Migrating from CMX Cloud to CMX Engage

Contents

This document describes how to migrate from CMX Cloud to CMX Engage.

Overview

The CMX Engage can be enabled for CUWN infrastructure by connecting the WLC to the CMX Engage, and performing the necessary configurations. For WLC 8.2 or earlier, you can connect the WLC to the CMX Engage using a CMX Proxy. The Cloud Proxy collects device presence information and access point details from WLC and pass it to CMX Engage. The CMX Engage uses this information for importing the location hierarchy, providing captive experience, executing the engagement and profile rules, and providing the location analytic reports.

Note The CMX Proxy is required only for WLC 8.2 or earlier. If you are using WLC 8.3 or later inbuilt cloud connector, you don't need the CMX Proxy to migrate to the CMX Engage.

For migrating from the CMX cloud to the CMX Engage, perform the following steps:

1. Connecting the WLC to the CMX Engage
   a. Connecting the WLC to the CMX Engage Using Proxy (For WLC 8.2 or earlier), page 1
   b. Connecting the WLC to the CMX Engage (for WLC 8.3 or later), page 4
2. Enabling Captive Experience Using CMX Engage, page 5
3. Removing CMX Cloud Configurations, page 6
4. Piloting CMX Engage in the Selected locations, page 7

Connecting the WLC to the CMX Engage Using Proxy (For WLC 8.2 or earlier)

The migration process is explained with an assumption that you are already using CMX Proxy to connect to CMX cloud. If you do not have the CMX Proxy installed, refer the "Installing the Cisco CMX Proxy" documentation for installing the CMX Proxy.

Note This configuration is not required for WLC 8.3 or later.

To configure the CMX Proxy to connect with the CMX Engage, perform the following steps:

Step 1 Log in to Proxy.

Step 2 Add an account using the command “proxyctl accounts add”.

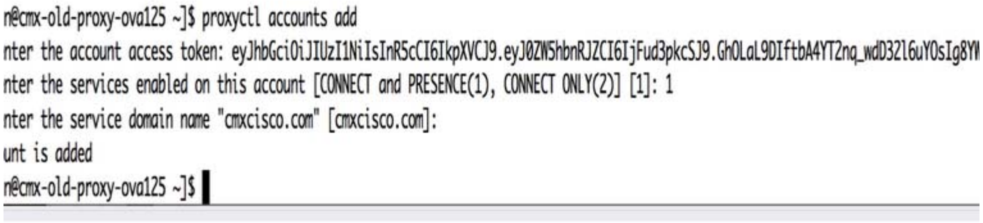
Step 3 Enter the CMX Engage access token.

Note To view the CMX Engage token, in the CMX Engage dashboard, choose **SSIDs**, click the **Setup SSIDs in Meraki/CUWN** link, and then click the “Configure SSID in CUWN-WLC” tab. The token is displayed in the step 3 under the caption “Configuring the Proxy to connect with the CMX Engage”. You can also contact the CMX Engage support team for the CMX Engage token. Ensure that there are no trailing/leading spaces.

Step 4 Enter the option to identify the services that are enabled on your CMX Cloud account. Enter 1, if you have signed up for CONNECT and PRESENCE.

