Get Started with Cisco CMX

Getting Started

Introduction to Cisco Connected Mobile Experiences

Cisco Mobility Services Engine (Cisco MSE) acts as a hardware 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.

Cisco CMX helps customers determine the location of devices in their network that can be used for various location based services. The overall location as a platform service from Cisco is known as Cisco Spaces.

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

Note   Cisco CMX supports the Cisco Mobility Express wireless network solution.

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 7 meters, 90% of the time with standard location technologies and +/- 3 meters, 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

- 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.

- 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

For more information, see The Cisco CMX Analytics Service.

- **MANAGE**: This service enables you to manage licenses, users, zones, beacons, and notifications. For more information, see Overview of the Manage Service.

- **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

For more information about Cisco CMX System Messages, see the *System Message Guide for Cisco Connected Mobile Experiences (CMX) Release 10.6.3*, at:

https://www.cisco.com/c/dam/en/us/td/docs/wireless/mse/10-6-3/cmx_syslog/b_cmx_syslog1063.xlsx

Tip   To clean up long queues and long-running processes, we recommend that you schedule a full restart of Cisco CMX once a month during a low activity time, such as late at night or early in the morning. The restart takes approximately 5 minutes to complete.

To restart Cisco CMX services, follow these steps:

1. Enter the **cmxctl stop -a** command.

2. Enter the **cmxctl start -a** command.

Contact Cisco Customer Support (https://www.cisco.com/c/en/us/support/index.html) for the patch file.

Cisco CMX Feature Parity

The following table lists the Cisco CMX feature parity with Cisco Prime Infrastructure and Cisco MSE.

Table 1: Feature Parity

Feature	Cisco CMX-Cisco Prime Infrastructure	Cisco MSE-Cisco Prime Infrastructure
Supported releases	• Cisco CMX Release 10.4 and later • Cisco Prime Infrastructure Release 3.3 and later	• Cisco MSE Release 8.0.x • All Cisco Prime Infrastructure releases
High Availability (HA)	Supported	Supported
RFID tags, wireless connected clients, rogue APs, rogue clients, and interferers	• Wireless associated clients are supported. • Probing clients are supported. • Rogue clients and access points are supported. • Interferers on Cisco Prime Infrastructure Release 3.3 or later is supported.	• RFID tags are displayed. • Wireless associated clients are supported. • Probing clients are supported. • Interferers on Cisco Prime Infrastructure Release 3.2 are supported.

Feature	Cisco CMX-Cisco Prime Infrastructure	Cisco MSE-Cisco Prime Infrastructure
Client history	Not supported. This feature is available on Cisco CMX and Cisco DNA Center Release 1.2 or later.	Supported.
Cisco CMX APIs used by Cisco Prime Infrastructure	• Use the /api/config/v1/version/image API to display the Cisco CMX version. • Use the /api/config/v1/campuses/import API to import a map file to Cisco CMX.	• Use the /api/config/v1/version/image API to display the Cisco CMX version. • Use the /api/config/v1/campuses/import API to import a map file to Cisco CMX.
Cisco Prime Infrastructure performs a Cisco CMX API query when the **Cisco Prime Infrastructure Map** window is displayed.	Supported.	-

Installing Cisco CMX 11.0.1

Run the **cmxos upgrade** command to perform an inline upgrade from Cisco CMX Release 11.0.0 to Cisco CMX Release 11.0.1.

Note Cisco CMX Release 11.0.1 does not support inline upgrade from Cisco CMX Release 10.x.x.

For more information about installing Cisco CMX, see *Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX Release 11.0.0*.

What's New in Cisco CMX Release 11.0.1

This section provides a brief introduction to the new features and enhancements introduced in Cisco CMX Release 11.0.1:

• **AlmaLinux 8.7 Stable upgrade**: Upgraded from AlmaLinux 8.4 to AlmaLinux 8.7 Stable release that includes various features and improvements.

• **FIPS Support**: Cisco CMX Release 11.0.1 has included FIPS recertification.

• **Data migration**: Data migration is supported from Cisco CMX Release 10.6.3-146 to Cisco CMX Release 11.0.1. For more information, see Data Migration.

• **TLS 1.3 support**: The Cisco Network Mobility Services Protocol (NMSP) connection supports TLSv1.1 and TLSv1.2 for backward compatibility. Other TLS connections only support the TLSv1.3 protocol.

• **Customer Success Management Software (CSM) Toolkit support**:

• **Critical issues fixes**: Includes critical bug fixes.

Data Migration

To migrate data from Cisco CMX Release 10.6.3-146 to Cisco CMX Release 11.0.1-129, follow these steps:

Before you begin

Cisco CMX Release 11.0.1 supports data migration from Cisco CMX Release 10.6.3-146 to the latest Cisco CMX Release 11.0.1-129.

Note

- Influx db data is not migrated if you upgrade from Cisco CMX Release 11.0.0-154 to Cisco CMX Release 11.0.1-129.

- VMware ESXi 6.0 is not supported. We recommend that you use ESXi 7.

Procedure

Step 1 On the Cisco CMX server running the image version of Cisco CMX Release 10.6.3-146, run the following commands:

a) To verify the date, run the **cmxos date** command.

b) To modify the date if there is no Network Time Protocol (NTP), run the **cmxos changedate** command.

Step 2 On the Cisco CMX server running the image version of Cisco CMX Release 10.6.3-146, run the following commands:

a) To verify the Cisco CMX Release, run the **cmxctl version** command.

b) Install the patch: cmx-11-migration-readiness-patch. For more information, see *README.txt* text file.

c) To create a backup file on Cisco CMX Release 10.6.3-146, run the **cmxos backup --path /home/cmxadmin --include_onlydatabase,cache,cassandra,floormaps** command.

Step 3 On the Cisco CMX server running the image version of Cisco CMX Release 11.0.0-154, run the following commands:

a) To stop the monit service, run the **cmxos monit stop** command.

b) To stop all Cisco CMX services, run the **cmxctl stop –a** command. This is mandatory as the restore fails during the cache services restart.

c) To restore backup on Cisco CMX Release 11.0.0-154 instance, (before pairing the High Availability), run the **cmxos restore** *--file /home/cmxadmin/cmx_backup.tar.gz –include_onlydatabase,cache,cassandra,floormaps –ignore_licenses* command.

You must replace the *cmx_backup.tar.gz* file with your specific Cisco CMX backup file.

d) Set up Cisco Smart Licensing after you restore the data.

Generate Root Password

In Cisco CMX Release 11.0.0, the root patch is replaced by a token-based root access. With this feature, you can generate a root password that is valid for six hours.

