Cisco CMX Configuration Guide, Release 10.5.0 and Later

First Published: 2017-03-31

Last Modified: 2018-07-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Preface

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Audience

This document is for network administrators who configure Cisco Connected Mobile Experiences (Cisco CMX) services.

Conventions

This document uses the following conventions:

Table 1: Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.

Convention	Indication
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string. Otherwise, the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means the following information will help you solve a problem.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Related Documentation

For more information on coding and specific assistance, see:

https://developer.cisco.com/site/cmx-mobility-services/

For more information about Cisco Mobility Services Engine and related products, see:

http://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/tsd-products-support-series-home.html

For more information about Cisco Connected Mobile Experiences (Cisco CMX), see:

http://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/index.html

For more information about Cisco DNA Spaces, see:

https://support.dnaspaces.io/

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

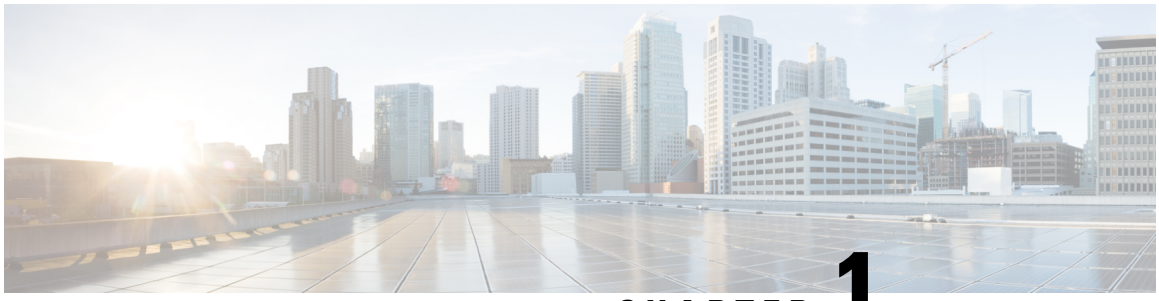
Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

CONTENTS

CHAPTER 4



CHAPTER 1

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 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, on page 27.

- **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, on page 77.

- **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, on page 101.

- **PRESENCE ANALYTICS**: Cisco Presence Analytics service is a new analytics engine that detects the presence of visitors via their mobile devices interactions with even a single network access point. The probe requests which are transmitted from the wireless devices provide information, which is used to identify the general location of a client, in respect to the location of even a single access point which hears the clients probing activity. The information available from even a single AP allows the Presence Analytics service to develop valuable business intelligence. Presence Analytics uses Received Signal Strength Indication (RSSI), along with the duration of high signal strength to determine whether a client device is in the site or just passing by. Even if a device is not connected to the access point, its presence is still detected if the device is within the signal range and the wireless is turned on. Given that Presence Analytics develops location information with respect to a given set of APs it has a simpler management overhead in that it does not require the importation or configuration of any maps into the CMX instance. By simply knowing the association of a given AP, or set of APs, to a physical location, Presence Analytics allows a business insight into the number of visitors to a location, whether these are first time or repeat visitors, the average amount of time each visitor spent in physical proximity to the AP, and the ability to ascertain whether a devise was just passing by a location or if they were actually within the location serviced by the AP. For more information, see Overview of the Presence Analytics Service, on page 145.

  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, on page 159.
- **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, on page 193.

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

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.

Prerequisites for Configuring Cisco CMX 10.5

The following components are mandatory for you to configure Cisco CMX 10.5:

- Exported maps (in the form of files) from Cisco Prime Infrastructure 3.2, 3.3, or 3.4.

  Note Import maps from Cisco Prime Infrastructure only if you are using the Cisco CMX Location service. You do not have to import them if you are using the Presence Analytics service because this service does not require maps; all configurations are accomplished using the Presence Analytics Dashboard.

- Cisco Wireless Controller (Cisco WLC) 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, or 8.7.
- Cisco CMX 10.5 License (Cisco CMX 10.5 ships with a fully functional 120-day evaluation license that is activated after Cisco CMX is installed and started the first time.)

For more information about license models, see Managing Licenses, on page 166. For information about adding permanent licenses, see Add a License, on page 167.

Tip If you are using the phycial appliance, ensure that your disk has good I/O (operations per second) rate. Use the **redis-benchmark** command to verify the same. The ideal I/O rate must be either equal to 1500 or above.

Installing Cisco CMX 10.5

Cisco CMX Release 10.4 was running with CentOS 6.6. With Cisco CMX 10.5, the entire operating system is upgraded to the latest CentOS 7.x. The CentOS 7 (1708) build is used as the new operating system version. The new minimal version of CentOS 7 release is used as the base operating system. Additionally, all packages are added to the release as done in Cisco CMX release versions earlier than Release 10.4.

The operating system upgrade also supports disk encryption, which is done by encrypting a file system. The encrypted file system protects against any kind of bare-metal attacks against the hard drive.

Cisco CMX 10.5 does not support a direct upgrade. Instead you need to take a backup of the existing Cisco CMX and install a new OVA or a bare metal ISO image. After the new OVA or ISO is configured suucessfully, perform a restore of Cisco CMX.

For more information about installing Cisco CMX 10.5, see *Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX Release 10.5* at:

https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-installation-guides-list.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, on page 166.

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 7.

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 be 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 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 database users with username assigned to them. You will also get a prompt to confirm what role to assign to a user i 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 th 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 download th metadata file from https://%3Cadfs-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 UR 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 S metadata file.
- The type of **NameIDFormat** used by Cisco CMX is email Address. Cisco CMX will use **emailAddress** ret in SAML resposne.
- Cisco CMX requires firstname, lastname, email address field information from IDP in SAML response. C CMX will extract the username from email address by stripping the @domain part from email address. Fo example, if email address is xyz@abc.com, Cisco CMX will strip @abc.com out and use **xyz** as username SSO user.
- Ensure that session timeout is configured on IDP. When you configure IDP, ensure that the value for **Secu Signature Algorithm** is set as **SHA1**. The default on ADFS is **SHA256** and change it to **SHA1** when config ADFS.

  We recommend that you remove the **X509 Cert parsed** from SP Metadata File on ADFS as it will result i 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 vali not yet expired. As a work around, you will have to close the browser window every time you logout of C CMX.
- For High Availability configuration, both Primary and Secondary server needs to be configured seperately 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>MIIFhDCCA2ygAwIBAgIEXUiZADANBgkqhkiG9w0BAQsFADBMMQswCQYDVQQ
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</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, on page 206.

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, on page 206.

Note

-
- 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, on page 196.

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 (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.

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 16.

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, on page 169.

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.

If you install Cisco CMX Release 10.5 or upgrade from a previous release, the password to access the Active Clients v3 API is generated in random manner. Use this password to start the server and open the prompt. Set the new credentials using the **cmxos apiserver** command.

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

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

Active Clients v3 API supports these additional parameters:

- mapHierarchy
- manufacturuer
- macAddressSearch
- associated/probing

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

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

Getting APIs

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

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

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/.

Changing Time Zones and NTP Server

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

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

Before you begin

- Ensure that your server has a valid hostname before making any NTP changes. If not, some of the ntp commands will fail, for example, ntpstat.
- Ensure that incoming and outgoing UDP port 123 for NTP communication is open in your configuration setup.
- Ensure to manually edit /etc/ntp.conf as admin user and appropriate time zone is selected using `/opt/cmx/bin/tzselect` before restarting ntpd using **service ntpd restart**.

Procedure

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

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

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

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

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

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

- **cmxctl start agent**
- **cmxctl start**

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.

Command	Description
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.
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

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:

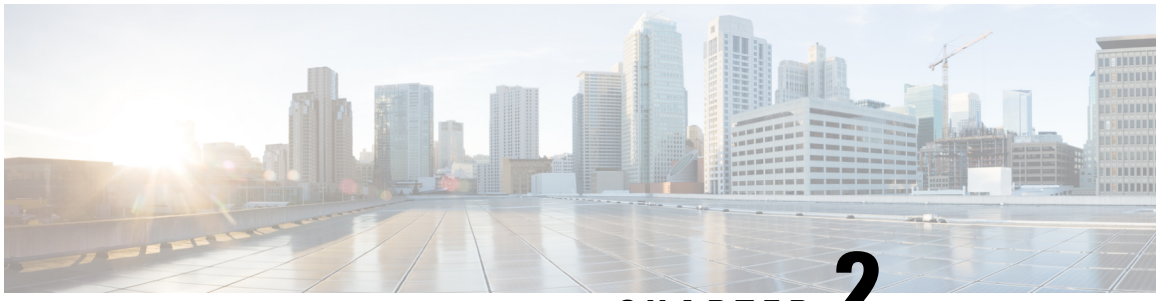
a) In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **System** > **Settings**.
b) From the **External Services** section, click **DNA Spaces/CMX Servers**.
c) Select the CMX server that you want to edit, make any changes, and click **Update**.
d) Select the CMX server that you want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



CHAPTER 2

The Cisco CMX Detect and Locate Service

Overview of the Detect and Locate Service

The Cisco Connected Mobile Experiences (Cisco CMX) **DETECT & LOCATE** service enables you to view and track devices in your deployment.

Using the **DETECT & LOCATE** service, you can either view all the access points (APs) deployed in all the buildings of a campus or view the APs deployed on the individual floors of each building. You can also locate Wi-Fi tags, Wi-Fi interferers, and Bluetooth low energy (BLE) Tags.

Initial Configurations

In order to use the **DETECT & LOCATE** service, the following initial configurations have to be performed:

- Import maps—For information about this, see Importing Maps and Cisco Wireless Controllers, on page 13.
- Add controllers—For information about concept, see Adding Controllers, on page 14.

Note To enable **DETECT & LOCATE** service, run the **cmxctl enable location** command followed by the **cmxctl start -a** command.

Viewing or Tracking Devices

Procedure

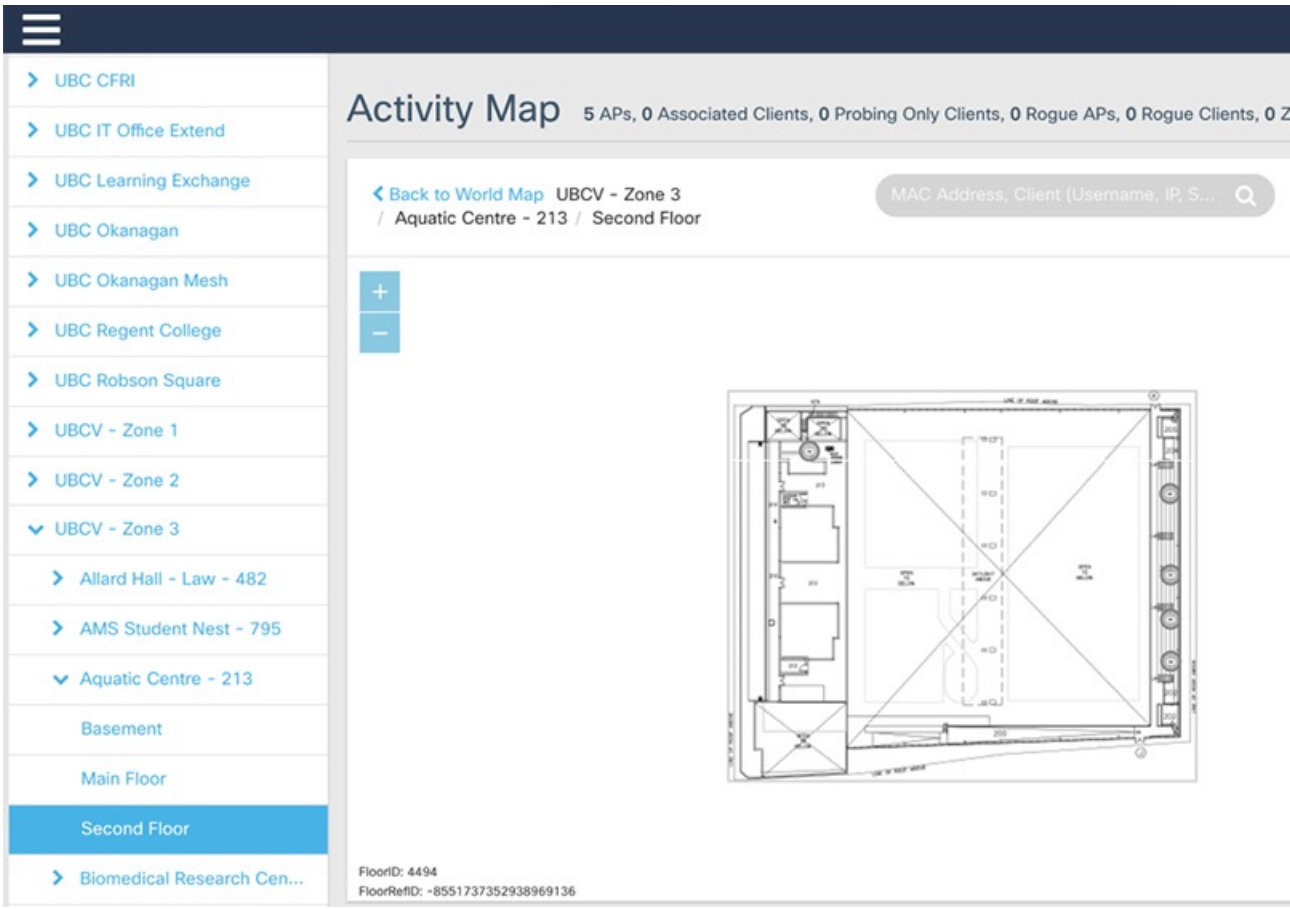
Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2 Click **DETECT & LOCATE**.

Step 3 Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

The **Activity Map** window displays a list of icons to the right.

Figure 1: Activity Map Window



Step 4 Choose any combination of the following icons to customize your view of the devices:

- **Clients**—Click the **Clients** icon to show or hide all the client devices (connected and detected) that are being tracked by your Cisco CMX. Client devices are displayed either as red dots (probing clients) or green dots (connected clients). Clicking on connected clients show the AP that the client is associated with (blue lines) and the APs that are participating in the location calculation (red lines), and while clicking on a probing of unassociated client displays the APs that are being used to detect the clients (red lines).

Note

- The maximum number of clients (connected and detected) that can be displayed at a given time is connected clients are displayed, again up to a maximum of 2000 (see the figure below). However also exceeds 2000, no clients are displayed. In such a scenario, we recommend that you use the Anal

- Associated clients probe less to save battery power and this has direct impact on locating them co probes when they go to ultra-power reserve mode (sleeping mode and screen blanked out). This b available on Cisco CMX. When the user unlocks the home screen or start streaming the content, th probes to the wireless network.

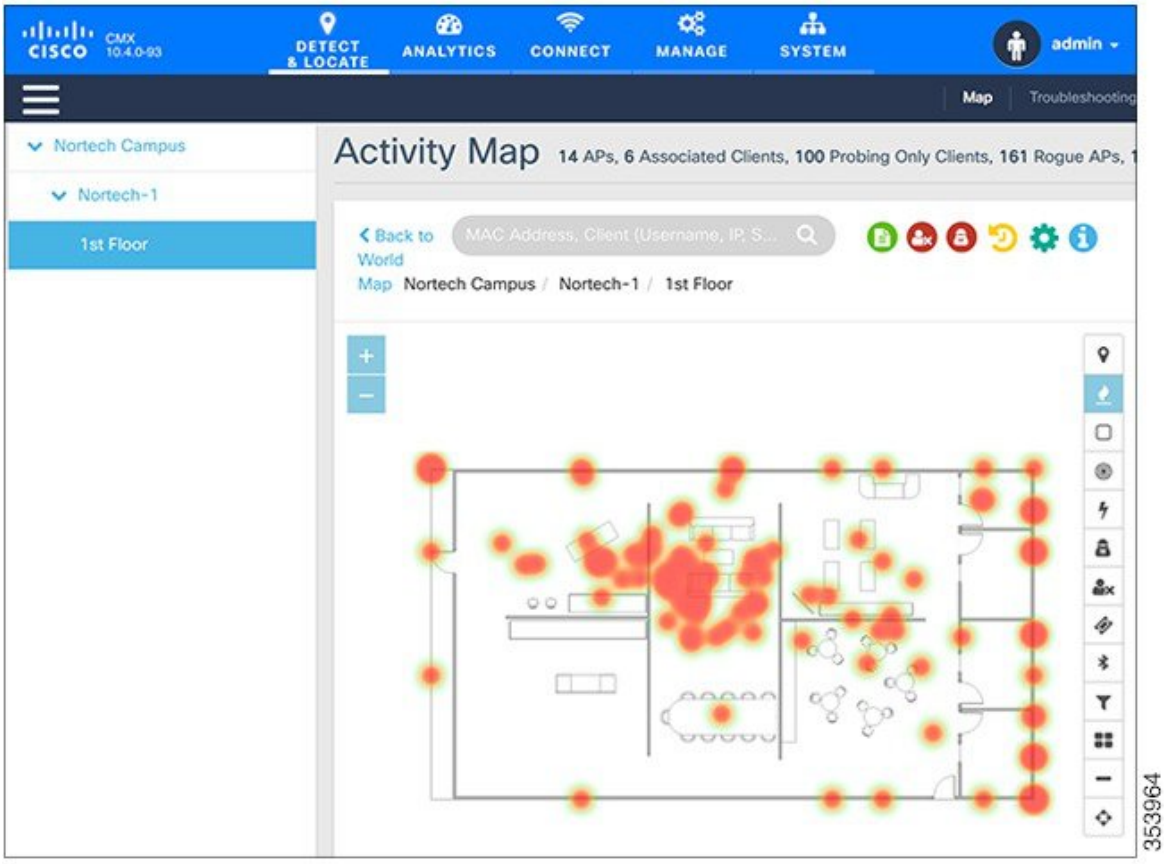
  This behavior depends on the phone usage and for such inactive, sleeping devices, Cisco CMX w

- Cisco CMX needs the WIFI devices to send RSSI probe messages to have the very first location a WIFI devices are expected to send regular updates to Cisco CMX so that Cisco CMX maintains t status displays as active on the controller. However they are not sending any RSSI probe message non-locatable devices. Such devices are not considered as active devices on Cisco CMX and is di

- Cisco CMX shows only active clients. Sleeping clients are not shown.

- Devices could be seen by an AP that have NOT be placed on map, if there are lots of APs on map reason of Cisco CMX dropping the clients.

- **Heatmap**—Click the **Heatmap** icon to show or hide areas with varying concentrations of client devices. Areas with a high concentration of client devices are marked bright red, as shown in this figure.



- **Zones**—Click the **Zones** icon to show or hide the zones on a specific floor.
- **Access Points**—Click the **Access Points** icon to show or hide all the APs that have been deployed on a specific floor. APs are displayed as circular objects, with a number in the center. This number indicates the number of clients connected to that specific AP. Inactive access points (red circle with a hyphen) are also detected when there is no RSSI probe packets coming to Cisco CMX. Inactive APs are detected usually in the following scenarios:
  - in the night time when there are no devices present on the venue.
  - when there is no controller added to Cisco CMX or the added Controller connection is not active.

Clicking an AP shows the clients connected to it (blue lines), the probing clients that are detected by the AP (red lines), and additional information such as height, orientation, and X,Y location of the AP.

If you have a Cisco Hyperlocation module that is attached to the back of your Cisco Aironet 3700 and 3600 Series APs, you can track the location of customers, visitors, or assets to about one meter in an ideal environment. Currently, the Hyperlocation solution works for the associated clients only.

Note When AP grouping feature is enabled, Cisco CMX shares Access Points grouping information to Cisco WLC every time when a NMSP connection is established. To get a list of APs connected to the Cisco WLC, Cisco CMX performs a NMSP APINFO get action on the Cisco WLC. Based on the list of APs received from the Cisco WLC and the APs on the map, identify the subset of APs and prepare a grouping request to send to the controller.

- **Interferers**—Click the **Interferers** icon to show or hide all the RF interferers that have been detected by the wireless network, and their zone of impact.

  Note
  - From Cisco CMX release 10.6.2, Interferers filtering is strengthened to protect Cisco CMX from burst of short lived interferers. For effective interferer filtering results, we recommend that you set the interferer filtering parameters for **Duty Cycle Cutoff (Interferer)** and **Severity Cutoff (Interferer)** correctly. For more information, see Setting Filtering Parameters, on page 199. With this change, short lived interferers would not be tracked by Cisco CMX and moved under **Not Tracked** category in the **System** tab > **Settings** > **Tracking** window.
  - From Cisco CMX release 10.4, the BLE Beacons management page is no longer available on the Cisco CMX user interface. Beacon notifications are no longer provided. BLE beacons detected by Cisco CleanAir are displayed on Cisco CMX as interferers. BLE-related information is no longer available on the apidocs file. BLE Beacons management functionality is moved to the Beacons Management on cloud.

- **Rogue APs**—Click the **Rogue APs**  icon to show or hide the rogue access points. Rogue access points are those access points that are not part of the Cisco CMX infrastructure access points and not managed by Cisco CMX. They are classified as Unclassified, Malicious, Friendly, and Custom and indicated by different colors on the Activity Map. Cisco CMX uses the pre-defined zone of impact (3.28 feet) for all rogue aps. This happens because Cisco CMX does not receive the Transmit Power (Tx) information from controller which is needed to compute zone of impact dynamically.

- **Rogue Clients**—Click the **Rogue Clients**  icon to show or hide rogue clients. Rogue clients are clients connected to rogue access points.

  Note To track rogue access points and clients, enable the tracking parameters **Rogue Access Points** and **Rogue Clients** in the **Network Location Service** window under the **System** tab. For more information, see Setting Device-Tracking Parameters, on page 197.

- **BLE Tags**—Click the **BLE Tags** icon to show or hide BLE-transmitting devices that have been detected by the wireless network.

  Note Cisco APs with BLE radios can detect BLE beacons natively. Other APs will detect Beacons as an interferer.

  A common problem faced in the context of beacons is tracking not being enabled. In such a scenario, you can modify the tracking configurations using the System service. For more information, see the Viewing or Tracking Devices, on page 28.

  Click **Beacons** to view the beacon attributes related to the selected beacon profile.
  - If the beacon is chirping with iBeacon profile, Cisco CMX displays the properties such as UUID, Major and Minor number.
  - If the beacon is chirping with Eddystone-UID profile, Cisco CMX displays the properties such as Namespace and Instance-Id.
  - If the beacon is chirping with Eddystone-URL profile, Cisco CMX displays the HTTP resource URL being broadcasted by that beacon.

- **Tags**—Click the **Tags** icon to show or hide Wi-Fi tags. The vendor specific information related to the tags are displayed in raw format.

  Note Cisco CMX allows you to configure the RFID timeout using the **cmxctl cofig rfid timeout** command. You can get the current setting using the **cmxctl cofig rfid timeout get** command.

  You can modify the timeout value using the **cmxctl cofig rfid timeout set** command. The default value is 300 seconds. The timeout value can be set to anything between 60 to 10800 seconds. Cisco CMX allows you to set the RFID timeout to as high as 10800 seconds, it is highly recommended that you set the value to something below 600 seconds.

- **Filters**—Click the **Filters** icon to filter the display of devices based on parameters such as Connection Status, Manufacturer, and Service Set Identifier (SSID).
- **Inclusion & Exclusion Regions**—Click the **Inclusion & Exclusion Regions** icon to view the inclusion and exclusion regions on a floor. The inclusion and exclusion regions are created in Cisco Prime Infrastructure. In Cisco CMX, you can view these regions, but you cannot modify them. The inclusion regions are shown in green, and the exclusion regions are shown in gray.
- **Thick Walls**—Click the **Thick Walls** icon to view any thick walls that have been created on prime infrastructure and included on the floor. Thick wall improves location by modeling areas of high RF signal attenuation with more accuracy.
- **GPS Markers**—Click the **GPS Markers** to view any GPS markers that are placed on the floor. When at least three GPS markers are placed on a floor, the system can use these to provide GPS co-ordinates, in additional to X, and Y co-ordinates in client location API requests. Cisco CMX shows the GPS Markers of green color when the GPS Markers are valid ones.

Enhanced Associated Clients Tracking

Associated clients probe less in the network to save battery power and this prevents Cisco CMX to track them efficiently. This behavior is more significant with the static associated clients and determining their location in the absence of probes becomes more challenging to Cisco CMX.

The following is a list of additional improvements done in this area to better track the ability to track such static associated clients:

1. Cisco CMX would leverage the Associated AP information location from the maps and use that as the primary location for the associated client. This can be identified by checking the **Compute Type** field and it display the value as **Associated AP**. For taking benefit from this feature, ensure that the Cisco CMX map has all the Access Points information, so that Associated AP location would be available to Cisco CMX.
2. After the associated device sends the regular probe, its location would be determined from the reported APs and the **Compute Type** field would be set to RSSI or AoA depending on the source of the location.

Note This feature is disabled by default.

3. Cisco CMX would poll the Associated Clients information periodically every hour. This feature is enabled by default.
4. To poll the Associated Clients on demand, run the **cmxctl config pollconnectedclients info** command.

   The following example shows how to poll an associated client:

```
[cmxadmin@server]# cmxctl config pollconnectedclients info
+--------------+---------+
| Controller | Status |
+--------------+---------+
| 10.22.243.39 | Success |
+--------------+---------+
```

To enable enahnced associated clients tracking, follow the steps:

Procedure

Step 1 To set the featureflag configuration, run the following command:

cmxctl config location.computelocthroughassociatedap true

Step 2 To restart Cisco CMX agent, run the following command:

cmxctl agent restart

Step 3 To stop location and NMSP services, run the following commands:

cmxctl location stop

cmxctl nmsplb stop

Step 4 To start location and NMSP services, run the following commands:

cmxctl location start

cmxctl nmsplb start

Viewing Device Details

Procedure

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

Step 2 Click **DETECT & LOCATE**.

Step 3 Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

The **Activity Map** window displays a list of icons to the right.

Step 4 Click the corresponding icon to show the desired devices, for example, client devices, APs, beacons, and so on.

Step 5 Click the corresponding device on the map.

A pane displaying details of the device, such as MAC address, IP address, status, and so on is displayed.

Customizing Client Refresh Rates

The DETECT & LOCATE service enables you to configure the refresh rate for clients' position on a floor map. The refresh interval can be used to configure how frequently a client's positions will be polled to determine their positions. The default refresh rate is five seconds. The refresh rate gets automatically reset when you navigate to another tab or log in again. The client refresh rates are temporary and is not stored in the CMX.

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX) either as an admin user or a user with Location role.

Step 2 Click **DETECT & LOCATE**.

Step 3 Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

The **Activity Map** window displays a list of icons to the right.

Step 4 Click the **Gear** icon to configure the client refresh rate.
A pane indicating the client refresh intervals is displayed.

Step 5 Use the + or - icon to increase or decrease the client refresh rates. The refresh rates are in seconds. The range is one to 30 seconds.

Step 6 Click **OK**.

The client, represented by dots on the map, will be refreshed with the new configured rate.

Customizing Device Views Using Filters

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX) either as an admin user or a user with Location role.

Step 2 Click **DETECT & LOCATE**.

Step 3 Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

The **Activity Map** window displays a list of icons to the right.

Step 4 Click the corresponding icon to show the desired devices, for example, client devices, APs, beacons, and so on. The more icons you click, the more filtering options are enabled.

Adding and Deleting Filters

Procedure

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

Step 2 Click **DETECT & LOCATE**.

Step 3 Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

The **Activity Map** window displays a list of icons to the right.

Step 4 Click the corresponding icon to show the desired devices, for example, client devices, APs, beacons, and so on. The more icons you click, the more filtering options are enabled.

Step 5 Click the **Filter** icon.

Step 6 In the **Filters** dialog box that is displayed, you can add or remove client filters based on the following parameters:

- **Connection Status**—Unassociated or Connected
- **Device Manufacturer Type**—Name of the device manufacturer, for example, Apple, Samsung, and so on
- **SSID**—Device's SSID

Searching for a Device

Procedure

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

Step 2 Click **DETECT & LOCATE**.

Step 3 Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

Step 4 In the **Search** field of the **Activity Map** window, enter any of the following parameters to search for or filter a desired device:

- **MAC Address**—Enter the corresponding client's MAC address in lowercase, colon delimited, for example, 00:a0:22:bc:e2:00.
- **Device IP Address**—Enter the client's IPv4 or IPv6 address in dotted format, for example, 10.22.12.212.
- **SSID**—Enter the client's SSID in free-form text.
- **Device Manufacturer**—Enter specific manufacturer names, for example, Apple, Samsung, and so on in free-form text.
- **Username**—Enter the client's username in free-form text.

Note

- In Cisco CMX dashboard, when performing a search for a user using username, SSID, IP Address, or Manufacturer, search is performed for clients located on the current floor. However, if you search using the MAC address, the search is performed on a global hierarchy.
- When performing a device search based on MAC address, if the device is not located on the specific floor that you are on, a dialog box is displayed that shows the floor in which the specific device is currently on. In addition, you can search based on MAC address for a specific date.

Client Playback

The Client Playback feature enables you to locate and track the movement of clients in a venue. You can track the activity of one client at a time.

Note (CSCvn33059) When you click the **Client movement history playback** icon on the **Detect & Location** > **Activity Map** > window, you can select a day—up to 30 days from the current date—to track the history of a client. This window of 30 days is independent of the Data Retention - Client History Pruning Interval.

Procedure

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

Step 2 Click **DETECT & LOCATE**.

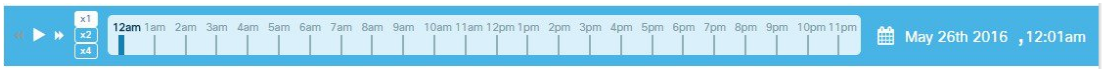
Step 3 Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

Step 4 Search the client you want to track using the its MAC ID.

For more information about how to search client devices, see Searching for a Device, on page 35.

Step 5 Click the **Client Movement History Playback** icon .

The Client Playback (see the image below) pane is displayed .



Step 6 Click the **Play** icon to start client playback.
You can also change the date in order to view the playback on a specific date, by clicking the **Calendar** icon.
You can increase the speed of the playback by clicking the **2x** button.

Data Privacy

In Europe, a new law, General Data Protection Regulation (GDPR) is in force effective May 25, 2018. GDPR intends to strengthen and unify data protection for individuals.

Cisco CMX 10.5 introduces the Data Privacy feature to be compliant with the GDPR requirements. This feature allows Cisco CMX to ensure data protection by not disclosing clients details such as MAC address, username, and IP address.

Note By default, the Data Privacy feature is disabled.

The Data Privacy feature works with the Mac Hashing **On**/**Off** options. This feature is applicable only for wireless clients. Other connected devices such as interferers, rogue clients, and RFID and BLE tags are not affected. When Data Privacy feature is enabled, Cisco CMX will not process client username, IP address, and will not determine the device manufacturer from the mac address of the device.

- **Mac Hashing On**—Cisco CMX hashes MAC address of all the clients. As a customer you need not explicitly opt to record the consent for this action. Active client count on the Cisco CMX Detect and Locate dashboard and Systems Service Dashboard will appear as double the actual number for the initial 5 to 10 minutes when clients already exist. After this duration, the active client count resumes to the correct count.

  If MAC Hashing is on, the MAC addresses of all the clients are hashed on the nmsplb service, and the location computed with the hashed MAC addresses.

- **Mac Hashing Off**—You must enter the MAC address of all the devices that have a location calculated manually to Cisco CMX. Alternatively, Cisco CMX can fetch the details from a CMX Connect interaction where a customer explicitly accepts the **Terms and Conditions** that allow customers' MAC address to have a calculated location associated with them. All Analytics and Connect data is based on the data from MAC addresses in which specific tracking has been enabled. If a customer does not explicitly approve, or a MAC address is not manually entered, Cisco CMX does not record the location of that MAC address.

After enabling Data Privacy, you can choose to perform these tasks:

- Not retain the connect data, and delete all the connect clients data by using the **cmxctl config connect deleteClientsAll** command.
- Delete all the history data by using the **cmxctl config data deleteAll** command. You may have to restart Cisco CMX if you delete history data.

The Data Privacy feature has 4 components:

- **Mac Hashing**—If Mac Hashing is turned on, you must input the SALT value (alphanumeric text used to safeguard passwords in storage) that is being used to anonymize the real MAC addresses. This is referred as current SALT. Cisco CMX uses the SHA1 one-way cryptographic function for MAC hashing. This helps to protect the user identity and the real MAC addresses are not stored in Cisco CMX. The Opt In client list is not checked in this mode and all client devices are tracked.

  You can specify a future date as SALT. Cisco CMX runs a job that checks for the SALT to be applied for that particular day. If a new SALT is available, this is used for MAC hashing. Cisco CMX requires the current SALT if MAC hashing is turned on.

- **Opt In**—This is used to collect user consent. As a Cisco CMX admin, you can decide the way you want to collect the consent. Cisco CMX stores the Location and Analytics consent separately. Also, because the Location service is the single source for Analytics data, devices that have not given consent for Location tracking will not be tracked for Analytics too.

Note Consent is stored in the database, and unless explicitly removed, will always be available in the system.

