Getting Started

Introduction to Cisco Connected Mobile Experiences

Cisco Mobility Services Engine (Cisco MSE) acts as a platform to deploy and run Cisco Connected Mobile Experiences (Cisco CMX). Cisco MSE is delivered in two modes—the physical appliance (box) and the virtual appliance (deployed using VMware vSphere Client) . Using your Cisco wireless network and location intelligence from Cisco MSE, Cisco CMX helps you create personalized mobile experiences for end users and gain operational efficiency with location-based services.

For more information about Cisco CMX features for this release, see the *Release Notes for Cisco CMX*, at:

https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-release-notes-list.html

Overview of Cisco CMX Services

Cisco CMX enables you to access the following services:

- **DETECT & LOCATE**—The Detect & Locate service uses the data provided by Cisco WLCs to calculate the X,Y location (based on 0,0 at the top left hand side of the map) of wireless devices that are detected by the access points that support the wireless LAN (WLAN) to a high degree of precision (generally +/-5 to 7M, 90% of the time with standard location technologies and +/-1 to 3M, 50% of the time with Hyperlocation technologies). Given the proper physical environment with access points deployed in

accordance with Cisco best practices for a location ready environment. The CMX GUI will be able to display the physical location of:

- Associated Wireless Devices (shown as green dots in default view)

- Unassociated Wireless Devices (shown as red dots in default view)

- RF Interferers (Lightning icon)

- Access Points (Circles)

- Rogue Access Points

- Rogue Clients

- BLE Tags (Bluetooth Icon)

- Active Wi-fi RFID Tags (Tag icon)

The background map can display:

- Inclusion and Exclusion Zones imported from Cisco Prime Infrastructure

- Analytics Zones created in Cisco CMX

- Thick Walls

- GPS Markers

Additionally when passed to the CMX Analytics service, this location information provides visibility into customer movements and behavior throughout the venue and throughout the day. The Cisco CMX Analytics service determines device parameters and can display this information as part of six different unique widgets.

If you choose Location during installation, you will see the following services in Cisco CMX GUI.

- DETECT & LOCATE—Active for 120 day trial period unless either a CMX base or advanced license is added.

- ANALYTICS—Active for 120 day trial period unless a CMX advanced license is added.

- CONNECT—Active for 120 day trial period unless either a CMX base or advanced license is added

- MANAGE

- SYSTEM

For more information, see Overview of the Detect and Locate Service.

- **ANALYTICS**—This service provides a set of data analytic tools packaged for analyzing Wi-Fi device locations. It functions as a data visualization engine that helps organizations use their network as a data source for business analysis to understand behavior patterns and trends, which can help them take decisions on how to improve visitor experience and boost customer service.

The ANALYTICS service allows for the creation of six different type of widgets.

- Device count

- Dwell time

- Dwell time breakdown

- Associated User Report

- Path

- Correlation

For more information, see The Cisco CMX Analytics Service.

- **CONNECT**—This service provides intuitive, simple, highly customizable, and location-aware guest services in the form of a captive portal that offers two types of guest on-boarding experiences:

    - Facebook Wi-Fi

    - Custom Portal

For more information, see The Cisco CMX Connect Service.

- PRESENCE ANALYTICS—Cisco Presence Analytics service is a new analytics engine that detects the presence of visitors via their mobile devices interactions with even a single network access point. The probe requests which are transmitted from the wireless devices provide information, which is used to identify the general location of a client, in respect to the location of even a single access point which hears the clients probing activity. The information available from even a single AP allows the Presence Analytics service to develop valuable business intelligence. Presence Analytics uses Received Signal Strength Indication (RSSI), along with the duration of high signal strength to determine whether a client device is in the site or just passing by. Even if a device is not connected to the access point, its presence is still detected if the device is within the signal range and the wireless is turned on. Given that Presence Analytics develops location information with respect to a given set of APs it has a simpler management overhead in that it does not require the importation or configuration of any maps into the CMX instance. By simply knowing the association of a given AP, or set of APs, to a physical location, Presence Analytics allows a business insight into the number of visitors to a location, whether these are first time or repeat visitors, the average amount of time each visitor spent in physical proximity to the AP, and the ability to ascertain whether a devise was just passing by a location or if they were actually within the location serviced by the AP. For more information, see Overview of the Presence Analytics Service.

If you choose Presence during installation, you will see the following services in the Cisco CMX GUI.

    - PRESENCE ANALYTICS

    - CONNECT

    - MANAGE

    - SYSTEM

- **MANAGE**—This service enables you to manage licenses, users, zones, beacons, and notifications. For more information, see Managing Cisco CMX Configuration.

- **SYSTEM**—This service enables you to verify the health of the system and view patterns and metrics. For more information, see Managing Cisco CMX System Settings.

For a complete list of new features supported by Cisco CMX for this release, see the *Release Notes for Cisco CMX*, at:

http://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-release-notes-list.html

Note The installation methods for Location and Presence are different. If you want to change the service, you must perform a fresh installation.