Procedure

Step 1	Log in to the Cisco CMX CLI as cmxadmin user.
Step 2	To generate a root challenge text, run the **cmxctl users get-root-challenge** command.
	The root challenge text is valid for 30 minutes.
Step 3	To get the root login key, open a case with Cisco's Support Services Technical Assistance Center (TAC).
Step 4	To generate a new password, run the **cmxctl users enable-root** command.
Step 5	Enter the token generated by the cloud support team and the new password.
	By default, the root access is disabled within six hours.
Step 6	(Optional) To manually disable the root access login, run the **cmxctl users disable-root** command.

Using the Evaluation License

Cisco CMX ships with a fully functional 120-day evaluation license that is activated after Cisco CMX is installed and started for the first time. The countdown starts when you start Cisco CMX and enable a service.

You must upload a permanent license to Cisco CMX before the evaluation license expires. Two weeks before the evaluation license expires, you will receive a daily alert to obtain a permanent license. If the evaluation license expires, 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.

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

Cisco 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.

The **Licenses** window displays the Cisco CMX licenses and the Cisco Spaces licenses.

Cisco Spaces is a single, scalable, reliable location platform that leverages existing wireless investments to digitize spaces - people and things. There are two licenses for Cisco Spaces, **DNA Spaces SEE** and **DNA Spaces ACT**. We recommend that you upload the **Term** license for Cisco Spaces before the expiry of the evaluation license.

Note   The license file has a .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.

Logging In to the Cisco CMX User Interface

From Cisco CMX 10.5.0 and later versions, SSL mode (https) is the default and recommended mode for enhanced security.

Before you begin

If you have performed a Cisco CMX install or upgrade operation, we recommend that you clear the browser cache before accessing the CMX GUI again.

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. If SSO is enabled in Cisco CMX, **Sign in with SSO** option is displayed. For more information about configuring SSO, see Configuring SSO Authentication in Cisco CMX, on page 8.

Step 3   Enter your username and password.

Note	• Cisco CMX GUI displays the last login details of the logged in GUI user if user has admin privileges. Cisco CMX CLI displays the last logged in cmxadmin user

As an **admin** user, click on the GUI header to navigate to **Manage > Users** > table to view additional details.

For a non-admin user, we recommend that you contact Cisco CMX admin user to view additional details such as IP Address.

- The default username is admin and the default password is admin.

- The default global session timeout for Cisco CMX GUI is 30 minutes. This is the absolute session timeout which works from the session establishment time to the session end time irrespective of whether the session remain active on Cisco CMX.

- If a Cisco CMX CLI or GUI user account is inactive for 60 days or more, the account is locked. A Cisco CMX admin user (cmxadmin) can unlock the account and use the applicable command:

    - **cmxctl users unlock gui <userID>** command to unlock the user's Cisco CMX GUI account.

    - **cmxctl users unlock cli <userID>** command to unlock the user's Cisco CMX CLI account.

If the Cisco CMX admin user account is locked out, the admin user must connect directly to the console and use the applicable command: **cmxctl users unlock gui <userID>** or **cmxctl users unlock cli <userID>**.

- You can use the **cmxctl config auth settings** command to set the expiration period for the password. The default expiration period is 9999 days.

Configuring SSO Authentication in Cisco CMX

Cisco CMX Release 10.6.2 supports Single Sign-On (SSO) for authenticating users to Cisco CMX. SSO authentication method uses SAML2.0 protocol binding. To take advantage of SSO, CMX users should have an Identity Provider (IDP) configured that supports SAML2.0.

Note	• By default, SSO is disabled in Cisco CMX. If SSO is disabled, you must provide the login credentials (username and password) to log in to Cisco CMX.
	• While using the SSO authentication method, Cisco CMX sends URLs with IP address instead of hostname even if a third party certificate is installed.

To use SSO in Cisco CMX, you must first configure a service provider (SP) and IDP with all the required information and then enable SSO on Cisco CMX. As a cmxadmin user, you need to run the **cmxctl config sso** command to manage SSO configurations. When SSO is enbaled, Cisco CMX welcome window is displayed with the **Sign In with SSO** option.

Users table under **Manage** tab displays whether the logged in Cisco CMX user is an SSO user or not. As an admin, log in to Cisco CMX when SSO is disabled and change the user role, if required.

The following is a list of prerequistes for configuring SSO:

- Cisco CMX integrated with SAML 2.0 framework

- IDP with SAML 2.0 support

- Cisco CMX with proxy confgured to reach IDP endpoint

The following is a list of limitations while configuring SSO:

- Only a cmxadmin user can manage SSO configurations. Ensure that you disable SSO before you log in to Cisco CMX.

- A user with cmxadmin or admin role is exempted from the SSO authentication while logging in to Cisco CMX.

- Ensure that you configure the SSO settings everytime when you install or generate a new server certificate on Cisco CMX.

- SSO authentication is not applicable for Web Installer, SSH login, and HA 4242 port login and for API Server user management and API Docs.

We recommend that you run the commands in the order specified below:

Procedure

Step 1	To setup proxy settings on Cisco CMX, run the following command: **cmxos sysproxy**
Step 2	To restart agent, run the following command: **cmxctl agent restart**
Step 3	To restart Cisco CMX services, run the following commands: - **cmxctl stop** - **cmxctl start**
Step 4	To configure SSO on Cisco CMX, run the following command: **cmxctl config sso configure**

Note

- After you run this command, you need to confirm if you want to perform a check on Cisco CMX da users with username assigned to them. You will also get a prompt to confirm what role to assign to a a user does not exist in Cisco CMX or if database lookup for a role is not allowed.

- Ensure that you have IDP metadata XML file available to download on Cisco CMX. You can downl metadata XML using the download link available in all standard identitiy provider service.

  The most common IDP is Active Directory Federation Services (ADFS). For ADFS, you can downl metadata file from https://%3Cadfs-server-name%3E/FederationMetadata/2007-06/FederationMeta

- If you are unable to download the IDP file, you must provide related information such as SSO endpo the IDP to successfully execute the **cmxctl config sso configure** command.

- To configure IDP, you need to extract the details such as **entityID=**, **Location=**, and **Binding=** fro metadata file.

- The type of **NameIDFormat** used by Cisco CMX is email Address. Cisco CMX will use **emailAddr** in SAML resposne.

- Cisco CMX requires firstname, lastname, email address field information from IDP in SAML respo CMX will extract the username from email address by stripping the @domain part from email addr example, if email address is xyz@abc.com, Cisco CMX will strip @abc.com out and use **xyz** as use SSO user.

- Ensure that session timeout is configured on IDP. When you configure IDP, ensure that the value fo **Signature Algorithm** is set as **SHA1**. The default on ADFS is **SHA256** and change it to **SHA1** when ADFS.