- **Data Retention**—This offers a configurable way to retain or purge long-live data such as location history and analytics raw data. When the Data Privacy feature is turned on for the first time, the database contains the real MAC addresses. As an administrator, you can decide to either back up the data and then purge it or directly purge it. Run the **cmxctl config data delete** command to purge this data. Restart the Cisco CMX after purging the data.
- **Disk Encryption**—Cisco CMX 10.5 supports CentOS7. You cannot upgrade to Cisco CMX 10.5.x from releases earlier than Cisco CMX Release 10.5. You must install and depoly the Cisco CMX 10.5.x OVA or ISO file on your system. For more information, see the *Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX Release 10.5* at:

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

CMX Grouping

The CMX Grouping feature (formerly known as AP Grouping) allows Cisco CMX to form an Access Point (AP) group consisting of all the APs learned from maps.

Note By default this feature is disabled.

The CMX Grouping feature helps to improve Cisco CMX performance in the following scenarios:

- Cisco CMX learns about the APs from the maps to compute the APs' location. However, in some instances, Cisco CMX will not have all the APs from the controller. In such a scenario, Cisco CMX will have to discard the RSSI probes received from the APs that are not available on maps.
- For Hyperlocation, Cisco CMX supports 1000 APs. Only 1 Cisco CMX with Hyperlocation enabled can be added to the controller. However, a large controller such as a Cisco 8500 Series Wireless Controller, managing 15,000 APs, has a lot to offer.
- Cisco CMX supports the exclusion of probing clients filter. This indicates that Cisco CMX discards the RSSI probes that is used for probing clients. However this filtering adds significant load on Cisco CMX when the probing clients are too many.

In Cisco WLC 8.7 or later, Cisco CMX communicates about the AP group to the controller, and the controller sends NMSP and UDP data for APs participating in the group. In Cisco WLC 8.7 or later, support is added to send only the required NMSP data to Cisco CMX. Note that Cisco CMX can subscribe to NMSP data of specific APs or AP groups based on the active services in Cisco WLC.

The performance of Cisco CMX can be optimized in the following ways:

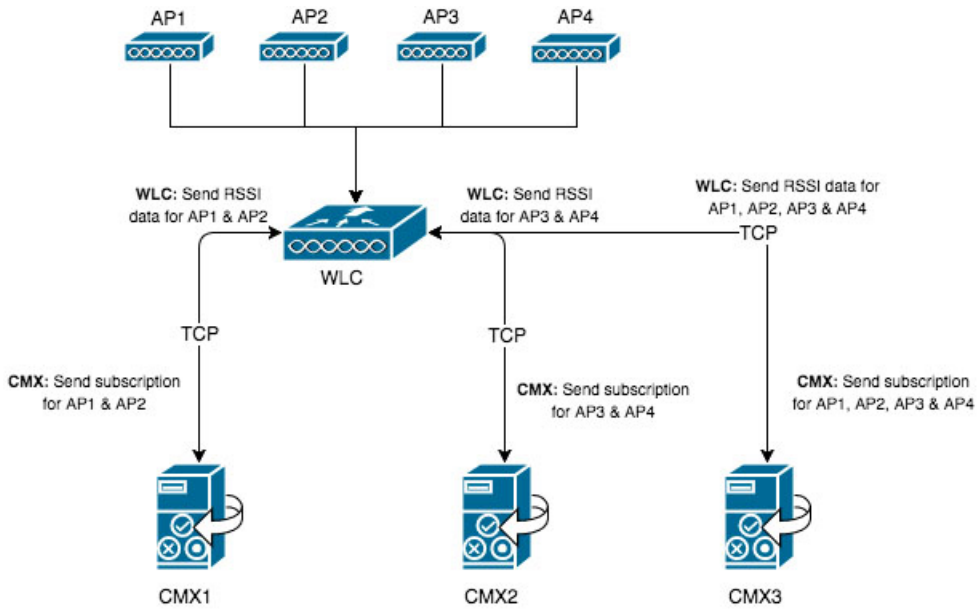
- Cisco CMX will not receive the NMSP and UDP data for the APs that are not available on maps.

- This helps Cisco CMX to form AP groups uniquely (no AP should be duplicated across AP groups) to receive the Hyperlocation data, which in turn helps leverage Cisco WLC's capacity to full extent.
- When exclude probing client filter is enabled, Cisco WLC 8.7 and later perform filtering and will do not send the NMSP data to Cisco CMX.

  For more information on how Cisco WLC supports NMSP by AP Groups, see the "NMSP by AP Groups with Subscription List from CMX" section in the *Cisco Wireless Controller Configuration Guide*.

This figure shows a sample architecture of a Cisco CMX Grouping:

Figure 2: Cisco CMX Grouping



Tip One important requirement for Cisco CMX grouping to work is that AP groups must always contain unique APs. This means that no AP should be repeated across the AP groups. If you have same APs in multiple AP groups, you must correct this error manually.

Note Caveats CSCvj54236 and CSCvi63871 provide information about Cisco WLC 8.7 and 8.7 special have limitations identified with respect to Cisco CMX. Cisco CMX Grouping does not work with hyperlocation deployments because of these limitations.

The CMX Grouping feature only supports wireless clients. Rogue clients are not supported.

Procedure

Step 1 Enable the Cisco CMX Grouping feature by entering this command: **cmxctl config feature flags nmsplb.cmxgrouping true**

Note To disable the feature, run the **cmxctl config feature flags nmsplb.cmxgrouping false** command.

Step 2 Restart Cisco CMX by entering this command: **cmxctl restart agent**

Step 3 Stop the Load Balancer service, used for NMSP messages to Location services by entering this command: **cmxctl nmsplb stop**

Step 4 Restart the Load Balancer service used for NMSP messages by running this command:**cmxctl nmsplb start**

To verfiy if the CMX Grouping feature is enabled, run the **cmxctl config featureflags** command and verify the value for *nmsplb.cmxgrouping*.

In WLC 8.7 and later, run the **show nmsp subscription group detail services** <*ip address*> *CMX_*<*ip address*> command to verify the subscription. In the command, replace <*ip address*> with your Cisco CMX IP address.

Enabling Cisco Hyperlocation and FastLocate in Cisco CMX

The Cisco Hyperlocation solution is a suite of technologies that enables advanced location capabilities through a mix of software and hardware innovations. The Cisco Hyperlocation Solution substantially increases the location accuracy for connected clients of the Connected Mobile Experiences. The FastLocate technology boosts the refresh rate so CMX captures more location data points. And the Angle-of-Arrival capabilities increases location accuracy to as close as one meter (50% Error Distance). The improved accuracy provides more granular analytics data compared to RSSI based location.

Cisco CMX Release 10.2.1 supports the Angle of Arrival (AoA) technology available on Cisco Aironet 3600, 3700, and 4800 access points with a Hyperlocation module and a Hyperlocation antenna. Cisco CMX uses advanced location algorithms to extract phase differences to accurately locate associated wireless clients up to one meter accuracy in an optimal deployment.

Cisco Hyperlocation is an enhanced location solution that takes advantage of the specialized hardware that is available on the Cisco Aironet 4800 Series wireless Access Points. It uses Angle-of-Arrival of Wi-Fi signals to determine the location of connected mobile devices. For more information about best practices to follow when deploying the AP4800 Hyperlocation solution, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_ap_4800_hyperlocation_deployment_guide.html.

The Cisco Hyperlocation module with advanced security also integrates Bluetooth Low Energy (BLE) beacons with the module. Customers can take advantage of BLE beacon deployment powered over Ethernet and centrally managed from the convenience of a data center. This eliminates the need for local IT engineers to perform an inspection walk of BLE beacon health, using an app on their Smart devices. Cisco Hyperlocation module enabled the capability for a single AP to beacon out five different BLE values to trigger different consumer applications.

Cisco CMX FastLocate technology enables quick location refresh for connected Wi-Fi clients. RSSI from data packets and probe frames, when available, are used for calculating a location. This technology is available with both centrally switched WLANs and FlexConnect (locally switched WLANs).

Cisco Aironet 700, 1700, 2600, 2700, 3600, 3700 and 2800 APs support Cisco CMX FastLocate when used with Cisco WLC Release 8.1.123.0 or later. Cisco Aironet 3800 APs support Cisco CMX FastLocate when used with Cisco WLC Release 8.7.102.0 or later.

Accuracy results for the Cisco FastLocate feature are reflected in the Cisco CMX Accuracy Tool under the **50% and 75% Error Distance** columns. Accuracy is considered good if the distance displayed under those columns is 10 meters or less, meaning the client will be detected less than 10 meters from its actual position.

For information about configuring Cisco FastLocate, see "FastLocate for Cisco Wave 2 Access Points" section in the *Cisco Wireless Controller Configuration Guide, Release 8.6* at:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-6/config-guide/b_cg86/location_services.html#ID2048

Note

- The above result is only valid for smart devices.
- We recommend that you have all the APs in the same group on a particular floor. If you cannot have APs in the same group, then plan to include nearby APs in the same group. All AP groups available on the same floor must be synchronized to the same NTP server.
- Ensure that you disable the global **Hyperlocation** option and enable **Hyperlocation** option speific for AP group. We recommend that you do not set the XOR radio to monitor mode manually. When you enable Hyperlocation in the AP group, the XOR radio settings are taken care by default.

The following are the recommended AP modes:

- Enhanced Local Mode—APs scan opportunistically on-current channel and off-channel with up to ~15 percent performance impact to data-serving radios.
- Monitor Mode—APs scan on 2.4 and 5 GHz bands.
- Modular Mode—Cisco 3600 and 3700 APs with Hyperlocation Module or Wireless Security Module (WSM) scan on 2.4 and 5 GHz bands with no impact to data-serving radios.

Note

- The FastLocate and Cisco Hyperlocation features are supported in Cisco CMX 10.2.1 and later.
- In Cisco CMX Release 10.4, FastLocate feature is supported on Cisco Aironet 2800/3800 access points running Cisco Release 8.6 or later.
- In Cisco CMX Release 10.3.1, the Cisco Hyperlocation feature supports 10,000 tracked devices—1000 Cisco access points (APs) with up to 10 connected clients per AP—on Cisco 3365 Mobility Services Engine (MSE) and Cisco high-end MSE Virtual Appliances (v MSE) running Cisco CMX Release 10.3.1 and later.
- The Hyperlocation and FastLocate features are supported in Cisco WLC 8.1.123.0 and later.
- Currently, a Hyperlocation-enabled Cisco WLC can support only one Hyperlocation-enabled Cisco CMX. However, starting from Cisco CMX release 10.5 and controller release 8, the CMX group subscription feature will allow one hyperlocation enabled WLC to connect to multiple CMX servers. For more information about CMX Grouping, see CMX Grouping, on page 38.
- The Cisco Hyperlocation feature is not supported on a virtual Cisco WLC.

Procedure

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

Step 2 Choose **SYSTEM** > **Dashboard**.

Step 3 Click the **Gear** icon at the top-right corner of the window.
The **SETTINGS** window is displayed.

Step 4 Click the **Location Setup** tab.

Step 5 In the **Location Calculation Parameters** window, check the **Enable Hyperlocation / FastLocate/ BLE Management** check box.

Step 6 Add Cisco WLC to Cisco CMX.

Note If hyperlocation is enabled and one controller is in active status, and no data is received for almost 15 minutes an alert is generated with the following description "Hyperlocation is enabled on CMX, however no AOA data is received". The alert service type is Hyperlocation and alert type is Service_Status.

As a work around, maintain a one to one mapping between controller and Cisco CMX. Only one controller can serve one Cisco CMX box with hyperlocation enabled. If two hyperlocation enabled Cisco CMX boxes are using the same controller, disable hyperlocation service in one of the Cisco CMX box.

Hyperlocation Mixed Mode Support

Cisco CMX Release 10.4 now supports a mixed deployment of Cisco Hyperlocation access points (AP) and non-Hyperlocation AP on the same floor map. If the client is associted to a regular access point but has a hyperlocation enabled access point near by, AoA computation is performed to provide an an acceptable accuracy. All Cisco Hyperlocation APs must be within a contiguous area. Increased accuracy on the floor is only within the convex hull of the Hyperlocation contiguous are

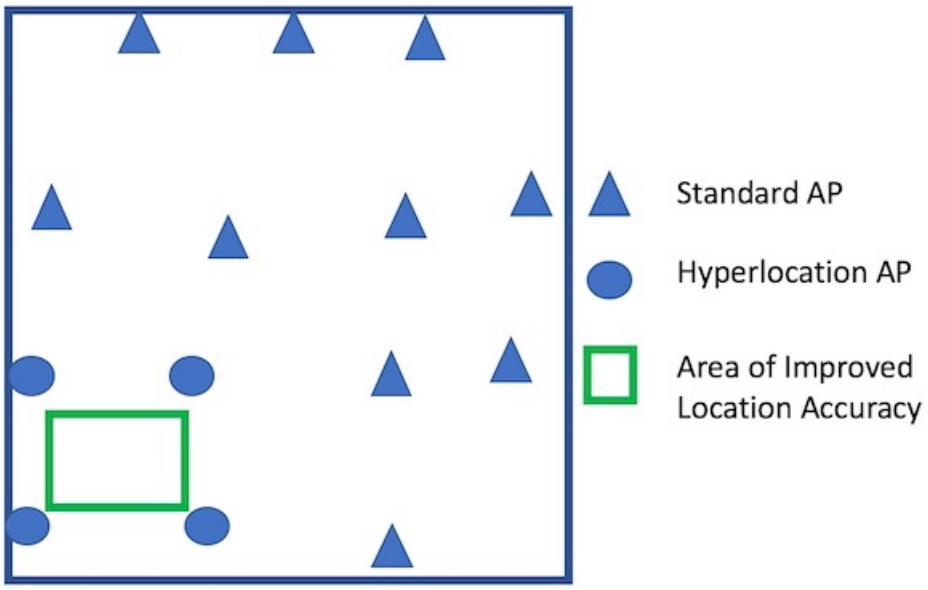
Hyperlocation groups are formed consisting both hyperlocation and regular access points. The floor mode is decided when generating the hyperlocation group. There following are the three supported modes:

- RSSI mode-All access points on the floor are regular APs.
- Mixed mode: Few APs on the floor are Halo APs.

Note Use the **cmxctl config hyperlocation mixmode***Floor ID* command to enable hyperlocation mixed mode.

We recommend that you use this command in a deployment senario where there are both Hyperlocation enabled APs and non Hyperlocation APs on the same floor map. The improved location accuracy that comes from the use of Hyperlocation AP will occur within the convex hull of the Hyperlocation APs. Outside of this convex standard location accuracy results will occur. At the edges of the convex hull there may also be lower accuracy then when clients are at least 10M inside of the convex hull. This command does not support the interspersion of Hyperlocation AP with non Hyperlocation AP. If this is type of deployment is used, then there will be no improvement in location over standard probe RSSI based location.

An example of an supported deployment is as follows:



- Halo mode: All APs on the floor are Halo APs.

Running Hyperlocation Diagnostics

Hyperlocation Diagnostics is a tool that can find common issues in a Hyperlocation deployment.

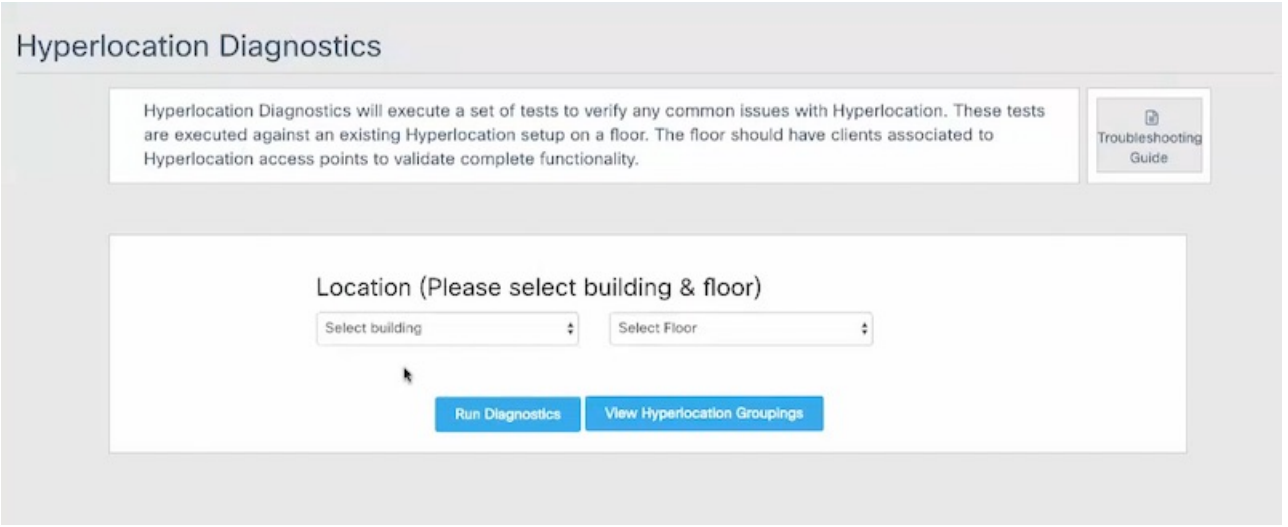
Hyperlocation Diagnostics executes a set of tests to verify any common issues with Hyperlocation. These tests are executed against an existing Hyperlocation setup on a floor. The floor should have clients associated to Hyperlocation access points to validate complete functionality.

Procedure

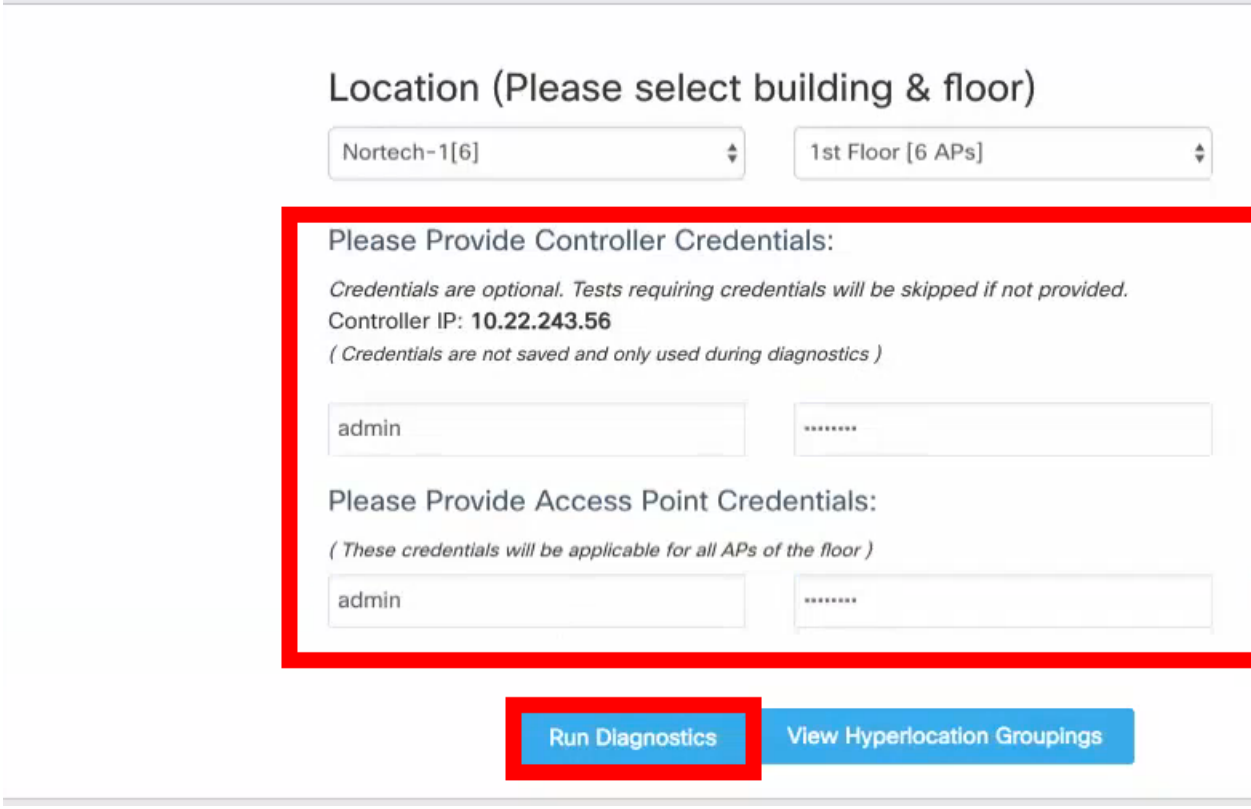
Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX) either as an admin user or a user with Location role.

Step 2 Choose **DETECT & LOCATE** > **Troubleshooting**.

The **Hyperlocation Diagnostics** window is displayed. As this is a floor-level test, select a building and floor. Note that only floors with hyperlocation access points are populated here.

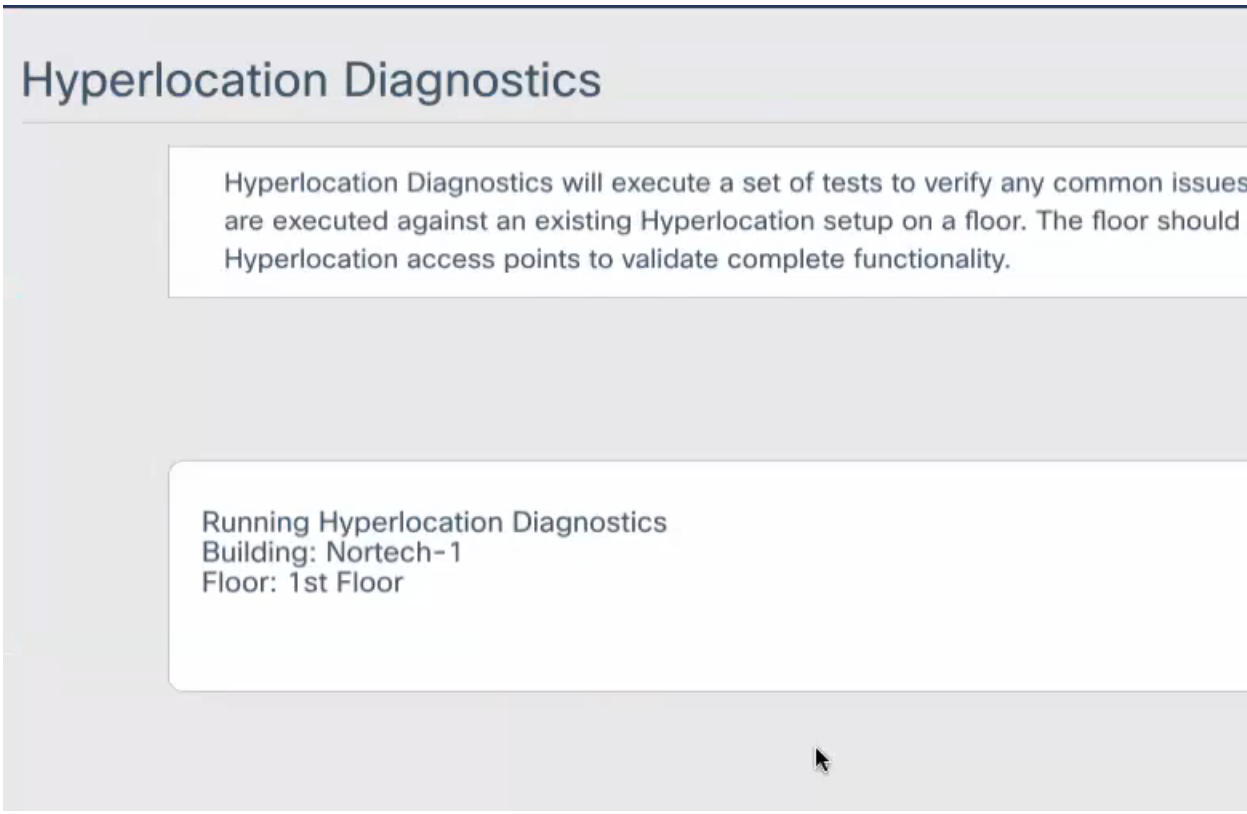


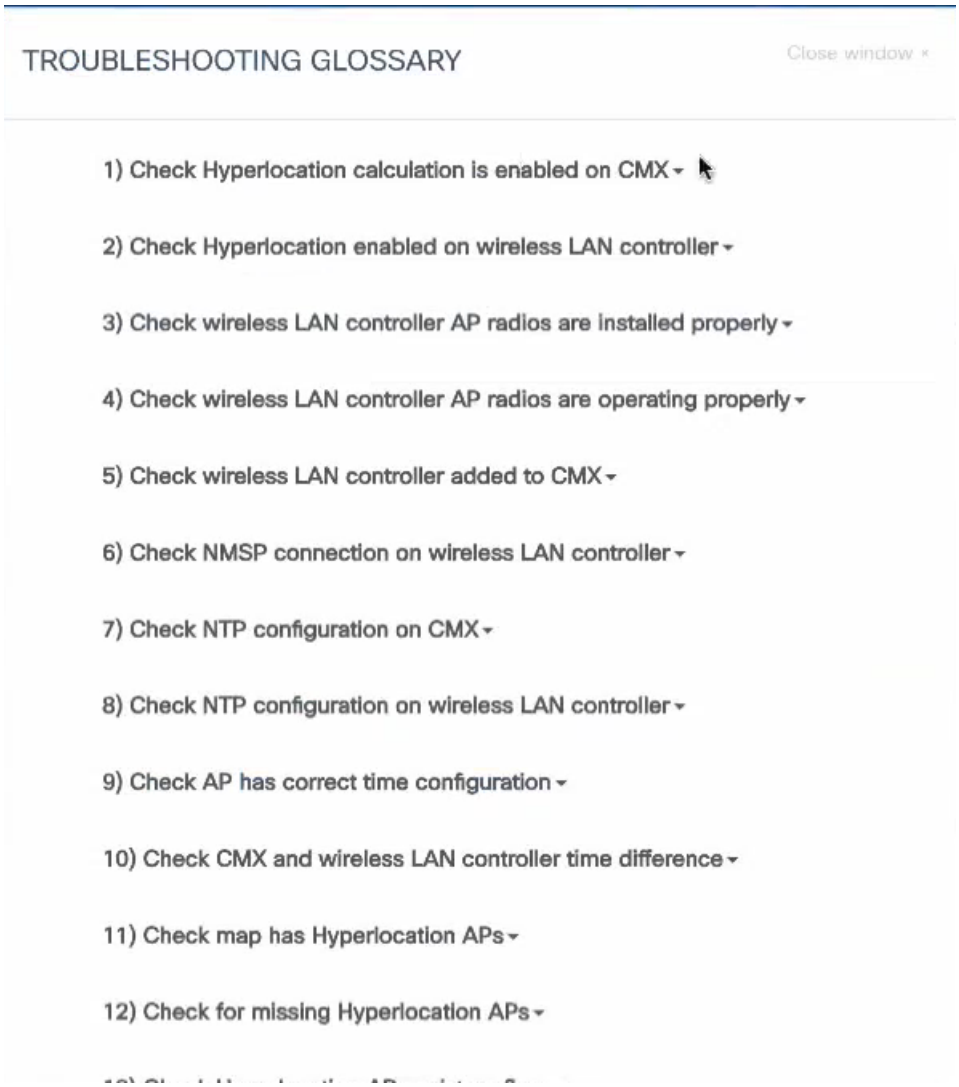
Step 3 (Optional) Add the details and credentials of a controller and an access point for a more detailed report.



Step 4 Click **Run Diagnostics** and wait for a few minutes.

a) Click the **Troubleshooting guide** for a detailed description of each test.

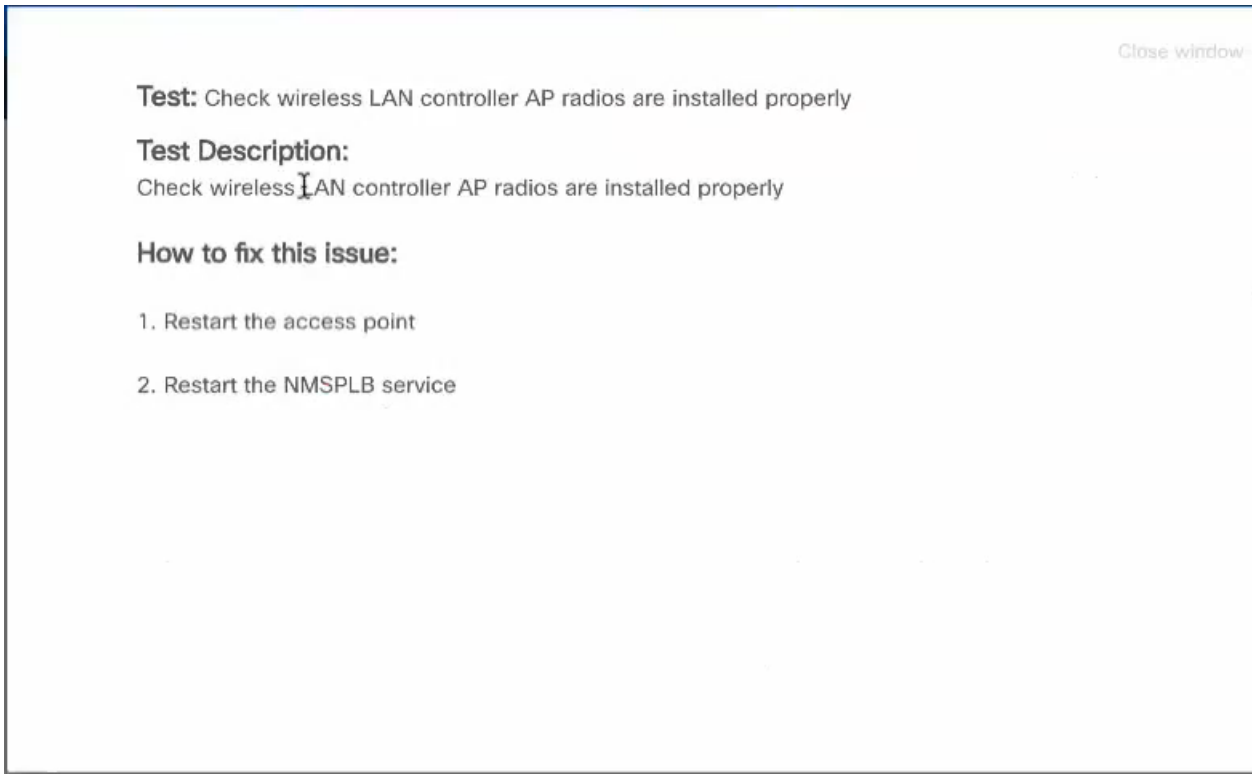

Hyperlocation Diagnostics
Hyperlocation Diagnostics will execute a set of tests to verify any common issues
are executed against an existing Hyperlocation setup on a floor. The floor should
Hyperlocation access points to validate complete functionality.
Running Hyperlocation Diagnostics
Building: Nortech-1
Floor: 1st Floor



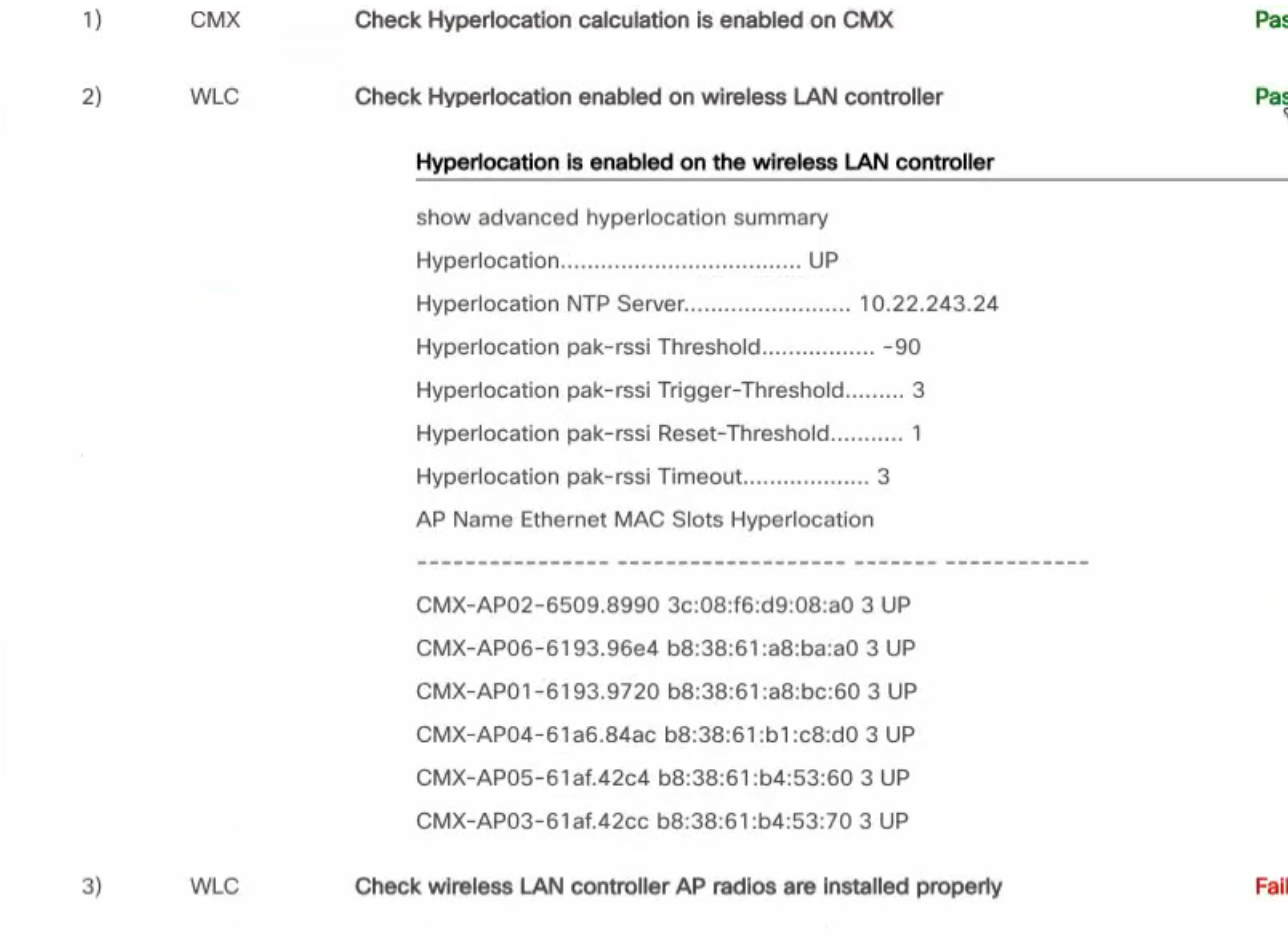
Step 5 Observe a sample test result. The Test Type indicates which deployment component is being tested, and it can be CMX, WLC, or AP.

