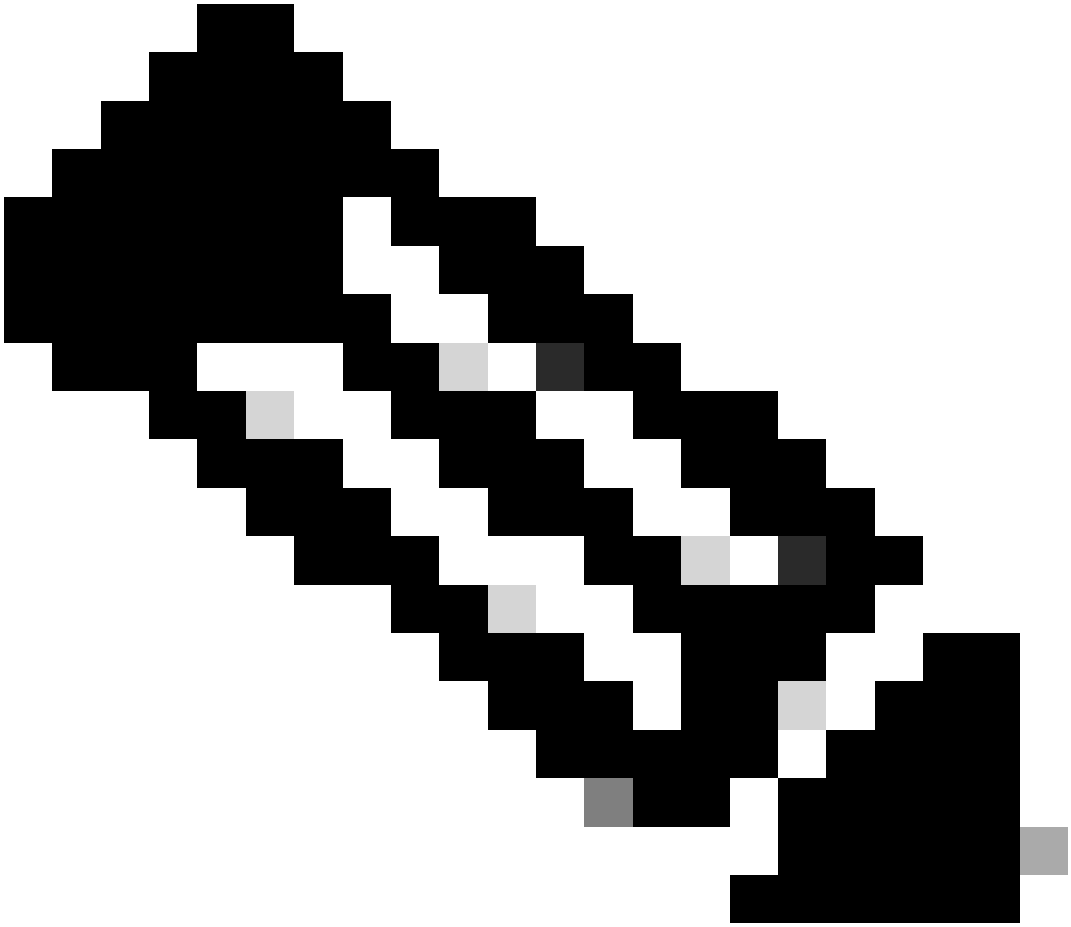
CSVファイルを開くと、WLCの情報が表示されます

CSVファイルのCMXへのインポート

現在のサーバからCMXにファイルを移動するには、Secure File Transfer Protocol(SFTP)またはSecure Copy Protocol(SCP)などの転送方式が必要です。MobaXtermやWinSCPなどのプログラムは、ファイルを簡単に移動するためのドラッグアンドドロップオプションを提供できます。Wireless LAN Controllers.csvファイルがSFTPを実行するサーバにある場合、SFTP経由でCMXからサーバへの接続が実行され、次のようにファイルが転送されます。

```
<#root>

[cmxadmin@cmx1063 ~]$

sftp tac@192.168.166.91


tac@192.168.166.91's

password:


Connected to 192.168.166.91.
sftp>

cd Desktop/CMX TZ


sftp>

dir


Wireless LAN Controllers.csv
sftp>

get "Wireless LAN Controllers.csv"


Fetching /cygdrive/c/Users/tac/Desktop/CMX/Wireless LAN Controllers.csv to Wireless LAN Controllers.csv
/cygdrive/c/Users/tac/Desktop/CMX/Wireless LAN Controllers.csv                  100% 224 2.3KB/s 00:00
sftp>
```

```
exit


[cmxadmin@cmx1063 ~]$
ls -lh


total 28K
dr-xr-xr-x. 2 cmxadmin cmxadmin 4.0K Aug 29 2022 bin
-rw-r--r--. 1 cmxadmin cmxadmin 224 Jan 22 14:29 Wireless LAN Controllers.csv
[cmxadmin@cmx1063 ~]$
```