  We recommend that you remove the **X509 Cert parsed** from SP Metadata File on ADFS as it will failure of SAML response generation.

- If session timeout is not configured and a user already logged in to Cisco CMX logs out and logs in credentials are not prompted and user is logged in automatically. This is because the IDP session is st not yet expired. As a work around, you will have to close the browser window every time you logou CMX.

- For High Availability configuration, both Primary and Secondary server needs to be configured sepe the **cmxctl config sso configure** command as both will have individual X509 certificate.

The following is a sample of SP metadata XML file:

```
<?xml version="1.0"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:
metadata" validUntil="2019-08-15T20:23:26Z" cacheDuration="PT604800S"
entityID="https://10.30.114.196/login/" ID="ONELOGIN_78ca24a0-8e9c-4fc9-b258-688e073540
<md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing"><ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig
<ds:X509Data><ds:X509Certificate>MIIFhDCCA2ygAwIBAgIEXUiZADANBgkqhkiG9w0BAQsFADBMMQswCQ
UzELMAkGA1UECAwCQ0ExETAPBgNVBAcMCFNhbiBKb3NlMQwwCgYDVQQKDANNU0Ux
DzANBgNVBAMMBlJvb3RDQTAeFw0xOTA4MDUyMTAwNDhaFw0yMjA4MDQyMTAwNDha
ME8xCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTERMA8GA1UEBwwIU2FuIEpvc2Ux
DDAKBgNVBAoMA01TRTESMBAGA1UEAwwJU2VydmVyQ3J0MIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCgKCAgEAtC0tqHb6eDG0P6KeyUjvmwfBTAt6yleSLoVbfNGz
X5j6/WKQkgMYQI6V40Ap9iKp9aSZ62wNydHoZSdt2icSQo+8Z3bfzn2ToWuiHbT4
LrD9fJ1WdlZW6Tu/U8KBy+sS4vL60GppjCJ0G5h6igPCYajaIaQd0eo9IWBenQXv
f/MNUG6wIa2ivstjWQsUv26uLhrgrIbZ7akZb/OKxcaFSyYOS17ueXqUrM27pKL2
IVFdvXBGJgFoiISaTcmYnAMJptYskJuAkc6GtqEPtgJKp0UYm0t/h/tgT2JEsvn8
v9yrmY8vicDJY40+OPLaghs0EMYc+8LoC/14YMYMkZhfGGVOVjQar+KEBlVfk1EA
mAKOgMTYk8u7+d/KvXoO7RWlk3zIYVZX9aJMrPxQAp9/YC2wwyoelOCAiaA4pxcU
yWw+0E7UBcU27fPSZO7puROk5bIhQ/gx6Sv4B5Rg0df2xjZeVsQq6G/r7TiJsWcH
```

```
THwGQXO92H/3E5s4u0L7TXI45vL0a2qGHReM6dtxq/hiFSW/AkDu2YyhmdZmwm5f
TE+GLSPqJgzWMrHXCdl+glliDQoaFvN0CorgayhKIKWKjZwvUKUCGb7ZA9OHS40V
d7uRBZlu66bxB19/gdWVjPZa/iiYfUPPKVu/wssdGUlvLSqQupwFEEWgYShfhkba
9jsCAwEAAaNrMGkwCQYDVR0TBAIwADAwBgNVHREEKTAnggxjbXgtdm1kZXYzMDaC
F2RhdGFiYXNlLnNlcnZpY2UuY29uc3VsMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggr
BgEFBQcDAjALBgNVHQ8EBAMCA6gwDQYJKoZIhvcNAQELBQADggIBAEPWA/9TlpnY
A6CNKlT2qSQrULaIyiaDQbkMjxTw0DoX/RsTreKX7CXCgk9jcLAkbU/zUBcUmC5b
PUMM1xJHpMWMZOWIWknPBvAGQ1ODePEj8Lejo8MwUVJKjSAfvoydLsgewyIXPlI3
eiVWkOgmNRmikq5N6Cn6FVCeL+pZF0COUvOXIs7frvB3hRGep4KujygPm732DKsH
Nwc9B8T7U2u/y1+U+uGzEa4DTp67Tih2O3t8nAEVD4mcBP9J6/c6lCFvQZhUhDma
+2qqhTttFyA3G6qEvkkx9z5B0Nd64quZKONENajR0OaFOkOotiSGLljQOKz/1dvE
iXos1PHVhZBnrkXejHW/Q/MwT9GIYehn6yKyHt1e0L2rj16ZHxUZd0Idm/ps2zTb
R3yM6DPZaCsgvybn2cIa7Vbqq54wBRDykGQv5nBib3CRKiDPpP38/z8nx1npIw6V
6L3pZscFaN/8fFB/UhK39OLUPfCp2RDgCWwrOv5u0B3JIb9gz5CGo8cb36DMghmw
6IilTE1ans4y0o4LJfUaljCHGWMCfIfKXu/3oPWSL0ogd+pgSRV8dDE0jhxfpu5e
4MwYYgLHJ3SfUDYvxmf1LaXU4v+OAWHJyE0Is5YayHyXuKxxshdxCjxA2CV5gOU6
EhYUqiDa/0YqCNGm7SKGzmkDC1ovMQmd
</ds:X509Certificate></ds:X509Data></ds:KeyInfo></md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://10.30.114.196/api/config/v1/ssoVerify" index="1"/>
</md:SPSSODescriptor></md:EntityDescriptor>
```