Test No	Test Type	Test Name	Re
1)	CMX	Check Hyperlocation calculation is enabled on CMX	Pa
2)	WLC	Check Hyperlocation enabled on wireless LAN controller	Pa
3)	WLC	Check wireless LAN controller AP radios are installed properly	Fa
4)	WLC	Check wireless LAN controller AP radios are operating properly	Pa
5)	CMX	Check wireless LAN controller added to CMX	Pa
6)	WLC	Check NMSP connection on wireless LAN controller	Pa
7)	CMX	Check NTP configuration on CMX	Fa
8)	WLC	Check NTP configuration on wireless LAN controller	Pa
9)	AP	Check AP has correct time configuration	Pa
10)	WLC	Check CMX and wireless LAN controller time difference	Pa

Step 6 If a test has failed, click **Fix Issue** for instructions on how to resolve the issue.



Step 7 Expand a passed test result to see further details of the test.



Step 8 If the **Check AoA messages increasing for access points** test has failed, expand the test.

This may happen if there aren't clients to communicate with the access point, and hence the message count does not increase.

1) CMX Check Hyperlocation calculation is enabled on CMX

2) WLC Check Hyperlocation enabled on wireless LAN controller

Hyperlocation is enabled on the wireless LAN controller

```
show advanced hyperlocation summary
Hyperlocation..................................... UP
Hyperlocation NTP Server..... 10.22.243.24
Hyperlocation pak-rssi Threshold..... -90
Hyperlocation pak-rssi Trigger-Threshold..... 3
Hyperlocation pak-rssi Reset-Threshold..... 1
Hyperlocation pak-rssi Timeout..... 3
AP Name Ethernet MAC Slots Hyperlocation
--------------- ----------------- ------- ------------
CMX-AP02-6509.8990 3c:08:f6:d9:08:a0 3 UP
CMX-AP06-6193.96e4 b8:38:61:a8:ba:a0 3 UP
CMX-AP01-6193.9720 b8:38:61:a8:bc:60 3 UP
CMX-AP04-61a6.84ac b8:38:61:b1:c8:d0 3 UP
CMX-AP05-61af.42c4 b8:38:61:b4:53:60 3 UP
CMX-AP03-61af.42cc b8:38:61:b4:53:70 3 UP
```

3) WLC Check wireless LAN controller AP radios are installed properly

a) Expand the test for a further look, and ensure that there is a significant difference for the first and second reading for access points that are connected to clients.

18) CMX Check AoA messages are increasing for access points Passed

All access points have increasing AoA messages

AP Name	AP MAC	AP IP	Result
CMX-AP01-6193.9720	b8:38:61:a8:bc:60	10.22.243.128	Message count is increasing
CMX-AP02-6509.8990	3c:08:f6:d9:08:a0	10.22.243.164	Message count is increasing
CMX-AP03-61af.42cc	b8:38:61:b4:53:70	10.22.243.113	Message count is increasing
CMX-AP04-61a6.84ac	b8:38:61:b1:c8:d0	10.22.243.123	Message count is increasing
CMX-AP05-61af.42c4	b8:38:61:b4:53:60	10.22.243.141	Message count is increasing
CMX-AP06-6193.96e4	b8:38:61:a8:ba:a0	10.22.243.126	Message count is increasing

Message count for AP-CMX-AP01-6193.9720

Message count for first reading 1700336

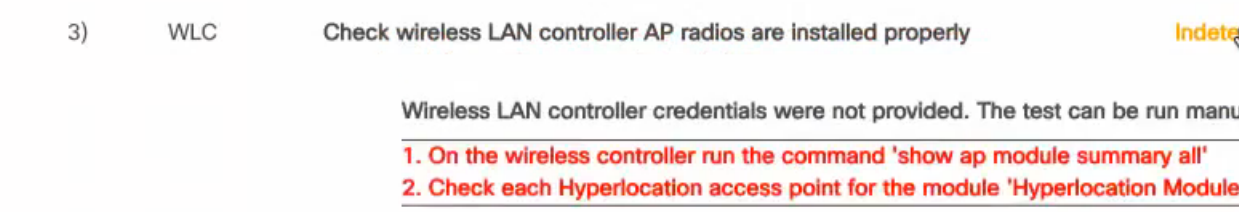
Message count after 10 second interval 1700348

Message count for AP-CMX-AP02-6509.8990

Message count for first reading 1706098

Message count after 10 second interval 1706110

Message count for AP-CMX-AP03-61af.42cc



If you haven't provided the optional controller and access point details, the corresponding tests will not be executed, and the result is marked INDETERMINATE for your reference.

View Hyperlocation Groupings

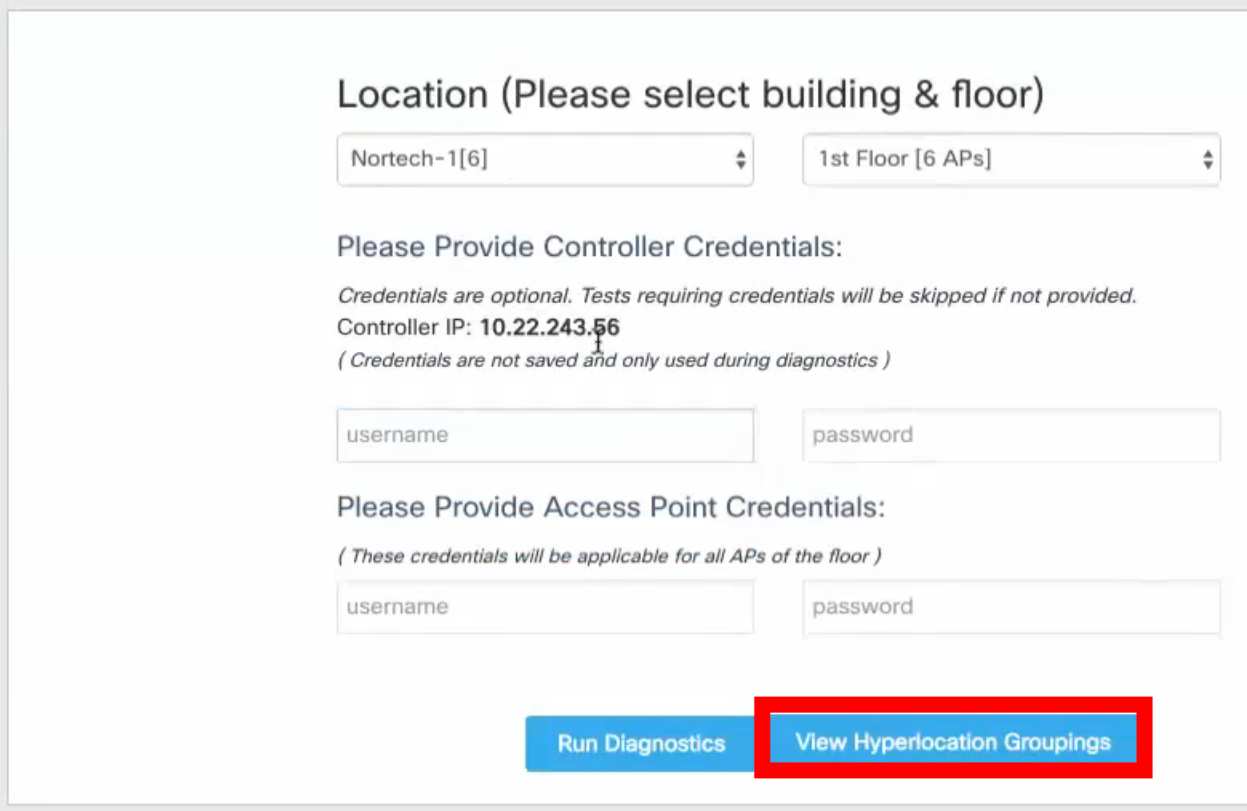
The Hyperlocation deployment calculates location in the following manner. During the time period of a slot, the respective primary emits bar packets. Bar responses are sent by client devices in the vicinity. The subordinates access point listen to these response packets. The primary and subordinates then use the collected information to calculate the location of a client, as a collective activity. This process is repeated, with the primary and subordinates of the next slot. If a floor is too large, there maybe more than one primary. The primary and subordinates form groups, and a floor may have more than one such group.

Procedure

Step 1 Open the CMX Dashboard, **Detect and Locate>Troubleshooting**. As this is a floor-level test, select a building and floor. Note that only floors with hyperlocation access points are populated here.

Step 2 Click **View Hyperlocation Groupings** to configure a different primary for a slot.

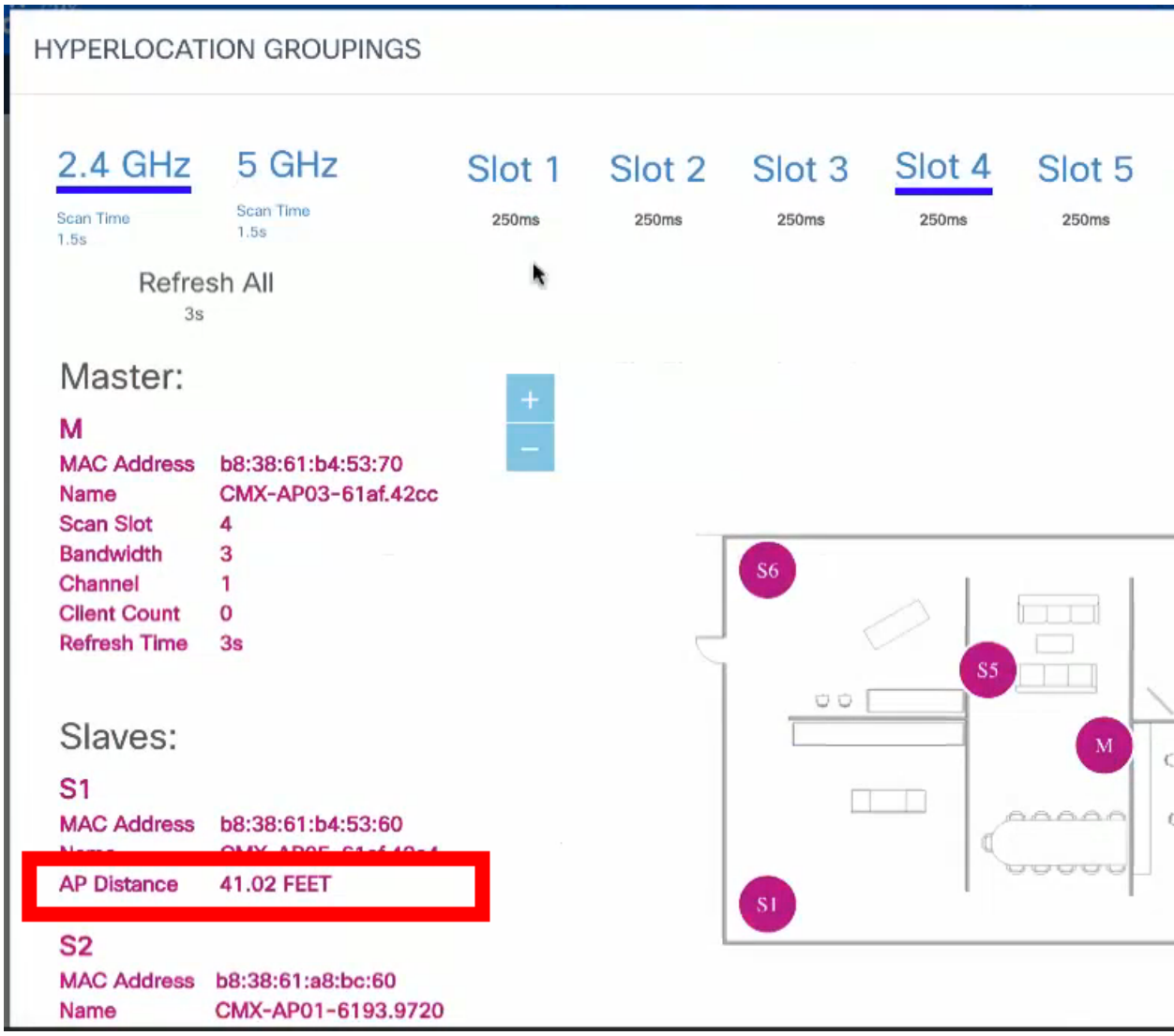
Note You can observe that each slot has an allocated time which is listed below the slot. There are also two frequency bands, 2.4 and 5 GHz, each with scan times. Scan time is the total time allocated to scan every slot of a band at least once. Since there are two such bands, 2.4 and 5 GHz, the total Refresh time is the sum of these two, and is the time taken to scan all slots of all bands.



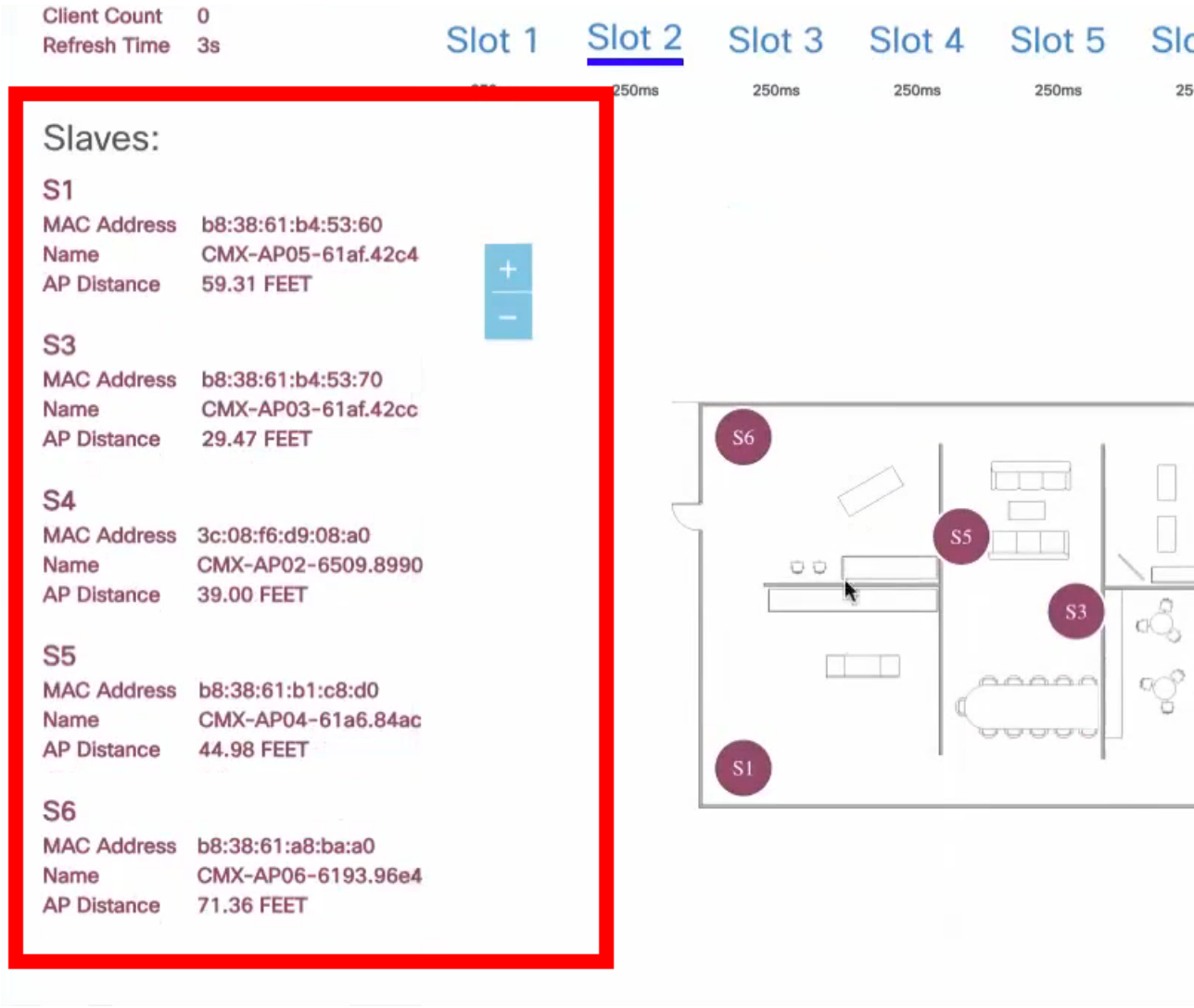
Step 3 Click a frequency band, and select a slot. You can observe the primary access point for the site marked by M, and the subordinates marked by S. You can also change the primary to a more appropriate one in this page.

Step 4 Observe details of the primary access point of a slot, like bandwidth, channel and client count.

Step 5 Observe the distance of a subordinate AP from the respective primary.



Step 6 Observe that each slot has an allocated time which is listed below the slot. There are also two frequency bands, 2.4 and 5 GHz, each with scan times. Scan time is the total time allocated to scan every slot of a band at least once. Since there are two such bands, 2.4 and 5 GHz, the total Refresh time is the sum of these two, and is the time taken to scan all slots of all bands.



Controlling the Probing Client Expiry Time

Probing clients count is usually more visible on CMX than compared to Wireless LAN Controller (WLC). WLC tracks the clients until the client no longer probes for more than five minutes, whereas CMX maintains the probing client for 10 minutes.

Connected Clients do not have this behavior because, WLC notifies CMX when the clients are disconnected from the network. You can perform additional configuration changes on CMX, if you want to minimize the probing client count on CMX.

Caution We do not recommend to set the value less than five minutes because some clients may not sent probe and in that case CMX will lose such clients. This configuration change could also increase the Analytics service processing time.

Procedure

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

Step 2 Click **DETECT & LOCATE**.

Step 3 Choose **SYSTEM > Settings > Filtering**.

Step 4 Specify the **RSSI Cutoff** value as -75.

Note Setting the RSSI cutoff to -75 affects the probing clients only. This allows Cisco CMX to filter out weak probing clients in the initial stage.

Step 5 Navigate to **`/opt/cmx/etc/`** and open the **`node.conf`** file.

Step 6 To set the expiry time, at the end of the Location Services section, add **user_options=-Dredis_ttl=5**.

Note Cisco CMX maintains the default age out for clients as 10 minutes and when the client leaves the network, CMX usually takes 10 to 15 minutes to clean up the stale client details. If you set the age out to five minutes, Cisco CMX will perform the clean up in five to 10 minutes. Together, the RSSI cutoff and age-out settings, help Cisco CMX to narrow down the probing client count with respect to the WLC count.

Step 7 To restart the CMX agent, run the command **cmxctl agent restart**.

Step 8 To restart the Location Services, run the command **cmxctl location restart**.

Supported Access Points for Cisco CMX 10.5 Location Features with Cisco WLC 8.7

The following table lists the Cisco CMX 10.5 Location features and the APs that support these features:

Table 3: Supported Access Points

Location Feature	Supported Marvel-Based Cheetah Access Points	Supported Cisco IOS Access Points (2700, 3700, 3600)
FastLocate	2800, 3800	2700, 3700, 3600
Hyperlocation	4800	3602E and 3702E with HALO radio module 3010 (RM3010L)
Hyperlocation Mix mode	HALO (3602E and 3702E with HALO radio module 3010 - RM 3010L) and non-HALO (all Cisco IOS)	

Location Feature	Supported Marvel-Based Cheetah Access Points	Supported Cisco IOS Access Points (2700, 3700, 3600)
Tuna antenna support	Not supported	3602E, 3702E
BLE	Integrated BLE: 1800, 1810, 1815, AP1542 (Outdoor) 5 dynamic beacons for AP 4800. Floor beacons are available as beta version only.	Not supported

Measuring Client Location Accuracy Using the Location Accuracy Test

From Cisco CMX 10.2, you can perform a location accuracy test for a single device with multiple location points. You can use the Location Accuracy Test tool to validate the placement and number of access points to ensure that the CMX deployment is giving the best location accuracy experience. The Location Accuracy tool provides an administrator the ability to quantify the location accuracy for a specific location by using a Wi-FI device to measure the difference between the actual and calculated location of a device

To run a location accuracy test, perform the following task:

Procedure

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

Step 2 Click **DETECT & LOCATE**.

Step 3 Using the left pane of the **Activity Map** window, navigate to the desired building and floor.

Step 4 Use the search option on the **Activity Map** window to search for a device, for example, Client, RFID Tag, or BLE Tag. In this task, we will choose a client.

Step 5 Click the corresponding connected client, indicated by a green dot.

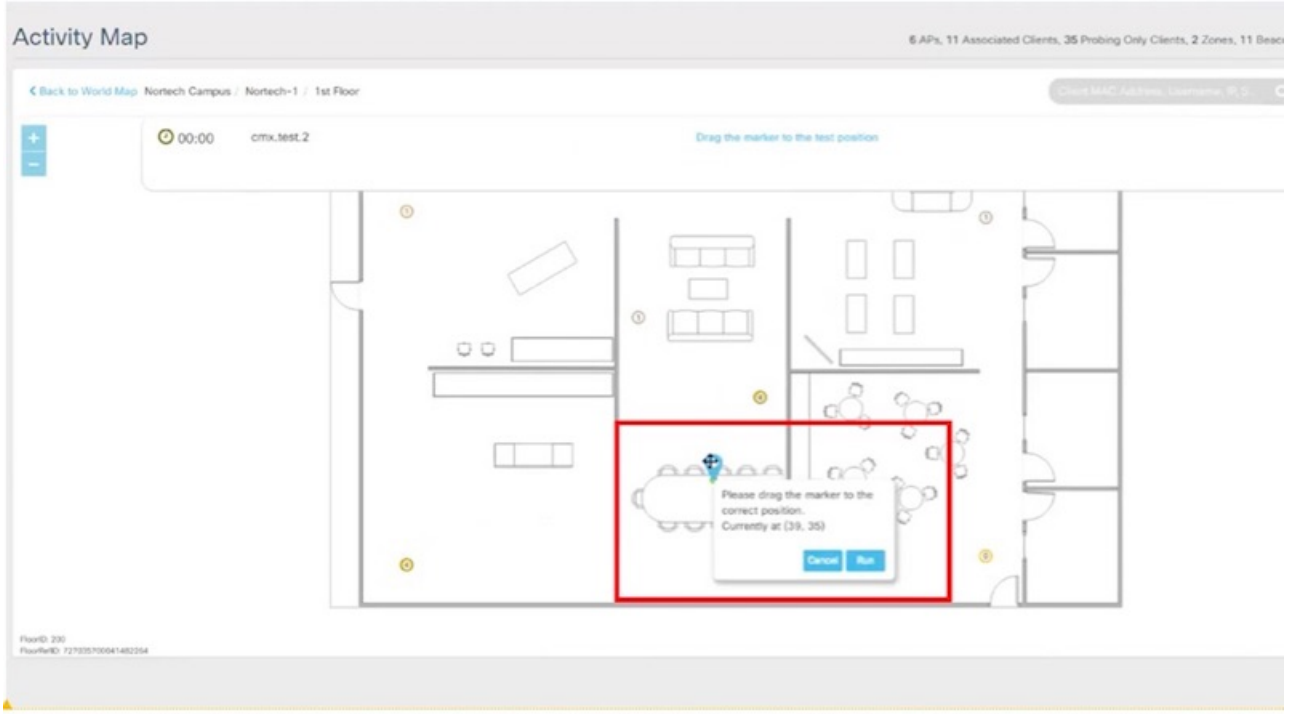
The **Client** dialog box is displayed.

Step 6 Click the **LOCATION ACCURACY TEST** icon to start the location accuracy test.

Step 7 In the **Enter a test name** text box, type a name for the location accuracy test, and then press the **Enter**.

A dialog box, asking you to place the marker at the client device's actual position on the map, is displayed.

Step 8 Drag the marker to the correct position.



Step 9 Click **Run**.

Observe the increasing samples. This indicates the number of times the client is detected at the pin-pointed location. You can run the test for any required amount of time. The elapsed time of the test is displayed.

Step 10 Refresh your client frequently so that it exchanges information with the access points around it.

Step 11 Click **Pause** when you finish testing of the current location.

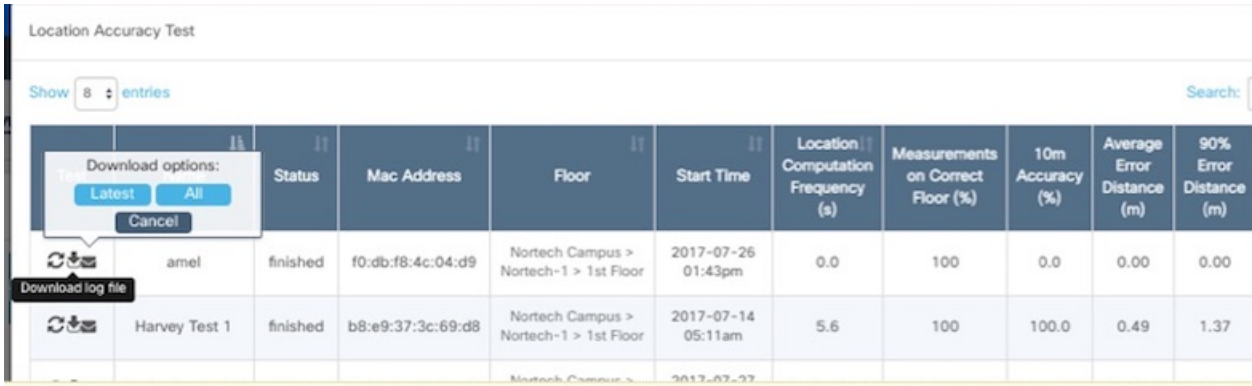
You can move your device to another location and continue testing (repeat Step 8 through Step 10). Wait for 30 seconds before resuming the test at a new spot, to eliminate any movement related discrepancies in the test result. Try to collect at least twenty samples at each spot, running the test at a spot for around five minutes.

Step 12 After you complete testing all the location points, click **Finished? View Result** to fetch the test results.

A dialog box, showing 10 m accuracy and Average Error Distance is displayed.

Step 13 Click **View accuracy test report** icon on the top-right corner of the window to view the list of accuracy tests that you performed. This report enables you to restart a test, download the latest log or all logs, or email the test results.

The Location Accuracy Test window is displayed with the test details such as test name, status, MAC address, floor, start time, location computation frequency, measurements on correct floor (in percentage), accuracy and error distance. Click **Export All** to export the test results as CSV files.



Note Even when the test is in progress, you can click **View accuracy test report** to monitor all the tests. You can pause a running test by clicking **Pause**. You can continue a paused test by clicking **Relaunch**. To finish the test and get the results, click the **Report** icon.

To remove a report from the test report table, click **Delete**.

The Location Accuracy Test window is displayed. You can view all the previous test results in this window, not restricted to the selected floor, but includes all test runs. You also can download the log files, email the test results, and delete the tests.

Step 14 Analyze the test results.

What to do next

You can also perform the Location Accuracy Test using the Cisco CMX mobile application. The Cisco CMX mobile application complements the Cisco CMX product by providing a set of monitoring and testing tools for CMX deployments. The application enables users to monitor the status of CMX, monitor the number of

devices being tracked, receive alerts, test the location accuracy of the deployment, and test the latency of location updates. For more information, see https://blogs.cisco.com/wireless/introducing-the-cisco-cmx-mobile-app-for-deployment-administrators.

Analyzing Location Accuracy Results

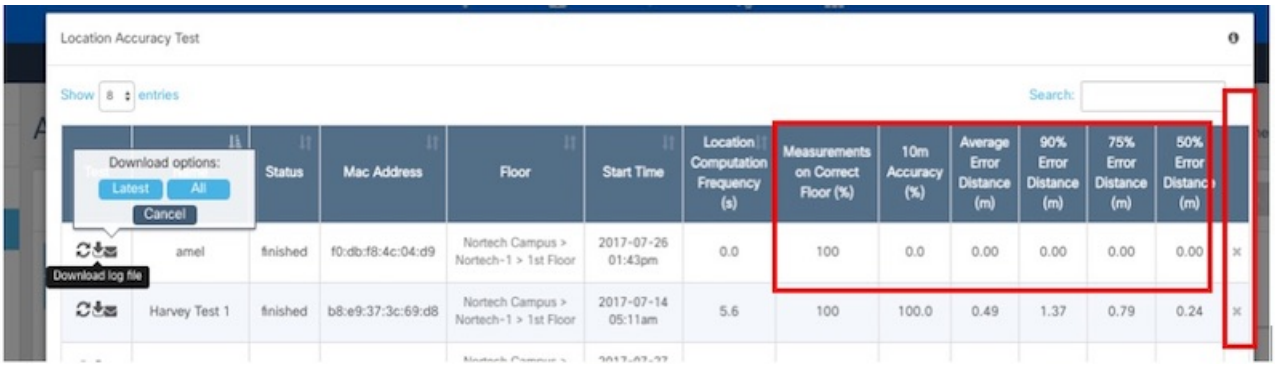
Observe the test results in the figure below.

The test results displayed indicate that for 100% of the time, Cisco CMX locates the client within this many meters from where the client is actually located.

It also indicates that for 50% of the time, Cisco CMX locates the client within this many meters from where the client is actually located. A good location accuracy test result for an RSSI deployment is 10 meters, and should be within 10M for FASTLocate with update rate of better then 1 update per 30 seconds.

Location Accuracy testing is not supported on Axel-E APs with external antennas (for example, Marlin 1,2,3,4). However, Location detection is supported on Axel-E APs.

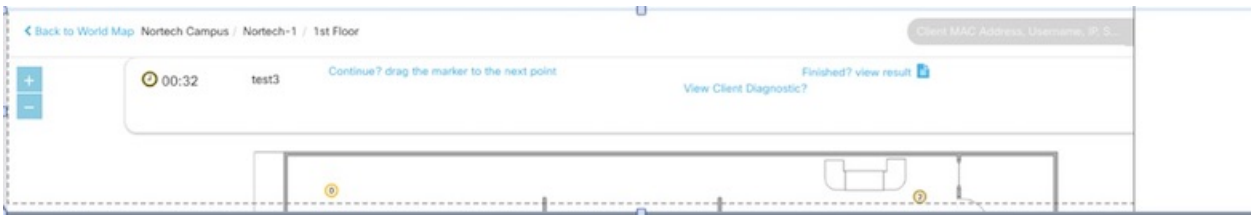
Observe the complete location-accuracy test below:



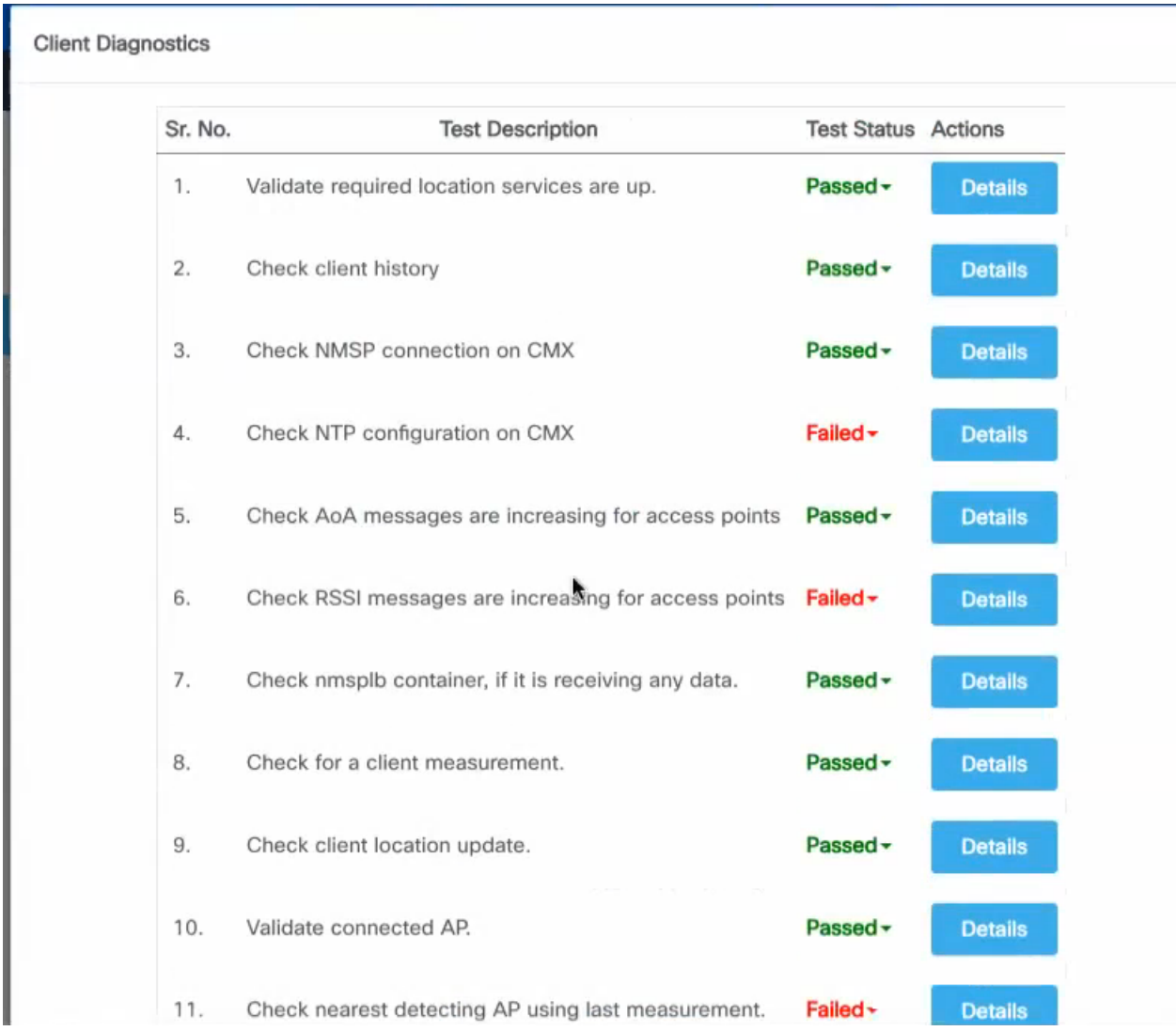
Ensure that **Measurements on Correct Floor** should be at 100%. This is an indicator of whether the client has been detected by the access points on the same floor, and not on a different floor. You can delete the test and the corresponding log files using the cross buttons here.