Step 5 Enter the service domain name:**proximitymx.io**

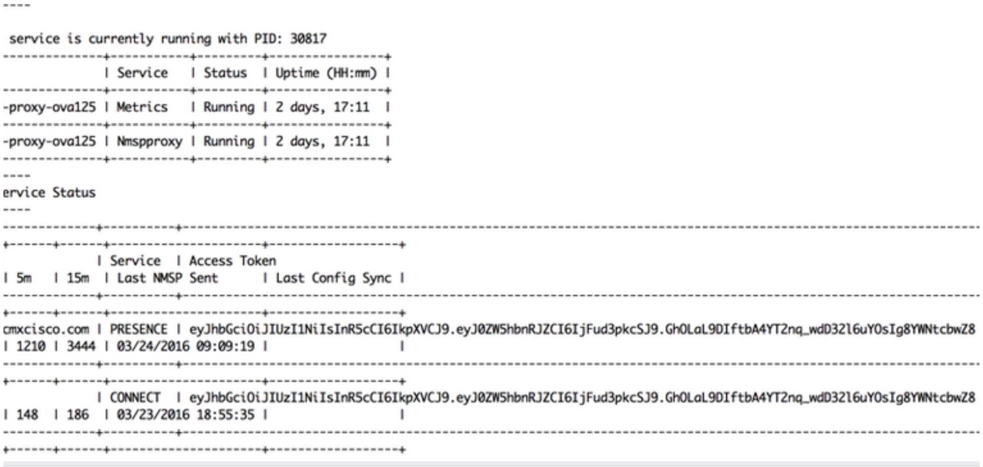
Sample screen



```
n@cmx-old-proxy-ova125 ~]$ proxyctl accounts add
nter the account access token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRJZCI6IjFud3pkcSJ9.GhOLaL9DIftbA4YT2nq_wdD32l6uYOsIg8YW
nter the services enabled on this account [CONNECT and PRESENCE(1), CONNECT ONLY(2)] [1]: 1
nter the service domain name "cmxcisco.com" [cmxcisco.com]:
unt is added
n@cmx-old-proxy-ova125 ~]$
```

Step 6 Check the status of the account added using the command “proxyctl status”.

Sample screen

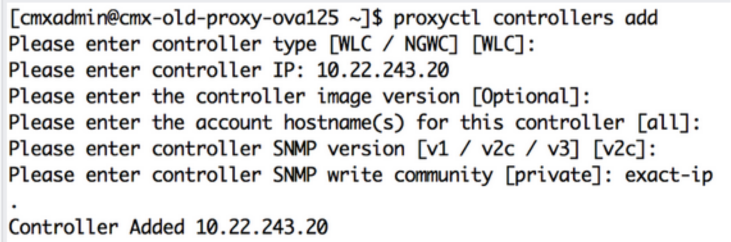


```
----
 service is currently running with PID: 30817
-------------+----------+--------+---------------+
             | Service  | Status | Uptime (HH:mm) |
-------------+----------+--------+---------------+
-proxy-ova125 | Metrics   | Running | 2 days, 17:11  |
-------------+----------+--------+---------------+
-proxy-ova125 | Nmspproxy | Running | 2 days, 17:11  |
-------------+----------+--------+---------------+
----
ervice Status
----
-----------+---------+--------------------------------------------------------------------------------------------------------
+-----+-----+------------------+----------------+
           | Service  | Access Token
| 5m   | 15m  | Last NMSP Sent       | Last Config Sync |
-----------+---------+--------------------------------------------------------------------------------------------------------
+-----+-----+------------------+----------------+
cmxcisco.com | PRESENCE | eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRJZCI6IjFud3pkcSJ9.GhOLaL9DIftbA4YT2nq_wdD32l6uYOsIg8YWNtcbwZ8
| 1210 | 3444 | 03/24/2016 09:09:19 |                |
-----------+---------+--------------------------------------------------------------------------------------------------------
+-----+-----+------------------+----------------+
           | CONNECT  | eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRJZCI6IjFud3pkcSJ9.GhOLaL9DIftbA4YT2nq_wdD32l6uYOsIg8YWNtcbwZ8
| 148  | 186  | 03/23/2016 18:55:35 |                |
-----------+---------+--------------------------------------------------------------------------------------------------------
+-----+-----+------------------+----------------+
```

Step 7 Add a controller in the Cisco CMX Proxy using the command “proxyctl controllers add”, and specify the following details.

- Controller Type: WLC
- Controller IP: WLC Controller IP
- Control Image Version[Optional]: [not required]
- Host name: specify a host name
- SNMP version: v2C
- SNMP write community: private