The following is a sample of IDP metadata XML file:

```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://app.onelogin.com/saml/metadata/dc4dfb68-3795-4d7a-9d2e-100b128e31cc">
  <IDPSSODescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIID1TCCAr2gAwIBAgIUKkG/l8NwhjuWBKXS/
C3EmKJH3sEwDQYJKoZIhvcNAQEF
BQAwQzEOMAwGA1UECgwFQ2lzY28xFTATBgNVBAsMDE9uZUxvZ2luIElkUDEaMBgG
A1UEAwwRT25lTG9naW4gQWNjb3VudCAwHhcNMTkwODA0MDA0MjI5WhcNMjQwODA0
MDA0MjI5WjBDMQ4wDAYDVQQKDAVDaXNjbzEVMBMGA1UECwwMT25lTG9naW4gSWRQ
MRowGAYDVQQDDBFPbmVMb2dpbiBBY2NvdW50IDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAK8KoxkPZ3Ew60SDtcSMI6PqSmnJt9vZTNElK4D6MllWKNmv
N4luXn2xpI/A3lbgWjGn2a3r31LakTinPQGAtwAdjxmUvRUz8VN/HkdOLg5hIA0e
qY/M+fk/hIn7ggjjVJr/pH0OyBFwJkOs6XLsnj8EOxoIcjseLtudLSL88NnNUukU
eNYSctgQtHb8UgRO6DBcHrH1Bl/K8a8BztOc5XSxTBYF87FNT0xJsd50LZFNzQ3Z
wuo0rpmSocCeNLwRLO0zzmVQBha3FurcTYei3t8ZUtUHHkEKywnvQLkMQo6ub1fF
w11ojLy0LlSIN5GJRDWkV2ZeWE4D2x11KizBfk8CAwEAAaOBwDCBvTAMBgNVHRMB
Af8EAjAAMB0GA1UdDgQWBBTYybqOQGCjZ+zR/pCdGdhqgwVACDB+BgNVHSMEdzB1
gBTYybqOQGCjZ+zR/pCdGdhqgwVACKFHpEUwQzEOMAwGA1UECgwFQ2lzY28xFTAT
BgNVBAsMDE9uZUxvZ2luIElkUDEaMBgGA1UEAwwRT25lTG9naW4gQWNjb3VudCCC
FCpBv5fDcIY7lgSl0vwtxJiiR97BMA4GA1UdDwEB/wQEAwIHgDANBgkqhkiG9w0B
AQUFAAOCAQEAWaY2Izz53TmO2oZGWszAef8y4G+GO0oyNnEoytKA+tT0vKoOK4Sh
hD0/GGl8sXuwCfhHCc7XMTrwHLdgkfhTqSO8tG4w/9XrDUTVPjI0eQan6e+0EyGq
CvzIe3/5Dlh0PDjybn5ar8Q3EmXEAwepiQYvUSeMkwl7p2uJQ2KGGG+k4yrphtmv
iyUI1LDQ+cHvIC/QMqpGJzM76cWSoSPKGjTjHmS5lKUqgTnnfcnpTwYFUG/R/DoR
Fw50/HSAxHM+w62STDBx5kdMGimiggd8L77JMNacCUCDX0pXq1be2Zzq9pFeaQp2
2qokyrcWNGB2tNhvleAap19UwC8ug4vfSA==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://samplecmx-dev.onelogin.com/trust/saml2/http-redirect/slo/968970"/>

        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDForma

    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://samplecmx-dev.onelogin.com/trust/saml2/http-redirect/sso/968970"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://samplecmx-dev.onelogin.com/trust/saml2/http-post/sso/968970"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://samplecmx-dev.onelogin.com/trust/saml2/soap/sso/968970"/>
  </IDPSSODescriptor>
</EntityDescriptor>
```

Step 5 To generate SP metadata file, run the following command:

cmxctl config sso generate

Use the generated file to provide the SP information required by your IDP.

Step 6 To enable SSO on Cisco CMX, run the following command:

cmxctl config sso enable

Note We recommend that you run this command after SP and IDP configurations are completed.

Step 7 (Optional) To verify the SSO authentication status on Cisco CMX, run the following command:

cmxctl config sso status

Step 8 Log in to Cisco CMX GUI.

Step 9   Click **Sign in with SSO**. The IDP login window is displayed.

Step 10   Enter the credentials and log in to Cisco CMX.

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.

Note   Cisco CMX reserves the map elements name for campus name as **Campus**, building name as **Building**, floor name as **Floor** and zone name as **Zone** for processing the heterarchy information. To avoid conflict with the maps coming from Cisco Prime Infrastructure or Cisco DNA Center, ensure that none of these reserved names are used in the Maps elements. If this recommendation is not followed, maps on Cisco CMX may not function well and you will see the campus, building, floor hierarchy incorrectly from the parent child relationship.

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 UID in the import map file, Cisco CMX performs a map sync operation under this campus if the override option is set to **Yes**. For more information about importing maps, see Importing Maps and Controllers into Cisco CMX.

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

- Cisco CMX does not support auto-synchronization of map updates from Cisco Prime Infrastructure. We recommend that you perform a manual synchronization in Cisco CMX to get the latest map updates from Cisco Prime Infrastructure.

- After upgrading to Cisco CMX Release 10.6.3, the Cisco Prime Infrastructure stops displaying clients on the Cisco Prime Infrastructure map. This is due to the deprecation of V1 and V2 client API calls in Cisco CMX Release 10.6.3. Cisco Prime Infrastructure Release 3.8 and older versions use V1and V2 API calls to CMA to get the client information and hence it fails. To work around this issue, in the Cisco Prime Infrastructure Release 3.9, there is an option to specify the Cisco CMX V3 API credentials while adding Cisco CMX in Cisco Prime Infrastructure and thus Cisco CMX Release 10.6.3 works with Cisco Prime Infrastructure Release 3.9.

Adding Controllers

You can add Wireless Controller using CLI or the CMX user interface. If you want to import controllers to Cisco CMX from Prime Infrastructure for:

- **AireOS**: Provide SNMP RW credentials for the AireOS WLCs after you import them to successfully add them to Cisco CMX.

- **Catalyst 9800**: Provide SSH credentials and enable password details.

Note Otherwise, controllers will display in yellow color indicating that SNMP or SSH credentials are missing. Such controllers may not have the NMSP connection active.

When the SNMP details are not correct, SNMP Timeout on controller alert will be generated.

Ensure that port **16113** is opened on the Controller, so that Cisco CMX can establish the TLS connection (NMSP connection) to the controller.

To add controllers 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

To add controllers using Cisco CMX UI, see Importing Maps and Controllers into Cisco CMX.

Note	• Cisco CMX does not support Cisco Catalyst 9800 Series Wireless Controllers with special characters > or # in the message-of-the-day (MOTD) banner.
	• After adding controllers, 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 an 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. For more information, see Understanding the Controllers Table.

Enabling or Disabling Cisco CMX Services

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

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

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

Installing Certificates in Cisco CMX

Cisco CMX requires certificates for serving the user interface over SSL/TLS and for other secure connections.

When certificates are imported, there is a validity check that verifies the start date and end date. If the dates are not within the range or if the certificates are going to expire soon (withhin 30 days), UI alarms and audit log messages are generated.

There are two options to install certificates – install self-signed certificates or import external CA-signed certificates. Following sections describes these 2 options in detail.

Note CMX Certificate is used for both Server and Client. Hence the Certificate Signing Request (CSR) contains *Extended Key Usage* as follows:

- TLS Web Server Authentication

- TLS Web Client Authentication

We recommend that while sending the CSR to Certificate Authority (CA), ensure that the signed certificate includes both *TLS Web Server Authentication* and *TLS Web Client Authentication* as in the CSR.

If the signed server certificate is missing *TLS Web Client Authentication* values in Extended Key Usage extension of the certificate, then certificate will get imported successfully but CMX services will fail to start and eventually crash.