Understanding Client Diagnostics

Client diagnostics is a way to understand whether the tested client is sending messages to Cisco CMX for location-accuracy calculations.You can view Client Diagnostics during the location accuracy test.



Below is a sample test report.



It is best to ensure that all the tests here are in Passed status.

You can also email a summary of the messages to your Technical Support department for troubleshooting. Given below are some of the outputs of individual tests.

Figure 3: Sample Output: Check Client History

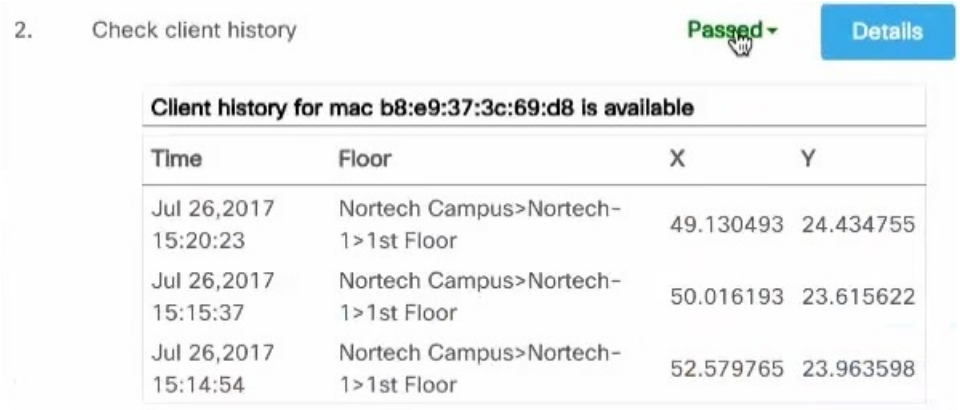


Figure 4: Sample Output: Check Heatmaps are generated

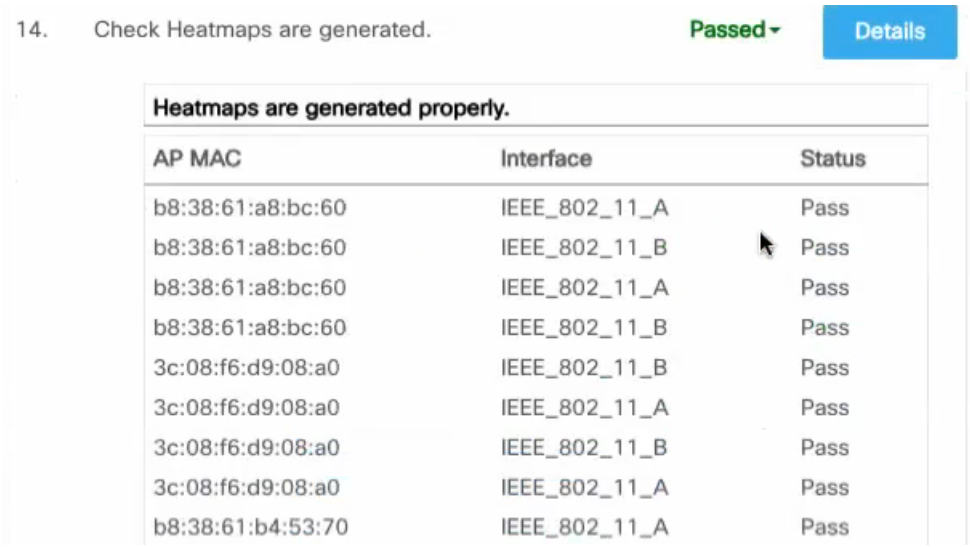
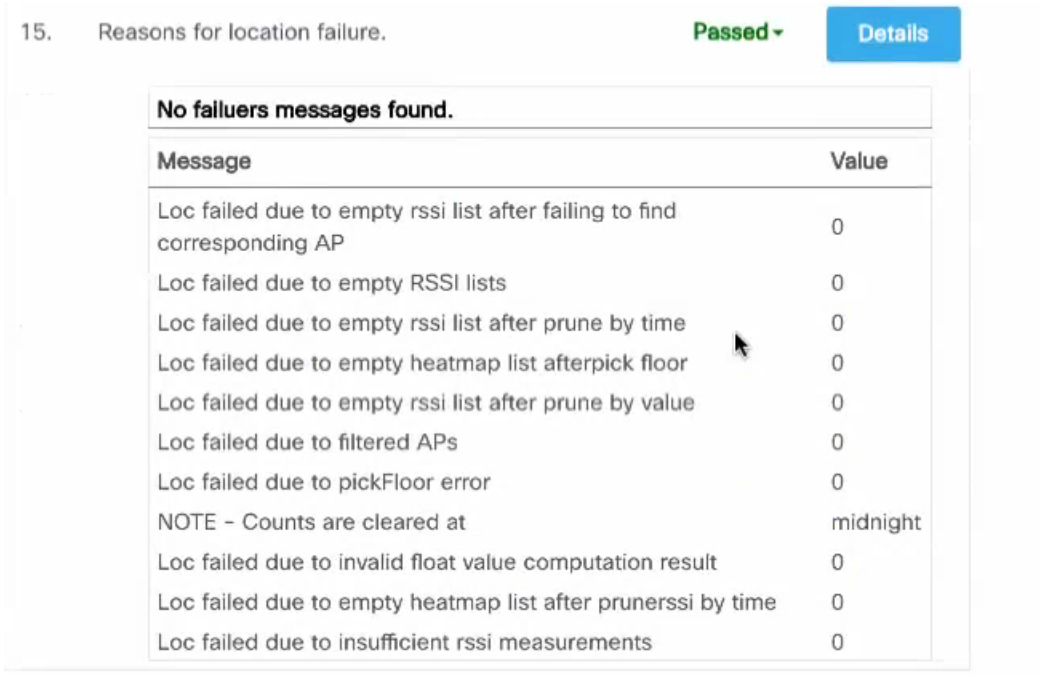


Figure 5: Sample Output: Reasons for location failure

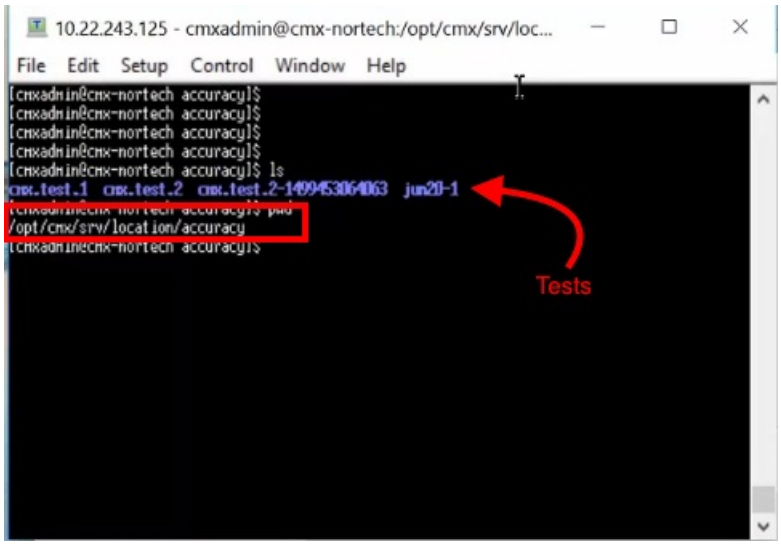


Analyzing Location Accuracy Log Files

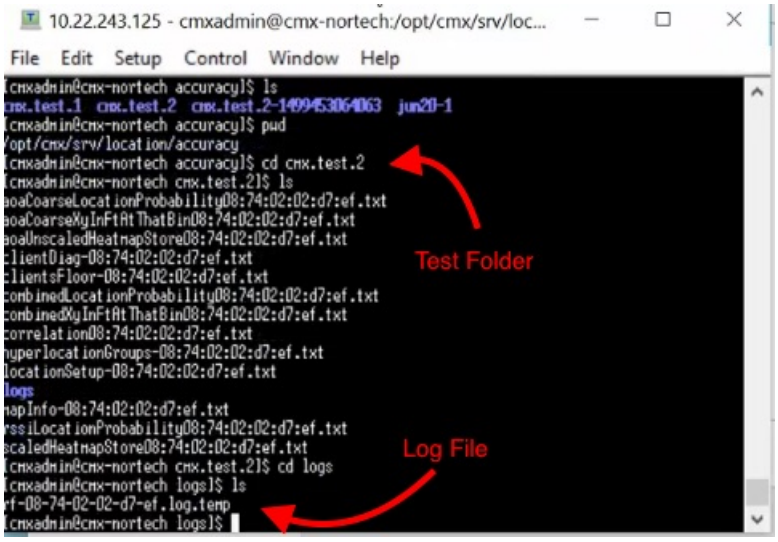
This task analyzes the Location Accuracy log files stored in `/opt/cmx/srv/location/accuracy`.

Procedure

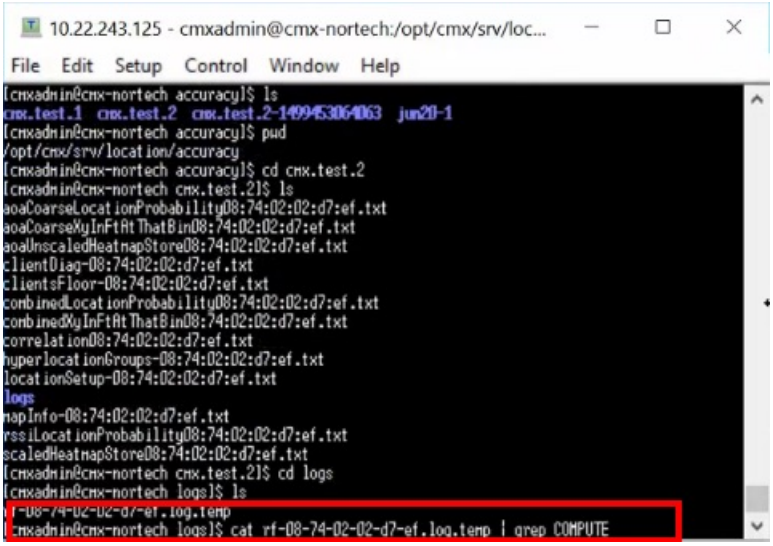
Step 1 Telnet into the CMX box and navigate to the `/opt/cmx/srv/location/accuracy` directory where location accuracy results are stored by default.



Step 2 Navigate to the folder named after your test.



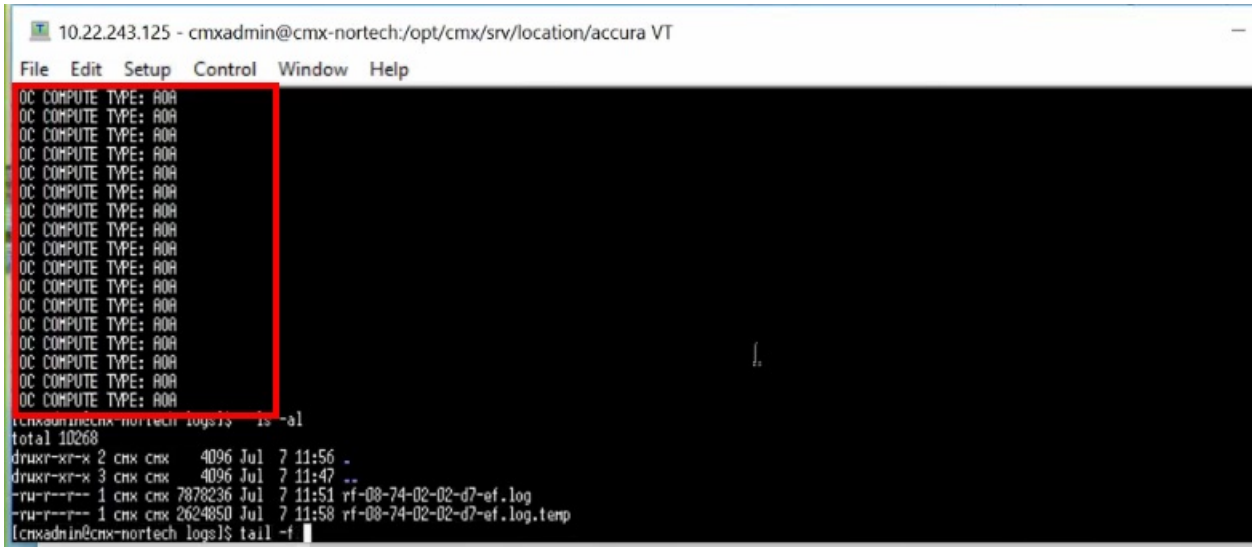
Step 3 Navigate into the `logs` folder, where the log files are stored.



Step 4 Use the grep command to find entries with COMPUTE in this log file.

```
cat <filename>.log.temp | grep COMPUTE
```

The following is a sample output that is displayed. You can see new entries added to the log file, while the location-accuracy test is performed. Activate your device to see the addition of fresh entries.



Location Accuracy for Hyperlocation Deployments

You can also run Location accuracy tests to test the efficiency of your hyperlocation deployment. Run the test from the **Map Tab** of **Detect and Locate**. Here are some points that will help improve the test results.

- As samples are collected every 3-5 seconds, set the refresh rate of the dashboard to five minutes before running the test.

- A good location accuracy result for a hyperlocation deployment has an Average Error Distance of around one meter.
- Convex hull is the perimeter formed by drawing lines connecting 3 or more APs in a AP group. Ensure that a test client is within the convex hull of an AP group.
- Do not choose a client that is in a spot between AP groups, our outside the convex hull of AP groups.
- You can use the Location Accuracy test to calculate latency in a Hyperlocation deployment. This is especially useful if you would like to know when clients visit your store in order to send personnel to greet them. You can find the latency by moving a test client, and observing how many seconds it takes for your Cisco CMX location accuracy dashboard to update itself with the new client location. Usually, it takes around 2-3 seconds to update its location. Ideally, latency should not be more than 5 seconds for a hyperlocation deployment.

Accuracy Testing

You need at least one connected client for accuracy testing. Creating a 5 GHz only WLAN SSID will ensure you have the most accurate location test.

Figure 6: WLAN configuration for 5 GHz-only SSID

Accuracy testing is done with a static device. Make sure your test points are inside the convex hull of your AP coverage. It is recommended to collect 25-50 samples per point. Repeat the test in multiple locations throughout your coverage area. Accuracy tests will not improve location accuracy as the results will not be used for any kind of calibration. You might want to use different clients at the same location to understand the client impact on accuracy.

- Choose a client for your accuracy test
- Pick multiple points across your venue, note the X, Y of your test points
- Execute the test on each of the points and collect 25-50 measurements per point
- Finish the test and review the test results

You can execute the tests using GUI or CLI. GUI is a bit more comfortable, while CLI gives you a few more details while the test is executed.

Testing accuracy using GUI

To execute accuracy tests, via the GUI on CMX navigate to the Detect & Locate tab. Selecting the client (green dot on the map) will expand the Client details pane on the left. Use the pin icon to start the test. The number of samples will be updated. After collecting enough sampled click pause and then finish to end the test.

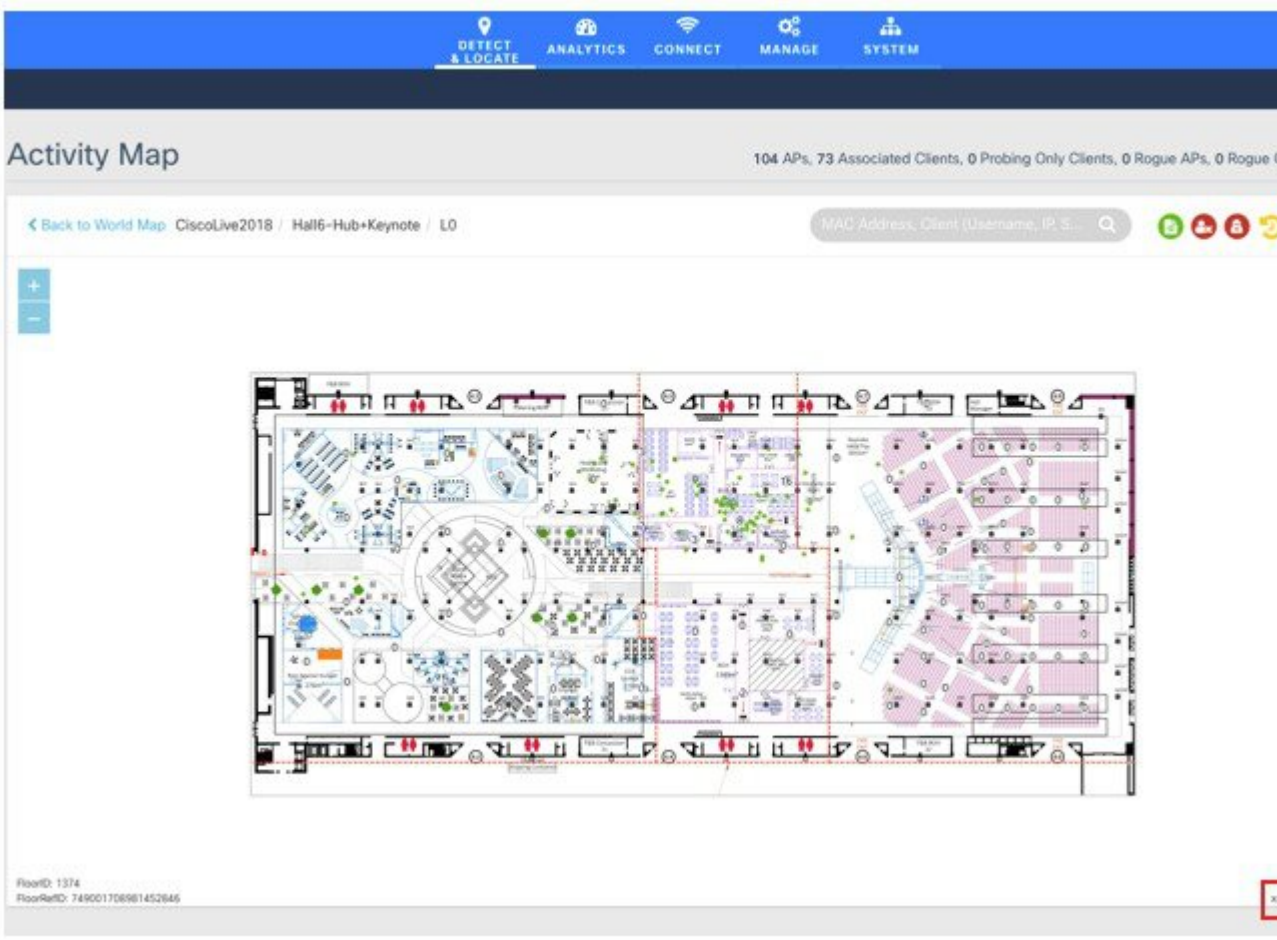
Figure 7: GUI accuracy testing

Test results can be viewed by clicking on the green icon .

Testing accuracy using CLI

You need the X, Y of your test points. You can use the CMX GUI Detect & Locate tab, select the map and move your mouse pointer to the test point, you can read the X and Y coordinates on the bottom right of your map.

Figure 8: Activity Map - X, Y Information



Login using console or SSH to your CMX. To start a location accuracy test, use the cmxloc start command. You will be prompted to enter the client MAC address, a test name and the X, Y of the real location. You can also select the duration of the test.

```
[cmxadmin@cmx ~]$ cmxloc start
MAC address: 40:98:ad:71:e8:b9

+-------------------+-------+-------+-------
| MAC Address       | X     | Y     | Comp T
+-------------------+-------+-------+-------
| 40:98:ad:71:e8:b9 | 23.87 | 30.08 | FUSION
+-------------------+-------+-------+-------

Accuracy test name: Test 1
X: 38
Y: 25
Test time in minutes [5]: 5
User input entered on: 2018-07-13 20:02:54
```

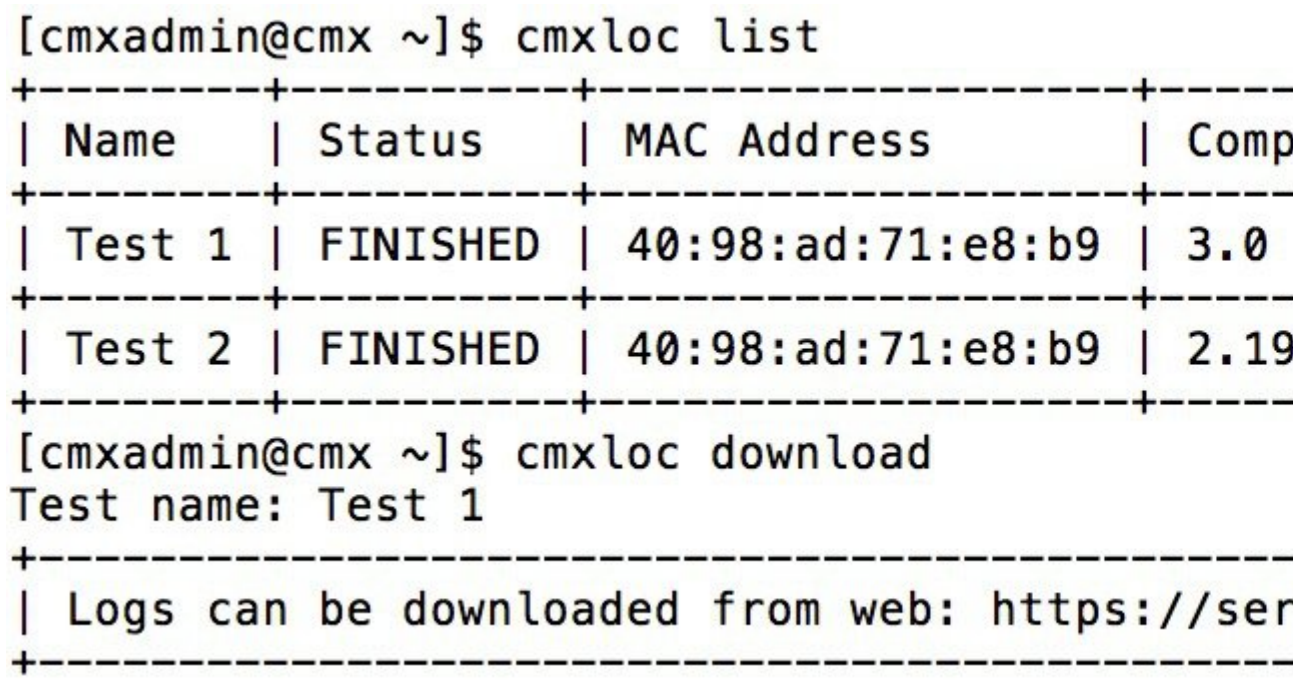
During the test you will see the computation method of each data point: RSSI, AoA or FUSION.

Figure 9: Output during accuracy test

```
Time                                X          Y
2018-07-13T20:12:32.191+0200        27.23      22
2018-07-13T20:12:34.328+0200        27.21      22
2018-07-13T20:12:36.483+0200        28.0       23
2018-07-13T20:12:38.586+0200        27.97      23
2018-07-13T20:12:40.593+0200        26.31      21
```

To view the test results, use the cmxloc list, cmxloc download can be used to prepare a zip file which is helpful for troubleshooting. Use the provided URL, replace the server_IP with the IP of your CMX server to download the zip file.

Figure 10: Listing and downloading test results



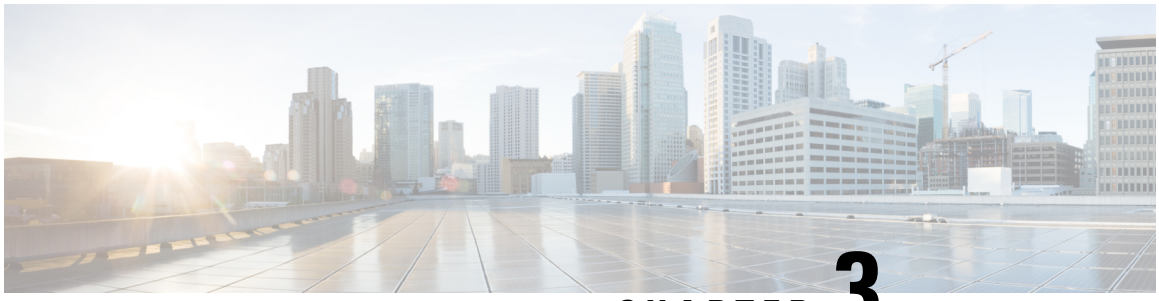
Understanding the test results

On CMX GUI navigate to Detect & Locate and click the green icon to view the test results table.

Figure 11: Location Accuracy Test Results

The table shows the following columns:

- Test: allows you to relaunch, download and send an e-mail with the test results
- Name: Name of the test
- Status: running, paused or finished. You can pause and finish a running test from here.
- Mac Address of the test device
- Floor of the accuracy test
- Start Time of the test
- Location Computation Frequency: Average time between location updates / calculations during the test. Should be better than 10s for Hyperlocation
- Measurements on Correct Floor in %: In some situation, especially when there are atriums / open ceilings the client will be detected from APs on other floors as well and the algorithm might choose the wrong floor
- 10m Accuracy in %: How many of the calculations are within 10 meters of the real location during the test
- Average distance error in meters: averaged location error during the test
- 90% / 75% / 50% error distance in meters: This indicates the radius of 90% / 75% and 50% of the calculated locations around the real location. Good deployments should be in the range of 1-3m for the 50% error distance



CHAPTER 3

The Cisco CMX Analytics Service

Overview of the Analytics Service

The Cisco Connected Mobile Experiences (Cisco CMX) Analytics service provides a set of data analytic tools for analyzing Wi-Fi device locations. The Analytics service helps organizations use the network as a data source to view visitors' behavior patterns and trends, which will in turn help businesses improve visitor experience and boost customer service.

The Analytics service enables you to:

- Analyze Wi-Fi device locations.
- Estimate the number of new visitors (visitors seen for the first time) and repeat visitors (recognized from an earlier visit), the amount of time they spend at a venue, and the frequency of their visits within a venue.
- Gain detailed insight into the behavior patterns of visitors moving and interacting within a venue.
- Analyze business performance by measuring the effect of in-venue marketing.
- Improve customer satisfaction through sufficient staffing during peak hours, proper signage, and making changes in underutilized areas.

The Analytics Dashboard

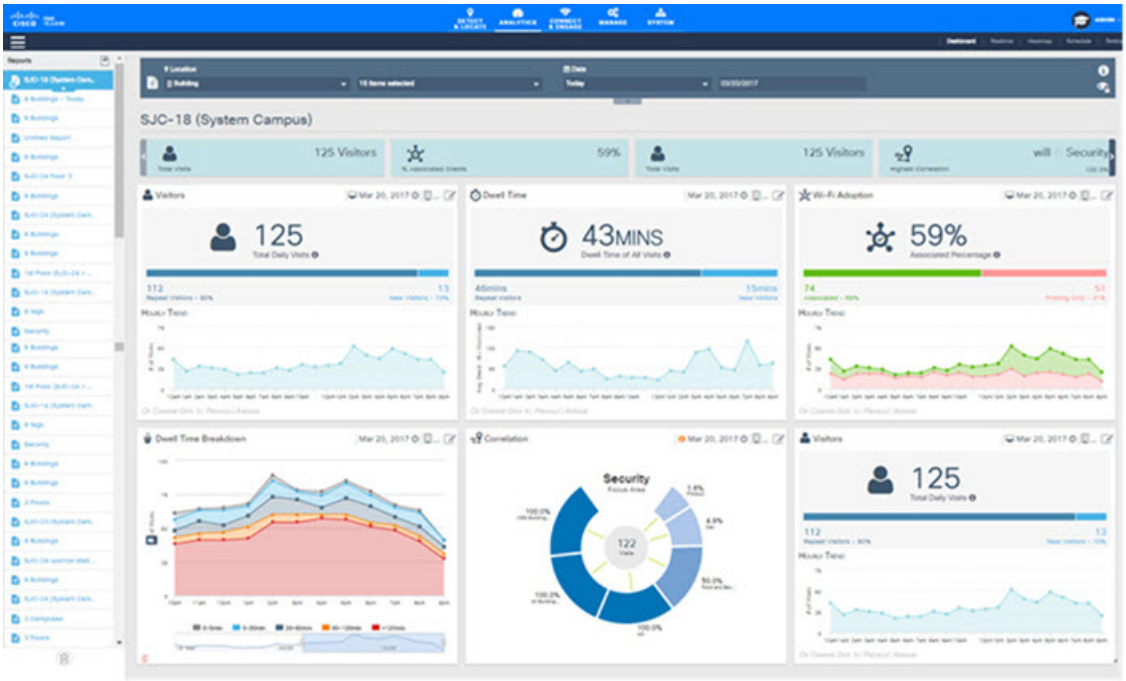
The Analytics service's Dashboard is designed to help you visualize and understand various parameters associated with visitors' movement within a given zone. You can use the Dashboard on a daily basis to examine current trends or events. You can also customize the Dashboard with different widgets, as per your requirements.

Accessing the Analytics Dashboard

Procedure

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

Step 2 Choose **Analytics > Dashboard**.



Step 3 Using the left pane of the Dashboard, navigate to the desired report using the deployment hierarchy (heterarchy). The details pertaining to that report are displayed on the Dashboard.

Filtering the Data Displayed in the Analytics Dashboard

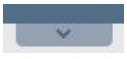
The data displayed in the Dashboard is filtered to include devices that are seen for more than 5 minutes and less than 8 hours.

To change the dwell time (the amount of time a visitor spends at a location):

Procedure

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

Step 2 Choose **Analytics > Dashboard**.

Step 3 Click the Expander icon  below the **Location and Date** pane.

The **Edit Report** window is displayed. For more information, see Edit a Report, on page 84.

Step 4 Specify the **Dwell Threshold** values.

Viewing a Device Count and Average Dwell Time Report

Procedure

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

Step 2 Choose **Analytics > Dashboard**.

Step 3 Click the location you want to analyze, **Region**, **Building**, **Floor**, **Zone**, or **Tags**.

Step 4 From the **Location** and **Date** pane, choose the timeframe for the report. The available options are:

- **Now**—The number of active devices in the last 15 minutes.

  Note In Cisco CMX Release 10.2.3, the **Now** option in the **Date & Time Filters** drop-down list is no longer available

- **Today**—The report you specified is run for the current day and the generated results are displayed.
- **Yesterday**—The report you specified is run using the previous day's values and the generated results are displayed.
- **This Week** —The report you specified is run using the current week's values (Monday to Sunday) and the generated results are displayed.
- **Last Week**—The report you specified is run using the previous week's values (Monday to Sunday) and the generated results are displayed.
- **Last 2 Weeks**—The report you specified is run using past two weeks' values and the generated results are displayed.
- **This Month**—The report you specified is run using this month's values and the generated results are displayed.
- **Last Month**—The report you specified is run using the previous month's values and the generated results are displayed.
- **Last 3 Months**—The report you specified is run using the past three months' values and the generated results are displayed.
- **This Year**—The report you specified is run using this year's values and the generated results are displayed.
- **Last Year**—The report you specified is run using the previous year's values and the generated results are displayed.
- **Custom Range**—The report you specified is run using the date values you specified in the Start and End date fields.