注：ファイル名にスペースが含まれている場合は、引用符を使用してSFTPでファイルを取り出してください。引用符を使用すると、SFTPではスペースを含むファイル名が1つの文字列と見なされます。

CMXでのファイルの実行

CMXへのSSH接続を確立し、次のコマンドを実行します。

<#root>

```
[cmxadmin@cmx1063 ~]$
```

cmxctl config controllers import

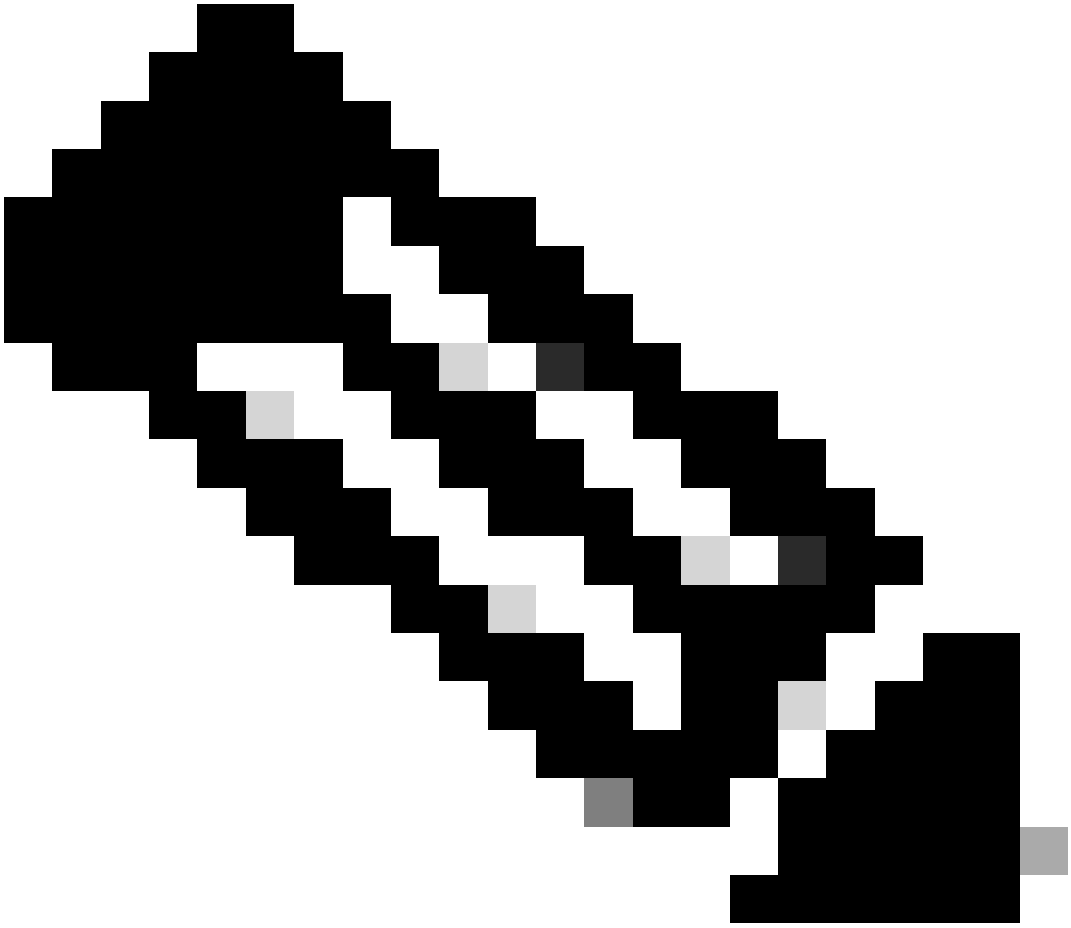
```
Please specify import type [PI/FILE] [FILE]:
```

FILE

```
Please enter CSV file path:
```

/home/cmxadmin/Wireless LAN Controllers.csv

```
Controller Added 192.168.166.33
Controller Added 192.168.166.34
Controller Added 192.168.166.65
[cmxadmin@cmx1063 ~]$
```