Importing Maps and Cisco Wireless Controllers

Cisco CMX relies on incoming Network Mobility Service Protocol (NMSP) data from any of the Cisco Wireless Controllers (Cisco WLCs) added to the system. The following sections describe the process to follow.

Exporting Cisco Prime Infrastructure Maps

To obtain maps for Cisco CMX, you have to export maps from Cisco Prime Infrastructure.

Procedure

Step 1   Log in to Cisco Prime Infrastructure.

Step 2   Choose **Site Maps** from the Maps menu.

Step 3   Choose **Export Maps** and click **Go**.

Step 4   Select the map to be exported and click **Export**.

The selected map is downloaded to a compressed tar file named ImportExport_*xxxx* .tar.gz, for example, *ImportExport_4575dcc9014d3d88.tar.gz*, in your browser's download directory.

Copying the Exported Maps

Use Secure Copy Protocol (SCP) to copy the exported maps to a directory of a server accessible by Cisco CMX.

Importing Maps

You can import maps from Cisco Prime Infrastructure into Cisco CMX using either GUI or CLI.

When you import maps, they are appended to the existing ones in Cisco CMX. When Cisco CMX finds that a campus whose name already exists in Cisco CMX has a different AesUID in the import map file, Cisco CMX performs a map sync operation under this campus if the override option is set to **Yes**.

To import maps using the CLI, use the **cmxctl config maps import   --type**   *FILE* **--path** *path to .tar.gz file* command.

For more information about Cisco CMX commands, see the *Cisco Connected Mobile Experiences (CMX) Command Reference Guide*, at:

https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-command-reference-list.html

Note
When importing the maps from Prime Infrastructure using CLI, you also can import the zones. To import zones, set the import zone option as **Yes** and import the maps. After importing maps from Cisco Prime Infrastructure, you can update them in Cisco CMX by drawing new zones. However, these changes are not synchronized back to Cisco Prime Infrastructure.

Adding Cisco WLCs

You can add Cisco WLCs using CLI or the CMX user interface. If you want to import controllers to Cisco CMX from Prime Infrastructure, you must provide SNMP RW credentials for the WLCs after your import them to suuccessfully add them to Cisco CMX. Otherwise, controllers will display as "Inactive."

To add Cisco WLCs from the Cisco CMX CLI, run one of these commands:

- **cmxctl config controllers add**

- **cmxctl config controllers import [PI/FILE]**

For more information about Cisco CMX commands, see the *Cisco Connected Mobile Experiences (CMX) Command Reference Guide*, at:

https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-command-reference-list.html

Note
After adding Cisco WLCs, you must verfiy if the controller status is up and running. Using the CLI, you can run the command **cmxctl config controllers show** to display the list of controllers with the status. An **Active** status indicates a established connection.

To validate the controller status using user interface, you need to navigate to the **System** tab. The controllers list is displayed in the tab and the new controller should appear in green.

Logging In to the Cisco CMX User Interface

Procedure

Step 1 Launch the Cisco CMX user interface using Google Chrome 50 or later.

Step 2 In the browser's address line, enter https://*ipaddress* , where *ipaddress* is the IP address of the server on which you installed Cisco CMX.

The Cisco CMX user interface displays the Login window.

Step 3 Enter your username and password.

(The default username is admin and the default password is admin.)

Using the Evaluation License

Cisco Connected Mobile Experiences (CMX) ships with a fully functional 120-day evaluation license, which is activated after Cisco CMX is installed and started for the first time. The evaluation license is based on Cisco CMX usage, not calendar days (meaning, days when Cisco CMX is not used are not counted).

You must upload a permanent license to CMX before the evaluation license expires. Otherwise, you will not be able to access the Cisco CMX GUI or APIs. Cisco CMX will continue to run in the background and collect data until you add a permanent license.

After the evaluation license expires, only users with admin privileges can log in to add additional licenses.

CMX provides multiple reminders that the evaluation license is about to expire:

- For two weeks before the evaluation license expires, a daily alert is displayed on the Cisco CMX **System > Alerts** window.

- An alert email is sent, if you have configured email settings.

- An alert is displayed when you log in to Cisco CMX.

To add a license, click **Add new license** from the alert. You can also add a license from the Cisco CMX **Manage > Licenses** window. For information about adding permanent licenses, see Managing Licenses.

> **Note** The license file has an .lic extension. Make sure it is the .lic file that you install on Cisco CMX. The .lic file is available as part of your licensing package and is sent as an email attachment from licensing. Extract the .lic file to your system and upload to Cisco CMX when adding a new license.

For details about procuring licenses, see the Cisco Connected Mobile Experiences (CMX) Version 10 Ordering and Licensing Guide.