  A report based on the chosen criteria is displayed in the Dashboard and contains the following widgets:

- Visitors widget

- In the Device Count report, information about the total number of visitors, along with percentage of repeat visitors and new visitors is displayed.
- In the Dwell Time report, the average dwell time of all the visitors, along with the dwell time of repeat and new visitors is displayed.

- Compared Data to widget—A comparative result of repeat visitors vs. new visitors is displayed. The available options are:
  - Previous
  - Average—The average value is calculated by averaging the current period and the previous period. If you select This Week in the Date pane, the previous to compared with is last week, and the average is over last week and this week.

- A line chart with a summary view and a detailed view of the criteria selected—You can customize the X-axis and Y-axis by applying the following filter criteria:
  - View Unique Devices or View Absolute Visits
  - Locations—Campus, Building, Floor, Zone, Zone Tag
  - Values—Ascending, Descending, Alphabetical

Analytics Reports

The Analytics Dashboard provides reports to understand and monitor the behavior pattern of visitors within a particular venue.

The Analytics service's report facility also provides a more regular and manager-oriented set of information through parameterized templates to measure various trends and patterns that occur over a period of time in a particular zone. You can create new reports as well as modify the existing reports. You can schedule a report at a customized frequency, print the reports, and download the reports in PDF, Excel, or HTML formats. You can either choose to auto-generate or customize a report.

Note In Cisco CMX Release 10.2.2:

- the Unique Device widget is no longer available for analytics reports
- reports where multiple zones and floors are selected can result in duplicate device counts when a device visits more than one zone or floor. So if a device visits zone 1 and zone 2, the device count is displayed as 2. However, this is not so in Cisco CMX Release 10.2. Hence a higher device count can be registered in a 10.2.2 report as opposed to 10.2.

  A workaround for this is to tag multiple campus/building/floors/zone with the same TAG and create reports at the TAG level.

Creating and Managing Customized Reports

To create your own reports, pick the locations, date/time, and various widgets, and decide how they should be displayed in the Analytics Dashboard. Your reports will be listed in the left pane under **Reports**. Click a report name to view the corresponding details in the Dashboard.

Figure 12: Analytics Reports

Note The maximum number of widgets you can include when creating a new report is 9. If you add more than 9 widgets, this message is displayed: *Analytics only supports 9 widgets in a report. Please reduce the number of widgets.*

If there is no report present in the dashboard, the **Create New Report** window is automatically displayed.

The following is the list of custom report-related tasks that you can perform:

Create a Custom Report

Procedure

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

Step 2 Choose **Analytics > Dashboard**.

Step 3 In the left pane of the Dashboard, click next to **Reports**.
The **Create New Report** window is displayed.

Step 4 To create a custom report, click **Customized** in the **Report Type** row in the right pane.

Step 5 From the **Focus Area Filter** drop-down list, choose the locations that you want to analyze.

The location types are **Building**, **Campus**, **Floor**, and **Zone**.

Step 6 From the **Date & Time filters** drop-down list, choose the date and time range you want to run the report for.

Step 7 In the Add Widgets area, click **Add Widget to Report +** to include any of the following widgets to the report:

- **Visitors**—Shows the number of visitors detected in the network.
- **Average Dwell Time**—Shows the amount of time visitors spent at a location.
- **Correlation**—Shows the relationship between devices and visits between locations.
- **Path**—Shows where visitors went before and after visiting a location.
- **Wi-Fi Adoption**—Shows how many devices are connected to the Wi-Fi network.
- **Dwell Time Breakdown**—Shows dwell-time distribution for selected areas, for example:
  - 20 percent of the visitors stayed less than an hour
  - 50 percent stayed for 1 to 2 hours
  - 30 percent stayed for more than 2 hours

Note
- The **Add Widget** is not available for the **Auto-Generate** report type.
- For each widget in the report, you can click **Edit/View Options** to edit the display options. The options available are **Chart**, **Summary**, and **Table**. By default, the **Summary** option is selected.

Step 8 From the **Advanced Widget Filter** area, choose the devices that you want to filter in the report.

Step 9 From the **Associated/Probing Devices** drop-down list, choose an option.

Step 10 You can set a threshold for dwell time. This is the amount of time spent by a client device (visitor) at a given location. Select the minimum and maximum time from the corresponding drop-down lists in the **Dwell Threshold** area.

a) From the **Minutes To** drop-down list, choose the minimum time, in minutes.
b) From the **Hours** drop-down list, choose the maximum time, in hours.
c) Click **No Filters**, if filtering is not to be applied while generating the report. When you click this option, the dwell-time threshold values are automatically set in the range of 0 to 24.
d) Check the **Stationary Devices** check box if you want to include stationary devices while filterting.

If stationary devices filtering must be included in the report, ensure that the dwell threshold maximum time is 24 hours. Stationary device filtering is only available for widgets with a count, such as **Visitors** and **Average Dwell Time**.

Step 11 Click **Done**.

Based on the **Focus Area and Date** filters that you specified, the report name is generated. The new report name is listed in the left pane under **Reports**.

The following is a list of tasks that can be performed after a Custom report is created:

- Schedule a Report—To schedule a report:
  a. Click the report for which you want to create a scheduled report.
  b. Click the **Expander** icon that is displayed.
  c. Click the **Clock** icon (Schedule) to schedule the report.
  d. In the **SELECT REPORT OPTION** dialog box, choose **HTML**, **PDF**, or **Excel** and click **Next**.

  Note When exporting a report with widgets such as **Visitor Count**, **Dwell Time**, **Dwell Time Breakdown**, or **Wi-Fi Adoption**, you can choose to display **Hourly Trend** (by default) or **Compare Data to** information. If **Compare Data to** chart is included for any of these widgets, when exporting, downloading or scheduling a report, the **Hourly Trend** information is displayed.

- PDF Report—Enables you to schedule a report in PDF format. You can customize the PDF report parameters.
  - In the **Header** text box, specify a Header for the PDF report.
  - Click **Select a Logo** to choose a logo for the PDF report. You can align the placement of the logo to left, center, or right.
  - If you want to provide comments, enter your comments in the **Add your comments here** field.

- In the **Footer** field, specify a footer for the PDF report.
- Enter the email address of the recipients to send the report to.
- Enter the start date and time from which the report has to be generated.
- Select the frequency of the report—**One Time**, **Daily**, or **Weekly**.

- Excel Report—Enables you to schedule a report in excel format.
  - Enter the email address of the recipients to send the report to.
  - Enter the start date and time from which the report has to be generated.
  - Select the frequency of the report—**One Time**, **Daily**, or **Weekly**.
- HTML Report—Enables you to schedule a report in HTML format.
  - Enter the email address of the recipients to send the report to.
  - Enter the start date and time from which the report has to be generated.
  - Select the frequency of the report—**One Time**, **Daily**, or **Weekly**.

e. Click **Schedule**.

- Print a Report—To print a report:
  a. Click the report that you want to print.
  b. Click the **Expander** icon that is displayed.
  c. Click the **Print** icon to print the report.
  d. Click **Next**.
- View Scheduled Report Manager—To view the scheduled reports, choose **Analytics > Schedule**. The **Scheduled Report Manager** page displays the following information:
  - **Report ID**—Shows the report ID.
  - **Report Title**—Shows the report title.
  - **Username**—Shows the name of the user who created the scheduled report.
  - **Start From**—Shows the date and time from which the report is scheduled to run.
  - **Recipients**—Shows the email addresses of recipients.
  - **History**—Displays the history of the scheduled report.
  - **Actions**—Modifies or deletes the scheduled report.

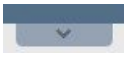
Edit a Report

You can use the **Edit Report** window to edit the report parameters and generate an updated report.

Procedure

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

Step 2 Choose **Analytics > Dashboard**.

Step 3 Click the Expander icon  below the **Location and Date** pane.

The window **Edit Report** window is displayed.

Step 4 Edit the report parameters and then click **Done**.

The Dashboard window is refreshed and the updated report is displayed.

Create a Scheduled Custom Report

Besides creating customized reports, you can add a logo, text, header, and footer to a report to align it with your organization. The reports can be scheduled at a customized frequency for a targeted set of recipients.

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **Analytics > Dashboard**.

Step 3 In the left pane of the Dashboard, expand the report name, and click **Schedule**.

The **Select Report Option** dialog box is displayed. The following options are available:

- **HTML Report**
- **PDF Report**

Step 4 Click the radio button corresponding to the kind of report you require and click **Next**.

If you select the PDF option, the following customization options are available:

- **Header**—Add a header to the report and provide a name. You can customize the position of the header text by using the right, top, and left arrow keys.
- **Logo**—Add a logo to the report by clicking the **Logo** icon. A few default logos are available to choose from. You can also upload a logo by clicking **Upload a Logo**.
- **Comments**—Add comments about the report by entering the corresponding text in the **Add your comments Here** field. You can move the sections by clicking the **Up** or **Down** arrow keys on the left side of the different components present in the sections in the report.
- **Footer**—Add footer text at the bottom of the report.

Note When scheduling a report with widgets such as **Visitor Count**, **Dwell Time**, **Dwell Time Breakdown**, or **Wi-Fi Adoption**, you can choose to display **Hourly Trend** (by default) or **Compare Data to** information. If **Compare Data to** chart is included in any of your widgets, when downloading or scheduling a report, the **Hourly Trend** information is displayed.

Step 5 Click **Next**.
The **Schedule Report** widget is displayed.

Step 6 Enter the email addresses of the recipients to send the report to.

Step 7 Enter the start date and time of the period for which the report has to be generated.

Step 8 Select the frequency of the report, **One Time**, **Daily**, or **Weekly**.

Step 9 Click **Schedule**.

Configure Custom Time Ranges for an Analytics Report

In Cisco CMX Analytics, the **Create New Report** window includes the date and time range option to select a specific period of time for creating Analytics reports. After creating or modifying these time ranges, you can proceed to select the corresponding range from the **Date and Time Filters** drop-down list, for example, Early Morning (12am -3:59am).

You can also modify the existing ranges or define custom time ranges for generating Analytics reports. You can configure the custom time using either the Cisco CMX GUI or CLI.

Add a New Time Range Using the Cisco CMX GUI

Procedure

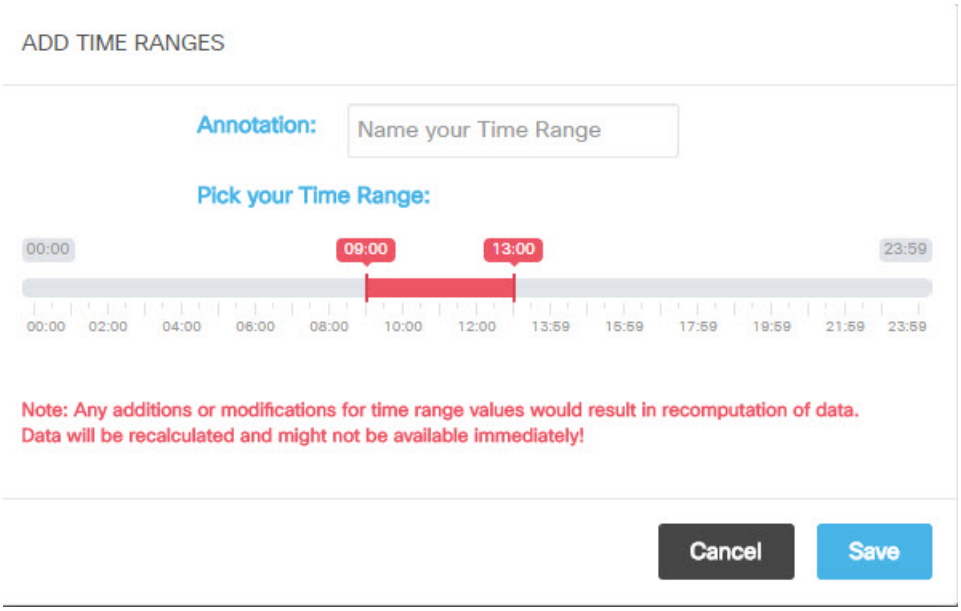
Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2 Choose **Analytics > Settings**.

The **Analytics Settings** window is displayed with a list of the available time ranges.

Step 3 To add a new custom time range, click **Add**.

The **Add Time Ranges** dialog box is displayed.



Step 4 In the **Annotation** field, enter a new name for the time range.

Step 5 Use the time range slide bar to pick a new time range.

Step 6 Click **Save**.

Note
- Any updates to the time range values will result in recomputation of the data.
- The new time is displayed in the **Global TimeRanges** drop-down list.
- By default, the interval time for a new time range is 15 minutes.

Add a New Time Range Using CLI

Procedure

Step 1 Log in to root through SSH.

Step 2 Use the CLI to edit the *analytics.params.json* file and change the time ranges. Optionally, you can use a third-party SFTP client to edit the file.

a) Enter **cd /opt/cmx/etc/**

b) Enter **vi analytics.params.json**

Step 3 (Optional) Delete all the older Analytics reports and reprocess the data with the new time ranges:

```
<USERNAME>:<PASSWORD> -X DELETE
"http://<IPADDRESS>:5556/api/analytics/v1/batch/daysProcessed/HistoricalVisitsJobProducer"
<USERNAME>:<PASSWORD> -X DELETE
http://<IPADDRESS>:5556/api/analytics/v1/batch/daysProcessed/TodayVisitsJobProducer
```

Step 4 To restart the Analytics services, use the **cmxctl analytics restart** command. This updates and displays all the new time ranges in the CMX UI. All the historical data will also be reprocessed using the new time ranges.

Note If the Analytics services are not restarted, only the unmodified time ranges will be available.

Download a Customized Report

You can use the Analytics service to download customized reports in PDF, Excel, or HTML formats.

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **Analytics > Dashboard**.

Step 3 In the left pane of the Dashboard, expand the corresponding report name, and click **Download**.

The **Select Report Option** dialog box is displayed. The following options are available:

- **PDF Report**
- **Excel Report**
- **HTML Report**

Step 4 Click the radio button corresponding to the format that you want the report to be downloaded in.

If you select the PDF option, the following customization options are available:

- **Header**—Add a header to the report and provide a name. You can customize the position of the header text by using the right, top, and left arrow keys.
- **Logo**—Add a logo to the report by clicking the **Select a Logo** icon. A few default logos are available to choose from. You can also upload a logo by clicking **Upload a Logo**.
- **Comments**—Add comments about the report by entering text in the **Add your comments** field. You can move the sections by clicking the **Up** or **Down** arrow keys on the left side of the different components present in the sections in the report.
- **Footer**—Add footer text at the bottom of the report.
- If you select **Excel Report**, the data for all the Dashboard widgets will be exported as tables in the report. If you want to download reports with filtering options, choose the **Table** report option from the **Edit/View Options** for each widget.

Note When downloading a report with widgets such as **Visitor Count**, **Dwell Time**, **Dwell Time Breakdown**, or **Wi-Fi Adoption**, you can choose to display **Hourly Trend** (by default) or **Compare Data to** information. If **Compare Data to** chart is included in any of your widgets, when downloading or scheduling a report, the **Hourly Trend** information is displayed.

Step 5 Click **Next**.
The customized reports are downloaded in the selected format.

Delete a Customized Report

You can delete any of the custom reports that you created.

Procedure

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

Step 2 Choose **Analytics > Dashboard**.

Step 3 In the left pane of the **Dashboard**, hover the cursor over a report, and click the **Delete** icon.

Creating an Analytics Report Based on Associated or Probing Only Devices

You can create filtered analytics reports based on all visitor devices associated to the network (regardless of SSID) and on all visitor devices detected by the network. These are categorized as **Associated** and **Probing Only** devices. In addition, any devices filtered by the Location service is also excluded from analytics reports.

Procedure

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

Step 2 Choose **Analytics > Reports** to display the **Create New Report** window.

Step 3 From the **Associated/Probing Only Devices** widget, select **Associated** or **Probing Only**, or select both.

If both are selected, all associated and probing only devices will be displayed (meaning, no filtering) in the Visitor Count area on the Analytics Dashboard.

Step 4 Click **Done**.

The Visitor Count information on the Analytics Dashboard reflects the following:

- If the **Associated** option is selected, a green Wi-Fi icon appears next to the **Visitor Count** heading. The visitor count displayed is the number of devices associated to the SSID.
- If the **Probing Only** option is selected, a gray Wi-Fi icon appears next to the **Visitor Count** heading. The visitor count displayed is the number of devices probing only by the SSID.
- If both options are selected (meaning, no filtering), no icon appears.

Viewing Global Alerts for Critical Services

The Global Alerts window displays information for all Cisco CMX service. You can navigate to this window from the respective Cisco CMX service window.

Procedure

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

Step 2 Choose **Analytics** > **Dashboard**.

The **Dashboard** window is displayed.

Step 3 In the top-right corner of the window, click the **Alerts**  icon.
The **Live Alerts** window is displayed with the global alert details for critical and major alerts. For more information about alerts, see Viewing Live System Alerts, on page 215.

Tip For the Analytics service, Job Processor runs multiple jobs in the background . The Analytics service's Dashboard displays success alerts when the job processor completes all the jobs.

Customized Widgets

Customized widgets enable you to view and analyze specific activities to better suit the objective of your analysis. For example, you can create a widget that focuses on visitor (client) activity in a zone of interest. The customized widget will gather and present only the data pertaining to visitor activity, and enable the analysis and interpretation of this data. The information in the customized widgets enable you to take meaningful decisions based on client activity.

Note Customized widgets can be generated only by Advanced users.

The Visitors Widget

The Visitor widget provides a detailed summary of the visitor (client device) count in an area of focus.

The Visitor widget can be viewed in the following formats:

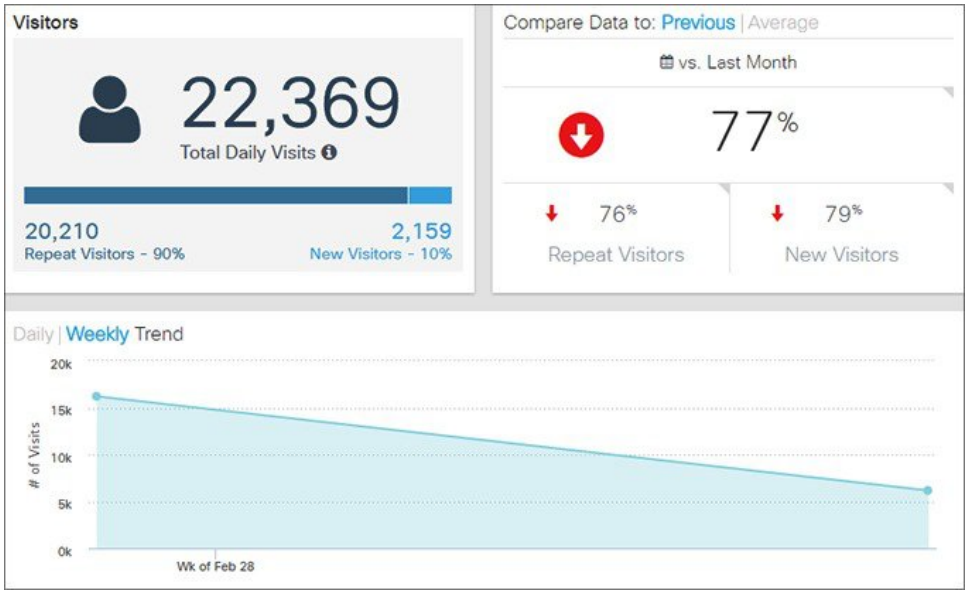
- **Summary**—This is the default view. This view consists of the **Visitors**, **Compare Data to**, and **Hourly Trend** charts. A breakup of new and repeat visitors is also provided. The **Compare Data to** chart presents comparative data for the current day and the previous day. You can also compare the current data with the average visitor count per day. A breakup distribution of repeat and new visitors is also shown as percentage. A graph shows the visitor count per hour from 12:00 a.m. to 12:00 p.m.
- **Chart**—A line chart with a summary view of the number of total visitors along the Y-axis and the activity at a given time of the day along the X-axis is displayed. You can configure the chart based on the following views:
  - **View Unique Devices or View Absolute Visits**
  - **Locations**—Campus, Building, Floor, Zone, By Hour
  - **Values**—Ascending, Descending, Alphabetical

The Y-axis value provides alternate views of the number of visitors and percentage of total visitors. Hover your cursor at any point along the line to view the connected and probing data at that instance.

- **Table**—Visitor count attributes are presented in a tabular format.

  The following trends are available for each view:

  - **View Unique Devices**
  - **View Absolute Visits**



The Dwell Time Widget

The Dwell Time widget presents detailed summary of the time spent by visitors (client devices) at a location.

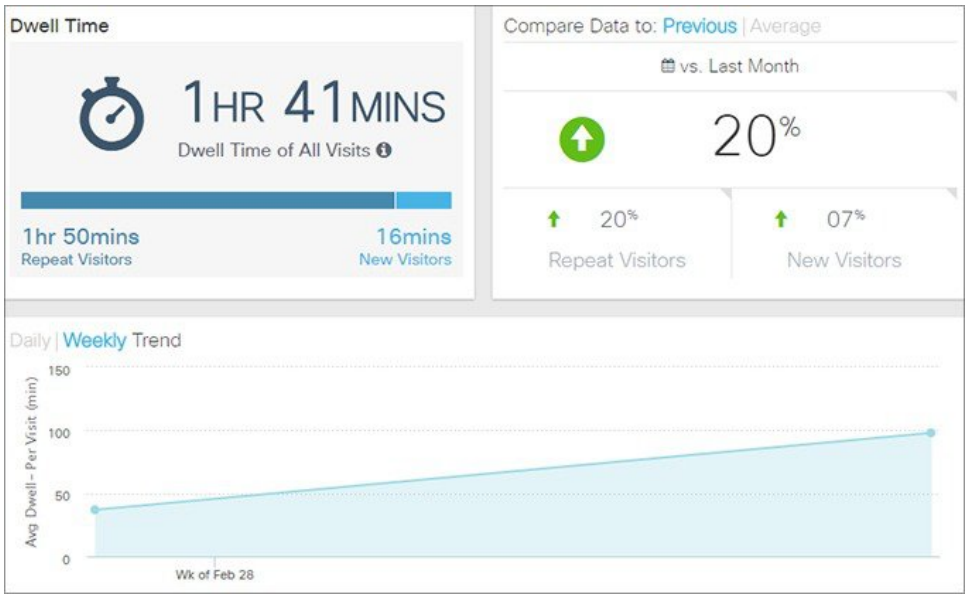
Average dwell time can be viewed in the following formats:

- **Summary**—This is the default view. The summary view consists of the **Average Dwell Time**, **Compare Data to**, and **Daily Trend** charts. A breakup of new and repeat visitors is also provided. The **Compare Data to** chart presents comparative data for the current day and the previous day. You can also compare the current data with the average visitor count per day. A breakup distribution of the repeat and new visitors is also shown as percentage. A graph shows the visitor count per hour from 12:00 a.m. to 12:00 p.m.
- **Chart**—A line chart with a summary view of the number of total visitors along the Y-axis and the activity at a given time of the day along the X-axis is displayed. You can configure the chart based on the following views:
- **Table**—Visitor count attributes are presented in a tabular format. You can view the following details:
  - Location
  - Parent Area(s)
  - Day

- Time
- Dwell Time

The following trends are available for each different view:

- **View Unique Devices**
- **View Absolute Visits**



The Correlation Widget

Note The Correlation widget of Cisco CMX 10.2 is referred to as Crossover widget in Cisco CMX Release 10.1.

The Correlation widget provides a detailed summary of correlation of client devices between two locations. Correlation data can be used to determine the relation between two zones. Low correlation between zones indicates lack of access between the two zones. For example, you can expect a high correlation between the food court and the cinema in a shopping mall. The Correlation widget can be viewed in the following formats:

- **Correlation**—Provides an interactive graphical representation of the correlation between zones. You can configure the correlation between zones by filtering according to the focus areas, building, or absolute versus unique devices.
- **Table**—The table format lists the data in a tabular format with the following columns:
  - **Area**-The zone around which correlation is configured.
  - **Grouping**—The focus area for which the correlation data is collected.
  - **Correlation**—The correlation data, in percentage, between the zone (Area column) and the focus area.

The following trends are available for each view:

- **View Unique Devices**
- **View Absolute Visits**

The Path Analysis Widget

The Path Analysis widget analyses the paths taken by visitors (or client devices) before and after visiting a focus location, and provides a graphical representation of the paths.

- The green (left) side represents where a device is coming from, for example, immediately before entering the focus zone.
- The blue (right) side represents where a device goes to, for example, immediately after exiting the focus zone.

Hovering your cursor over the focus reveals a breakdown based on:

- Percentage of paths that either started or ended in the focus zone.
- Percentage of paths that either arrived or departed from the focus zone.

Hovering your cursor over a green section shows the number of paths that entered the focus zone originated in this zone.

Hovering your cursor over a blue section shows the number of paths that originated in the focus zone ended in this zone.

Note All paths are calculated based on the overall data set defined, but only the top 15 (by percentage) paths can be displayed in the widget due to space constraints.

In a generated report with **Path Analysis** widget, the **Focus on** drop-down displays the focus area with the correct floor level granularity.

The **Edit Widget** link allows you to define the heterarchy level from which the data pool is collected from, and then define the specific focus of this widget. That way, you can add more than one widget to the report and perform side-by-side comparisons of one zone with another.

The Wi-Fi Adoption Widget

You can now view real-time analytics reports in the Cisco CMX GUI. This tab that shows you a Wi-Fi adoption widget based off of the REAL TIME information. The **NOW** parameter for Analytics has been removed.

The Wi-Fi Adoption widget displays a detailed summary of the number of clients that are associated with a network, and the clients that are probing the network:

- **Probing Only**—Refers to the client devices that are detected by APs in the network when they are probing the network.
- **Associated**—Refers to the client devices that have established a connection with an AP at least once during the time period selected in the report.

Associated status can be viewed in the following formats:

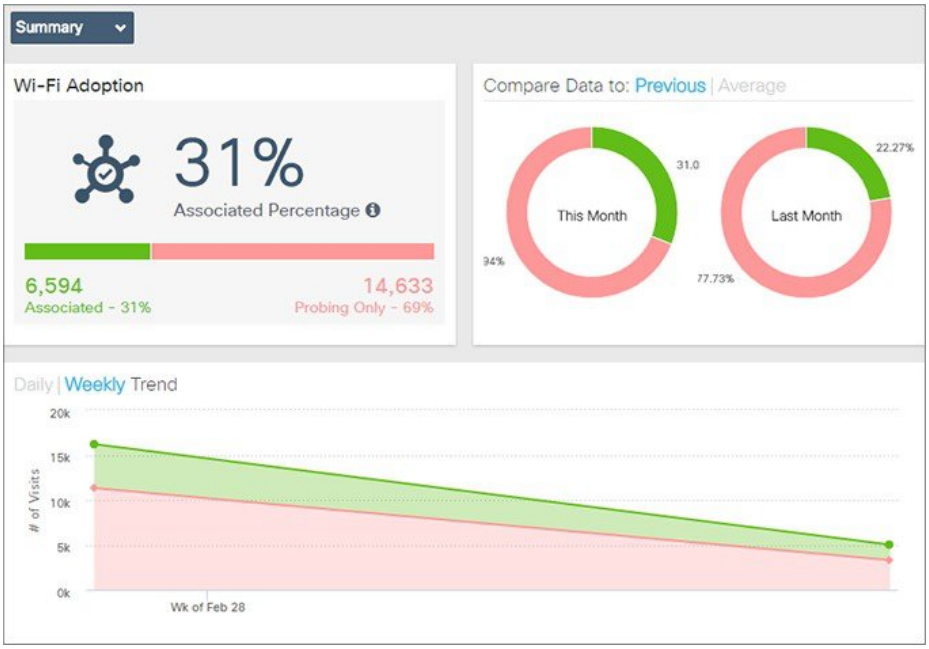
- **Summary**—This is the default view. The Summary view consists of the **Associated Status**, **Compare Data to**, and **Hourly Trend** charts.
- **Chart**-A line chart with a summary of associated and probing clients. The view can toggle to show associated clients in terms of percentage and total clients. The X-axis can be based either on location or time. A line chart with a summary view and a detailed view of the criteria selected is also available. You can customize the X and Y axis by applying the following filter criteria:
  - View Unique Devices or View Absolute Visits
  - Locations--Campus, Building, Floor, Zone, By Hour
  - Values--Ascending, Descending, Alphabetical

Hover your mouse pointer at any point along the line to view the connected and probing data at that instance.

- **Table**-Connected and detected attributes of clients are presented in a tabular format.

The following trends are available for each different view:

- View Unique Devices
- View Absolute Visits



The Dwell Time Breakdown Widget

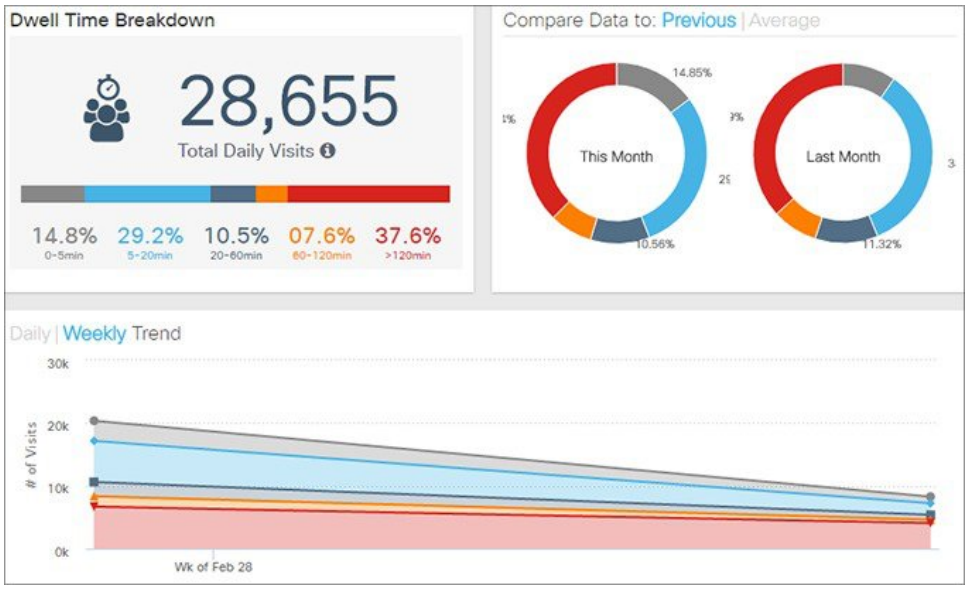
The Dwell Time Breakdown widget displays the dwell time distribution for selected areas.

Dwell Time Breakdown can be viewed in the following formats:

- **Summary**—This is the default view. The summary view consists of the **Dwell Time Breakdown**, **Compare Data to**, and **Daily Trend** charts. The dwell time breakdown is displayed in the following ranges:
  - **0-5 minutes**
  - **5-20 minutes**
  - **20-60 minutes**
  - **60-120 minutes**
  - **>120 minutes**
- **Chart**—A line chart with a summary view of the dwell-time breakdown in the time ranges of **0-5 minutes**, **5-20 minutes**, **20-60 minutes**, **60-120 minutes**, and **> 120 minutes**. You can configure the chart based on the following views:
  - **View Unique Devices or View Visits**
  - Locations—Allows you to filter by any of these values: Campus, Building, Floor, Zone, Day, Hour of Day, Hour, Region, Building, Floor, Zone, Tag
  - Sort order—Ascending, Descending, Alphabetical
- **Table**—The tabular view provides information about the dwell-time breakdown in the time ranges of **0-5 minutes**, **5-20 minutes**, **20-60 minutes**, **60-120 minutes**, and **> 120 minutes**.

Note This view allows you to search for records within the table. The search text box is available above the table.

Note The Dwell Time filters are not available for the Dwell Time Breakdown widget.



Creating Customized Widgets

Procedure

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

Step 2 Choose **Analytics > Dashboard**.

Step 3 In the left panel of the Dashboard, click the **Add**icon next to **Custom Reports**

The **Create New Report** window is displayed.

Step 4 Choose **Customized** from the Report Type widgets row in the right pane.

Step 5 Choose the locations that you want to analyze from the **Focus Area Filter** drop-down list.

The location types are **Building**, **Campus**, **Floor**, **Zone**.

Step 6 Choose the date and time range you want to run the report for from the **Date & Time filters** drop-down list.

Click the dot at the bottom of the **Add Widget** area to scroll to the next set of options. You can select multiple widgets to combine in one overall widget.

Step 7 In the **Add Widgets** area click the**Add**+ icon to include any of the following widgets to the report:
Click the dot at the bottom of the **Add Widget**area to scroll to the next set of options. You can select multiple widgets to combine into one overall widget.

Step 8 You can set a threshold for dwell time. This is the amount of time spent by a client device(visitor) at a given location. Select the minimum and maximum time from the drop-down options in the **Advanced Widget Filters** area.

Step 9 Click **Done**.

The widget is created.

Step 10 Click the report title to name to your report.

Step 11 Click **Save**.

Create a Realtime Report

Procedure

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

Step 2 Choose **Analytics > Realtime**.

Step 3 In the left pane of the Dashboard, click next to **Now Reports**.
The **Create New Report** page is displayed.

Step 4 From the **Focus Area Filter** drop-down list, choose the floor that you want to analyze.

