



Getting Started

- [Introduction to Cisco Connected Mobile Experiences, on page 1](#)
- [Overview of Cisco CMX Services, on page 2](#)
- [Cisco CMX Feature Parity, on page 4](#)
- [Installing Cisco CMX 10.6, on page 5](#)
- [What's New in Cisco CMX Release 10.6.0 and Later, on page 6](#)
- [Using the Evaluation License, on page 7](#)
- [Logging In to the Cisco CMX User Interface, on page 7](#)
- [Configuring SSO Authentication in Cisco CMX, on page 8](#)
- [Importing Maps and Cisco Wireless Controllers, on page 15](#)
- [Enabling or Disabling Cisco CMX Services, on page 17](#)
- [Installing Certificates in Cisco CMX, on page 17](#)
- [Adding Users and Managing Roles, on page 22](#)
- [Using the Cisco CMX Setup Assistant, on page 23](#)
- [Supporting Active Clients Version 3 API, on page 23](#)
- [Getting APIs, on page 23](#)
- [Restricted CLI, on page 24](#)
- [Encrypting Cisco CMX Connection to Remote Syslog Server Using IPSec Protocol, on page 25](#)
- [About Cisco CMX Integration with Cisco DNA Center, on page 26](#)

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 DNA 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
 - 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 device 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>

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/cm_x_syslog/b_cm_x_syslog1063.xlsx



Note

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

•



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	<ul style="list-style-type: none"> • Cisco CMX Release 10.4 and later • Cisco Prime Infrastructure Release 3.3 and later 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • RFID tags are displayed. • Wireless associated clients are supported. • Probing clients are supported. • Interferers on Cisco Prime Infrastructure Release 3.2 are supported.
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	<ul style="list-style-type: none"> • Use the <code>/api/config/v1/version/image</code> API to display the Cisco CMX version. • Use the <code>/api/config/v1/campuses/import</code> API to import a map file to Cisco CMX. 	<ul style="list-style-type: none"> • Use the <code>/api/config/v1/version/image</code> API to display the Cisco CMX version. • Use the <code>/api/config/v1/campuses/import</code> 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 10.6

Cisco CMX Release 10.6 supports inline upgrade from Cisco CMX Release 10.5.

For more information about installing Cisco CMX 10.6, see the *Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX Release 10.6* at:

<https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-installation-guides-list.html>

What's New in Cisco CMX Release 10.6.0 and Later

This section provides a brief introduction to the new features and enhancements introduced in Cisco CMX Release 10.6.2:

- **Single Sign On through SAML:** Cisco CMX supports SAML (Security Authentication Markup Language), which is an implementation of Single Sign On (SSO). You can configure Cisco CMX to authenticate users. For more information, see [Configuring SSO Authentication in Cisco CMX, on page 8](#).
- **Validate SSL certificate for Northbound notifications:** This feature ensures that a valid HTTPS packet is created when webhooks are sent from Cisco CMX. For more information, see [Configuring Notification Listener in FIPS Mode](#).

This section provides a brief introduction to the new features and enhancements introduced in Cisco CMX Release 10.6:

- **Cisco DNA Spaces integration:** Cisco DNA Spaces is a cloud-based location platform that provides a single pane for all Location services. From Cisco CMX, you can choose to configure location updates to services enabled in Cisco DNA Spaces. For information about Cisco DNA Spaces, see <https://dnaspaces.cisco.com/>.
- **Enhanced traffic notifications:** When Cisco CMX and Cisco DNA Spaces have an established connection, Cisco CMX provides traffic-related notifications, such as the destination of the traffic and the amount of traffic sent to Cisco DNA Spaces. For more information, see [Managing the Cisco CMX Cloud Apps](#).
- **Cisco DNA Spaces SEE and ACT licenses:** From Cisco CMX, you can install the Cisco DNA Spaces SEE and ACT licenses. For more information about licensing, see [Managing Licenses](#).
- **Restricted CLI:** On Cisco CMX, Linux commands are restricted to prevent unauthorized users from inadvertently modifying the system configuration. For more information, see [Restricted CLI, on page 24](#).
- **Federal Information Processing Standard (FIPS):** Cisco CMX implements software changes required for FIPS 140-2 security standard compliance. This standard is used to validate cryptographic modules.
This feature is disabled by default, but FIPS mode can be configured on Cisco CMX. For more information, see [FIPS, CC, and UCAPL Support in Cisco CMX](#).
- **Common Criteria (CC):** Cisco CMX implements software changes required for CC certification process. This is a testing standard to verify that a product provides security functions.
CC is enabled when FIPS mode is enabled on Cisco CMX. This feature is disabled by default. For more information, see [FIPS, CC, and UCAPL Support in Cisco CMX](#).
- **U.S. Department of Defense (DoD) Unified Capabilities Approved Product List (UCAPL) compliance:** Cisco CMX implements software changes required for US Department of Defense (DoD) Unified Capabilities Approved Product List (UCAPL) compliance and the certification for it is in progress.
This feature is disabled by default, but UCAPL can be configured on Cisco CMX. For more information, see [FIPS, CC, and UCAPL Support in Cisco CMX](#).

For detailed release recommendations, see *Release Notes for Cisco Connected Mobile Experiences (CMX), Release 10.6.0* at:

https://www.cisco.com/c/en/us/td/docs/wireless/mse/release/notes/cmx_10_6_rn.html

Using the Evaluation License

Cisco 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 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 DNA Spaces licenses.

Cisco DNA 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 DNA Spaces, **DNA Spaces SEE** and **DNA Spaces ACT**. We recommend that you upload the **Term** license for Cisco DNA 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.

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

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

- 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 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 enabled, 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 prerequisites for configuring SSO:

- Cisco CMX integrated with SAML 2.0 framework
- IDP with SAML 2.0 support
- Cisco CMX with proxy configured 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 database users with username assigned to them. You will also get a prompt to confirm what role to assign to a user if 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 download the metadata XML using the download link available in all standard identity provider service.

The most common IDP is Active Directory Federation Services (ADFS). For ADFS, you can download the metadata file from <https://%3Cads-server-name%3E/FederationMetadata/2007-06/FederationMetadata.x>

- If you are unable to download the IDP file, you must provide related information such as SSO endpoint URL to 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=** from the SSO metadata file.
- The type of **NameIDFormat** used by Cisco CMX is email Address. Cisco CMX will use **emailAddress** returned in SAML response.
- Cisco CMX requires firstname, lastname, email address field information from IDP in SAML response. Cisco CMX will extract the username from email address by stripping the @domain part from email address. For example, if email address is xyz@abc.com, Cisco CMX will strip @abc.com out and use xyz as username for SSO user.
- Ensure that session timeout is configured on IDP. When you configure IDP, ensure that the value for **Security Signature Algorithm** is set as **SHA1**. The default on ADFS is **SHA256** and change it to **SHA1** when configuring ADFS.