Enabling or Disabling Cisco CMX Services

- To enable a Cisco CMX service using the CLI, run the following command:

  cmxctl enable {consul | qlesspyworker | cassandra | iodocs | cache_6382 | cache_6380 | cache_6381 | cache_6383 | cache_6385 | influxdb | metrics | confd | cache_6379 | cache_6378 | haproxy | database | analytics | connect | location | configuration | matlabengine | hyperlocation | nmsplb | agent}

- To disable a Cisco CMX service using the CLI, run the following command:

  cmxctl disable {consul | qlesspyworker | cassandra | iodocs | cache_6382 | cache_6380 | cache_6381 | cache_6383 | cache_6385 | influxdb | metrics | confd | cache_6379 | cache_6378 | haproxy | database | analytics | connect | location | configuration | matlabengine | hyperlocation | nmsplb | agent}

For detailed information about these commands, see the *Cisco Connected Mobile Experiences (CMX) Command Reference Guide*, at:

https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-command-reference-list.html

Importing Certificates

Cisco CMX requires certificates for serving the user interface over SSL. You can import self signed certificates or certificate authority (CA) signed certificates to Cisco CMX. Before initiating the import process, ensure that you have a self signed or a CA signed certificate and the key file. We recommend you to consult your CA authority to generate certificate signing requests (CSR) and certificates.

The certificate should be in the PEM format (with .pem extension) as shown below:

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

Note
Cisco CMX has multiple internal servers that work with SSL certificates. If these certificates use passphrase, after a Cisco CMX restart, the passphrase must be manually entered to use the certificates. As the internal servers within Cisco CMX do not directly interact with the user, there is no interface to input the required passphrases. Hence, at this point, Cisco CMX cannot support certificate with passphrases.

To work around this issue, remove the passphrase from the certificates, by running the following command: **openssl rsa -in** *<OriginalKeyfile>* **-out** *<NewKeyfileWithoutPassphrase>*.

Procedure

Step 1 Run the following **scp** command to copy the PEM certificate into Cisco CMX system.

scp cert.pem cmxadmin@10.10.10.10:~/

Step 2 Run the following scp command to copy the key file into Cisco CMX system.

scp host.key cmxadmin@10.10.10.10:~/

Step 3 Log in to Cisco Connected Mobile Experiences (Cisco CMX) as cmxadmin user.

The PEM certificate and the key file must be in the home directory of the cmxadmin user.

Step 4 Ensure that the certificate and key files have minimum global read permissions (0644).

Step 5 Run the following command to verify whether the certificate is valid.

openssl verify -CAfile /home/cmxadmin/cert.pem /home/cmxadmin/cert.pem

A valid certificate returns an OK message.

Step 6 To install the new certificate in Cisco CMX, run the following command:

cmxctl node sslmode enable --pem /home/cmxadmin/cert.pem --key /home/cmxadmin/host.key

Step 7 Run the following commands to restart the agent and haproxy services:

cmxctl restart agent

cmxctl restart haproxy

Step 8 Navigate to Cisco CMX URL in your web browser and then use the browser tools to confirm the new certificate.

Installing Self-signed and Third Party SSL Certificate in Cisco CMX

This section describes the installation of self-signed and 3rd party signed certificates in CMX.

Installing a self-signed certificate

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX) as cmxadmin user.

Step 2 Run the following command:

```
[root@cmx]# cd /opt/haproxy/ssl/
[root@cmx]# mkdir newcert
[root@cmx]# cd newcert
[root@cmx newcert]# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/opt/haproxy/ssl/newcert/private.key -out /opt/haproxy/ssl/newcert/cert.crt
Generating a 2048 bit RSA private key
.............................................................+++
.......................................................+++
writing new private key to '/opt/haproxy/ssl/newcert/private.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:BE
State or Province Name (full name) []:Brussels
Locality Name (eg, city) [Default City]:Brussels
Organization Name (eg, company) [Default Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (eg, your name or your server's hostname) []:cmx.example.com
Email Address []:cmx@example.com
[root@cmx newcert_byserge]# ls
cert.crt  private.key
[root@cmx newcert_byserge]# cat cert.crt private.key | tee cert.pem
```