Step 5 In the Add Widgets area, click the **Add Widget to Report +** to include any of the following widgets to the report:

- **Realtime Device Count**—Shows the number of devices currently detected on the Wi-Fi network. You can add a maximum of three Realtime device Count widgets to generate the report.

Step 6 Click **Done**.
Based on the **Focus Area Filter** filters that you specified, the report name is generated. The new report name is listed in the left pane under **Now Reports**.

Performing Heatmap Analysis

A heatmap is a graphical representation of client movement, which shows areas having a large concentration of devices in red, and those with less activity in blue.

Note If you have an exclusion area, the heatmap will not consider that area for analysis.

Procedure

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

Step 2 Choose **Analytics > Heatmap**.

Step 3 In the **Activity Heatmap** window, click the **Date** icon and select the date.

Step 4 Click the **Time** icon to show or hide the display of time.

Step 5 Choose from the following options:

- From the **Campus** drop-down list, select the campus on which you want to run the heatmap analysis. The drop-down list contains all the campuses that are synchronized with Cisco CMX.
- From the **Building** drop-down list, select the building on which you want to run this analysis. The drop-down list contains all the buildings that are synchronized with Cisco CMX.
- From the **Floor** drop-down list, select the floor on which you want to run the analysis.

Step 6 Click the **Heatmap** and **Zone** icons to display heatmap distribution and zones respectively.

Step 7 Click the **Zoom in** (+) and **Zoom out** (-) buttons to increase or decrease the view of the map.

Step 8 Click **Realtime** to view heatmap data.

Step 9 Click **Playback** to play back the client movement for the selected date.

Using the Schedule Manager

To access the Schedule Manager window, log in to Cisco CMX, and choose **Analytics > Schedule**. The **Schedule Manager** window is displayed with the following information:

- **Report ID**—Shows the report IDs of scheduled reports.
- **Report Title**—Shows the titles of reports.
- **Username**—Shows the user who created the scheduled report.
- **Start From**—Shows the date from which reports will be emailed to recipients.
- **Recipients**—Shows the email addresses of recipients.
- **History**—Shows the status of past reports.
- **Action**—Click **Delete** to delete a scheduled report.

Set SSID Filter Parameters for Analytics Service

In the Analytics service, use the **SSID Filter** tab to exclude the SSIDs. You also can click the **Refresh** option to get any updates to the SSIDs.

Note If you filter out an SSID in the Location service, it will be automatically filtered out in the Analytics service too.

The **SSID Filter** feature helps you to filter out clients that need not be tracked by Cisco CMX. Cisco CMX will block the SSIDs associated with these clients. Cisco CMX requires the association event (INFO message on NMSP) to be reported daily to continue blocking of these SSIDs.

Cisco CMX has a scheduled job running every midnight to clean up the blocked SSIDs and clients associated with these SSIDs. However, **Location** service still continues to process these clients associated with blocked SSIDs. Devices that are stationary such as a barcode scanner are always in a static location and hence do not

send association information frequently. These devices should be associated with blocked SSIDs. As they do not send association event, Cisco CMX will try to track them again.

If you want Cisco CMX to not clear the blocked SSID's through midnight job, follow the steps:

1. To set the featureflag configuration, run the following command:

   cmxctl config featureflags location.filteredssidscleanupatmidnight false

2. To restart Cisco CMX agent, run the following command:

   cmxctl agent restart

3. To stop location and NMSP services, run the following commands:

   cmxctl location stop

   cmxctl nmsplb stop

4. To start location and NMSP services, run the following commands:

   cmxctl location start

   cmxctl nmsplb start

With Cisco CMX Release 10.6.2, feature flag configuration (location.computelocthroughassociatedap) for computing location through associated access points is turned on and this enhancement helps Cisco CMX to track and show more associated clients. Depending upon the feature flag configuration settings, the **location.filteredssidscleanupatmidnight** job is configured in a way to include and exclude clean up of blocked SSIDs. The scheduled job periodically polls the association events every one hour to get associated client events more frequently and thereby reducing the reporting time.

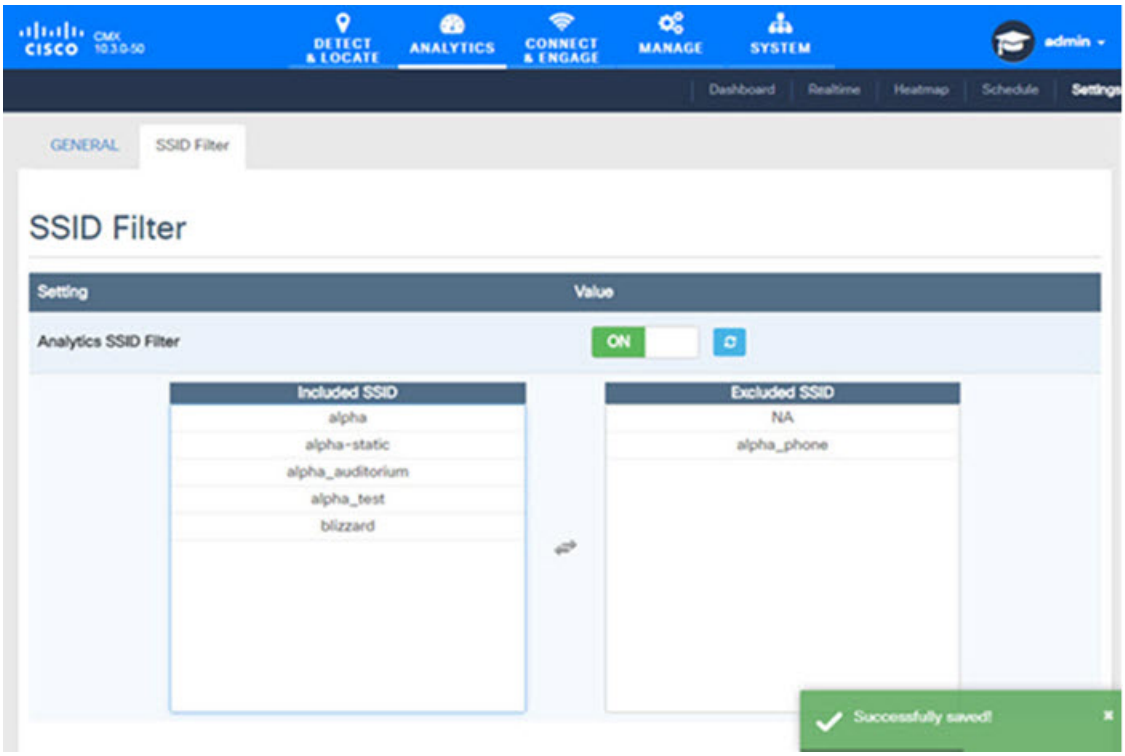
Procedure

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

Step 2 Choose **Analytics > Settings**.

Step 3 Click the **SSID Filter** tab.

The **SSID Filter** window is displayed.



Step 4 To enable the SSID Filter, click **Analytics SSID Filter**.

A green **ON** option indicates that SSID is filtering is on. The SSID Filter list displays the SSIDs from all the controllers. All duplicate instances of SSIDs are merged and displayed as a single ID. The **Included SSID** list will be empty if there are no associated clients.

In the **Included SSID** list, the value **NA** indicates that SSID is not applicable. This option is available only for the **Analytics** service.

Note With Cisco CMX Release 10.5.1 or later, Cisco CMX relies on controller notification (INFO messages) to populate the SSID list. For all earlier Cisco CMX releases, this was achieved using SNMP polling.

Step 5 To filter out an SSID, click the corresponding SSID in the **Included SSID** list. This SSID is moved to in the **Excluded SSID** list.

Disable Cisco CMX Analytics Service (CLI)

Before you begin

Use CLI to disable Cisco CMX Analytics Service. There is no option to disable Cisco CMX Analytics Service on Cisco CMX UI.

Procedure

Step 1 Connect to Cisco CMX through the console.

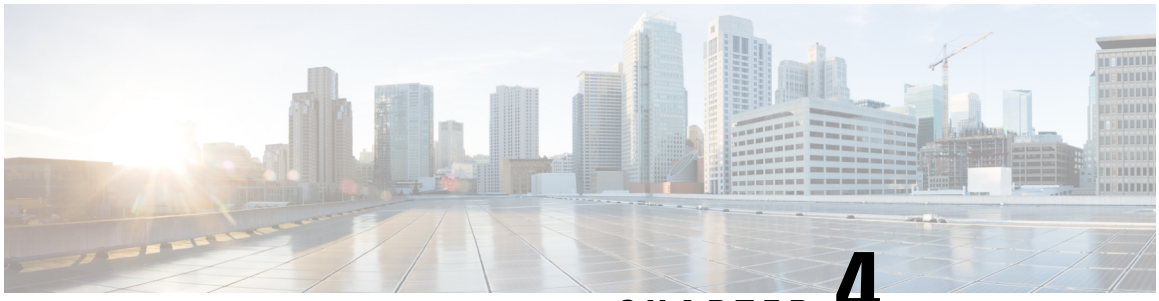
Step 2 To disable Cisco CMX Analytics Service, run the **cmxctl disable analytics** command.

Step 3 To restart location services, run the **cmxctl restart location** command.

Step 4 (Optional) To restart the location services, run the following commands:

a. **cmxctl stop location**

b. **cmxctl start location**



CHAPTER 4

The Cisco CMX Connect Service

Overview of the Connect Service

CONNECT is a customizable and location-aware guest captive service that enables you to create customized, intuitive on-boarding experiences for your visitors. It enables you to provide two types of on-boarding experiences for your visitors:

- Facebook Wi-Fi:
  - Allows the administrator of a facility to enable the facility's Facebook page as a free Wi-Fi hotspot for visitors
  - Allows visitors to access free Wi-Fi after accessing the facility’s Facebook page.
  - Provides insight into a facility's customer base through demographic reports.

Note Cisco CMX supports Facebook Connect through access points in local mode or FlexConnect mode.

- Custom Portal:
  - Enables the administrator of a facility to create and host a guest splash page with customized branding and advertisements.
  - Provides social network authentication with Facebook, Instagram, and Foursquare using OAuth 2.0.
  - Collects OAuth 2.0 user social information

For a complete list of new features in the Cisco CMX Connect service, see the What's New in This Release section of 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

- You cannot install both the Location service and the Presence Analytics service on the same Cisco CMX instance in this release. Therefore, you can have either of the following:
  - Connect with Location
  - Connect with Presence Analytics

    For the Connect Service to operate as intended, ensure to add Presense sites.
- (CSCve73287) The default setting of Cisco CMX Connect allows for a maximum of approximately two clients per second continuously. A higher number can be achieved at peak, for example, 4,000 HTTP connections can be made during a 5-minute window. In addition, special configuration changes can be made to increase this rate. Contact Cisco Technical Support for more information on these recommendations.

Restrictions

- The Facebook Wi-Fi authentication feature for Cisco CMX Connect is not supported in Cisco IOS XE 3.3.x SE, Cisco IOS XE 3.6.x E, Cisco IOS XE 3.7.x E.
- After you upgrade from Cisco CMX 10.1 to 10.2, you need to clear your browser's cache, and then launch the Cisco CMX Connect UI. If you do not perform this operation, the portal will not be upgraded, and all CMX Connect features will not work properly.
- For Cisco CMX Release 10.5.x and later, all HTTP functions are no longer supported on Cisco CMX Connect Services.
- (CSCvh13119) (On Apple MacBook Pro laptops) After accepting the terms and conditions and clicking Submit, the Cisco CMX portal page with the Facebook icon keeps redisplaying and does not connect to the Internet. Opening a separate browser session results in connecting to the Internet, but bypasses portal authentication.

  (On Apple iPads) The custom portal page appears twice before authentication is successful.

Comparison of Facebook Wi-Fi and Custom Portal

Table 4: Comparison of Facebook Wi-Fi and Custom Portal

	Facebook Wi-Fi	Custom Portal
Landing page	Hosted on Facebook (Facebook page)	Hosted on Cisco Connected Mobile Experiences (Cisco CMX)
Social authentication	Facebook only	Facebook, Instagram, and Foursquare (Using OAuth 2.0)

	Facebook Wi-Fi	Custom Portal
Facebook app permission pop-up	No	Yes
Post on timeline	Check-in is visible on users' timeline (Dependent on privacy setting)	Check-in is unavailable
Demographic data	Stored on Facebook at an aggregate level (Requires more than 30 check-ins to be enabled)	Stored on Cisco CMX (at an individual level)
Export of demographic data	No	Yes
Customer profile	• Marketing teams with Facebook advertising budget or social media teams or both • Service providers managing multiple small stores	Marketing teams and IT teams that prefer to keep data in-house
Support for Post Auth URL	No	Yes

Preparatory Tasks

You must have a Facebook account for a business page. For more information, see the Creating a Facebook Page for Your Organization, on page 109.

Adding a Connect or ConnectExperience User

Procedure

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

Step 2 Choose **MANAGE** > **Users**.

Step 3 Click **New User**.

Step 4 In the Add New User dialog box, enter the first name, last name, username, and password of a user.

Step 5 From the **Roles** drop-down list, select **Connect** or **ConnectExperience**.

Note For information about access rights for the Cisco CMX services available to the Connect and ConnectExperience user roles, see User Role Summary, on page 103.

Step 6 Click **Submit**.

User Role Summary

The following table lists the user roles that have access to the Connect & Engage service.

Table 5: User Role Summary

Role	Connect & Engage Service				Other Services
	Dashboard	Experiences	Policy	Settings	
Admin	Read	Read/Write	Read/Write	Read/Write	Read/Write
Connect	Read	Read/Write	Read/Write	Read/Write	No
ConnectExperience	No	Read/Write	Read	Read*	No

* Write permission for SMS, Number of Devices, and Time to Expire.

The Connect Dashboard

To view the Connect Dashboard, log in to Cisco CMX and choose **CONNECT> Dashboard**.

The Connect Dashboard window displays the summary report and two historical reports.

Use the navigation bar at the top of the page to set the location and interval of reports.

Location consists of the following levels:

- **Global**
- **Campuses**
- **Buildings**
- **Floors**
- **Zones**
- **Sites**

From the **Interval** drop-down list in the Connect & Engage Dashboard window, you can select the time frame for generating historical reports:

- **Last 7 Days** (default)
- **Last 28 Days**
- **Last 365 Days**

Summary Information

The summary information presents users' usage information for the present day. Note that the time used is server time, and not web browser time.

Historical Information

The Connect & Engage Dashboard displays historical information:

- **New and Repeat Visitors**—New Visitors are the people seen for the first time. Repeat Visitors are those recognized from an earlier visit.
- **Network Usage**—Network Usage is the total amount of data uploaded and downloaded by all visitors.
- **Pages Served vs Submitted**—Pages Served is the number of times a portal page was displayed to the visitors' devices. Pages Submitted is the number of times a portal page was submitted by the visitors.
- **SMS Sent vs Authenticated**—SMS Sent is the total number of texts sent. SMS Authenticated is the number of texts that were used to successfully authenticate visitors.
- **Languages Used**— Languages used is the count of visitors authenticated using each language.

In historical reports, you can choose the type of chart you want to be displayed in the reports:

- Area Chart
- Line Chart
- Column Chart

Visitor Search

The Connect & Engage Dashboard provides a search option, where the following types of searches can be performed:

- Advanced Search
- Export All Visitors

To search for a visitor, enter a search term, for example, name or email address, in the **Visitor Search** field.

Additional Information

The following is a list of additional information:

- The Search table provides a preview of up to 100 clients per page.
- The entire search result can be exported to a .CSV file.
- The search time range is based on the Cisco CMX system time, and not on the web browser time.
- Partial search is supported; however, wildcards (*) are not supported.

Connect Experiences

(CSCve56353) End users using Android devices are unable to open the Cisco CMX landing page URL configured from the Connect & Engage > Connect Experiences window. In addition, the Guest Portal might also close after an end user registers. This is a known “Redirection to Success Page” Android bug from Google. For more information, see:

https://support.cmxcisco.com/hc/en-us/articles/115007357987

Overview

Using Connect Experiences, you can choose between two types of guest on-boarding experiences:

Facebook Wi-Fi

The Facebook Wi-Fi feature provides organizations with a simple and fast guest access solution. With Cisco CMX for Facebook Wi-Fi, organizations can:

- Save time and effort on designing their own captive portal by directing guests to a facility's Facebook page.
- View aggregate social data gathered from visitors connected to Wi-Fi with their Facebook logins for tailoring social media marketing strategy.

Facebook Wi-Fi is based on WLAN web passthrough authentication on Cisco Wireless Controllers (Cisco WLCs). Cisco WLC intercepts HTTP traffic and redirects the client browser to Cisco CMX. Cisco CMX finds the client location and redirects the client browser location to the configured location-specific Facebook page. After a successful Facebook sign-in and check-in, Cisco CMX redirects the client browser to the specific Facebook page. For Facebook Wi-Fi feature, both the client and Cisco CMX uses HTTPS traffic to communicate with Facebook.

Note Only http traffic will be redirected to Facebook. Facebook Wi-Fi/OAuth login is not useful for any https traffic.

For information about setting up Facebook Wi-Fi, see the Setting Up a Facebook Wi-Fi Portal, on page 106.

Custom Portal

Custom Portal enables you to perform the following tasks:

- Create location-specific splash pages
- Enable branding consistency using splash pages
- Own registration information from customer sign-in page, which turns the captive portal into a data source for targeted marketing later via email marketing

For information about setting up a custom portal, see Setting Up a Custom Portal, on page 110.

Setting Up a Facebook Wi-Fi Portal

Setting up a Facebook Wi-Fi portal involves the following tasks:

Configuring Access Control Lists on Cisco Wireless Controller

Procedure

Step 1 Log in to the web UI of a Cisco Wireless Controller (Cisco WLC) that is associated with Cisco CMX.

Step 2 Choose **SECURITY > Access Control Lists > Access Control Lists**.

Step 3 On the **Access Control Lists** window, click **New** to add an access control list (ACL).

Step 4 On the **Access Control Lists > Edit** window, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 5 Choose the ACL type as either **IPv4** or **IPv6**.

Step 6 Click **Apply**.

Step 7 On the **Access Control Lists** window, click the name of the new ACL.

Step 8 On the **Access Control Lists > Edit** window, click **Add New Rule**.

The **Access Control Lists > Rules > New** window is displayed.

Step 9 Configure the following ACLs, as listed in the table below:

Note The following ACL table lists the rules for social login. If you use HTTPS as the authentication method, use the rules one and two to access Facebook.com.

Table 6: ACLs for Facebook Wi-Fi Portal

Seq.	Action	Source IP/ Mask	Destination IP/ Mask	Protocol	Source Port	Destination Port	DSCP	Direction
1	Permit	0.0.0.0/ 0.0.0.0	0.0.0.0/ 0.0.0.0	TCP	HTTPS	Any	Any	Any
2	Permit	0.0.0.0/ 0.0.0.0	0.0.0.0/ 0.0.0.0	TCP	Any	HTTPS	Any	Any
3	Permit	MSE_IP/ 255.255.255.255	0.0.0.0/ 0.0.0.0	TCP	HTTP	Any	Any	Any
4	Permit	0.0.0.0/ 0.0.0.0	MSE_IP/ 255.255.255.255	TCP	Any	HTTP	Any	Any

Table 7: ACLs for Facebook Authentication using Cisco CMX

Seq.	Action	Source IP/ Mask	Destination IP/ Mask	Protocol	Source Port	Destination Port	DSCP	Direction
1	Permit	CMX_IP/ 255.255.255.255	0.0.0.0/ 0.0.0.0	TCP	HTTPS	Any	Any	Any
2	Permit	0.0.0.0/ 0.0.0.0	CMX_IP/ 255.255.255.255	TCP	Any	HTTPS	Any	Any

Note For Facebook to work in the DNS ACL, configure the below URLs:

- facebook.com
- m.facebook.com
- fbcdn.net

To create DNS-ACL, you must create an ACL and and add DNS entries to the selected ACL. For more information, see the "Configuring and Applying Access Control Lists" in the Cisco Wireless Controller Configuration Guide, Release 7.6.

Configuring WLAN for Web Passthrough Authentication

Note After upgrading to Cisco CMX 10.2, or after newly installing Cisco CMX 10.2, the sslmode is enabled by default. Therefore if you want to have the HTTP redirect, you need to disable sslmode. Otherwise, you need to conigure https://<CMX>/… in WLC SSID config. And modify ACL rules to reach MSE_IP using HTTP.

To provide network access to users, you must configure a wireless LAN (WLAN) on the Cisco WLC, for which you must set up the web passthrough on Layer 3 security of WLAN for Connect & Engage.

Procedure

Step 1 From the web UI of Cisco WLC, click **WLANs**.

Step 2 On the **WLANs** window, click the corresponding WLAN ID.

Step 3 On the **WLANs > Edit** window, choose **Security > Layer 2**.

Step 4 From the **Layer 2 Security** drop-down list, choose **None**.

Step 5 Click **Apply**.

Step 6 Under the **Layer 3** tab, from the **Layer 3 Security** drop-down list, choose **Web Policy**.

Step 7 For web passthrough, choose **Passthrough**.

Step 8 Choose the **Preauthentication ACL** defined using the procedure described in the Configuring Access Control Lists on Cisco Wireless Controller, on page 106.

Step 9 To override the global authentication and web authentication pages, check the **Over-ride Global Config** check box.

Step 10 To define the web authentication pages for wireless guest users, from the **Web Auth Type** drop-down list, choose **External (Re-direct to external server)**.

This redirects clients to an external server for authentication.

Step 11 In the **URL** field, enter the Facebook Wi-Fi page URL. The external redirection URL should point to the corresponding portal on Cisco CMX for Facebook Wi-Fi, for example:

Example:

```
https://<CMX>/fbwifi/forward
```

Step 12 Enable this Service Set Identifier (SSID).

Step 13 Click **Apply**.

Step 14 Click **Save Configuration**.

Note Connect & Engage redirection requires special configuration on Cisco WLC for Apple iOS devices.

Run the following command using the Cisco WLC CLI:

config network web-auth captive-bypass enable.

For more information, see the *Cisco Wireless LAN Controller Command Reference, Release 8.0*, at:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/command-reference/b_cr80/b_cr80_chapter_

Creating a Facebook Page for Your Organization

Follow the instructions provided in Facebook to create a Facebook page for your organization. To create a Facebook page, go to https://www.facebook.com/pages/create.php.

Note Currently, Facebook Wi-Fi does not support age and country restricted Facebook Pages. We recommend to remove any age and country restrictions from the Facebook Page in order to successfully pair Facebook Wi-Fi with Cisco CMX.

Assigning a System Default Facebook Page

Procedure

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

Step 2 Choose **CONNECT > Connect Experiences** .

Step 3 In the **Facebook Wi-Fi** column, click **Assign Default**.

The Facebook Wi-Fi Configuration option opens in a new browser tab.

Step 4 Perform the following tasks:

a) Select the page.
b) Select the **Bypass Mode**.
c) Select the **Session Length**.
d) Click the optional Terms of Service if additional Terms of Service are required.
e) Click **Save Settings**.

Step 5 After assigning Facebook Wifi Configuration, navigate to **Connect Experience** tab and click **Click Here When Finished**.

Note When on boarding guest Wi-Fi using Fabcebook Wi-Fi, some guest client browsers displays "Network Not Found" error message. However, if you are using default Facebook WiFi settings for all the locations, you will not encounter this issue. This issue occuers only if you have setup your Facebook WiFi configuration in a Parent-Child location hierarcy, for example, **Campus >Bulding>Floor>Zone**.

You can pair different facebook pages with different child nodes in the hieraracy, like Campus is paired with Facebook page 1 and Building with Facebook page 2. In this scenarion, you can get the network not found error message while using Facebook Wi-Fi. To resolve this issue, remove the Facebook pairing with all the child nodes to inherit the pairing from the parent.

Assigning a Location-Specific Facebook Page

After the system default page has been set, you can assign a location-specific Facebook page:

Procedure

Step 1 Select a specific campus, building, floor, or zone and click or hover over the Gear  icon.

Step 2 Click **Assign New**.

Setting Up a Custom Portal

You can create a custom portal page using the following four types of templates:

- **Registration Form**—This template contains the following elements:
  - Logo or image
  - Registration form to specify name, email address, and phone number of a visitor
  - Terms and conditions
  - The **Submit** button

  Note When you specify a phone number, select the **SMS Auth** check box to get notification through SMS. For more information, see Enabling Multi-language Support in Custom Portals, on page 112.

- **Social Login**—This template contains the following elements:
  - Logo or image
  - Social login element that includes three options: Facebook, Instagram, and Foursquare.

    The Social login element enables on-boarding of visitors using social OAuth 2.0.

Note If you have the **Terms and Conditions** checkbox element in the live portal, all the social login elements are enabled only when you select the **Terms and Conditions** checkbox.

- **Social or Registration Login**—This template contains both the Social Login element and the Registration Form element.
- **SMS Form**—This template enables you to create a portal for SMS authentication. Verify your portal has a Registration Form element, or add one if required. All that this element requires is a phone number field, but you may include others if required. The Registration form allows you to receive the auth code on a SMS capable device and still enter it on a non-SMS capable device.
- **Custom**—This template is empty and allows you to create your template from scratch. The template choice does not limit the type of elements you can add. For example, if a Social Login template is selected, you can always modify it to use the Registration Form elements instead.

  The following options are available to design a custom portal:

  - The left side of the window shows a preview of the custom portal and the right side of the window shows the options to edit the portal and its elements.
  - The **CONTENT** tab allows you to add or edit the portal elements. Click an element to preview an area of the portal and edit the element's settings. For more information, see Using Content Elements for Creating Portals, on page 126.
  - The **BACKGROUND** tab allows you to:
    - Upload an image from the image library
    - Specify the background color and opacity for the portal.
  - The **THEMES** tab allows you to specify a theme for the portal.
  - The **LANGUAGES** tab allows you to choose the language of your choice. To add a language, choose your desired language from the **Select language** drop-down list, and then click **Add to list**.

Note
- You can get a preview of the custom portal for a mobile, PC, or tablet.
- For **Registration Form** element, you can add three input fields: **Text**, **Drop-down**, and **Checkbox/Radio**. If you choose to add a check box or a radio button, you must specify at least one field value. An error message is displayed when you try to save a portal with no input field values and **Submit** button added to the **Registration Form** element.

- **Engage**—This template enables you to create a portal for engage services.

Creating a Default Custom Portal Page

Procedure

Step 1 Log in to Cisco CMX as an admin user.
Step 2 Choose **CONNECT** > **Connect Experiences**.
Step 3 Under **Custom Cisco CMXs**, click **Create Default**.
Step 4 In the **Portal Title** field, enter the name of your custom portal.
Step 5 Click the template that you want to use and click **Next**.
Step 6 Design the template according to your requirements.
Step 7 Click **Save**.

Assigning Location-Specific Custom Portal Page

After the system default portal has been set, you can assign a location-specific custom portal page.

Procedure

Step 1 Select a specific campus, building, floor, or zone from the corresponding custom portal drop-down list.
Step 2 Click **Create New** to create a new portal and assign it to that location. Alternatively, assign an existing portal to that location.

Enabling Multi-language Support in Custom Portals

Cisco CMX does not contain any language translation engine. Administrator must edit each language page individually and manually translate all text entries.

Note The portal page translations are not supported for right-to-left languages such as Hebrew and Arabic.

To support multiple pages by a portal page, each page must have the desired languages added to the page before it can be enabled. Multi-language support can be added when the portal is created. The non-English languages can be disabled or re-enabled one at a time when translations are completed.

To enable multi-language support, the admin user should perform the following tasks:

- Create a portal.
- Add the languages that have to be supported.
  - To add a language, click the **Languages** tab inside the portal editor. Select the language from the drop-down, and click **Add Language**. Only the Enabled languages(languages that are selected) are used.
- Provide translations for each language that is enabled.

- Change which portal translation is currently being viewed by selecting different language from the drop-down list above the preview area in the portal editor.
- Most elements' translations are portal specific, which means, translating a text element in one portal does not effect a text element in another portal.
- However, the registration fields' translations are shared across all portals. When a field is changed in one portal, the field is changed in every other portal.

- Confirm that translations are correct by using the Live View, switching between each language and verifying translation, and then saving the portal.

When the splash page is displayed to an end user, Cisco CMX uses the browser's settings to determine the end user's most preferred languages. It then selects the preferred language that is available and displays that version of the portal. An end user can manually select a different language by using the drop-down list on the top-right corner of the splash page.

End-user devices will have a predefined language. This list of preferred languages is passed as part of the HTTP header. Cisco CMX analyzes the HTTP header and displays the closest available translation of a portal.

For example, if a user prefers languages such as English, Spanish, and French (in this order) and the portal only has languages such as Russian, Spanish, Italian, German, then Spanish is displayed because it is the most preferred language from among the available languages.

To view a portal in a different language, a portal user can use the Language drop-down list to select from the list of available translations.

Configuring Connect Portal Pages for Sites

After you create a portal, you can assign it to a site by performing the following steps:

Procedure

Step 1 Choose **Connect** > **Connect Experiences**.

Step 2 In the **Custom Portal column**, click **Create Default** for the site that you want to assign as default.

Note If portals are already existing, select the desired portal from the available list.

Step 3 In the **Post Auth URL** column, click **Assign Default** for the site that you want to assign to the portal.

Step 4 In the **Post Auth URL for <site name>** dialog box, enter the post Auth URL, then click **Set**.

Note After a successful authentication, the clients will be redirected to the URL entered as the post Auth URL.

Viewing Connect Clients with Sites

To view the Connect clients with sites, perform the following steps:

Procedure

Step 1 Choose **Connect & Engage** > **Dashboard**.

Step 2 From the **Location** drop-down list, choose **Sites**.

Step 3 From the **Select a Location** drop-down list, select a site.

Step 4 From the **Interval** drop-down list select the interval.

Device-Browser Matrix

Device-Browser Matrix for Connect and Engage

The following table lists the tested devices and browsers for Connect & Engage in the context of custom portals.

Table 8: Device-Browser Matrix for Connect and Engage for Custom Portals

Device and Name	OS Version	Default Browser and Version	Remarks
Google Nexus 7	4.3	Google Chrome 32.0.1700.99	—
Amazon Kindle	13.3.2.2	Silk 1.0.454.220	—
Apple iPad	7.0	Safari 7.0	—
Apple iPhone	6.1.3	Safari 6.0	—
Apple Macbook Pro	10.8.4	Safari 6.0	—
Samsung (Snow OS)	33.0.1750.152	Google Chrome 33.0.1750.152	—
Apple iPad Mini	7.0	Safari 7.0	—
Microsoft Windows tablet	Windows RT 8.1	Internet Explorer 11	Issues with social connector
Samsung	4.2.2	Default browser	—

Device-Browser Matrix for Facebook Wi-Fi

Note The portal pages with Social OAuth do not work properly on Mozilla Firefox browser.

The following table lists the tested devices and browsers for Facebook Wi-Fi.

Table 9: Device-Browser Matrix for Facebook Wi-Fi

Device and Name	OS Version	Default Browser and Version	Other Browser and Version
Google Nexus 7	4.3	Google Chrome 32.0.1700.99	—
Amazon Kindle	13.3.2.2	Silk 1.0.454.220	—

Device and Name	OS Version	Default Browser and Version	Other Browser and Version
Apple iPad	7.0	Safari 7.0	—
Apple iPhone	6.1.3	Safari 6.0	—
Apple Macbook Pro	10.8.4	Safari 6.0	—
Samsung (Snow OS)	33.0.1750.152	Google Chrome 33.0.1750.152	—
Apple iPad Mini	7.0	Safari 7.0	Google Chrome 34.0.1874.114
Microsoft Windows tablet	4.2.2	Internet Explorer 11	—
Samsung	4.2.2	Default browser	—
One+ phone	5.0.1	Google Chrome	—
Amazon Reader	5.6.2.1	Default browser	—

Offering Opt-Out and Opt-In Options for Cisco CMX Services

Overview of the Opt-Out Option

Your login portal can include the **Opt-Out** option, which allows a client to opt out of having their mobile device location history maintained and used by Cisco CMX.

When a client opts out, Cisco CMX stops detecting the client's device MAC address and thus stops storing analytics data for that device. Either the client no longer appears on maps or appears not to be moving (that is XY location data remains the same).

The default is **Opt-In**.

The **Opt-Out** option is applicable when location tracking is enabled by default. With Cisco CMX Release 10.4 or earlier, the **Opt-Out** configuration was applicable for the complete Cisco CMX system. In Cisco CMX Release 10.5, the **Connect** service offers the **Opt-In** configuration that allows administartors or partners to collect consent from end users to being tracked using Cisco CMX.

Overview of the Opt-In Option

Cisco CMX is now complaint with GDPR and allows a client to opt for having their mobile device location history maintained and used by Cisco CMX. The **Data Privacy** feature enables you to secure your data. If you choose to enable the Data Privacy mode with MAC hashing disabled, the Cisco CMX **Connect** service seeks the approval of the Cisco CMX end user to opt for storing and maintaining data.

The Opt-in configurations allows the administrators or partners to collect the consent from end users and provide it to Cisco CMX. Your login portal can include an opt-in option, which allows a client to opt-in from having their mobile device location history maintained and used by Cisco CMX.