Sample screen

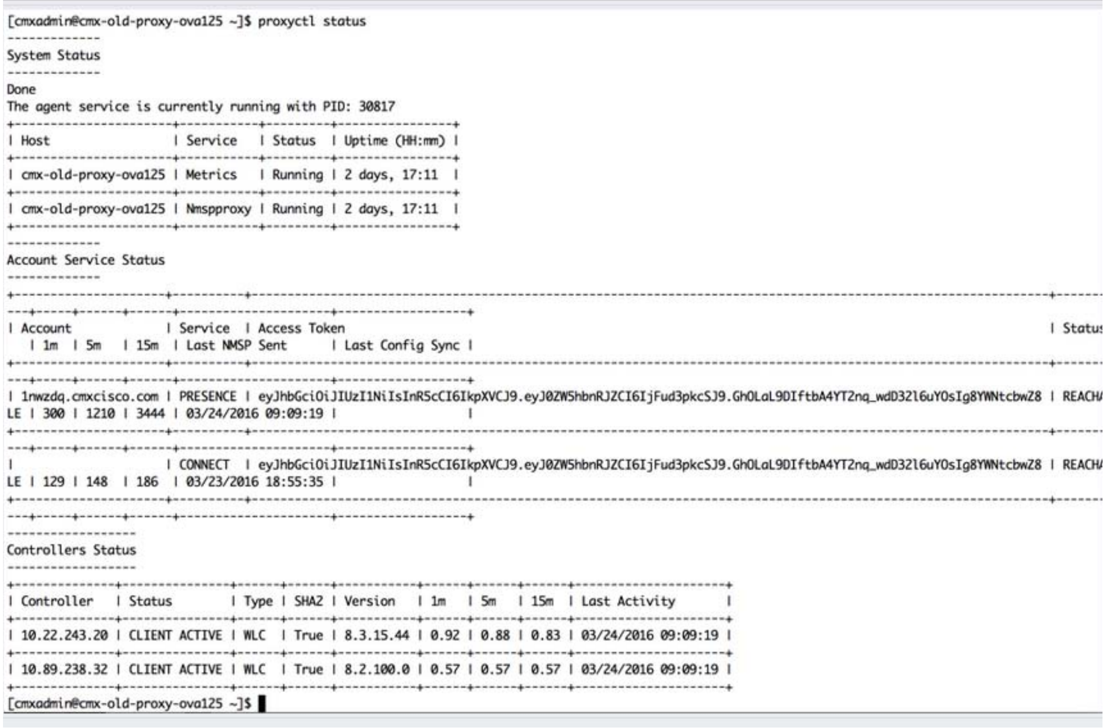


```
[cmxadmin@cmx-old-proxy-ova125 ~]$ proxyctl controllers add
Please enter controller type [WLC / NGWC] [WLC]:
Please enter controller IP: 10.22.243.20
Please enter the controller image version [Optional]:
Please enter the account hostname(s) for this controller [all]:
Please enter controller SNMP version [v1 / v2c / v3] [v2c]:
Please enter controller SNMP write community [private]: exact-ip
.
Controller Added 10.22.243.20
```

Note Ensure that you have enabled Read-Write permission for the SNMP Community in the WLC. SNMP Read Only community does not work.

Step 8 Verify that the Proxy is successfully connected to both WLC and CMX Engage using the command "proxyctl status".

Sample screen



```
[cmxadmin@cmx-old-proxy-ova125 ~]$ proxyctl status
-------------
System Status
-------------
Done
The agent service is currently running with PID: 30817
+----------------------+-----------+---------+----------------+
| Host                 | Service   | Status  | Uptime (HH:mm) |
+----------------------+-----------+---------+----------------+
| cmx-old-proxy-ova125 | Metrics   | Running | 2 days, 17:11  |
+----------------------+-----------+---------+----------------+
| cmx-old-proxy-ova125 | Nmspproxy | Running | 2 days, 17:11  |
+----------------------+-----------+---------+----------------+
-------------
Account Service Status
-------------
+---------------------+----------+---------------------------------------------------------------------------------------------------------------+------
---+-----+------+------+---------------------+------------------+
| Account             | Service  | Access Token                                                                                                  | Statu
   | 1m  | 5m   | 15m  | Last NMSP Sent      | Last Config Sync |
+---------------------+----------+---------------------------------------------------------------------------------------------------------------+------
---+-----+------+------+---------------------+------------------+
| 1nwzdq.cmxcisco.com | PRESENCE | eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRJZCI6IjFud3pkcSJ9.GhOLaL9DIftbA4YT2nq_wdD32l6uYOsIg8YWNtcbwZ8 | REACH
LE | 300 | 1210 | 3444 | 03/24/2016 09:09:19 |                  |
+---------------------+----------+---------------------------------------------------------------------------------------------------------------+------
---+-----+------+------+---------------------+------------------+
|                     | CONNECT  | eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRJZCI6IjFud3pkcSJ9.GhOLaL9DIftbA4YT2nq_wdD32l6uYOsIg8YWNtcbwZ8 | REACH
LE | 129 | 148  | 186  | 03/23/2016 18:55:35 |                  |
+---------------------+----------+---------------------------------------------------------------------------------------------------------------+------
---+-----+------+------+---------------------+------------------+
------------------
Controllers Status
------------------
+--------------+---------------+------+------+-----------+------+------+------+---------------------+
| Controller   | Status        | Type | SHA2 | Version   | 1m   | 5m   | 15m  | Last Activity       |
+--------------+---------------+------+------+-----------+------+------+------+---------------------+
| 10.22.243.20 | CLIENT ACTIVE | WLC  | True | 8.3.15.44 | 0.92 | 0.88 | 0.83 | 03/24/2016 09:09:19 |
+--------------+---------------+------+------+-----------+------+------+------+---------------------+
| 10.89.238.32 | CLIENT ACTIVE | WLC  | True | 8.2.100.0 | 0.57 | 0.57 | 0.57 | 03/24/2016 09:09:19 |
+--------------+---------------+------+------+-----------+------+------+------+---------------------+
[cmxadmin@cmx-old-proxy-ova125 ~]$ █
```