If the signed certificate has both *TLS Web Server Authentication* and *TLS Web Client Authentication* values in Extended Key Usage extension, then server certificate will get imported successfully and all CMX services will start successfully.

Installing a Self-Signed Certificate

To use self-signed certificate in Cisco CMX, follow these steps.

Procedure

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

Step 2 Run the following commands:

a) To clear certificates, run the **cmxctl config certs clear** command.

```
[cmxadmin@cmx]# cmxctl config certs clear
Certificates cleared successfully
```

b) To install new certificates, run the **cmxctl config certs installnewcerts** command.

```
[cmxadmin@cmx]# cmxctl config certs installnewcerts
Keytype is RSA, generating RSA key with length  4096
Generating RSA private key, 4096 bit long modulus
.........................
.................
e is 65537 (0x10001)
Generating RSA private key, 4096 bit long modulus
...
......
e is 65537 (0x10001)
Signature ok
subject=/C=US/ST=CA/L=San Jose/O=MSE/CN=ServerCrt
Getting CA Private Key
Validation of server certificate is successful
Certificates are valid.
New self-signed certificates installed successfully.
To apply these certificate changes, CMX Services will be restarted now.
Please press Enter to continue.
```

Step 3 Press **Enter** to restart the Cisco CMX services.

Step 4   To view the installed certificates, run the **cmxctl config certs show** command.

Installing a CA-Signed Certificate

If you want to get Cisco CMX server certificates signed by an external Certificate Authority (CA), follow the below steps:

Procedure

Step 1   To clear current certificates, run the **cmxctl config certs clear** command.

Step 2   To generate Certificate Signing Request (CSR), run the **cmxctl config certs createcsr** command.

    a) Provide the details for CSR such as Country, State, City, Company Name, and Org Unit Name.

    b) Enter hostname of your Cisco CMX system as the Common Name.

    c) Ignore the remaining fields such as email address, challenge password and optional company name as blank if you wish.

```
[cmxadmin@server]# cmxctl config certs createcsr
Keytype is RSA, so generating RSA key with length  4096
Generating RSA private key, 4096 bit long modulus
..............................
.....................
e is 65537 (0x10001)
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) [AU]:US
State or Province Name (full name) [Some-State]:Your State
Locality Name (eg, city) []:Your City
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Your Company Name
Organizational Unit Name (eg, section) []:Your Org Unit Name
Common Name (e.g. server FQDN or YOUR name) []:hostname
Email Address []: email@yourco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
The CSR is stored in : /opt/cmx/srv/certs/cmxservercsr.pem
The Private key is stored in: /opt/cmx/srv/certs/cmxserverkey.pem
CSR created successfully.
```

Step 3   SCP the CSR and the private key files to another system.

The following example shows how to scp the key files to another system:

```
[cmxadmin@server]# scp /opt/cmx/srv/certs/cmxservercsr.pem root@192.0.2.1:/root
root@192.0.2.1's password:
cmxservercsr. 100% 1825     1.5MB/s   00:00
[cmxadmin@server]# scp /opt/cmx/srv/certs/cmxserverkey.pem root@192.0.2.1:/root
root@192.0.2.1's password:
cmxserverkey.pem    100% 3243     2.7MB/s   00:00
```

Step 4   Send the CSR file to the CA who is going to sign your Cisco CMX certificate.

Step 5   Once the CA has signed your CMX server certificate, you will receive 2 certificates files – *CMX server certificate* and *CA's own certificate chain*.

> **Note**   Ensure that both files are in PEM format. If the signing CA is an intermediate CA, ensure that you have certificate of the CA who signed that intermediate CA's certificate and all the way up to Root CA. Ensure that all the certificates in this chain are in PEM format and are concatenated into a single file.

Step 6   Combine the private key (from step 2) with signed CMX server certificates (from CA) into a single file and save it as a .pem file. To combine private key and signed server certificate, copy and paste the signed certificate and private key into a text editor.

The following example shows the format of the final certificate.

```
-----BEGIN RSA PRIVATE KEY-----               < Your Private Key
MIIEpAIBAAKCAQEA2gXgEo7ouyBfWwCktcYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----                    < Your CMX server signed certificate
MIIFEzCCAvugAwIBAgIBFzANBgkqhkiG9w0BAQsFADCBlDELMAkGA1UEBhMCVVMx
...
-----END CERTIFICATE-----
```

> **Note**   On a Linux system, use **cat** command to combine 2 files and redirect it to final .pem file.
>
> **cat cmxserverkey.pem cmxsignedcert.pem > key-cert.pem**

Step 7   SCP the CA certificate file (from step 5) and key-certificate files (from step 6) to Cisco CMX.

The following example shows how to SCP the certificate files.

```
[cmxadmin@server ~]$ scp root@192.0.2.1:/root/key-cert.pem /home/cmxadmin
key-cert.pem              100% 3243    2.3MB/s    00:00
```

Step 8   On Cisco CMX server, run the **cmxctl config certs clear** command to clear or remove any old or stale certificate files.

Step 9   On Cisco CMX server, run the **cmxctl config certs importcacert** command to import CA certificate.

Step 10   Enter a password and repeat it for all the other password prompts, when prompted for password.

```
[cmxadmin@server]# cmxctl config certs importcacert ca.crt

Importing CA certificate.....

Enter Export Password:
Verifying - Enter Export Password:
Enter Import Password:

No CRL URI found. Skipping CRL download.
Import CA Certificate successful
0
```

Step 11   To import server certificate and private key (combined into single file), run the **cmxctl config certs importservercert** command.

Step 12   Select a password and repeat it for all the password prompts.

```
[cmxadmin@cmx]# cmxctl config certs importservercert key-cert.pem

Importing Server certificate.....
```

```
Successfully transferred the file
Enter Export Password:
Verifying - Enter Export Password:
Enter Import Password:
Private key present in the file: /home/cmxadmin/key-cert.pem
Enter Import Password:

No CRL URI found. Skipping CRL download.
Validation of server certificate is successful
Import Server Certificate successful
Restart CMX services for the changes to take effect.
Server certificate imported successfully.


To apply these certificate changes, CMX Services will be restarted now.
Please press Enter to continue.
```

Step 13   Press **Enter** to restart the Cisco CMX services.

Step 14   To view the installed certificates after Cisco CMX services is restarted, run the **cmxctl config certs show** command.

Generating a CSR for Third-Party Certificate and Installing on Cisco CMX

You can generate a Certificate Signing Request (CSR) to get a third-party certificate and download a chained certificate to Cisco CMX.

Procedure

Step 1   Connect to Cisco CMX CLI.