Table 10: Connect Portal Options and Tracking Status

End-User Scenario	Data Privacy	MAC Hashing	Tracking	Available Connect Options	Query Location with Hashed MAC Address
Scenario 1	Disabled	Disabled	Available	Opt Out	Not Possible

End-User Scenario	Data Privacy	MAC Hashing	Tracking	Available Connect Options	Query Location with Hashed MAC Address
Scenario 2	Enabled	Enabled (By default)	Available	Opt Out	Yes
Scenario 3	Enabled	Disabled	Not Possible	Opt In	No

From Cisco CMX Release 10.5, Cisco CMX tracks and saves client location information only if a client opts to get tracked. Use the Cisco CMX **Connect** service's **Opt-in** configuration to collect consent from clients to allow Cisco CMX to track and maintain client data.

If you are an existing Cisco CMX user who is upgrading from Cisco CMX 10.x to Cisco CMX 10.5 with Data Privacy enabled and MAC hashing enabled (by default), location tracking is available for clients, and the **Connect** service can offer them an option to opt out of from being tracked.

Configuring the Opt-Out Option

In Cisco CMX Release 10.4 or earlier, location tracking was enabled by default. In this scenario, the Cisco CMX **Connect** service offered clients an option to opt out from being tracked. The portal login page included the **Opt-out** option that clients could select to opt out from being tracked by Cisco CMX.

Procedure

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

Step 2 Choose **Connect > Library > Templates.**

Step 3 Click a portal template, such as the **Registration Form** template.

Note You can add the **Opt-Out** element to any template.

Step 4 Enter the name of the portal that you want to create, and then click **OK.**

Step 5 Click the **Content** tab.

Step 6 Click the **Opt-Out** element.

Step 7 Edit your opt-out message text.

Note If you do not want your portal to display the **Opt-Out** option, click **Remove element**.

Step 8 Click **Save.**

Changing the Opt-Out Period

The default opt-out period is 180 days. When this period ends, the **Opt-Out** option reappears when the client displays your login portal.

You can:

- Modify the opt-out period to be longer or shorter.
- Add the opt-out element to any template.

- Remove the opt-out element so that it does not appear on your portal.

Procedure

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

Step 2 Choose **Connect > Library > General**.

Step 3 In the **Connect Settings** window, change the value in the **User Retention Period** field.

The valid range is 1 to 1000 days. The default is 180 days.

Step 4 Click **Save.**

Configuring the Opt-In Option

To configure the Opt-In option for client tracking:

Procedure

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

Step 2 Choose **Connect > Library > Templates**.

Step 3 Click a portal template, such as the **Registration Form** template. (You can add the **Opt-In** element to any template.)

Step 4 Enter the name of the portal that you want to create, and then click **OK**.

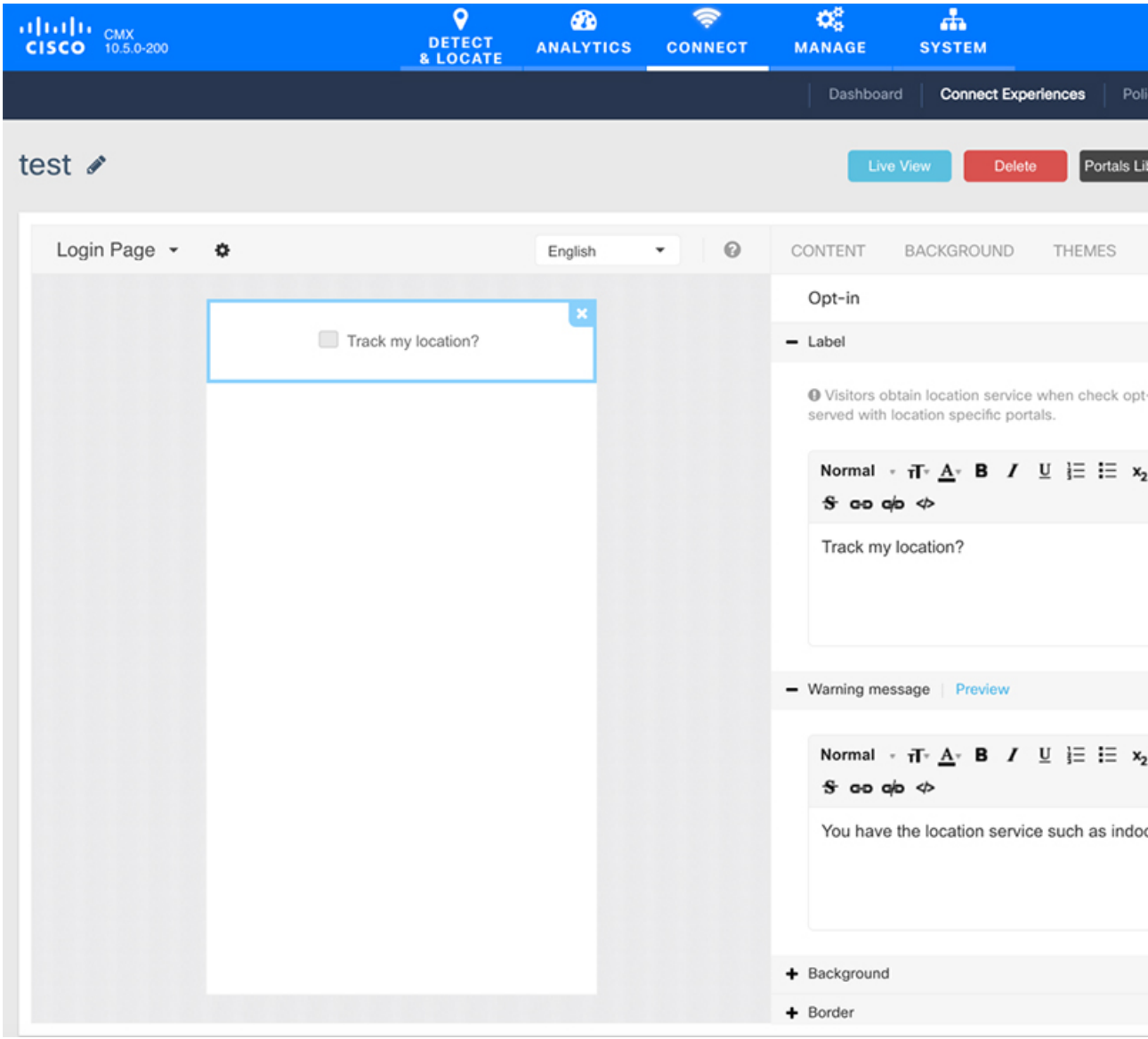
Step 5 Click the **Content** tab.

Step 6 Click the **Opt-In** element to add the same to the portal.

Step 7 Edit the opt-in message text. (If you do not want your portal to display the **Opt-In** option, click **Remove element**.)

For more information about Opt-out configurations, see Configuring the Opt-Out Option, on page 116.

Figure 13: Opt-In Element



Step 8 Click **Save**.

Managing Opt-In for Cisco CMX Services

If you are an existing Cisco CMX user upgrading from Cisco CMX 10.x to Cisco CMX 10.5 with Data Privacy enabled and MAC hashing disabled, the following points are applicable:

- By default, the locations of your clients are not calculated. However, your clients will be provided with the location based portal and the location calculated based on the corresponding access point location.
- If you select **Opt-In** in the portal login window, Cisco CMX tracks clients and applies portal frequency for these clients.

- If you do not select **Opt-In**, Cisco CMX gnores clients and does not save client data. The same clients are treated as new clients every time they visit the portal. Also portal frequency is not applied to clients.
- Run the **cmxctl configure connect deleteClientsAll** command to delete all the connect client data.
- Legacy portals with the **Opt-Out** option selected do not work. We recommend that you delete legacy portals, if any.

Note Use the **Opt-In** API to collect the consent. Depending on the consent, location or analytics tracking is achieved. The consent that is provided is stored in the Cisco CMX database, and with every new SALT schedule, Cisco CMX regenerates the new hash.

Configuring Elements for Custom Portal Navigation

Configuring URLs for Custom Portal Navigation

After you create a custom portal, use the **Content** tab in the **Portal** window to design and customize the portal. You can select the elements (such as, Social Auth, Image & Text, Image Slider, External Content) in the right side of the window to edit the portal and the elements. You can configure website URLs for URL enables elements such as images and logo. The URL enabled elements are **Image**, **Menu**, and **Image Slider**.

Note If you configure a URL enabled element in the login page, configure DNS-ACL to white list URL domain on WLC which requires 8.3 version. If you configure a URL enabled element in the success page, you need not perform any more configuration on WLC, because the client already has Wi-Fi access.

To configure a URL, perform the following steps:

Procedure

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

Step 2 Choose **CONNECT > Library**.

Step 3 Create a portal. For more information about setting up a custom portal, see Creating a Default Custom Portal Page, on page 112.

Step 4 From the **Content** tab, click any of the following elements:

- **Image Element**
- **Menu**
- **Image Slider**

Step 5 In the **Link** field or **Image URL** field, enter the URL.

In the live view, you can click the image or logo to view the Website.

Check the **Enable back button** check box to display the **Back to Portal** option in the live view of the portal page. Click **Back to Portal** to navigate back to the portal view. Not all the URLs are displayed within the frame view. Use the **Live View** option in the window to verify if the URL provided is displayed in the frame

view. If the URL you configured is not compatible to be displayed within the same frame, the website is displayed as a separate web page in the browser window.

- If the **Enable back button** option is selected, links with HTTP response header "X-Frame-Options" will not be rendered on the portal.
- If the **Enable back button** option is selected and SSL is enabled on CMX, use HTTPS links for the login portal. However, if SSL is not enabled on CMX, use either HTTP or HTTPS links for login portals.

FlexConnect AP Support on Cisco CMX

FlexConnect AP communicates through Cisco WLC for Authentication. FlexConnect AP is responsible for Policy Plan enforcement such as ACL, Rate-limiting and session timeout. Enforcement message comes from AAA to Cisco WLC, which the Cisco WLC pushes according to the per-user network policy to FlexConnect AP. FlexConnect Access Point cannot function when communication with Cisco WLC is down. CMX Connect relies on Web Authentication which is handled by Cisco WLC. The supported FlexConnect modes are Local Switching and Central Switching.

The following Cisco CMX features are supported on a FlexConnect Access Point:

- Location
- Analytics
- Connect

Note Cisco CMX supports FlexConnect mode for both Facebook OAuth and Facebook Wi-Fi.

Configuring FlexConnect ACLs

You need to configure FlexConnect Access Control Lists (ACLs) only for Flex mode deployments. To configure FlexConnect ACLs, follow these steps:

Procedure

Step 1 Choose **Security > Access Control Lists > FlexConnect ACLs** from the Controller UI.

The FlexConnect ACL page is displayed. This page lists all the FlexConnect ACLs configured on the controller. This page also shows the FlexConnect ACLs created on the corresponding controller. To remove an ACL, hover your mouse over the blue drop-down arrow adjacent to the corresponding ACL name and choose Remove.

Step 2 Add a new ACL by clicking New.

The **Access Control Lists > New page** is displayed.

Step 3 In the **Access Control List Name** text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply**.

Step 5 When the Access Control Lists page reappears, click the name of the new ACL.

Step 6 When the **Access Control Lists > Edit** page appears, click **Add New Rule**.

The **Access Control Lists > Rules > New** page is displayed.

Step 7 Configure a rule for this ACL as follows:

Note The controller supports up to 64 rules for each ACL. These rules are listed in order from 1 to 64. In the Sequence text box, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL.

If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number of a rule, the sequence numbers of the other rules are automatically adjusted to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.

a) From the **Source** drop-down list, choose one of these options to specify the source of the packets to which this ACL is applicable:

- Any—Any source (This is the default value.)
- IP Address—A specific source. If you choose this option, enter the IP address and netmask of the source in the corresponding text boxes.

b) From the **Destination** drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

- Any—Any destination (This is the default value.)
- IP Address—A specific destination. If you choose this option, enter the IP address and netmask of the destination in the text boxes.

c) From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL. The protocol options that you can use are the following:

- Any—Any protocol (This is the default value.)
- TCP
- UDP
- ICMP—Internet Control Message Protocol
- ESP—IP Encapsulating Security Payload
- AH—Authentication Header
- GRE—Generic Routing Encapsulation
- IP in IP—Permits or denies IP-in-IP packets
- Eth Over IP—Ethernet-over-Internet Protocol
- OSPF—Open Shortest Path First
- Other—Any other Internet-Assigned Numbers Authority (IANA) protocol

Note If you choose **Other**, enter the number of the desired protocol in the Protocol text box. You can find the list of available protocols in the INAI website.

The controller can permit or deny only the IP packets in an ACL. Other types of packets (such as Address Resolution Protocol (ARP) packets) cannot be specified. If you chose TCP or UDP, two additional parameters, Source Port and Destination Port, are displayed. These parameters enable you to choose a specific source port and destination port or port range. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications, such as Telnet, SSH, HTTP, and so on.

d) From the **DSCP** drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header text box that can be used to define the quality of service across the Internet.

- Any—Any DSCP (This is the default value.)
- Specific—A specific DSCP from 0 to 63, which you enter in the DSCP text box

e) From the **Action** drop-down list, choose **Deny** to cause this ACL to block packets, or Permit to cause this ACL to allow packets. The default value is Deny.

f) Click **Apply**.

The **Access Control Lists > Edit** page is displayed on which the rules for this ACL are shown.

g) Repeat this procedure to add additional rules, if any, for this ACL.

Step 8 Click **Save Configuration**.

What to do next

For setting up WLC with FlexConnect ACL, see Setting Up a Controller with FlexConnect ACLs, on page 122.

Setting Up a Controller with FlexConnect ACLs

After configuring the FlexConnect ACLs, you must apply the FlexConnect ACLs to the SSID.

Procedure

Step 1 From the web UI of Cisco WLC, click **WLANs**.
The **WLANs** window is displayed.

Step 2 Click the corresponding WLAN ID.
The **WLANs > Edit** window is displayed.

Step 3 Click **Advanced** tab.

Step 4 To configure the WLAN for FlexConnect Local Switching, select the **FlexConnect local Switching** check box in the **FlexConnect** section.

Step 5 Click **Security > Layer 3**.

Step 6 From the **Layer 3 Security** drop-down list, select **Web Policy** to configure the security policy for the WLAN.

To enable External Web Authentication, you must configure **Web Policy** as the security policy for the WLAN.

Step 7 From the **Preauthentication ACL IPv4** and **IPv6** drop-down list, select **None**.

Step 8 To apply FlexConnect ACLs to the SSID, select **FlexConnect ACL on SSID** from the **WebAuth FlexAcl** drop-down list.

Offering Portal Pages on HTTP from Cisco CMX Connect

Disabling HTTPS

Procedure

Step 1 In the Cisco MSE CLI, disable SSL mode by entering the **cmxctl node sslmode disable** command.

Step 2 In Cisco WLC (**WLANs > Security > Layer 3**), use HTTP instead of HTTPS for URL. For example, enter http://<IP address>/visitor/login instead of https:/<IP address>/visitor/login.

Step 3 In Cisco WLC (**Management > HTTP-HTTPS**), set the **WebAuth SecureWeb** and **HTTPS Redirection** options to **Disable**.

Note If the **WebAuth SecureWeb** option is enabled, you need to upload a proper certification to WLC to avoid certificate warning. We recommend to disable this option to avoid certificate warning on client.

Adjusting ACLs on Cisco WLC

Procedure

Step 1 Adjust the ACLs on the Cisco WLC to match HTTP.

Step 2 In Cisco WLC, (**WLANs > Security > Access Controller**), use HTTPS instead of HTTP.

SMS Authentication

To provide a proof of the identity of the connected individual, Cisco CMX 10.2 offers the ability to add SMS based authentication to a custom portal. Currently this feature only integrates with Twillio accounts for SMS authentication. You must establish your own Twillio account (see https://www.twilio.com/user/account/settings). Also, this feature requires you to have an SMS capable device to gain access to the network.

Without an appropriately configured preauth ACL the wireless client will not be able use the link provided in the SMS message to return the auth code to Cisco CMX and will remain in the WebAuth required state.

To use this feature, either edit an existing portal or use a template to create a new portal to use SMS Auth. You can only have one Twillio account, but that account can have many phone numbers associated with it so you can use the same account with multiple portals, but each portal can only have a single number associated

with it. The Reset button is used to remove the association between the portal and the configured Twillio account.

The From Number that you configure in the Twillio Configuration area should be purchased from Twillio. You cannot use an existing number.

Procedure

Step 1 Ensure that your portal has a Registration Form element, or add one if required

Step 2 Ensure that you specify a phone number field, but you may include other fields if desired.

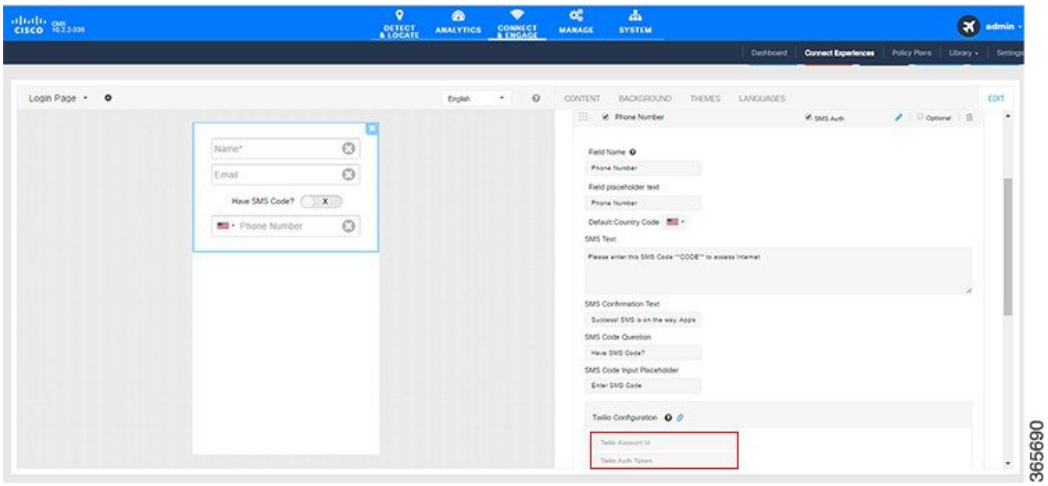
Step 3 In the **Registration Form** area, check the **SMS Auth** check box.

The Registration form allows you to receive the auth code on a SMS capable device and still enter it on a non-SMS capable device.

Step 4 Select the **Edit** icon (next to the SMS Auth check box) to enter the Twilio account information.

Step 5 In the **Twilio Configuration** area (see the figure below), enter the following parameters:

Figure 14: Twilio Account Configuration



You can click the **Edit** button next to the Twillio Configuration field to access your Twillio account information.

a) Enter your **Twilio Account ID**. This is a 34 character string that uniquely identifies the Twilio account.
b) Enter the **Twillio Auth Token**.
c) Enter the **From Number**. This number is purchased from Twillio. You cannot use an existing phone number.
d) Click **Create**.

   You can click the **Reset** button to remove the association between the portal and the configured Twillio account (that is, removing the connector).

Step 6 Click **Save**.

Customizing a Policy Plan

The Cisco CMX Policy Plans feature gives you the option to provide your client with the highest available bandwidth as the client moves from one location to the next. Use the CMX Policy Plans window to configure this feature. Use this feature to offer specific Wi-Fi policies for each site or location and thereby enhance the guest Wi-Fi experience.

For example, the bandwidth provided to clients in a hotel room is higher than the bandwidth provided in a hotel lobby. If the CMX Policy Plans feature is active, the bandwidth to the client is automatically increased when the client moves from the lobby to their hotel room. In addition, if the **Keep Highest Bandwidth** check box on the CMX Policy Plans window (**Cisco CMX > Connect > Policy Plans**) is selected, the client retains the higher bandwidth when returning to the lobby.

Note The CMX Policy Plans feature is not supported when you add a PMS server.

Before creating the policy plans, ensure that you have the configured FreeRADIUS and Wireless Controllers. For more information, see Configuring the FreeRADIUS on Cisco CMX, on page 135 and Cisco WLC Configurations, on page 137.

Procedure

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

Step 2 Choose **Connect > Policy Plans**.

Step 3 Click **New Policy Plan**.
The **CREATE POLICY PLAN** window is displayed.

Step 4 Enter a name for the new policy plan.

Ensure to specify the name without spaces and special characters. For example, `PolicyOne`. The maximum characters allowed for a policy name is 20.

Step 5 Enter the bandwidth, in kbps.

The maximum bandwidth allowed is a 10 digit value.

Step 6 Click **Create**.

Note The new policy plan is displayed in the **Policy** drop-down list in the **Connect Experiences** (**Connect > Connect Experiences**) tab.

Using the Connect Library

To view the Connect Library, log in to Cisco CMX and choose **CONNECT** > **Library**. The following options are available:

- Portal Library—Lists the portals that you have created, both drafts and completed ones. Click **Create Portal** to create a new portal using the available template.

  Note Select the Disable Portal Cache check box to disable HTTP cache for all portals.

  In the Portal Library, you can:

  - Edit—Edit a portal that is in progress.
  - Copy—Allows you to copy or duplicate a portal.
  - View—Allows you to view a portal.
  - Delete—Allows you to delete a portal.

- Templates Library—Provides pre-defined templates that you can use to create your own portal. The following templates are available:

  - Registration Form
  - Social Login
  - Social or Registration Login
  - SMS Form
  - Custom
  - Engage
  - PMS Auth Form—Available in the template library if a PMS server is configured.

- Image Library—The image library allows an imported image to be used for multiple portals. There is no size limit on uploaded images as they are scaled during the upload. Once uploaded, the images can be rotated, cropped, or have their aspect ratio changed using the built-in image editor. In the Image Library, you can:

  - Add—Allows you to add new images. Images are scaled down so that you get a thumbnail view of the image.
  - View—Allows you to preview an image. When you preview an image, you can crop, resize or set its aspect ratio. After making changes in the image editor, click **Save** and **Close** to copy the image into the Image Library or overwrite the existing image.
  - Delete—Allows you to delete images from the Image Library.

Using Content Elements for Creating Portals

If you want to create a new Portal, use any of the existing templates available under **Connect > Library > Templates**.

The **Content** tab includes **Common** and **Advertisement** elements that can be used to create a login page or a success page. To add an element, drag and drop the element from the Content tab to the canvas or just click the required element.

The following table list some of the common elements available:

Table 11: Common Elements

Elements	Description
Image	To add a logo or image
Text	To add a text field
Registration Form	To add registration form fields such as name and email address.
Social Auth	To add preferres social login credentials
Terms & Conditions	To add terms and conditions for accessing Wi-Fi
Image and Text	To add image with text content
Sumit Button	To add Submit button
Contact us	To add contact information
Spacer	To add space element
PMS	To add PMS details
Menu	To add menu items
Opt-out	To add opt-out check box For more information, see Configuring the Opt-Out Option, on page 116.
Opt-in	To add opt-in check box For more information, see Configuring the Opt-In Option, on page 117.

Authentication with Social Network Accounts

To configure OAuth for each social network platform (Facebook, Instagram or Foursquare), you need to first register your app/client with the Cisco CMX Connect service. If you want to remove a particular social network connection, uncheck the check box to the left of the social network name.

Configuring OAuth with Facebook

Note If Facebook is configured with OAuth, the client uses HTTPS to communicate with Facebook.

The portal pages with Social OAuth do not work properly on Mozilla Firefox browser.

Procedure

Step 1 In the Social Login element of the custom portal, click on the link ( ) icon to the right of Facebook to go to the associated developer website.

Step 2 Log in to Facebook with your username and password.

Step 3 Click the **+Add a New App** button.

Step 4 Click the **Website** button.

Step 5 Enter a name for the application, and then click the **Create New Facebook App ID** button.

Step 6 From the **Choose a Category** drop-down list, choose a category for the new application, and then click the **Create App ID** button.

Step 7 Scroll down to the **Tell us about your website** area and enter the same URL as the Wireless LAN Controller (WLC) redirect URL (http://<CMX>/visitor/login) in the **Site URL** field, and the click the **Next** button.

Note This configuration will fail if Cisco CMX has an IP address in the 172.x.x.x range as it will be seen as a Facebook URL.

Step 8 Click the **Skip to Developer Dashboard** link.

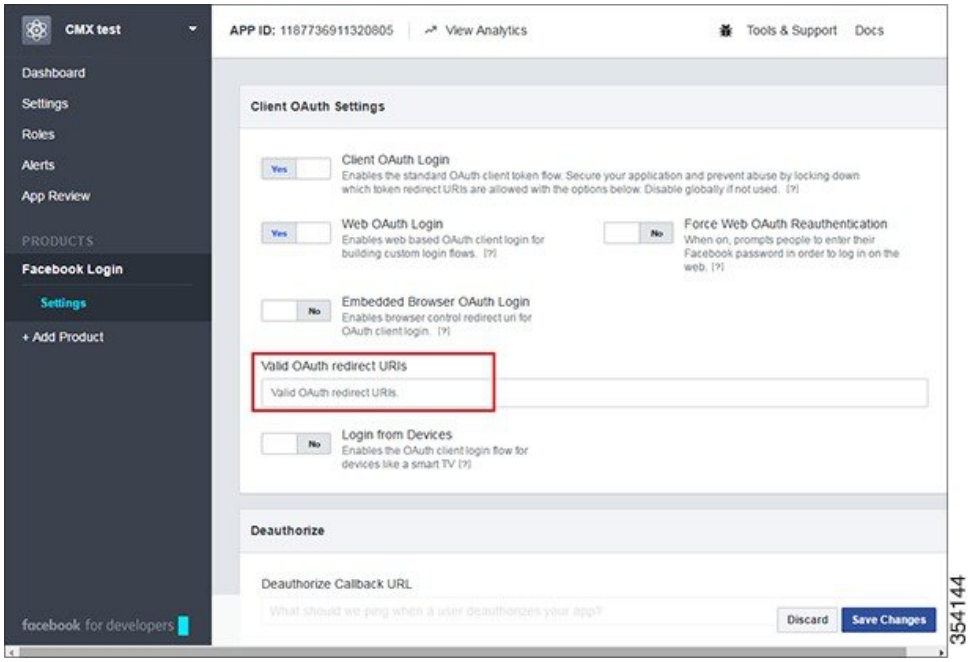
Step 9 Select and copy the App ID for a later step.

Step 10 To add Facebook Login as a new product, under **Product Setup**, click **Get Started** next to the Facebook Login option.
Facebook Login is added as a new product and is displayed under **PRODUCTS** in the left navigation pane.

Step 11 Click **Settings** under **Facebook Login** product, and enter the client OAuth settings.

Step 12 To configure a private IP address for the Facebook OAuth configuration, enter **http://cmxIP/visitor/login** in the **Valid OAuth redirect URIs** field. By default, the **Valid OAuth redirect URIs** field is empty.

Figure 15: Client OAuth Settings



Step 13 Click **Save Changes** to save the client authentication settings.

Step 14 (Optional) To view basic and advanced settings, click **Settings** in the left navigation pane, update the settings, and click **Save Changes**.

Figure 16: Basic Settings

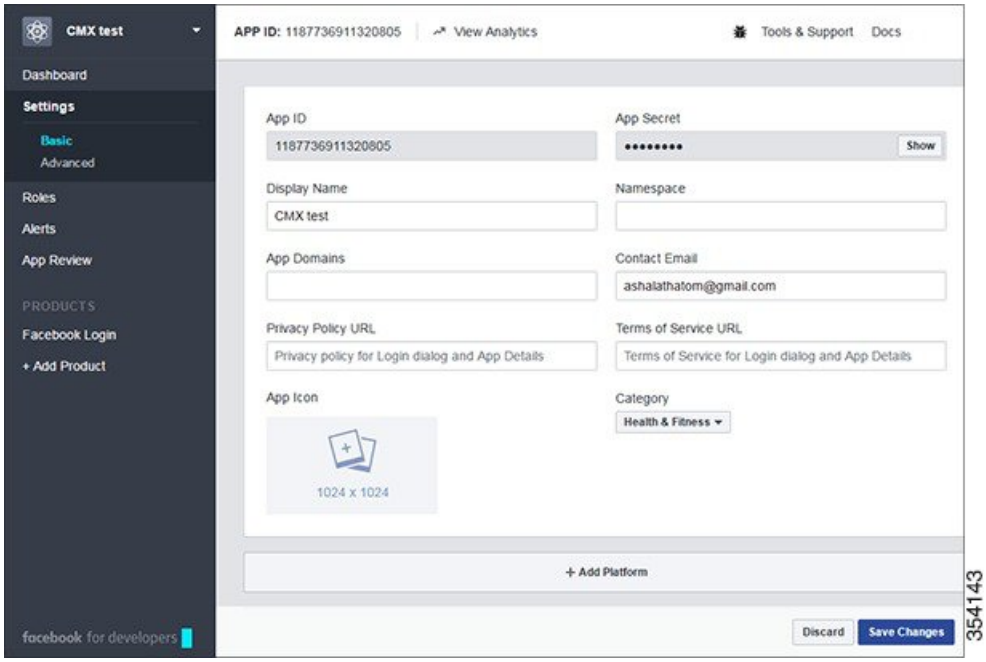
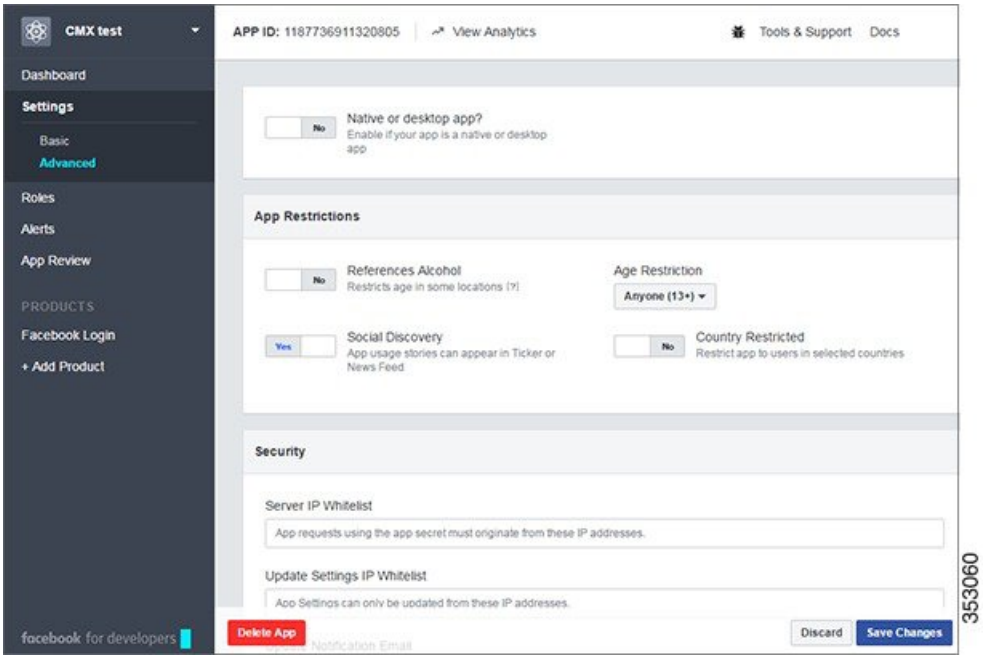
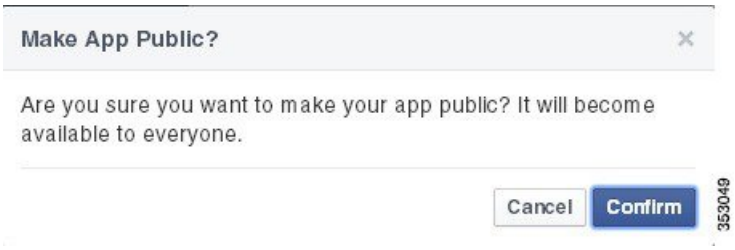


Figure 17: Advanced Settings



Step 15 Click **App Review** in the left navigation pane, and click **Yes** in the slider to make the app available to the general public.

Step 16 Click **Confirm**.



Step 17 If you want to collect information such as first name, last name, friend list, submit those items for approval by Facebook.

Step 18 Go to the custom portal and click **Create New**, add the App name, paste the App ID information that you generated using the preceding steps.

Step 19 From the **Scope** drop-down list, choose the scope to collect Social Network data, and then check the **Facebook** checkbox.

Facebook Data Collection

Cisco CMX collects information about Facebook Friends, but the Facebook API only returns the information about friends who also using the same app.

Configuring OAuth with Instagram

Procedure

Step 1 In the Social Login element of the custom portal, click on the link ( ) icon to the right of Instagram to go to the associated developer website.

Step 2 To log in to Instagram, click **Log In** on the top right hand side, then enter username and password and click **Log in**.

Step 3 In the **Manage Clients** tab, click **Register a New Client**.

Step 4 Enter the application name and the description.

Step 5 Enter the same URL as the Wireless LAN Controller (WLC) redirect URL (https://<CMX>/visitor/login/) in the website field and in the **OAuth redirect_url** field. Check the **Disable Implicit OAuth** check box.

Note In Cisco CMX Release 10.4 or earlier, ensure that you use the redirect URL as http://<CMX>/visitor/login in the website field.

Step 6 Enter the **Captcha** and click the **Register** button.

Step 7 Select and copy the Client ID for the next step.