Connecting the WLC to the CMX Engage (for WLC 8.3 or later)

Note This configuration is not required for WLC 8.2 or earlier.

To connect the WLC to the CMX Engage and to import the WLC Controller to the CMX Engage, perform the following steps:

Step 1 If WLC version is 8.3, execute the following command to force the system to resolve to a fixed IP address:

```
config cloud-services server url https://customerpathkey.proximitymx.io 50.16.12.224
```

Note This step is not required for the WLC 8.3.111.0 or later releases.

Note To view the “customerpathkey”, in the CMX Engage dashboard, choose **SSIDs**, click the **Setup SSIDs in Meraki/CUWN** link, and then click the “Configure SSID in CUWN-WLC” tab. The customerpathkey is displayed in the server URL in the step 1 under the caption “Configuring the WLC to Import the WLC Controller to the CMX Engage”.

Step 2 In the WLC CLI mode, execute the following commands:

1. config cloud-services cmx disable
2. config cloud-services server url https://customerpathkey.proximitymx.io
3. config cloud-services ip address 50.16.12.224
4. config cloud-services server id-token [token]
5. config cloud-services cmx enable

Note To view the “customerpathkey” and service ID token, in the CMX Engage dashboard, choose **SSIDs**, click the **Setup SSIDs in Meraki/CUWN** link, and then click the “Configure SSID in CUWN-WLC” tab. The customerpathkey and token are displayed in the step 1 under the caption “Configuring the WLC to Import the WLC Controller to the CMX Engage”. You can also contact the CMX Engage support team. Ensure that there are no trailing/leading spaces.

Step 3 Check the summary using the following command:

```
show cloud-services cmx summary
```

The result appears.

Now in the CMX Engage dashboard, when you choose “CUWN-WLC” in the “Add a Wireless Network” window, the WLC will be listed. So, you can import the APs of that WLC to the CMX Engage.

Sample Result

```
(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ...................................... https://$customerpathkey.proximitymx.io
```

```
IP Address................................... 50.16.12.224
Connectivity................................. https: UP
Service Status .............................. Active
Last Request Status.......................... HTTP/1.1 200 OK

Heartbeat Status ............................ OK
```

Enabling Captive Experience Using CMX Engage

After connecting the WLC to the CMX Engage, to migrate the captive portal experience from the CMX Cloud to CMX Engage, perform the following steps:

1. Import the Location Hierarchy, page 5
2. Import SSIDs, page 5
3. Create Portals, page 6
4. Create Captive Portal Rules, page 6
5. Configure the WLC, page 6

Import the Location Hierarchy

To import the location hierarchy, perform the following steps:

Step 1 In the CMX Engage dashboard, choose **Manage Locations**.

Step 2 In the Locations page, click the **More Actions** at the far right of the customer name.

Step 3 Click **Add a Wireless Network**.

Step 4 From the Add Wireless Network drop-down list, choose **CUWN-WLC**.

The WLCs available gets listed.

Step 5 Choose the required WLC, and click **Add**.