Step 3 The following example shows the certificate:

```
-----BEGIN CERTIFICATE-----
MIID8TCCAtmgAwIBAgIJAOWdn/1xqQKNMA0GCSqGSIb3DQEBBQUAMIGOMQswCQYD
VQQGEwJCRTERMA8GA1UECAwIQnJ1c3NlbHMxETAPBgNVBAcMCEJydXNzZWxzMQ4w
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMRgwFgYDVQQDDA9zZXJnZWNhc0B0
ay5jb20xITAfBgkqhkiG9w0BCQEWEnN5YXNtaW5lQGNpc2NvLmNvbTAeFw0xNTEx
MjYxMDU0MzlaFw0xNjExMjUxMDU0MzlaMIGOMQswCQYDVQQGEwJCRTERMA8GA1UE
CAwIQnJ1c3NlbHMxETAPBgNVBAcMCEJydXNzZWxzMQ4wDAYDVQQKDAVDaXNjbzEM
MAoGA1UECwwDVEFDMRgwFgYDVQQDDA9zZXJnZWNhc0B0ay5jb20xITAfBgkqhkiG
9w0BCQEWEnN5YXNtaW5lQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKOwDC5Y/dRCTSp8mnL40M0QXvrLjzsb2U9++oUsB+e7g0pYlTqp
PaPK9KEem17WhoYMqFJ4+AXvuRxsY8ElT/cEs0BfM38QDzDxc42X6TBe7eiFX+MH
WODwk3p3sGLbdVWckWViz99b3eMnPoRdlXPQhQS/LVZcCiNdoHQdwwyPQ321O7gF
x1FVHcjLpUE4FmqhvIttcPypwEMoq/3s1tOP3OiJkB9Doy7wrEF+bKHEi6b8N453
jwY7OQG7wLrKBRz7QFXxWWurxb3PBOtQohWJ16e2aABUDBq9Ata02BVxPaw+dfrC
XCq5Yc8mmDxqc+B7THOPdN9jLzhenMiRJrECAwEAAaNQME4wHQYDVR0OBBYEFGQu
ZDeZNoTENM4cO8NNzEdU421cMB8GA1UdIwQYMBaAFGQuZDeZNoTENM4cO8NNzEdU
421cMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAGL7U4Ls/3bj11dd
5O0IluEbxPF+SPId+C+dM7BWEf6deeby+b2KwjmsV0k9CFw9Hs0lqOen5LbnqtzN
3rDWqpkAiaXxKUR34oUONgdnjuCQZwRaTpzQmB0CzwGqu5JuoNSHNtvfOtTErKRH
oNt6ZlDt/poPTdoj2cUWFrPS7FTkre+lTmKXPORPYoq/vteYtjde5geW6dAV98CQ
3HL+FDeWGmQDSwnDQcnANUh88cR3HQge5hx5rLLof/xHExrkx/e19Jmw+ft92AC1
sbPb6dR/svR7Gl7jRyzoO4AMaqlZloHgiXq3Su8OqcV9MP6k3ArOkUjHzhGX+fLw
8wIsYX8=
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCjsAwuWP3UQk0q
fJpy+NDNEF76y487G9lPfvqFLAfnu4NKWJU6qT2jyvShHpte1oaGDKhSePgF77kc
bGPBJU/3BLNAXzN/EA8w8XONl+kwXu3ohV/jB1jg8JN6d7Bi23VVnJFlYs/fW93j
Jz6EXZVz0IUEvy1WXAojXaB0HcMMj0N9tTu4BcdRVR3Iy6VBOBZqobyLbXD8qcBD
KKv97NbTj9zoiZAfQ6Mu8KxBfmyhxIum/DeOd48GOzkBu8C6ygUc+0BV8Vlrq8W9
zwTrUKIVidentmgAVAwavQLWtNgVcT2sPnX6wlwquWHPJpg8anPge0xzj3TfYy84
XpzIkSaxAgMBAAECggEAYlO2fYDnuUG6qPMAtF/SzdwvsefluIQYTjCwvJ6egQ2a
6GYd/ob7iBC6sq54Fpg3Zv7jfec81hQS1oglxDhtuK0SIHEPthwng/cGut+uLGhZ
8XttBiu7sCPT85VCV6AM88iBbq3UwQ+mUnWYkFrHFDMGNLvCuEXBsUzkvdvC9x+C
GvtXBLERJJmLbGh4kyEPFUiTYzXBOTsh+oRaZ5gh4YLicV6a5Cjwu8wm/xZlLwbZ
NKCD1RYxAZ7vxASU5Lagi72hIZM5r9kDlDj2zhzdPGo/+R5fIPN92UWjur9r5QM0
9+LU+qeTbjdNojOnYrckBStGySx2+r22FLkWBKcqIQKBgQDSibalRqpMxgZENBfo
RsgHP532AB7cufaDkjEV+vmLupExZ9yRRIwIrqZ7XYkdFRCHTCFt5zrzN8bz5nO5
OdigOZ1Ae7yACmwsSmyBACbNrcVpwE4gcckVzw/V2xT+c331rCEd2tzDivIC7Dr0
7s8D3J4zq+KwGEguCYXiPCUh3wKBgQDHCIH7as1RGQzizVQkN+rDvzo8+TjOHZSF
9BYXQqknCSYuT2d3bFqOdAhqxRL8zKn5qvUOSSr8TvLh4aowVR4ZSO0HMVCbjs1W
QZ9PLKKaVyz3Awqwv+UFF0SG7SROjJM8YSMI9qp1rgPY3jrotgZZ02I/TJ8wn9m2
NBsx5s1pbwKBgGf0FVm/7YBg2mE8s309zbA+ihkX8CUeMQi/2zq2JBcI9H3HgZG8
ncP/sDYDdhsE9pdHUM46ONI0fSiaZhNT65EZQXrAXc9+1fB8gtyjHYW6wlm32RuN
8zKwfWojdVc54Ty3U9aw5QYsCdjFmUqsy0xl1zs+KHy4UJNioleVSORTAoGAaA+5
rhLsID+hrh8+o+UceJXNxD1lhtaOZe71cdnniMJO1R2s8hKT0jE2iWRahhQXtrK8
h2iX8ezxLkqHadfG8d9gFkehZoOmNjf/LC0hIuL7XnaXq0vZWO0OZiEsv2jePk5n
O/ODsh12Y3flgvBQp7xOfNv5yzl4Ybwij9elhD8CgYAr1K7aM6YZnlHaIL0my37Y
cqYE5/EUaLSng33Rk65krS6k1xFKwRXbq0Nmzln7iWnWA5EMr5WWDKASqJ35niYm
9PIqda0jCDcjTBIbJ9SVmQ8E0I6A7WRrqDc9CLY2JjY8KnB1RC9sJ936AErcKiOj
cudhWiCshs6n9Tmfsw6LJQ==
-----END PRIVATE KEY-----
```