Step 2   Access as root and go to the certificate directory.

Step 3   Create a folder for the CSR and the key file.

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

Note   The default directory for certificates on Cisco CMX is /opt/haproxy/ssl/.

Step 4   Generate the CSR and key file.

```
[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
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]:MX
State or Province Name (full name) []:Tlaxcala
Locality Name (eg, city) [Default City]:Tlaxcala
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
```

Step 5   Sign the CSR by the third-party.

Step 6   To get the certificate from Cisco CMX and sent it to the third-party, run the **cat** command to open the CSR.

Step 7   Copy and paste the output into a *.txt* file or change the extension based on the requirements of the third-party, for example,

```
[root@cmx newcert]# cat cert.crt
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCAbkCAQAwgYsxCzAJBgNVBAYTAk1YMREwDwYDVQQIDAhUbGF4Y2FsYTER
MA8GA1UEBwwIVGxheGNhbGExDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANUQUMx
GDAWBgNVBAMMD2NteC5leGFtcGxlLmNvbTEeMBwGCSqGSIb3DQEJARYPY214QGV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2YybDkDR
vRSwD19EVaJehsNjG9Cyo3vQPOPcAAdgjFBpUHMt8QNgn6YFdHYZdpKaRTJXhztm
fa/7Nevb1IP/pSBgYRxHXQEhl9Gj4DT0gT2T+AZ8j3J9KMSe8Bakj4qY8Ua7GCdC
A62NzVcDxDM83gUD92oGbxOF9VFE2hiRvCQc+d6gBRuTOXxtyLBAtcL3hkiOEQx7
sDA55CwZU7ysMdWHUBn4AglzI1gPyzlmT3dwR0gfOSYN4j5+H0nrYtrPBZSUbZaa
8pGXVu7sFtV8bahgtnYiCUtiz9J+k5V9DBjqpSzYzb3+KxeAA+g0iV3J1VzsLNt7
mVocT9oPaOEI8wIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAI6Q/A4zTfrWP2uS
xtN8X6p6aP8guU0bTWhGEMBEgBQd0bBWYdhxaItGt1a1tdNcIGLACeMPuk7WpsiH
rUs5kiIjlAc2/ANBao6/nlv56vhGUx0dOq0fk/glbrKL+a8Lx9ixtee77aPZ1xVD
A/n3FdNdSIidWH0M4q8JunxbT33vM9h8H6oqe/JI3BDnw4tRnkYaGWJsyWUlPCuO
TWPMagMkntv0JaEOHLg4/JZyVSdDiTnmb/U8cEH2RrcUP8iwjykDpb/V4tb4VtgM
7+9HKxQRQHq5Qji8/QyMG6ctoD+B7k6UpzXvi5FpvqGQWwXJNC52suAt0QeeZj1J
rpudLUs=
-----END CERTIFICATE REQUEST-----
[root@cmx newcert]#
```

Step 8   Create the certificate chain to import into Cisco CMX.

Step 9   To create the final certificate, copy and paste the signed certificate into a *.txt* file with the private key, intermediate certificate, and root certificate.

Step 10   Save the certificate as a **.pem** file. This following example shows the format of the final certificate:

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

Step 11   To transfer the final certificate into Cisco CMX from your computer, open your SFTP application and connect to Cisco CMX with the admin credentials.

Step 12   Drag and drop the chained certificate to the folder `/home/cmxadmin/`.

> **Note**   The default directory when you open a SFTP connection to Cisco CMX is `/home/cmxadmin/`.

Step 13 Change the permission of the final certificate and owner.

Step 14 Move the certificate to the folder that contains the private key, for example,

```
[root@cmx ~]# cd /home/cmxadmin/
[root@cmx cmxadmin]# chmod 775 final.pem
[root@cmx cmxadmin]# chown cmx:cmx final.pem
[root@cmx cmxadmin]# mv final.pem /opt/haproxy/ssl/newcert/
[root@cmx cmxadmin]# cd /opt/haproxy/ssl/newcert/
[root@cmx newcert]# ls -la
total 16
drwxr-xr-x 2 root root 4096 Apr 25 12:30 .
drwxr-xr-x 4 cmx  cmx  4096 Apr 25 09:25 ..
-rw-r--r-- 1 root root 1054 Apr 25 11:01 cert.crt
-rwxrwxr-x 1 cmx  cmx     0 Apr 25 12:29 final.pem
-rw-r--r-- 1 root root 1708 Apr 25 11:01 private.key
[root@cmx newcert]#
```

Step 15 Ensure that everything is properly built and you receive an `OK` message.

```
[root@cmx newcert]#openssl verify -CAfile /opt/haproxy/ssl/newcert/final.pem
/opt/haproxy/ssl/newcert/final.pem
/opt/haproxy/ssl/newcert/final.pem: OK
```

Step 16 Install the final certificate and reboot Cisco CMX.

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

[root@cmx newcert]#reboot
```

Step 17 (Optional). If you run Cisco CMX 10.3.1 or above, you might encounter the bug CSCvh21464: CMX WEBUI doesnt use the installed self signed or third party certificate.

This bug prevents Cisco CMX to update the certificate path. To work around this issue, create two soft-links to point to the new certificate and private key, and reload Cisco CMX.

The following example shows how to workaround this issue:

```
[root@cmx ~]# cd /opt/haproxy/ssl/
[root@cmx ssl]# mkdir backup
[root@cmx ssl]# mv host.pem backup/
[root@cmx ssl]# mv host.key backup/
[root@cmx ssl]# ln -s /opt/haproxy/ssl/newcert/final.pem host.pem
[root@cmx ssl]# ln -s /opt/haproxy/ssl/newcert/private.key host.key
[root@cmx ssl]#
[root@cmx ssl]# ls -la
total 16
drwxr-xr-x 4 cmx  cmx  4096 Apr 25 12:59 .
drwxr-xr-x 6 cmx  cmx  4096 Mar 31  2017 ..
lrwxrwxrwx 1 root root   36 Mar 26 09:58 host.key -> /opt/haproxy/ssl/newcert/private.key
lrwxrwxrwx 1 root root   38 Mar 26 09:58 host.pem -> /opt/haproxy/ssl/newcert/final.pem
drwxr-xr-x 2 root root 4096 Apr 25 12:30 newcert
[root@cmx ssl]#
[root@cmx ssl]# reboot
```

Step 18 Open the Cisco CMX GUI.

Step 19 To open the certificate, click the **Secure** tab next to the URL and review the details.
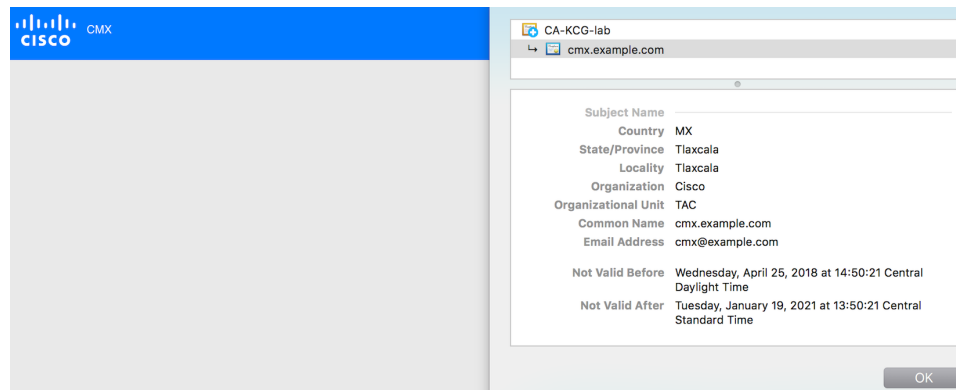
OCSP Support for Certificates

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of certificates. OCSP is newer, better, and faster way to validate certificate revocations. OCSP does not require special configuration.

Cisco CMX Release 10.6.1 provides OCSP and OCSP Stapling support. OCSP stapling cron job is scheduled to run once a day and update haproxy with OCSP response (without need of restart). OCSP feature, OCSP validation and stapling gets triggered automatically when the server certificate being installed/imported contains OCSP URI.

If the server certificate does not contain OCSP URI, then OCSP feature (OCSP cron job) is not triggered.

Wildcard Certificate Support for Cisco CMX

Cisco CMX supports wildcard characters in CommonName (CN) and SubjectAlternativeName (SAN). Certificate Signing Request (CSR) can be generated with wildcards in both these fields of the CSR.

Installing a CA-Signed Certificate for High Availability in Cisco CMX

You must install CA-signed certificates seperately on primary and secondary servers for High Availability (HA) in Cisco CMX.

Before you begin

Ensure that the High Availability pair is not created. If HA is already paired, break the pair and proceed to install the CA-signed certificate.

Procedure

Step 1 Install CA-signed certificates on primary server.

a) To clear current certificates, run the **cmxctl config certs clear** command.

b) To generate Certificate Signing Request (CSR), run the **cmxctl config certs createcsr** command

c) On Cisco CMX server, run the **cmxctl config certs importcacert** command to import CA certificate.

d) To import server certificate and private key (combined into single file), run the **cmxctl config certs importservercert** command.

Note   For more information, see Installing a CA-Signed Certificate, on page 18.

Step 2   Install CA-signed certificates on secondary server. The CA-signed certificate installation process is the same as primary server. However, you just consider the below limitations:

> **Note**
> - If **Secondary CMX** is selected during the initial web installation, then entire CMX services are not installed and the **cmxctl config certs** commands are not available to install CA-signed certificates. As a workaround, use the **cmxos seccerts** commands to clear, create a CSR, import a CA certificate, or import a server certificate. The commands are exactly same as corresponding keyword options under the **cmxctl config certs** command.
> - If Cisco CMX was installed as primary server and then converted to a secondary server using the **cmxha secondary convert** command, use the cmxctl config certs command to install the secondary server certificates.
> - Ensure that both primary and secondary certificates are signed by the same Certification Authority.

After certificates are successfully installed on both primary and secondary servers, you must restart the CMX services.

Step 3   Press **Enter** to restart the Cisco CMX services.

Step 4   Enable HA pairing.

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

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.

REST APIs Version 3 Support in Cisco CMX

Prior to Cisco CMX Release 10.6.3, V3 API support was available for wireless clients only. In Cisco CMX Release 10.6.3, REST API V3 support is extended to the following additional devices:

- Wi-Fi Tags

- Rogue Clients

- Rogue Access Points (AP)

- Interferers

> ✎
>
> **Note** Note that BLE tags tracking is excluded from the V3 APIs. The BLE tags tracking support is not available from Cisco CMX Release 10.6.3 onwards.

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.

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

Note

• The apiserver must be running on Cisco CMX before the API call is initiated.

• For support in using APIs, including the GitHub version of API Version 3, contact the Cisco DevNet Community at: https://developer.cisco.com/site/cmx-mobility-services/.

Restricted CLI

In Cisco CMX, Linux commands are restricted to prevent unauthorized users from inadvertently modifying the system configuration. This is to control access to the Cisco CMX so that users can be prevented from running the commands that a normal user should never run under normal operations or standard troubleshooting situations. Also, the restricted access prevents users from modifying the system configuration.

The following table lists the commands allowed in the Restricted CLI.

Table 2: Linux Commands Allowed in the Restricted CLI

Command	Description
cat	Prints file contents.
cp	Copies file.
df	Prints the file system disk space usage.
du	Prints the file space usage.
grep	Prints the lines matching a pattern.
ifconfig	Displays the network interface configuration.
ls	Lists the directory contents.
nslookup	Queries the internet name servers.

Command	Description
passwd	Changes the cmxadmin password.
ping	Sends Internet Control Message Protocol (ICMP) echo requests to network device.
pwd	Prints the current or working directory.
route	Displays the routing table.
rm	Removes the files.
scp	Secures the remote copy files.
sftp	Secures file transfer.
ssh	Use Secure Shell (SSH) to connect with the client.
tail	Outputs the last part of a file.
top	Displays the Linux process.
wget	Network downloader

Encrypting Cisco CMX Connection to Remote Syslog Server Using IPSec Protocol

To enable IPSec on Cisco CMX, follow the below steps:

Before you begin

You should enable audit settings, remote syslogging, and configure IP address of remote syslog server. You should import CA certificate of the remote syslog server into Cisco CMX using the **cmxctl config certs importrsyslogca***<certificate-file>* command.

You should perform configuration changes on Remote syslog server for strongwan library to establish IPSec tunnel. You should configure IP address and hostname for Cisco CMX and CA certificate (/opt/cmx/srv/certs/ca.crt) on remote syslog server and then start the IPSec service and connection.

Note Currently, Cisco CMX supports only one syslog server configuration.

Procedure

Step 1 Run the **cmxctl config ipsec enable** command to enable IPSec.

The default authentication type for IPSec is "PUBKEY"/Public Key. The authentication type is set when you run the **cmxctl config ipsec enable** command.

Step 2   Run the **cmxctl config ipsec status** command to view the IPSec status and security association details.

Step 3   (Optional) Run the **cmxctl config ipsec authtype** command to change the default authentication type from **Public Key (PUBKEY)** to **Pre-Shared Key (PSK)**.