We recommend that you remove the **X509 Cert parsed** from SP Metadata File on ADFS as it will result in 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 again, credentials are not prompted and user is logged in automatically. This is because the IDP session is still valid not yet expired. As a work around, you will have to close the browser window every time you log out of Cisco CMX.
- For High Availability configuration, both Primary and Secondary server needs to be configured separately using 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-b258-688e07354084">
<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>MIIFhDCCA2ygAwIBAgIEXUiZADANBgkqhkiG9w0BAQsFADEBMMQswCQYDVQQQ
UzELMAkGA1UECAwCQ0ExETAPBgNVBACMCFNhbiBk3N1MQwwCgYDVQQKDANNU0Ux
DzANBgNVBAMMB1Jvb3RDQTAeFw0xOTA4MDUyMTAwNDhaFw0yMjA4MDQyMTAwNDha
ME8xCzAJBgNVBAYTA1VTMQswCQYDVQQIDAJDQTERMA8GA1UEBwwIU2FuIEpvc2Ux
DDAKBgNVBAoMA01TRTESMBAGA1UEAwJU2VydMvYyQ3JOMIICiJANBgkqhkiG9w0B
AQEFAAOCAG8AMIICGkCAGeAtC0tqHb6eDG0P6KeyUjvmwFBTAt6yleSLoVbfNGz
X5j6/WKQkgMYQI6V40Ap9iKp9aSz62wNydHoZSdt2icSQo+8Z3bfzn2ToWuiHbT4
LrD9fJlWdLZW6Tu/U8KBy+sS4vL60GppjCJ0G5h6igPCYajaIaQd0e09IWBENQXv
f/MNUG6wIa2ivstjWQsUv26uLhrgrIbZ7akZb/OKxcaFSyYOS17ueXqUrm27pKL2
IVFdvXBGJgFoiISaTcmYnAMJptYskJuAkc6GtqEPtgJKp0UYm0t/h/tgT2JESvn8
v9ymY8vicDJY40+OPLaghs0EMYc+8LoC/14YMYMkZhFGGVOVjQar+KEBlVfk1EA
mAKOgMTYk8u7+d/KvXo07RWlk3zIYVZX9aJMrPxQAp9/YC2wwoelOCAiaA4pxcU
yWw+0E7UBcU27fPSZ07puROk5bIhQ/gx6Sv4B5Rg0df2xjZeVsQq6G/r7TiJsWch
```