注：ファイルパスは常に/home/cmxadmin/で始まります。

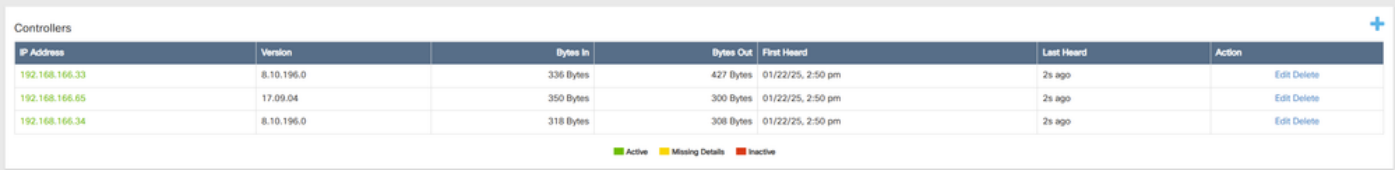
確認

CMXからの確認

CMX GUIおよびCLIから、追加したWLCをチェックして、正しく動作していることを確認できます。

CMX GUI:

SYSTEMに移動し、下にスクロールしてWLCを見つけます。図に示すように、IPアドレスが緑色で表示されている必要があります。その他の色は、問題があることを意味します。



CMXのGUI

CMX CLI:

<#root>

```
[cmxadmin@cmx1063 ~]$
```

cmxctl config controllers show

```
+----------------+----------------------+------------+------+--------+
| IP Address     | Type                 | Version    | SHA2 | Status |
+----------------+----------------------+------------+------+--------+
| 192.168.166.65 | Catalyst (IOS XE) WLC | 17.09.04   | Yes  |
```

ACTIVE

```
 |
+----------------+----------------------+------------+------+--------+
| 192.168.166.33 | AireOS WLC           | 8.10.196.0 | Yes  |
```

ACTIVE

```
 |
+----------------+----------------------+------------+------+--------+
| 192.168.166.34 | AireOS WLC           | 8.10.196.0 | Yes  |
```

ACTIVE

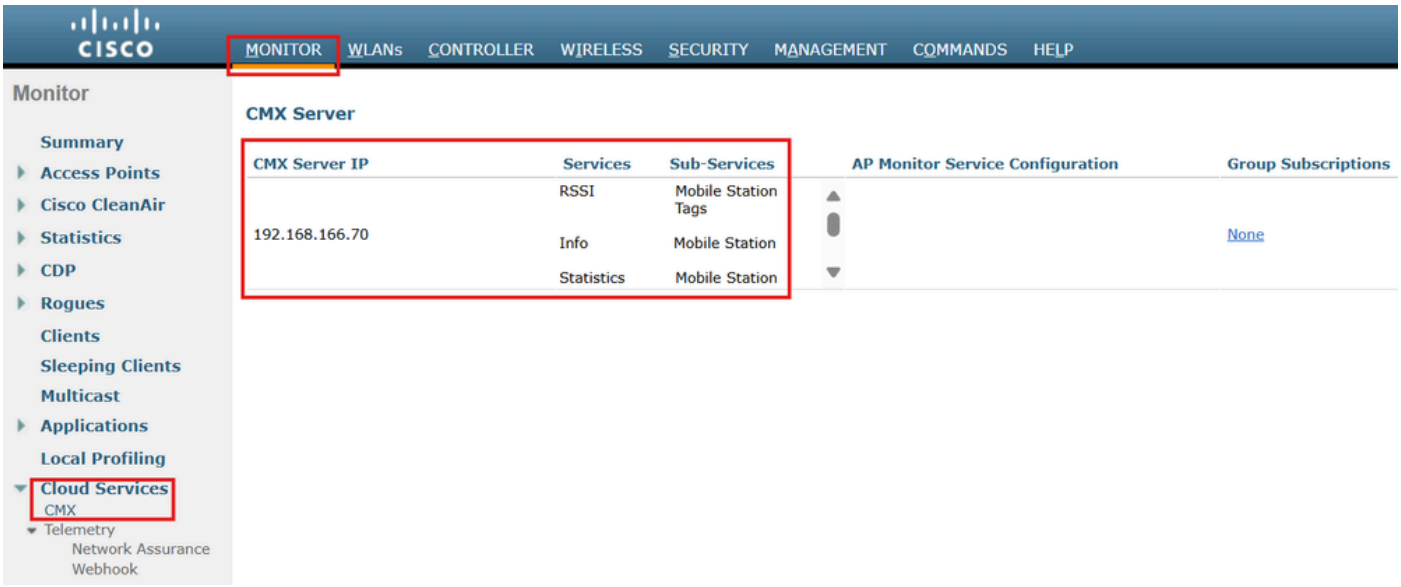
```
 |
+----------------+----------------------+------------+------+--------+
[cmxadmin@cmx1063 ~]$
```