```
[cmxadmin@cmx]# cmxctl config ipsec authtype
Current IPSec Auth Type = PUBKEY
Do you want to change it? (y/n) [n]: y
Select IPSec Auth Type: (PUBKEY/PSK) [PUBKEY]: PSK
IPSec auth type changed to PSK.
IPSec is configured with PSK : nIXRjNrMiNzcKj7yVZ0Nod5IzxUyO9XZ
Configuring ipsec ....
In primary
Stopping strongSwan IPsec...
Starting strongSwan 5.6.2 IPsec [starter]...
```

Cisco CMX generates a new PSK as shown in the above example. You should configure the PSK on remote syslog server and restart the IPSec service.

Step 4   Run the **cmxctl config ipsec restart** command to restart IPSec on Cisco CMX.

Step 5   (Optional) Run the **cmxctl config ipsec status** command to view the authentication type.

About Cisco CMX Integration with Cisco DNA Center

Cisco DNA Center supports the integration of Cisco Connected Mobile Experiences (CMX) for wireless maps. With the Cisco CMX integration, you can get the exact location of your wireless clients, rogue access points and interferers on the floor map within the Cisco DNA Center user interface.

Depending on your requirements, you can create Cisco CMX settings either at the global level or at the site, building, or floor level. For a small enterprise, you can assign Cisco CMX at the global level, which is the parent node. All children inherit their settings from the parent node. For a medium enterprise, you can assign Cisco CMX at the building level and for a small enterprise, you can assign Cisco CMX at the floor level.

For more information about Cisco DNA Center, see the *Cisco DNA Center User Guide* at:

https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html

Note   Cisco CMX should be anonymized for security purposes.

Create Cisco CMX Settings

Procedure

Step 1   In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **System** > **Settings**.

Step 2   From the **External Services** section, click **DNA Spaces/CMX Servers**.

The **DNA Spaces/CMX Servers** window appears.

Step 3   From the **CMX Servers** table, click **Add**.

Step 4   Complete the fields in the **Add CMX Server** slide-in pane:

- **IP Address**: Enter the valid IP address of the CMX web GUI.

- **User Name**: Enter the CMX web GUI username.

- **Password**: Enter the password credentials.

- **SSH User Name**: Enter the CMX admin username.

- **SSH Password**: Enter the CMX admin password credentials.

     Note   Make sure that Cisco CMX is reachable.

Step 5   Click **Add**.

     Result: The Cisco CMX server is added successfully.

Step 6   To assign a Cisco CMX server to a site, building, or a floor, click the **Menu** icon and choose **Design** > **Network Settings**.

Step 7   Click the **Wireless** tab.

Step 8   In the left tree view menu, select either Global or the area, building, or floor that you are interested in.

Step 9   In the **DNA Spaces/CMX Servers** section, use the drop-down list, choose the Cisco CMX server.

Step 10   Click **Save**.

     The **Create CMX Settings** page appears.

     After the Cisco CMX is added, if you make any changes to the floor on the **Network Hierarchy** page, the changes are synchronized automatically with the Cisco CMX.

     When the Cisco CMX is synced, Cisco DNA Center starts querying the Cisco CMX for the client location and displays the location on the floor map.

Step 11   From the floor map, you can do the following:

- View the location of the client, which is shown as a blue dot.

- Hover your cursor over an AP. A dialog box is displayed with **Info**, **Rx Neighbor**, and **Clients** tabs. Click each tab for more information. Click **Device 360** to open the Device 360 window and view issues. Click an issue to see the location of the issue and the location of the client device.

- Click an AP to open a side bar with details about the AP.

- Perform real-time client tracking when Intelligent Capture and CMX are integrated.

Step 12   If the Cisco CMX was down when you made changes, you must synchronize manually. To do so, on the **Network Hierarchy** page, hover your cursor over the ellipsis ●●● next to the building or floor on which you made the changes in the left tree pane, and then choose **Sync: DNA Spaces/CMX** to push the changes manually.

Step 13   To edit the Cisco CMX server details or delete a Cisco CMX server, do the following:

a) In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Settings**.
b) From the **External Services** section, click **DNA Spaces/CMX Servers**.
c) Select the CMX server that you want to edit, make any changes, and click **Update**.
d) Select the CMX server that you want to delete and click **Delete**.

e) Click **OK** to confirm the deletion.

For Cisco CMX Authentication Failure

- Check if you are able to log in to the Cisco CMX web GUI with the credentials that you provided at the time of CMX settings creation on Cisco DNA Center.

- Check if you are able to log in to the Cisco CMX console using SSH.

- Check if you are able to exercise Cisco CMX REST APIs using the API Documentation link on the Cisco CMX GUI.

If Clients Do Not Appear on the Cisco DNA Center Floor Map

- Check if the Cisco wireless controller on the particular floor is configured with CMX and is active.

- Check if the Cisco CMX GUI shows clients on the floor map.

- Use the Cisco DNA Center Maps API to list the clients on the floor: `curl -k -u <user>:<password> -X GET /api/v1/dna-maps-service/domains/<floor group id>/clients?associated=true`

Remote HTTPS Server Support for Windows OS

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS) and also not sending the HTTP information. HSTS is an optional response header configured on the server to instruct the browser to only communicate using HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

The remote host also supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but has the potential to leak information if used improperly.

To enable HTST on the **Windows OS**, follow these steps:

Procedure

Step 1	Choose **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
Step 2	Click **HTTP Response Headers**.
Step 3	In the Actions panel, click **Add**.
Step 4	In the Add Custom HTTP Response Headers dialog box, enter the value: **2 Value: max-age=31536000**.
Step 5	Confirm the changes and close **IIS Manager**.
Step 6	To redirect users to visitors to the HTTPS URL, follow these steps:
	a) Open the **IIS Manager**.
	b) Click **HTTP Redirect**.
	c) Check the **Redirect** check-box.
	d) Enter the target URL (HTTPS).

e) Set the status to Permanent Redirect (301).

What to do next

We recommend that you disable CBC as it is running on EBC mode for SSL Cipher Block Chaining Cipher Suites.

Support for Proxy with Basic Authentication

To set the proxy server address with basic authentication enabled, use the **cmxos sysproxy proxy** command. When you use the command, you must provide the `username` and `password` in the proxy server URL. The proxy server URL format is:

`http://<username>:<password>@<hostname/ip>:<port>`

For example: **cmxos sysproxy proxy** *http://myuser:mypassword@myproxyhost:3128*

During runtime, a client URL (`curl`) call is made through Cisco CMX to ensure that the proxy is reachable. The `curl` call includes the username and password in the server URL. If the proxy is not reachable, an error is displayed. You can view the proxy logs to verify if the call reaches proxy successfully.