Step 4   Run the following commands:

```
[root@cmx newcert]# ls
cert.crt   cert.pem   private.key
```

```
[root@cmx newcert]# cmxctl node sslmode enable --pem /opt/haproxy/ssl/newcert/cert.pem
enabling ssl
ssl enabled
[root@cmx newcert]#reboot
```

Installing a Third Party Signed Certificate

Procedure

Step 1 Generate the certificate signing request.

Step 2 Run the following commands:

```
[cmxadmin@cmx]$ su -
Password:
[root@cmx]# cd /opt/haproxy/ssl/
[root@cmx]# mkdir newcert
[root@cmx]# cd newcert

[root@cmx newcert]#openssl req -nodes -days 365 -newkey rsa:2048 -keyout
/opt/haproxy/ssl/newcert/private.key -out /opt/haproxy/ssl/newcert/cert.crt
```

Step 3 Get the certificate signed by the third party CA.

Step 4 Create the certificate chain for import into CMX.

The following example shows the format for signed SSL certificate:

```
-----BEGIN RSA PRIVATE KEY----- < Your Private Key
MIIEpAIBAAKCAQEA2gXgEo7ouyBfWwCktcYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...snipped
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- < Your CMX server signed SSL certificate
MIIFEzCCAvugAwIBAgIBFzANBgkqhkiG9w0BAQsFADCBlDELMAkGA1UEBhMCVVMx
...snipped
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < Your intermediate CA certificates
...snipped
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < The root CA certificate that signed your certificate above
MIIGqjCCBJKgAwIBAgIJAPj9p1QMdTgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
...snipped
-----END CERTIFICATE-----
```

```
-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEAuRPbZqm6JlTR6FCvWF8PejHF+HpTTrwgypqty4mviw78gC2G
TGrIYdA2eErpj1UCYVc/0rm5OU68Qr0X2DUm1lukopXgTF3dWtg8FZ77sj8+RN8L
YAaHySHJc9tRF8QUDB8zyHryXSM/5aw1z1F+4DSMP5nVYoZroiM+WXhP3BYFvyHm
nBbgOKZ8Zmln0idJMu8qI53/HfH3pNsuFjR9sCh+jbIEpUh9Jt54jifcFFUY+7Xt
GJ7GVjyCsGKFHWx6EgrCOb4uqS1crEUjO9/vDlp6M559F1hMQRHkAY5sSFDq5qY+
XEPY7mopyQmNBRZxWgOogtQ2fsK1XFDZ4ZBW0QIDAQABAoIBAQCklWv+l+DaRYOF
PHsx8xcoayrKFL4QvmvKwFLdNcvNtb4FnnZXbn5TvX0y7CtXMxmyxowTMOXueH4i
```

