

# Configurazione e risoluzione dei problemi di connettività CMX con Catalyst serie 9800 Wireless LAN Controller

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Verifica sincronizzazione ora](#)

[Verifica hash chiave](#)

[Verificare l'interfaccia](#)

[Comandi show](#)

[Risoluzione dei problemi](#)

[Debug](#)

[Acquisizione pacchetti](#)

[Riferimento](#)

---

## Introduzione

In questo documento viene descritto come aggiungere Catalyst 9800 Wireless LAN Controller a Connected Mobile Experience (CMX), con la verifica e la risoluzione dei problemi del tunnel NMSP. Il documento è inoltre utile quando si utilizzano Spazi DNA tramite il connettore o il tethering on-prem CMX.

## Prerequisiti

### Requisiti

In questo documento si presume che l'utente abbia eseguito la configurazione di base e la connettività di rete sia del modello 9800 WLC che del modello CMX e si riferisce solo all'aggiunta del WLC al modello CMX.

È necessario che le porte TCP 22 (SSH) e 1613 (NMSP) siano aperte tra il WLC 9800 e il CMX.

### Componenti usati

Cat9800 con versione 16.12

CMX con versione 10.6.x

## Configurazione

Esempio di rete

Configurazioni

Passaggio 1. Prendere nota dell'indirizzo IP di Wireless Management e del nome utente e della password con il privilegio 15 insieme alla password enable o enable secret, se applicabile.

CLI:

```
# show run | inc username  
# show run | inc enable  
# show wireless interface summar
```

Passaggio 2. Su CMX, per aggiungere il controller LAN wireless, selezionare Sistema > Impostazioni > Impostazioni controller e mappe, quindi fare clic su Avanzate.

È possibile ottenere una procedura guidata pop-up (se non è stata ancora completata in quel punto) o la pagina delle impostazioni effettive. Di seguito sono illustrati entrambi i tipi:

The screenshot displays the Cisco CMX configuration interface. A 'SETTINGS' dialog box is open, showing the 'Maps' and 'Controllers' sections. The 'Maps' section includes a 'Browse...' button and options to 'Delete & replace existing maps & analytics data' and 'Delete & replace existing zones'. The 'Controllers' section includes fields for 'Controller Type' (AireOS WLC), 'IP Address', 'Controller Version [Optional]', 'Controller SNMP Version' (v2c), and 'Controller SNMP Write Community' (private). The 'Advanced' option is selected in the left sidebar. The background shows the 'System at a Glance' dashboard with a table of nodes and a 'Settings' button highlighted in red.

Node	IP Address
CMX-01	192.168.1.19

Placed AP	Missing AP	Active AP
0	4	0

IP Address	Version
192.168.1.14	8.10

Passaggio 3. Dall'elenco a discesa per Tipo controller, selezionare Catalyst (IOS-XE) WLC (sulla versione 10.6.1 la casella a discesa mostra Unified WLC per i Cat9800 WLC).

The screenshot shows a 'SETTINGS' window with a sidebar on the left containing various configuration options. The main content area is divided into two sections: 'Maps' and 'Controllers'.

**Maps Section:**

- Header: 'Maps'
- Text: 'Please select maps to add or modify:'
- Form: A text input field followed by a 'Browse...' button.
- Options: Two checkboxes with labels: 'Delete & replace existing maps & analytics data' and 'Delete & replace existing zones'.
- Button: A blue 'Upload' button.

**Controllers Section:**

- Header: 'Controllers'
- Text: 'Please add controllers by providing the information below:'
- Form: A series of dropdown menus and text inputs:
  - 'Controller Type': A dropdown menu currently showing 'AireOS WLC', with a tooltip showing 'AireOS WLC' and 'Catalyst (IOS-XE) WLC' as options.
  - 'IP Address': A dropdown menu.
  - 'Controller Version [Optional]': A text input field.
  - 'Controller SNMP Version': A dropdown menu currently showing 'v2c'.
  - 'Controller SNMP Write Community': A text input field containing 'private'.
- Button: A blue 'Add Controller' button.

At the bottom right of the window, there are two buttons: a dark grey 'Close' button and a blue 'Save' button.

Passaggio 4. Fornire l'indirizzo IP, il nome utente e la password Priv 15 e abilitare la password Cat9800 WLC per consentire alla configurazione CMX di accedere al WLC di Cat9800. CMX utilizzerà la connettività SSH (e quindi avrà bisogno di una porta SSH aperta tra i due dispositivi) per raggiungere il router 9800 e configurare il tunnel NMSP. Selezionare Add Controller e quindi Chiudere la finestra popup.