```

THwGQXO92H/3E5s4u0L7TXI45vL0a2qGHRm6dtxq/hifSW/AkDu2YyhmdZmwm5f
TE+GLSPqJgzWMrHXcd1+g1liDQoaFvN0CorgayhKIKWKjZwvUKUCGb7ZA9OHS40V
d7uRBZlu66bxB19/gdWVjPza/iifUPPKVu/wssdGULvLSqQupwFEEWgYShfhkba
9jsCAwEAAANrMGkwCQYDVR0TBAlwADAwBgNVHREKTAnggxjbXgtmdlkZXYzMDaC
F2RhdGFjYXNlLnNlcnZpY2UuY29uc3VsMB0GAlUdJQOWMBQGCCsGAQUFBwMBBggr
BgEFBQcDAjALBgNVHQ8EBAMCA6gdDQYJKoZIhvcNAQELBQADggIBAEPWA/9TlpnY
A6CNk1T2qSQRULaIyiaDQbkMjxTw0DoX/RsTreKX7CXCGk9jcLAKbU/zUBcUmC5b
PUMM1xJHpMWMZOWIWknPBvAGQ1LODePEj8Lejo8MwUVJKjSAfvoydLsgewyIXPII3
eiVWkOgmNRmikq5N6Cn6FVCeL+pZF0COUvOXIs7frvB3hRGep4KujygpM732DKsH
Nwc9B8T7U2u/y1+U+uGzEa4DTp67Tih2O3t8nAEVD4mcBP9J6/c6lCFvQZUhDma
+2qqhTttFyA3G6qEvkx9z5B0Nd64quZKONENajR0OaFOkOotiSGLljQOKz/ldvE
iXos1PHVhZBnrkXejHW/Q/MwT9GIYehn6yKyHt1e0L2rj16ZHxUZd0Idm/ps2zTb
R3yM6DPZaCsgvybn2cIa7Vbqq54wBRDykGQv5nBib3CRKiDPPp38/z8nx1npIw6V
6L3pZscFaN/8fFB/UhK39OLUPfCp2RDgCWwrOv5u0B3Jib9gz5CGo8cb36DMghmw
6IilTElans4y0o4LJfUaljCHGWMcfIfKXu/3oPWSL0ogd+pgSRV8dDE0jhxfpu5e
4MwYYgLHJ3SfUDYvxfmflLaXU4v+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>MIID1TCCAr2gAwIBAgIUkKkG/18NwhjuWBKXS/
C3EmKJH3sEwDQYJKoZIhvcNAQEF
BQAwQzEOMAwGA1UECgwFQ21zY28xFTATBgNVBAsMDE9uZUxvZ21uIEIelkUDEaMBGg
A1UEAwRT251TG9naW4gQWNjb3VudCAwHhcNMjkwODAMDA0MjI5WhcNMjkwODAM
MDA0MjI5WjBDMQ4wDAYDVQQKDAVDAxNjBzEVMBMGAlUECwwMT251TG9naW4gSWRQ
MR0wGAYDVQQDDDBFBmVmb2dpcihBBY2NvdW50IDCCASiWdQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBBAK8KoxkPZ3Ew60SDtcSMI6PqSmnJt9vzTNElK4D6M1lWKNmv
N4luXn2xpI/A31bgWjGn2a3r31LakTinPQGAtwAdjxmUvRUz8VN/HkdOLG5hIA0e
qY/M+fk/hIn7ggjJVjr/pH0OyBfWJKOs6XLsnj8EOxoIcjsLtudLSL88NnNuUkU
eNYSctgQtHb8UgRO6DBcHrH1B1/K8a8BztOc5XSxTBYF87FNT0xJsds50LZFNzQ3Z
wuoOrpmSocCeNLwRLO0zmvQBha3FurcTYei3t8ZUtUHHkEKYwnvQLkMQo6ub1fF
w11ojLy0LlSIN5GJRDWkV2ZeWE4D2x11KizBfk8CAwEAAAOBwDCBvTAMBGNVHRMB
Af8EAjAAMB0GA1UdDgQWBbTYyBqOQGCjZ+zR/pCdGdhggwVACDB+BgnVHSMEdzB1
gBTYyBqOQGCjZ+zR/pCdGdhggwVACKFHpEUwQzEOMAwGA1UECgwFQ21zY28xFTAT
BgNVBAsMDE9uZUxvZ21uIEIelkUDEaMBGAlUEAwRT251TG9naW4gQWNjb3VudCCC
FCpBv5fDcIY71gSl0vwtXJiiR97BMA4GA1UdDwEB/wQEAwIHgdANBgkqhkiG9w0B
AQUFAAOCAQEAWaY2Izz53TmO2oZGwSzAef8y4G+GO0oyNnEoytKA+tT0vKoOK4Sh
hd0/GG18sXuwCfhHCC7XMTrwHLdGkfhTqSO8tG4w/9XrDUTVPjI0eQan6e+0EyGq
CvzIe3/5Dlh0PDjybn5ar8Q3EMXEAwepiQYvUSEmKw17p2uJQ2KGGG+k4yrphtmv
iyUIlLDQ+cHvIC/QMqpGJzM76cWS0SPKGjTjHmS51KUqgTnnfcnpTwYFUG/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</NameIDFormat>
      <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 AesUID 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>

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

-
- After adding controllers, you must verify 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:

```
cmxctl enable {consul | qlesspyworker | cassandra | iodocs | cache_6382 | cache_6380 | cache_6381 | cache_6383 | cache_6384 | 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_6384 | 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>

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 (within 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.

- Provide the details for CSR such as Country, State, City, Company Name, and Org Unit Name.
- Enter hostname of your Cisco CMX system as the Common Name.
- 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
MIIEpAIBAAKCAQEAgXgEo7ouyBfWwCkctYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----                                    < Your CMX server signed certificate
MIIFEzCCAvugAwIBAgIBFzANBgkqhkiG9w0BAQsFADCB1DELMAkGA1UEBhMCMVVMx
```

```
...
-----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 importcert** 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 importcert 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.
-

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 separately 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.
- To clear current certificates, run the **cmxctl config certs clear** command.
 - To generate Certificate Signing Request (CSR), run the **cmxctl config certs createcsr** command
 - On Cisco CMX server, run the **cmxctl config certs importcert** command to import CA certificate.
 - 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
- 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
- manufacturer
- 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.



Note 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.
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.

Command	Description
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 importsyslogca**<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.

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/wireless/dna-spaces/series.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
```