The WLC node with the associated APs gets added to the location hierarchy.

Step 6 If you want to group the APs, click the **More Actions** at the far right of the WLC node, and click **Add Zone**.

Step 7 In the Add Zone screen that appears, select the access points for the zone, and click **Add**.

Note Creating zones help you to group APs and create logical locations.

Import SSIDs

Import the required SSIDs to the CMX Engage. To know how to import the SSIDs to the CMX Engage, see Importing SSIDs.

Create Portals

In the CMX Engage dashboard, create the captive portals to be displayed when a customer connects to the various SSIDs in your business locations.To know how to create portals in the CMX Engage, see Creating Portals.

Create Captive Portal Rules

In the CMX Engage dashboard, define the Captive Portal Rules to provide various captive experiences for the customers connecting to your SSIDs. To know how to create captive portal rules in the CMX Engage, see Defining the Captive Portal Rules.

Configure the WLC

You must do this configuration only if you want to completely migrate the captive experience from the CMX Cloud to the CMX Engage. To know the WLC configurations required, see WLC Configurations.

Note As there are SSIDs already created for the CMX cloud, you just have to update the SSID configuration required for CMX Engage.

If you want to migrate the captive experience only for the selected locations, proceed to Piloting CMX Engage in the Selected locations, page 7

Removing CMX Cloud Configurations

Based on how you are connected to CMX Cloud, select the appropriate procedure from the following:

- Removing CMX Cloud Configurations when Connected Using CMX Proxy, page 6
- Removing CMX Cloud Configurations when Connected Using WLC 8.3 or Later, page 7

Removing CMX Cloud Configurations when Connected Using CMX Proxy

Note You must do this step only after completing migration from CMX cloud to CMX Engage.

After completely migrating the captive experience to the CMX Engage, you can remove the CMX Cloud configurations from the Proxy.

To remove the connection between CMX Cloud and CMX Proxy, perform the following steps:

Step 1 Log in to the Proxy using the cmxadmin credentials.

Step 2 Enter the command “proxyctl accounts show”.

Step 3 Identify the CMX cloud account identifier.

Step 4 Enter the command “proxyctl accounts delete”.

The CMX cloud configurations are removed from the proxy.

Removing CMX Cloud Configurations when Connected Using WLC 8.3 or Later

To remove the connection between CMX Cloud and WLC 8.3 or later, perform the following steps:

Step 1 In the WLC CLI mode, execute the command “config cloud-services cmx disable”.

Step 2 Verify the status using the command “show cloud-services cmx summary”.

The message “Service Status......Admin Disabled” is shown.

Piloting CMX Engage in the Selected locations

Note This step is not required if you have completely migrated the captive experience from the CMX cloud to the CMX Engage.

If you want to migrate the captive experience only for selected locations from CMX cloud to CMX Engage, perform the following steps:

1. Create SSIDs, page 7
2. Create AP Groups, page 7
3. Configure AP Groups for CMX Engage, page 7
4. Remaining WLC Configurations, page 8

Create SSIDs

To create SSIDs perform the following steps:

Step 1 Log in to the WLC with your credentials

Step 2 Create a new SSID (WLAN) in WLC with the same name used for the CMX Cloud.

Step 3 Set a different Profile Name from the one that is used for the CMX cloud.

Create AP Groups

You must create a new AP group and move the APs for which you want to show the CMX Engage captive experience to this AP group.

To create AP groups, perform the following steps:

Step 1 In the WLC dashboard, choose **WLANs > Advanced >AP Groups**.

Step 2 Click **Add Group**, and create an AP group for CMX Engage.

Configure AP Groups for CMX Engage

To configure AP groups, perform the following steps:

Step 1 In the AP Groups, choose the AP group that you created for the CMX Engage previously.

Step 2 Choose **WLAN> Add New.**

Step 3 Select the SSIDs created previously for the CMX Engage, and click **Add**.

Note Ensure to select the correct WLAN ID.

Step 4 Choose **APs**.

Step 5 Select the APs that are to be moved to the CMX Engage, and click **Add APs**.

Remaining WLC Configurations

You must do the remaining WLC configurations such as creating ACLs, configuring the splash page, security layers, and so on in the WLC. To know the WLC configurations, see WLC Configurations.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.