Tracking

Filtering

Location Setup

Data Privacy

Data Retention

Mail Server

▼ Controllers and  
Maps Setup

Import

Advanced

Upgrade

High Availability

## Maps

Please select maps to add or modify:

  Delete & replace existing maps & analytics data Delete & replace existing zones

## Controllers

Please add controllers by providing the information below:

Controller Type	Catalyst (IOS-XE) WLC ▼
IP Address	192.168.1.15
Controller Version [Optional]	
Username	admin
Password	*****
Enable Password	*****



CMX distribuirà automaticamente queste configurazioni al WLC di Cat9800 e stabilirà un tunnel NMSP

```
# nmsp enable
# aaa new-model
# aaa session-id common
# aaa authorization credential-download wcm_loc_serv_cert local
# aaa attribute list cmx<mac>
# username <CMX mac address> mac aaa attribute list cmx_<mac>
# attribute type password <CMX key hash>
# netconf-yang
```

## Verifica

Verificare che il tunnel NMSP sia attivo e trasmettere i dati dalla prospettiva 9800:

```
9800#show nmsp status
```

```
NMSP Status
```

```
-----
```

CMX IP Address	Active	Tx Echo Resp	Rx Echo Req	Tx Data	Rx Data	T
10.48.71.119	Active	16279	16279	7	80	T

Verificare lo stesso stato del tunnel dalla prospettiva CMX nella parte inferiore della pagina Sistema:

The screenshot shows the Cisco CMX System at a Glance dashboard. The top navigation bar includes 'DETECT & LOCATE', 'ANALYTICS', 'CONNECT', 'MANAGE', and 'SYSTEM'. The main content area is divided into three sections:

- System at a Glance:** A table showing the system node 'NicoCMX1' with IP address '10.48.71.119' and 'Low-End' type. It lists various services like Configuration, Location, Analytics, Connect, Database, Cache, Hyper Location, Location Heatmap Engine, NMSP Load Balancer, and Gateway. Memory usage is 22.60% and CPU usage is 9.00%.
- Coverage Details:** A table showing 'Access Points' (Placed AP: 2, Missing AP: 0, Active AP: 0, Inactive AP: 2) and 'Map Elements' (Campus: 2, Building: 1, Floor: 1, Zone: 0, Total: 4). It also shows 'Active Devices' (Associated Client: 0, Probing Client: 0, RFID Tag: 0, BLE Tag: 0, Interferer: 0, Rogue AP: 0, Rogue Client: 0, Total: 0) and 'System Time' (Fri Aug 09 11:47:58 CEST 2019).
- Controllers:** A table showing one controller with IP address '10.48.71.120', Version '16.12.1.0', Bytes In '207 KB', Bytes Out '208 KB', First Heard '08/06/19, 3:56 pm', Last Heard '1s ago', and Action 'Edit Delete'.

## Verifica sincronizzazione ora

La procedura ottimale consiste nel puntare sia CMX che WLC allo stesso server Network Time Protocol (NTP).

Nella CLI 9800, eseguire il comando:

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

Per modificare l'indirizzo IP del server NTP in CMX:

Passaggio 1. Accedere alla riga di comando come cmxadmin

Passaggio 2. Controllare la sincronizzazione NTP con ntp integrità cmxos

Passaggio 3. Se si desidera riconfigurare il server NTP, è possibile utilizzare `cmxos ntp clear` e quindi `cmxos ntp type`.

Passaggio 4. Dopo aver sincronizzato il server NTP con CMX, eseguire il comando `cmxctl restart` per riavviare i servizi CMX e tornare all'utente `cmxadmin`.

## Verifica hash chiave

Questo processo deve essere eseguito automaticamente quando si aggiunge il WLC a CMX, quindi CMX aggiunge l'hash della chiave nella configurazione WLC. Tuttavia, è possibile verificarlo o aggiungerlo manualmente in caso di problemi.