WLCからの確認

WLCからCMXへの接続をGUIおよびCLIで確認できます。

AireOSのGUI:

図に示すように、Monitor > Cloud Services > CMXの順に選択します。



AireOSによるCMX接続の確認

AireOS WLC CLI:

<#root>

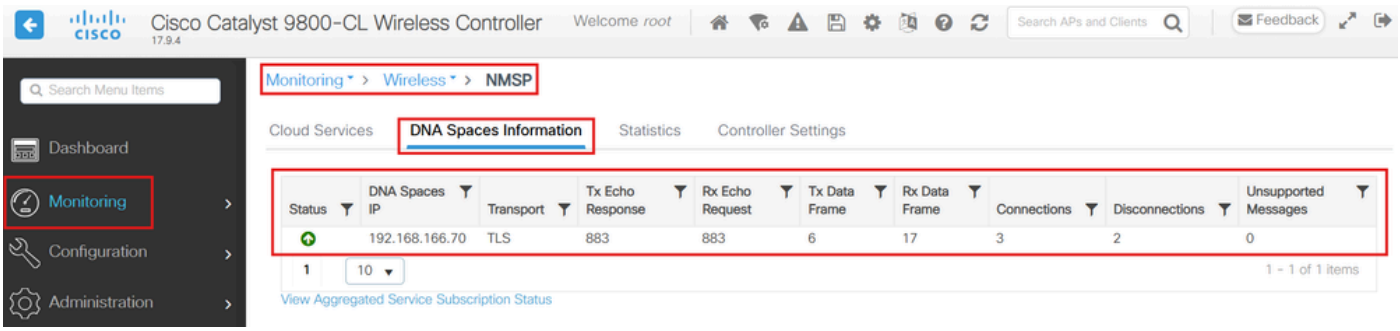
```
(Cisco Controller) >
```

show nmsp status

```
Number of Nmsp TLS Connections supported..... 5
Number of Nmsp HTTPS Connections supported..... 1
 CMX Server            Echo Resp   Echo Req   Tx Data  Rx Data
----------------     ------------ ----------- -------  -------
192.168.166.70            847         847       861      17
(Cisco Controller) >
```

9800 WLCのGUI:

図に示すように、Monitor > Wireless > NMSP > DNA Spaces Informationの順に移動します。



9800 WLC GUIからのCMXチェック

9800 WLCのCLI:

```
<#root>

#

show nmsp status


NMSP Status
-----------

DNA Spaces/CMX IP Address   Active   Tx Echo Resp  Rx Echo Req   Tx Data   Rx Data   Transport
-------------------------------------------------------------------------------------------------
192.168.166.70              Active      877           877          6         17        TLS
```

トラブルシュート

CMXとWLCから同時にトラブルシューティングを行うことをお勧めします。SNMPとNMSPなどのプロトコルは双方向の通信プロトコルと見なされ、両方のデバイスからトラブルシューティングを行って通信を理解します。トラブルシューティングを成功させるには、SNMPとNMSPのネゴシエーションが重要です。

AireOS WLCのトラブルシューティング

SNMPデバッグは、次のようにイネーブルにできます。

```
(Cisco Controller) >debug snmp all enable
```

NMSPデバッグは次のように有効にできます。

```
(Cisco Controller) >debug nmsp all enable
```

デバッグを無効にするには、コマンドを次のように入力します。

```
(Cisco Controller) >debug disable-all
```

9800 WLCのトラブルシューティング

NMSPデバッグは、次のようにイネーブルにできます。

```
#set platform software trace nmspd chassis active R0 all-modules verbose
```

パケットキャプチャでは、次のようにCMX IPアドレスでフィルタリングします。

```
#config t
(config)#ip access-list extended NMSP
(config-ext-nacl)#permit ip host <CMX IP Address> any
(config-ext-nacl)#permit ip any host <CMX IP Address>
#monitor capture NMSP interface <Interface - port> both access-list NMSP buffer size 100
#monitor capture NMSP start
```

デバッグを収集してモニタするには、次のコマンドをキャプチャします。

```
#request platform software trace archive last 1 days target bootflash:NMSPArchive
#monitor capture NMSP stop
#monitor capture NMSP export bootflash:NMSP.pcap
```

デバッグとパケットキャプチャを無効にするには、次の手順を実行します。

```
#no monitor capture NMSP
#set platform software trace nmspd chassis active R0 all-modules notice
```

CMXのトラブルシューティング

次のようにCMXログを収集します。

```
[cmxadmin@cmx1063 ~]$ cmxos techsupport dump
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。