O1YBBwNKjKSTkQSt5Kr8Jl8IOyFJGcSeKltLQYNu8YTcaqRqpgvN29GI7wyolrgz
3jjb7HUPnKs7w+lmfHMq9Hx1w/.AAnm/Fb7/sXUww80cdfGFHlYfqBvC5FJKe3N/f
sg5Npjhaqrvs9bsd7MUKu5LjcdUN9nVWU604NWaMJHUQPoHmf3vwNND4l1YDbGS7
Aj8exOW4+2WKYz9c9Ry1qivkIgnneGUvaI3mR4Z0Rc+lJckie+UhfttHxz4DmO4M
pEw5wjIhAoGBAPEQfmDSme8Ur9V6zNaXtcaAL77JozNuSyEzpvSduUf4HLTJBY34
U4V6AWyQR2koSZON2tBbuC8s/D2cas2A1htoD8fflL/dWefoJmNzOTyyjQNKepf0
NfEOvGKQdOpI/DG62ngxbT5zkUspV/qSxdQw9xZoYV7FkPrst+7kv8gLAoGBAMSL
XA7aVSkFmrBDsag6YNsmOaBp8geEAll/N3dazXulIHUCnpUpY//Cgeb+LBrKQmWA
Fuf5gcb7GR4oFmu4jaTpXvKz8eqnsNeDmzVKMoB31wd9QTrYMc+SBuyX3nHldRFF
CXU1UlAj/ujoMz+wYuyE/qtOISZ2FITkZQvjRjoTAoGBALa76QDeRB/uj4eFCeeV
ow5wt0CputPOxJbLf8CoGv5KPwBv7Yz789wXayLvj6JQDs4SVw9gp5LjR+YwPum+
ww6NaID7o9d5JKDd4tO6UWYId0pKV/n9/jHYGMeid23tm3bbDKbV2NjhY/8UvQNN
5TZ/U54hy8W6f7cmYBtwPUyXAoGAC1bS79Ru11gIbaTqKf98OQiCiJu0J/TYwdsS
EyO8+SY0sit9hLOHnmjVX8NIPh9vJzX1nFqLvzQbZd8ANCTInzwLi0sQaO5VyIlC
OhfWxAyl7juuuLtiXExbc+jrH30SfPWTrxxtbEw3V66VzlXZzzV5D98JEJP9aRFY
NxBcq9sCgYBSIZfEKW9DTuPAHfYLToQpDRLM/1sT2Kg9CcASHlj4jmV+7CfJggKY
TQnshZuvArjlYlUCjrSubwt6FYmP+O6hbnHEBHo6RTCc2qnvS7J+GGk8C/CH/iTO
PbXaW7rcUuX6hEFdZQQ8OOJBstnKjZn2sI+OIX+VBrqnDOYWlFwlEA==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIFEjCCAvqgAwIBAgIBGDANBgkqhkiG9w0BAQsFADCBlDELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAk5DMQwwCgYDVQQHEwNSVFAxHDAaBgNVBAoTE0Npsc2NvIFN5c3Rl
bXMsIEluYy4xDDAKBgNVBAsTA1RBQzEbMBkGA1UEAxMSbGludXhsYWIuY29tu
Y29tMSEwHwYJKoZIhvcNAQkBFhzsc2NobWlkdEBjaXNjby5jb20wHhcNMTYwNTA1
MTQ0MDAxWhcNMTcwNTA1MTQ0MDAxWjCBhjELMAkGA1UEBhMCVVMxCzAJBgNVBAgM
Ak5DMRwwGgYDVQQKDBNDaXNjbyBTeXN0ZW1zLCBJbmMuMQwwCgYDVQQLDANUQUMx
GzAZBgNVBAMMEmxhdWdodGVyLmNpc2NvLmNvbTEhMB8GCSqGSIb3DQEJARYScmFt
a3JpczJAY2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
uRPbZqm6JlTR6FCvWF8PejHF+HpTTrwgypqty4mviw78gC2GTGrIYdA2eErpj1UC
YVc/0rm5OU68Qr0X2DUm1lukopXgTF3dWtg8FZ77sj8+RN8LYAaHySHJc9tRF8QU
DB8zyHryXSM/5aw1z1F+4DSMP5nVYoZroiM+WXhP3BYFvyHmnBbgOKZ8Zmln0idJ
Mu8qI53/HfH3pNsuFjR9sCh+jbIEpUh9Jt54jifcFFUY+7XtGJ7GVjyCsGKFHWx6
EgrCOb4uqS1crEUjO9/vDlp6M559F1hMQRHkAY5sSFDq5qY+XEPY7mopyQmNBRZx
WgOogtQ2fsK1XFDZ4ZBW0QIDAQABo3sweTAJBgNVHRMEAjAAMCwGCWCGSAGG+EIB
DQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUeKxp
ACe19Jpz6QuXGALJik41DjcwHwYDVR0jBBgwFoAUUPGERegtBFb+1WJ+1ZLqRpWK
G84wDQYJKoZIhvcNAQELBQADggIBAJzykVSWLvNuFk/Q1PRFU7pdX5z8g5KOaQjo
4erSl48m1WoM7vJNXjqqHD6JdcOMINGeuxElI1Vd7prpARhE+Qj7xSMfDMilzSFy
mKVpTNQzT/9yHytAycVsvbGYJDh8R3jTpxJXWPBcvErE8OuaxkCbePNzQD56KqFC
Sjibw2GgwLJa8GaHZdL0lGQ9djDfsQwriqvphBX9Dkd9qeMPnxYCXVsE4SsbLUWC
n0tasfJ4pcrgRqEi6OBw8zh3twcy6vEBJvp0tA3/z3yPdvG0sZ5x5WCTCCOmLvUE
BswbZusCMQFCHg14wbEoNo/I3GDoqRHzw1j0hA887r4AWnMOeXjkHjA7YxtrSzJ4
cQL5WEXj8di6UqwQA+dNBCLv488huLFEcEL8YjMLV4Z6nfaXzNF2FLJZByaD4/sP
TcZ2BkKS53YKKE7LUaIbUH3ymdfejQuIVabtBnc/of5bw7WODlyBZIhd4MW3eFJK
puoXXxp0xqmS3/VMnefyaVqBz3eV4KXkg0Z6w6KbCXst9aTP+NtSGEBeXgM36TvR
2SIVCwKH/RlDQp+vk1QykQdj6JSMJUrl6fdRAtpAZssMGIT2KsreRVnJ8ig7VAKp
17ES4FZ/7rg87GoUYfmAl+AhvZCCu2SjJBdW6/IO1rHHkB+1UkU+yswY85Ccq7Wj
+9TmdHX8
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIGqjCCBJKgAwIBAgIJAPj9p1QMdTgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCTkMxDDAKBgNVBAcTA1JUUDEcMBoGA1UEChMTQ2lz
Y28gU3lzdGVtcywgSW5jLjEMMAoGA1UECxMDVEFDMRswGQYDVQQDExIsaW51eGxh
Yi5jaXNjby5jb20xITAfBgkqhkiG9w0BCQEWEnNzY2htaWR0QGNpc2NvLmNvbTAe
Fw0xNjA1MDUxMzQ5MTlaFw0xNjA0MzAxMzQ5MTlaMIGUMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTkMxDDAKBgNVBAcTA1JUUDEcMBoGA1UEChMTQ2lzY28gU3lzdGVt
cywgSW5jLjEMMAoGA1UECxMDVEFDMRswGQYDVQQDExIsaW51eGxhYi5jaXNjby5j