I comandi immessi da CMX sono:

```
(config)#username <CMX mac> mac aaa attribute list cmx_<CMX MAC>
(config)# attribute type password <CMX key hash>
```

Per conoscere il significato del tasto SHA2 sul CMX, utilizzare:

```
cmxctl config authinfo get
```

## Verificare l'interfaccia

NMSP verrà inviato solo dall'interfaccia impostata come "wireless management interface" (Gig2 per impostazione predefinita su 9800-CL). Le interfacce utilizzate come porta di servizio (gig0/0 per l'accessorio o Gig1 per 9800-CL) non inviano il traffico NMSP.

## Comandi show

È possibile verificare i servizi sottoscritti a livello NSMP sul WLC 9800

```
9800#show nmsp subscription detail
CMX IP address: 10.48.71.119
Service          Subservice
-----
RSSI             Tags, Mobile Station,
Spectrum
Info             Mobile Station,
Statistics       Tags, Mobile Station,
AP Info          Subscription
```

## È possibile ottenere le statistiche del tunnel NMSP

9800#show nmsp statistics summary

NMSP Global Counters

-----  
Number of restarts : 0

SSL Statistics

-----  
Total amount of verifications : 0  
Verification failures : 0  
Verification success : 0  
Amount of connections created : 1  
Amount of connections closed : 0  
Total amount of accept attempts : 1  
Failures in accept : 0  
Amount of successful accepts : 1  
Amount of failed registrations : 0

AAA Statistics

-----  
Total amount of AAA requests : 1  
Failed to send requests : 0  
Requests sent to AAA : 1  
Responses from AAA : 1  
Responses from AAA to validate : 1  
Responses validate error : 0  
Responses validate success : 1

9800#show nmsp statistics connection

NMSP Connection Counters

-----  
CMX IP Address: 10.48.71.119, Status: Active

State:

Connections : 1  
Disconnections : 0  
Rx Data Frames : 81  
Tx Data Frames : 7  
Unsupported messages : 0

Rx Message Counters:

ID	Name	Count
1	Echo Request	16316
7	Capability Notification	2
13	Measurement Request	2
16	Information Request	69
20	Statistics Request	2
30	Service Subscribe Request	2
74	BLE Floor Beacon Scan Request	4

Tx Message Counters:

ID	Name	Count
2	Echo Response	16316
7	Capability Notification	1
14	Measurement Response	2
21	Statistics Response	2
31	Service Subscribe Response	2

# Risoluzione dei problemi

## Debug

Per ottenere i log di debug per l'istituzione del tunnel NMSP, è possibile utilizzare il trace radioattivo a partire dalla versione 16.12 e successive.

```
#debug wireless ip <CMX ip> monitor-time x
```

Questo comando abilita il debug per x minuti per l'indirizzo IP CMX indicato. Il file verrà creato in bootflash:/ e seguirà il prefisso "ra\_trace\_IP\_x.x.x.x...". Conterrà tutti i registri fascicolati relativi al debug NMSP.

Per visualizzare i debug in tempo reale sul terminale del WLC, immettere il comando:

```
#monitor log process nmspd level debug
```

Per interrompere i debug in tempo reale, premere CTRL+C.

## Acquisizione pacchetti

Raccogliere l'acquisizione dei pacchetti sul WLC utilizzando un ACL per filtrare solo il traffico tra WLC e IP CMX. Esempio con WLC ip 192.168.1.15 e CMX ip 192.168.1.19:

```
eWLC-9800-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
eWLC-9800-01(config)#ip access-list extended CMX
eWLC-9800-01(config-ext-nacl)#permit ip host 192.168.1.15 host 192.168.1.19
eWLC-9800-01(config-ext-nacl)#permit ip host 192.168.1.19 host 192.168.1.15
eWLC-9800-01(config-ext-nacl)#end
eWLC-9800-01#monitor capture CMX access-list CMX interface gigabitEthernet 2 both start
eWLC-9800-01#
Jan 30 11:53:22.535: %BUFCAP-6-ENABLE: Capture Point CMX enabled.
...
eWLC-9800-01#monitor capture CMX stop
Stopped capture point : CMX
eWLC-9800-01#
Jan 30 11:59:04.949: %BUFCAP-6-DISABLE: Capture Point CMX disabled.

eWLC-9800-01#monitor capture CMX export bootflash:/cmxCapture.pcap
```

È quindi possibile scaricare l'acquisizione dalla CLI o dalla GUI in Risoluzione dei problemi > Packet Capture > Export. In alternativa, selezionare Amministrazione > Gestione > File manager > bootflash:.

## Riferimento

[Debug wireless e raccolta di log su 9800](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).