b20xITAfBgkqhkiG9w0BCQEWEnNzY2htaWR0QGNpc2NvLmNvbTCCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgoCggIBALDXzffE4YyvCakwDop2gKcfOAOgn96hzbVC
OvVGDNwYE/070u9Rh8Tf4yCX8tknrkN2QnqZVarWgUPYvc0zSVqXiT6bxWkuvGYL
nO+PiXFKAFMlF+BjF0L8Fdm0B+ZowSUlrFwLCX7yOsemn62NfwVHo0MUImJoglF0
JW+8pJrxrfoWG78AgRUsKFi5R4IuTPWV1PSWiD1nDEEkxn1JKNmwtnNC7iAUHWMs
gKK64VBpoSTNWpiyHCD0B4Col2x+R9NNWOQ9X7NnMhtR16AYKm60ElkMYvP1Zjrl
aZFfzkZXLmsxluxjbU9mv4lUhGzeJxbcBUPuvLbM6WoOYp6/lYoSdd5PtfX9Ixim
7zO/uL7w2vyI4+kJYm7HHtFVHuhEcWEhyEdW0JcvT61L68F/iB79WezJd0VbPCel
gFSJFhx5F2jhyYlZq2bbjOdzf0RC+U053W+xfqQUTt17BDnb6n+UvPSDfwDpnKMH
RbZlis0nC7YfqscDnrpBETRPNvNfRsQznoBgqqPWrfJ/RVU+CnjxZB+SiEWhV2ei
Wla6P8iB+MmMBYoHXbk1pBf0BkZEXd2uGk74o7a3rj1MAlzdppoGYAW2hfvYYqNW
kDGOgkHLf1KzawB9gaiWNHo6UujaHZNi/jKL6FQlor+HQ/EggWtflTLl1YBTz4cB
iNlK3wQ7AgMBAAGjgfwwgfkwHQYDVR0OBBYEFFDxhEXoLQRW/tViftWS6kaVihvO
MIHJBgNVHSMEgcEwgb6AFFDxhEXoLQRW/tViftWS6kaVihvOoYGapIGXMIGUMQsw
CQYDVQQGEwJVUzELMAkGA1UECBMCTkMxDDAKBgNVBAcTA1JUUDEcMBoGA1UEChMT
Q2lzY28gU3lzdGVtcywgSW5jLjEMMAoGA1UECxMDVEFDMRswGQYDVQQDExJsaW51
eGxhYi5jaaXNjby5jb20xITAfBgkqhkiG9w0BCQEWEnNzY2htaWR0QGNpc2NvLmNv
bYIJAPj9p1QMdTgoMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggIBAD0R
CmpKKygd3oRip8NaRssHYndwm6t3Add4+BM/wZ5TbNi5POg5JZIDgV2qT6elJIux
dLTTCJcHaoeITWW/CTpYrve+Q3NAPTImmXTX2swN7zVX3GXNoBQWhIuZh4A9YMVb
tAST3O7qCCQq+6NU1LKBjTdnc6qw/VLe2WD9vvhDcq+i5HyHJWJqsTcO8iU8fyTGv
Q1i8MFZ7VPgnr2RGaIki8yCsFG+bSKuiVQgylnQLMKSkqCtWww+eBj1bPr/MecgC
1bO5OJ+id08UalM6KhlRQYY9o5q7lkRIFVgUvHyhsNdvmwSa15kpWLeKqsNrFt5A
jipNPJW4Cf2HLutZZZGGIDNc9kQlD7XyPXlV41n/4uoYuKjea6RgcJYR/lFh0rTo
nUp3LbZkpRQksWrhKfO7BoFOif7s9Ko6YDuOu2o/dzU1XUf937ovNmGqvOPRPrV2
5cUrQKEXeTsGbuxvvxkEFv39BZsefc0tiSMRkpN84FOBoYUkc0zioiURQa8gs6Eo
w5CuB/DH65uxQ2yowV4KVktHA5az5j0ZUoayLX0vOktr54g+z3+li+QN2yfTiOOS
zvz4k6Ylu4ySosg4BdWVmPXbLLkTpb+AEHpK+IZF6I6qMVPU5wz6VMAVKhilaEkN
o1d/c05RYSTy8/SlROa4ms68xqCpQIdaWg10VIDQ
-----END CERTIFICATE-----

Installing the Certificate

Procedure

Step 1   Log in to Cisco Connected Mobile Experiences (Cisco CMX) as cmxadmin user.

Step 2   Run the following command to make a directory on CMX to hold the new certificate: **[root@cmx ~]#mkdir /opt/haproxy/ssl/newcert/**

Step 3   Copy your properly formatted signed certificate to the new directory.

Step 4   Run the following commands on Cisco CMX to ensure that everything is property built: **openssl verify**

```
[root@cmx newcert]#cd /opt/haproxy/ssl/newcert

[root@cmx newcert]#openssl verify -CAfile /opt/haproxy/ssl/newcert/localhost.pem
/opt/haproxy/ssl/newcert/localhost.pem

/opt/haproxy/ssl/newcert/localhost.pem: OK
```

You must get an OK message.

Instructions for CMX build 324: (10.2.2 beta) or 10.2.2 CCO and Later

In CMX 10.2.1-219 there is a bug that will not allow the install to work properly (CSCux30499 Need exact steps in the config guide for certificates). The issue will be fixed in CMX 10.2.2 which will be out May 2016. If there is a business need to continue with CMX 10.2.1-219, please contact the TAC for the workaround.

Procedure

Run the following command:

```
[root@cmx newcert]#cmxctl node sslmode enable --pem /opt/haproxy/ssl/newcert/localhost.pem
enabling ssl
ssl enabled

 [root@cmx newcert]#reboot
```

Adding Users and Managing Roles

Using the **MANAGE** service in Cisco CMX, you can create new users and assign roles to them based on the tasks they have to perform, that is, enabling role-based access control.

The following list displays the types of users:

- Admin users—An admin user can access all the services and functionalities (based on the license type) of Cisco CMX.

- Others—An admin user can create other users and assign roles to them.

The following is a list of roles that can be assigned to users:

- System

- Manage

- Analytics

- Read Only

- Location

- Admin

- ConnectExperience

- Connect

For more information about the creation of users and assignment of roles, see Managing Users.

Using the Cisco CMX Setup Assistant

The Cisco CMX Setup Assistant pop-up helps you through the basic steps before you start using your system. The Cisco CMX Setup Assistant is automatically displayed when you log in to Cisco CMX. To relaunch the Cisco CMX Setup Assistant, click the Help ( )icon.

Supporting Active Clients Version 3 API

Cisco CMX release 10.4 supports new active clients version 3 API under Location REST API. The new Active Clients v3 API allows frequent requests without impacting other services such as location service. The new **Node.js** processes API requests in the API v3.The location service sends the local notifications to the API server and active clients are tracked in the API server memory.

The Active Clients v3 API has its own user ID and password for accessing the REST APIs. Use the **cmxos apiserver** command to define the unique user ID and password. The Cisco CMX web UI username and passwords will not work for API v3.

Note Active Clients v3 API under Location API documentation section includes better parameter testing.

Active Clients Version 2 API has been deprecated in Cisco CMX 10.4 release.

Active Clients v3 API supports these additional parameters:

- mapHierarchy
- manufacturuer
- macAddressSearch
- associated/probing

The following log files are located in the directory /opt/cmx/var/log/apiserver for troubleshooting:

- cmxapiserver.pid—Processes ID file for the top process.
- server.log—Log file for messages and errors
- stdout.log—Standard output messages

Getting APIs

To obtain the following APIs, use the https://*cmx-ip-address* /apidocs/ URL:

- Configuration REST APIs for configuring different aspects of Cisco CMX.
- Location-based REST APIs for finding location-specific details about visitors.
- Analytics-based REST APIs for finding analytical data on visitors.

- Connect-based REST APIs for finding user session information.

- Presence-based REST APIs for finding presence data on visitors.

Changing Time Zones and NTP Server

After the initial CMX configuration, you can change the time, time zone, and NTP server details using the CLI. You can edit the ntp.conf file to change the NTP server. Ensure that you are logged in as root user to change the NTP settings.

To change time zones and NTP server after initial configuration using CLI, perform the following task:

Before you begin

- Ensure that your server has a valid hostname before making any NTP changes. If not, some of the ntp commands will fail, for example, ntpstat.

- Ensure that incoming and outgoing UDP port 123 for NTP communication is open in your configuration setup.

- Ensure to manually edit /etc/ntp.conf as admin user and appropriate time zone is selected using `/opt/cmx/bin/tzselect` before restarting ntpd using **service ntpd restart**.

Procedure

Step 1   To stop all the services on the CMX, run the **cmxctl stop** command.

Step 2   To change the current user to admin root user, run the **su** command.

Step 3   In the /opt/cmx/bin/tzselect path, run the time zone script.

Step 4   To log out from the configuration setup, run the **exit** command.

Step 5   Log in again and verify the time, time zone, and date settings.

Step 6   To restart the services, run the following commands:

- **cmxctl start agent**

- **cmxctl start**