Step 8 Go to the custom portal and click **Create New**, add the App name, paste the Client ID that you generated using the preceding step.

Configuring OAuth with Foursquare

Procedure

Step 1 In the Social Login element of the custom portal, click on the link ( ) icon to the right of Foursquare to go to the associated developer website.

Step 2 Log in to Foursquare by clicking on the My Apps tab at the top right hand side.

Step 3 Enter your email address and password and click the **LOG IN** button.

Step 4 Click the **CREATE A NEW APP** button.

Step 5 Enter the same URL as the Wireless LAN Controller (WLC) redirect URL (http://<CMX>/visitor/login) in **Download/welcome page url** field, in the **Your privacy policy url** field, and in the **Redirect URI(s)** field.

Step 6 Click **SAVE CHANGES**.

Step 7 Select and copy the Client ID for the next step.

Step 8 Go to the custom portal and click **Create New**, add the App name, paste the Client ID that you copied using the preceding step.

Step 9 From the **Scope** drop-down list, choose the scope to collect Social Network data, and then check the checkbox.

Connect Settings

To view the **Connect Settings** window, log in to Cisco CMX as an admin user and choose **CONNECT > Settings**.

Connect Settings

The following data retention settings available:

- **User Retention Period**—This value indicates how long a user entry is retained in data store if the user does not reconnect. The default user retention value is 180 days. The oldest entries are removed if the system has reached the capacity even if the value specified in the User Retention Period is not reached. This is to ensure that the system continues to serve new users.
- **Statistics Retention Period**—Statistics are calculated once every day for each location. The statistics entries, which were caluclated before the value that you configured in this text box will be purged. The range is 7 to 1000 days. The default retention value is 365 days.
- **SMS: Number of Devices**—This is the total number of devices that can use a single SMS code. The range is 1 to 10 devices. The default value is three devices.
- **SMS: Time to expire** (in min)—This value indicates how long you want to keep the SMS code active. The range is 3 to 1440 minutes. The default retention value is 15 minutes.

Connect prunes users based on the user retention period. This task is run once every day at three AM server time. If the maximum user capacity is exceeded, older users within the retention period are pruned to make room for new users. To avoid losing any user data, we recommend that you perform the following tasks:

- Periodically export data from Cisco CMX.
- Adjust the retention period based on projected days for full capacity, which is calculated based on usage patterns. The usage patterns are established after the system has been operational for a while.

Changing the Portal Login Frequency

You can define how often your login page is displayed to a visitor each time their device associates with the SSID in your network. By default, a repeat visitor does not need to go through the portal login process for 180 days from the day the visitor associated with the SSID.

Procedure

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

Step 2 Choose **Connect > Settings > General** to display the **Connect Settings** window

Step 3 From the **Connect Settings** window, change the value in the **Visitor: Portal Frequency** field. The range is 0 to 1000 days. The default is 180 days.

Examples:

- If the login frequency is set to 0, the portal is displayed is each time the visitor’s device associates with the SSID.

- If the login frequency is set to 1, the portal is displayed when the visitor's device first associates with the SSID and is not displayed again until after a 24-hour period. Within that 24-hour period, the portal is not displayed regardless of the number of times the visitor's device disassociates and associate to the SSID.

Step 4 Click **Save**.

Using the CMX Connect Debugging Tools

The CMX Connect debugging tool allows you to delete a client record based on its MAC address.

Note The debugging tools are meant for debugging purpose only.

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).
Step 2 Choose **CONNECT** > **Settings**.
Step 3 Click the **Debugging Tools** tab.
Step 4 Under the **Delete User Tool** area, enter the user's MAC address to delete its record based on the MAC address
Step 5 Click **Delete User**.

Configuring the Property Management System

Use the Connect service in Cisco CMX 10.2.2, to integrate a Property Management System (PMS) solution (for example, a PMS solution used by a hospitality industry).

Note Currently, Cisco CMX Connect integrates only with Unlink Rest Management accounts. Unilink Rest Management is a paid service that customers subscribe to for getting access to the PMS console.

The PMS solution provides customers with the following capabilities:

- Provides guest Wi-Fi portal at a hotel.
- Provides the flexibility to assign different Wi-Fi plans to different portals at different locations.

  For example, a hotel can offer a click-through guest portal in common areas such as the lobby and recreational spaces. However, in guest rooms, the portal may require guests to enter their Room Number and Last Name, while the convention area may require guests to enter the Guest Code on the portal to access Wi-Fi. Besides these, guest rooms can also be charged for Wi-Fi usage.

The following are the components of the PMS:

- Client—Client devices (connected and detected) that are being tracked by your Cisco CMX. The clients can be classified as new clients and repeat clients.
  - New Clients—Clients seen by Cisco CMX Connect for the first time.
  - Repeat Clients—Clients that have been tracked by Cisco CMX Connect previously.
- Cisco WLC—Cisco Wireless Controller (Cisco WLC) is responsible for imposing policies.
- Cisco CMX—Cisco CMX helps you create personalized mobile experiences for end users and gain operational efficiency with location-based services. For example, by linking a hotel's property management service with Cisco CMX, the hotel can seamlessly guide guests through the check-in and Wi-Fi login process.
- Cisco CMX AAA Lite—Cisco CMX uses a customized AAA server (named AAA Lite), which enables you to control session duration and bandwidth throttling. CMX AAA Lite is based on the free, open-source FreeRADIUS. Cisco Connect uses FreeRADIUS to support PMS configuration. For example, a hotel may provide different Wi-Fi plans to its customers. Based on the time that a customer is buying the Wi-Fi plan, the AAA server controls the session duration and manages the upload or download speed.
- Nevotek—Cisco CMX uses the Nevotek gateway that helps hotels connect with guests. By linking the hotel's property management service with Cisco CMX, the hotel can seamlessly guide guests through the check-in and Wi-Fi login process. Guests are seamlessly authenticated and provided the correct level of access based on their reservation, preferences, and/or past loyalty history. Using the Nevotek gateway, Cisco CMX can even support different Wi-Fi access levels based on the location within the corresponding hotel, including guest rooms, conference rooms, and public spaces. Resulting charges, if any, are automatically posted to the guests' accounts.

Prerequisites for the Property Management System

Before you begin

- Configure a fully-functional Cisco CMX solution
- Configure fully-functional Cisco WLCs
- Ensure that you have an account with Nevotek and the setup is fully-functional.
- Configure and run FreeRADIUS
- Ensure that you have configured FreeRADIUS on Cisco CMX before configuring PMS.

PMS Policy Enforcement

When you add a PMS server into CMX, the policies defined in the PMS system are imported into CMX.

Location Based and Site Based PMS Policy Enforcement

Based on a user's location or site, Cisco CMX can enforce a policy using AAA. For example, if a user enters a hotel and goes to the lobby area, specific policy can be enforced (the user might receive a certain amount of bandwidth). Similarly, if the user goes to a room, the user might get a different bandwidth because of a different policy that is enforced.

The policy enforcement features perform the following tasks:

- Managing session timeout—If a user has been connected for more than the specific duration within the same day, the user will be disconnected. The session duration is within a day.
- Managing bandwidth—Cisco CMX Controller enforces the bandwidth limit sent from FreeRADIUS server.
- Managing the number of clients— Limit the number of devices connected per account (room number, and last name or passcode).

Configuring the FreeRADIUS on Cisco CMX

Procedure

Step 1 Use Secure Shell (SSH) to connect to Cisco CMX.

You must have root access credentials to configure the FreeRADIUS in Cisco CMX.

Step 2 Run the **su -l** command and provide the root password.

Step 3 Run the **freeradius-conf** command to execute the script to configure the FreeRADIUS in Cisco CMX.

Note that you can run this command from any directory in Cisco CMX. For more information about the FreeRADIUS configuration script, see Customizing the FreeRADIUS Server, on page 135.

Step 4 Press 1 to configure the FreeRADIUS.

Step 5 Enter the Cisco CMX UI admin user name and password.

Step 6 Enter the IP address of the Cisco WLC.

Step 7 Enter the secret key.

Step 8 Confirm the entered values.

Customizing the FreeRADIUS Server

To support the AAA functionality, the Cisco CMX Connect service uses a customized version of the FreeRADIUS server. This acts as an agent between Cisco CMX and Cisco WLC by providing policy enforcement. The Cisco CMX Connect service uses the FreeRADIUS server to provide the following functionalities:

- Session Duration Policy—A PMS policy with a 60 minute session duration can be enforced using the FreeRADIUS server. The server will disable the connection at the end of 60 minutes.
- Bandwidth Policy—A PMS policy with limited upload and download speed can be controlled by the FreeRADIUS server. The bandwidth can be throttled.

You can run the executable shell script to setup the FreeRADIUS.

Using the FreeRADIUS Configuration Script

To configure the FreeRADIUS server to work in your environment, use the executable script. This script allows you to configure the FreeRADIUS server to be used with the Cisco CMX Connect service. You must set up a fully functional Cisco CMX server along with a configured Cisco WLC before running the script.

The following example shows the output of the FreeRADIUS configuration script:

```
[root@cmx-server]# freeradius-conf

****************************************
** This script will help you configure  **
**      FreeRADIUS for CMX Connect      **
****************************************

 1)  Configure FreeRADIUS
 2)  Show FreeRADIUS Config
 3)  Add CMX Information
 4)  Add WLC(s)
 5)  Remove WLC
 6)  Check FreeRADIUS Status
 7)  Start FreeRADIUS
 8)  Stop FreeRADIUS
 9)  Restart FreeRADIUS
10) Start FreeRADIUS Debug
11) Tail FreeRADIUS Log (Control \) to Exit
12) Quit Config Script

Please choose an option or ENTER for menu :
.
.
.
```

The following table lists the key fields in the FreeRADIUS script output.

Table 12: FreeRADIUS Script Key Fields

Option	Description
Configure FreeRADIUS	Initial configuration option to run the FreeRADIUS. Sets up the environment by adding a Cisco CMX client, and one or more Cisco WLCs and to start the RADIUS server. This option is mandatory for a new installation.
Show FreeRADIUS Config	Displays the FreeRADIUS server's configuration changes.
Add CMX Information	Updates the Cisco CMX configuration information by overwriting the existing configuration.
Add WLC(s)	Sets up additional Cisco WLCs.
Remove WLC	Removes an existing Cisco WLC from the configuration. You must restart the FreeRADIUS server for the changes to take effect.
Check FreeRADIUS Status	Checks the running status of the FreeRADIUS server.
Start FreeRADIUS	Starts the FreeRADIUS server.

Option	Description
Stop FreeRADIUS	Stops the FreeRADIUS server.
Restart FreeRADIUS	Restarts the FreeRADIUS server.
Start FreeRADIUS Debug	Starts the FreeRADIUS server in debugging mode.
Tail FreeRADIUS Log (Control \) to Exit	Displays the running server log to inspect logged issues, if any.
Quit Config Script	Quits the configuration script.

Cisco WLC Configurations

Creating an Access Control List

Procedure

Step 1 Log in to the web UI of a Cisco Wireless Controller (Cisco WLC) that is associated with Cisco CMX.

Step 2 Choose **SECURITY > Access Control List > Access Control Lists**.

Step 3 In the **Access Control Lists** window, click **New** to add an access control list (ACL).

Step 4 In the **Access Access Control Lists > Edit** window, enter a name for the new ACL.

You can enter up to 32 alphanumeric characters.

Step 5 Choose the ACL type as either **IPv4** or **IPv6**.

Step 6 Click **Apply**.

Step 7 In the **Access Control Lists** window, click the name of the new ACL.

Step 8 In the **Acess Control Lists > Edit** window, click **Add New Rule**.

Configuring Authentication Server

Procedure

Step 1 Log in to the web UI of a Cisco Wireless Controller (Cisco WLC) that is associated with Cisco CMX.

Step 2 Choose **SECURITY > AAA > RADIUS > Authentication**.

Step 3 Click **New**.

Step 4 Enter the RADIUS server's IP address, shared secret key.

To view the added server, choose **WLANs > <*WLAN ID*> > Security > AAA Servers**. In the AAA Servers window, the newly added server name is displayed in the **Authentication Server** drop-down list.

Step 5 Click **Apply**.

Configuring WLAN

Procedure

Step 1 Log in to the web UI of a Cisco Wireless Controller (Cisco WLC) that is associated with Cisco CMX.

Step 2 Click **WLANs** and then choose **Create New** from the drop-down list.

Step 3 Click **Go** .
The **WLAN > New** window is displayed.

Step 4 Add profile name and SSID information.

Step 5 Click **Apply**.

Step 6 In the **WLANs > Edit** window, click the **Security** tab.

Step 7 To configure the security settings:

a) To configure Layer 2 settings, check the **Mac Filtering** check box.

b) To configure Layer 3 settings, click the **On MAC Filter Failure** radio button so that if Layer 2 fails, a redirection will be made to the server that you specified in the URL field and also specify the IP address of Cisco CMX in the **URL** field.

c) To configure AAA servers settings, specify the IP address and port number of the AAA server that you want to use for authentication.

Step 8 Choose the **Advanced** tab.

a) Select the **Allow AAA Override** check box to enable AAA override.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Configuring a PMS User's Account and Wi-Fi Plan

Before you begin

You must have a user account (with a username and password) with Unilink Rest Management to access the PMS console.

Procedure

Step 1 Log in to the PMS console (that is, the Unilink Rest Management console).

Step 2 Choose **Configuration > Parameter Maintenance**.

Step 3 Configure the required parameters.

Step 4 Choose **Price > Price Plan**.

Step 5 Click **Add new record**.

Step 6 Enter the required parameters for the price plan.

The **Free** field should not be left empty. Even if the price plan is free, price value should be entered as 0.00 in the **Free** field.

Note Default price plans should be created according to **Connection Types** using the same page. When Cisco CMX synchronizes with PMS, all price plans created on the PMS are populated on the portal. When configuring the PMS element, the price plans associated with the property are displayed and you can select as per the customer requirement.

Configuring Connect Settings for PMS

Procedure

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

Step 2 Choose **Connect** > **Settings**.

Step 3 Click **PMS**.

Step 4 Click the **PMS Account** tab.

Step 5 In the **PMS Connect Account** area, enter the following information pertaining to the REST credentials in Nevotek:

- **Server IP**—Username that is used to access the PMS server.
- **Username**—Username that is used to access the PMS server.
- **Password**—Password that is used to access the PMS server.

Step 6 Click **Create**.

Click **Refresh** to enable the Wi-Fi plans that you configured in the PMS to be listed in the **Plans** area of the **Settings** window.

Click **Delete** to delete the pairing between your PMS Connect account and Cisco CMX Connect. If you delete the PMS server information from CMX, the PMS configurations in all the portals will be deleted.

Editing the PMS Connect Settings

You can edit the pairing between your PMS Connect account and Cisco CMX Connect.

Procedure

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

Step 2 Choose **Connect** > **Settings**.

Step 3 Click **PMS**.

Step 4 Click the **PMS Account** tab.

Step 5 Click **Edit**.
A dialog box is displayed asking you to confirm the modifications.

Caution Portals will be modified automatically if they offer the plans that are affected by this edit.

Setting Up a Custom Portal for PMS

You can use a PMS template to create a custom portal page for PMS.

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **CONNECT > Library**.

Step 3 Click **Templates**.

Step 4 Click the **PMS Auth Form** template.

Note All available templates will have the **PMS** element in active state . You can either select the **PMS Auth Form** template or the **PMS** element in any other template to configure PMS.

all templates that are available will have the PMS element in active state

Step 5 Enter a name for the PMS portal.

Step 6 Ensure that your portal has a **Registration Form** element, or add one from the **Content** elements.

Step 7 Choose the required PMS Property from the **Select a Property** drop-down list.
The PMS plan types for the selected property is displayed in the **PMS Properties** section.

Step 8 Select the required **PMS Plan Types** by checking the appropriate check boxes under **PMS Properties**.

Step 9 Click **Save**.

Assigning a PMS Portal to Sites or Locations

After you create a PMS portal, you can assign it to a site or location by performing the following steps:

Procedure

Step 1 Choose **Connect > Connect Experiences**.

Step 2 In the **Custom Portal** column, from the **Click to assign portal** drop-down list, choose the custom portal that you want to assign to the site.

Step 3 In the **PMS Property** column, from the **Click to assign property** drop-down list, choose the property to be assigned to the site.

Using the Visitors Search to Find PMS Information

You can view PMS-related information pertaining to a client when you perform a Visitors Search in the Cisco CMX Connect Service.

Procedure

Step 1 Choose **Connect** > **Dashboard**.

Step 2 In the **Visitors Search** area, click the **Search** icon.
The following information is displayed in the **Visitors Search** window:

- MAC Address—MAC address of the client device
- State—Client state, that is Active or Inactive
- First Login Time—Date and time when the client logged in to Cisco CMX for the first time.
- Last Login Time— Date and time when the client logged in to Cisco CMX for the last time.
- Last Accept Time
- Location/Site
- Portal
- Type—Type of the portal
- Auth Type—Type of the authentication
- Device
- Operating System
- Bytes Received
- Bytes Sent
- Social Facebook Name
- Social Facebook Gender
- Social Facebook Locale
- Social Facebook Timezone
- Social Facebook Friends
- Social Facebook Email
- Social Foursquare Name
- Social Foursquare Email
- Social Instagram Name
- Social Instagram Email
- Email
- Phone Number
- Gender
- Username
- Profile Downloaded

- Profile Downloaded on
- Secure Login On
- PMS Property Name of the Hotel
- PMS Plan Type
- PMS Plan
- PMS Title
- PMS First Name
- PMS Last Name
- PMS Room Number
- PMS Guest Code
- PMS User Name
- PMS Check In Date
- PMS Check Out Date

Configuring Connect Services in Cisco CMX High Availability

Procedure

Step 1 To create a WLAN for the connect portals, use a Virtual IP address (VIP), for example, https://<*VIP*/visitor/login> Or http://<*VIP*/visitor/login>.

Step 2 Allow HTTP and HTTPS traffic on the ACL for the VIP.

Step 3 To configure the Facebook Wi-Fi WLAN, use the VIP, for example, https://<*VIP*>/fbwifi/forward.

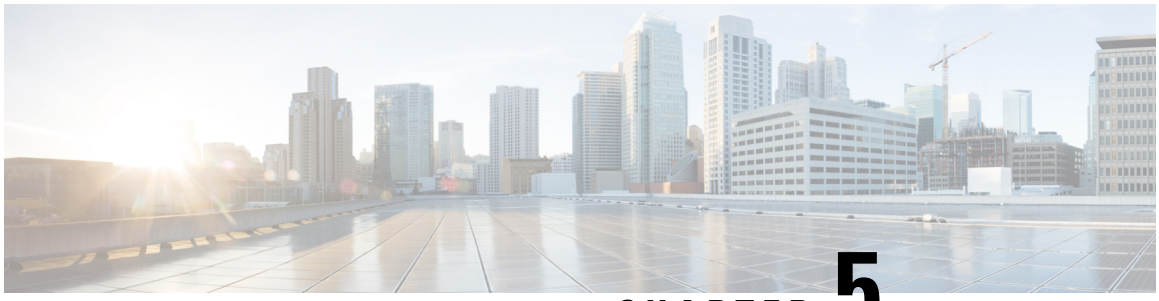
Step 4 To work with policy plan or Property Management System (PMS), create an authentication server for the VIP in Cisco WLC. The "Configuring Authentication Server" section explains how to create authentication server for an IP address (Cisco CMX Primary IP or Virtual IP). For more information, see Cisco WLC Configurations, on page 137.

Note

- During a failover or failback event, if new clients or existing clients in an unauthorized state on Cisco WLC tries to connect to WLAN, they will not be redirected to the portal and will not have access to the internet.
- If the VIP is down, all Virtual IP address will be replaced with the Cisco CMX IP address that is in active state for all the redirect URLs in WLANs, and the authentication server must be changed. The following error message is displayed on the clients if the IP address of Cisco CMX that is not in an active state is given in the redirect URLs of the WLANs:

  503 Service Unavailable

  No server is available to handle this request



CHAPTER 5

The Cisco CMX Presence Analytics Service

Overview of the Presence Analytics Service

The Cisco Connected Mobile Experiences (Cisco CMX) Presence Analytics service enables organizations with small deployments, even those with only one or two access points (APs), to use the wireless technology to study customer behavior.

The Cisco CMX Presence Analytics service is a comprehensive analytics and engagement platform that uses APs to detect visitor presence based on their mobile devices' Received Signal Strength Indication (RSSI). The AP detects these client mobile devices irrespective of the latter's wireless association state as long as they are within the specified signal range, and the wireless option is enabled on the mobile device (ability to detect devices wirelessly even if they are not connected to the network).

You can use the **PRESENCE ANALYTICS Dashboard** to view the following key performance indicators (KPIs) of the various client mobile devices at a specific site:

- Visitors
- Average Dwell Time
- Peak Hour
- Passerby-to-visitor conversion rate
- Manufacturers of popular client mobile devices detected by AP

These KPIs can be viewed for any duration (day, week, month, or custom) not exceeding 180 days from the current date. You can also customize the display to show data for a specific day, weekend, or even trends over a month.

Installing the Presence Analytics Service

You cannot run the Presence Analytics and the Location services on the same box. Therefore, you should choose either the Location service or the Presence Analytics service during the initial installation.

Benefits of the Presence Analytics Service

- Enables organizations with small deployments, even those with just one or two APs, to understand customer behavior.
- Enhances on-site customer experience through insights into their mobile behavior across locations.
- Measures customer engagement and loyalty across sites through location statistics.
- Compares visitor trends between sites to gauge the effect of marketing actions.

Initial Configurations

In order to use the Cisco CMX Presence Analytics service, choose the **Presence** option when you install Cisco MSE Virtual Appliance. For more information, see the "Installing a Cisco MSE Virtual Appliance" section in the *Cisco MSE Virtual Appliance Installation Guide* for this release at: http://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-installation-and-configuration-guides-list.html. After installation, perform the following operations:

- Add Controllers.
- Add sites.
- Add APs.

Presence Analytics Dashboard

The Presence Analytics Dashboard contains the following charts:

Table 13: Presence Analytics Charts

Chart	Description
Insights	Shows key insights for a week and month, including busiest days, busiest hours, peak days, and peak counts. **Note** Insight data allows comparison of current site metrics in comparison to the previous week and month. It is computed daily for all sites during aggregation.
Proximity	Shows information such as those pertaining to passersby, visitors, and connected devices, by hour (if it is a single day or last 3 days), or by day, for the given site.
Proximity Distribution	Shows information such as those pertaining to passers-by or visitors, and connected percentages for a given site for a given duration.
Dwell Time	Shows the visitor dwell levels by hour or by day. You can see the following dwell levels: 5-30 mins—Visitors who spent 5-30 mins in the site. 30-60 mins—Visitors who spent 30-60 mins in the site. 1-5 hours—Visitors who spent 1-5 hours in the site. 5-8 hours—-Visitors who spent 5-8 hours in the site. 8+ hours—-Visitors who spent more than 8 hours in the site.
Dwell Time Distribution	Shows visitor dwell-level percentages for a given site for a given duration.

Chart	Description
Repeat Visitors	Shows repeat visitors by hour or by day. You can see the following repeat visitor categories: Daily—Visitors who visited the selected site at least 5 days in the last 7 days. Weekly—Visitors who visited the selected site at least on 2 different weeks over the last 4 weeks. First Time—Visitors who visited the selected site for the first time. Occasional—Visitors who are not daily, weekly, or first-time visitors. Yesterday—Visitors who visited the site the previous day.
Repeat Visitors Distribution	Shows the repeat visitor distribution percentage.

Adding Sites

You can add new sites individually, or upload a .CSV list of sites to add sites in bulk.

You can add new sites using one of the following methods:

- Add sites individually. For more information, see Adding Sites Individually, on page 148.
- Add sites in bulk. For more information, see Adding Sites in Bulk, on page 149.
- Create sites from APs. This allows administrator to create sites by filtering APs by name and adding them directly to a new site. For more information, see Adding an AP to a Site, on page 151.

Adding Sites Individually

To add a site individually, perform the following task:

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **PRESENCE ANALYTICS** > **Manage**.

Step 3 Click the **Sites** tab.

Step 4 Click **Add Site**.

Step 5 In the **Name** field, enter the name of the site.

Step 6 In the **Address** field, enter the address of the site.

Step 7 Configure the **Signal Strength Threshold** to determine whether a client device is in the site or is just a passer-by. You can move the circular blue buttons to specify the Visitor Signal Threshold and Ignore Signal

Threshold values.There are two RSSI threshold values defined for a site, low (-95 dBm default) and high (65 dBm default).

Note The lower RSSI threshold is bounded to -95 dBm to -45 dBm and the higher threshold is bounded to -90dBm to -40 dBm.

The difference between the two threshold must not be less than 5.

The minimum dwell time is bound to 0 to 20

- Clients with RSSI below the low threshold (-95 dBm default) are discarded.
- Clients with RSSI above the low threshold are classified as “passer-by”. The RSSI threshold range for passer-by clients is between -95dBm and -75 dBm.
- Clients with RSSI above high threshold over *x* minutes (default 5) in past 20 minutes are classified as visitors.
- Clients associated with AP in a site are classified as connected clients at the site.

Step 8 In the **Configure the Minimum Dwell Time For Visitor (minutes)** field, specify the minimum dwell time for visitors. The minimum dwell time for visitors is 20 minutes.

Step 9 Click **Save**.

Adding Sites in Bulk

Procedure

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

Step 2 Choose **PRESENCE ANALYTICS** > **Manage**.

Step 3 Click **Import**.

Step 4 Under **Sites**, click **Browse**.

The **File Upload** dialog box is displayed.

Note The file that you upload for importing site information must be in .csv format.

Step 5 Navigate to the location of the CSV file that contains the list of sites you wish to upload, select the CSV file, and click **Open**. To import the site details correctly, store them in the following order and format: *Site Name*, *Address, RSSI High Threshold, RSSI Low Threshold, Dwell Time in Minutes, Timezone*. For example, *Test Site,123 Main Street City CA US,-65,-95,5 US/Pacific*.

Step 6 Click **Import**.

A set of new sites is created and added to the table of sites under **PRESENCE ANALYTICS** > **Manage**.

Viewing Available Sites

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **PRESENCE ANALYTICS** > **Manage**.

Step 3 Under the **Sites** tab, you can view a list of available sites in a tabular format, sorted alphabetically by site name. You can customize your view of the Sites table by sorting according to **Location**, **Timezone**, or **AP count**.

Editing an Existing Site

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **PRESENCE ANALYTICS** > **Manage**.

Step 3 Under **Sites**, click the name of the corresponding site listed in the table of available sites.

The dialog box is displayed.

Step 4 Edit the site **Name**, site **Address**, **Signal Strength Threshold** limits, or the **Minimum Dwell Time for Visitor**.

Step 5 Click **Save**.

Deleting an Existing Site

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **PRESENCE ANALYTICS** > **Manage**.

Step 3 Under **Sites**, check the check box of the site that you want to delete.

Step 4 Click **Delete**.

You will receive a confirmation dialog box when you try to delete a site. Click **OK** to confirm the delete action.

Note If you want to delete all available sites simultaneously, select the check box in the header row, and then click **Delete**.

Searching for a Site

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **PRESENCE ANALYTICS** > **Manage** > **Sites**.

Step 3 In the **Search** field on the top right-corner of the window, enter the site's name, and press the **Return** key. If the specified site has already been added to **PRESENCE ANALYTICS**, it is displayed in the search results.

Adding APs

You can add new APs individually or by uploading a .CSV list of APs to add them in bulk.

You can add new APs, with or without maps, using one of the following methods:

- Add APs individually—Add individual APs to specific sites. For more information, see Adding an AP to a Site, on page 151.
- Add APs in bulk—Add multiple APs at one go by importing a list of APs in .CSV format. For more information, see Adding APs in Bulk, on page 152.

Adding an AP to a Site

Note If you do not see the AP list, youshould update the community string of the WLC using the **System** > **Settings** window. The AP information is retrieved from the WLC using SNMP.

Procedure

Step 1 Log in to Cisco CMX.

Step 2 To add an AP to a site individually:

a) Choose **PRESENCE ANALYTICS** > **Manage** > **Sites**.

b) In the table of available sites, click the name of the site to which you want to associate the new AP.

c) Click the **Details** icon next to **AP count**.

A list of available APs is displayed in a tabular format.

d) Enter the MAC address of the AP you want to add and associate to the specified site.
e) Click **Add**.

The specified AP is added and associated to the specified site.

Step 3 To add one or more APs to a site:

a) Choose **PRESENCE ANALYTICS** > **Manage** > **Access Points**.
b) From the **APs by Controller** drop-down list, select the APs that you want to add to a site.

You can use the **Ctrl+a** or **Command+a** keys to select all sites from drop-down list.

c) After selecting the APs, click **Close**.

The count of the APs you selected from the available APs is shown in the drop-down list, for example, 8 of 160 selected.

d) Click **Add to Site**.
e) Select the site to which you want to add the selected APs.
f) Click **Add**.

The selected APs are added and associated to the specified site.

To create a site from this page, click **Create Site**.

Step 4 Under **Controller AP list**, click **Download CSV** to download the .CSV file, add the missing site names for APs, and import the file again from the Import tab.

CSV Format: Radio MAC Address,Ethernet MAC Address,Name,Site Name,Site Address

Example: aa:bb:cc:dd:ee:ff,bb:cc:dd:ee:ff:11,AP-1,Site-1,123 Main St City CA US

Adding APs in Bulk

To add APs to a site in bulk:

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **PRESENCE ANALYTICS** > **Manage** > **Import**.

Step 3 Under **APs**, click **Browse**.

The **File Upload** dialog box is displayed.

Step 4 Navigate to the location of the .CSV file that contains the list of APs you want to upload, select the .CSV file, and click **Open**.

To import the AP details correctly, store them in the following order and format:*Radio MAC Address,Ethernet MAC Address,Name,Site Name,Site Address*, for example, *aa:bb:cc:dd:ee:ff,bb:cc:dd:ee:ff:11,AP-1,Site-1,123 Main St City CA US*

Step 5 Click **Import**.

A set of new APs is created and added.

Deleting an AP

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **PRESENCE ANALYTICS** > **Manage** > **Sites**.

Step 3 In the table of available sites, click the name of the site from which you want to delete and unassociate the corresponding AP.

The dialog box is displayed.

Step 4 Click the **Details** icon next to **AP count**.

A list of available APs is displayed in a tabular format.

Step 5 Click the **Delete** icon next to the AP that you wish to delete.

Viewing Site Details for a Specified Period

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Click **PRESENCE ANALYTICS**.

Step 3 Select a site from the **SITE** drop-down list.

Step 4 Select a duration from the **DATE** drop-down list. You can choose from the following options:

- **Today**
- **Yesterday**
- **Last 3 Days**
- **Last 7 Days**
- **Last 30 Days**
- **This Month**
- **Last Month**
- **Custom**—Specify a date range and click **Change**. You can either manually enter the dates in the **FROM** and **TO** fields in yyyy-mm-dd format, or select the dates from the respective calendars. These calendars

are displayed when you select **Custom** or click the **FROM** or **TO** fields. The window is refreshed to show the site KPIs based on your selection.

Note You can choose a single day by selecting the same date in both the **FROM** and the **TO** fields.

Viewing KPI Summary

You can click any of the following KPI buttons that appear at the top of the window to view further details about a visitor's behavior at the site:

- **Visitors**—Clients associated with AP in a site are classified as visitors at the site.
- **Average Dwell Time**—Average dwell time or a wait time of all the visitors in a location.
- **Peak Hour**—The hour at which maximum number visitors are found in a location.
- **Conversion Rate**—Conversion rate is a percentage of passersby who are converted to visitors and is computed as visitors / (visitors + passersby) x 100.
- **Top Device Maker**—Manufacturer of popular client mobile devices detected by AP

Viewing Device Proximity, Count, and Distribution for a Specific Site

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Click **PRESENCE ANALYTICS**.

Step 3 Select a site from the **SITE** drop-down list.

Step 4 Select or specify a duration from the **DATE** drop-down list.

The window is refreshed to show the site details based on your selection.

Step 5 Click the corresponding elements within the **Proximity** or **Proximity Duration** chart to view hourly breakdown of passersby, visitors, and connected devices for the selected site during the specified duration.

Note If the duration selected in **Step 4** exceeds one day, clicking the elements in the **Proximity** chart will display the details for the selected site for the specific date.

Emailing a Report

Procedure

Step 1 Log in to Cisco CMX.
Step 2 Click **PRESENCE ANALYTICS**.
Step 3 Click the **Email** icon.
Step 4 Enter the email address of a recipient.
Step 5 Enter notes, if any.
Step 6 Click **Send**.

If you want to send this email later, check the **Schedule** check box and enter Schedule parameters such as **Start From** (date and time) and **Frequency** (**Daily** or **Weekly**), and then click **Schedule**.

Printing a Report

Procedure

Step 1 Log in to Cisco CMX.
Step 2 Click **PRESENCE ANALYTICS**.
Step 3 Click the **Printer** icon.
Step 4 Specify the printer settings.
Step 5 Click **OK**.

Generating a PDF Report

Note You can customize the logo on the PDF reports. To view an archived report, choose **PRESENCE ANALYTICS** > **Manage** > **Reports**.

Procedure

Step 1 Log in to Cisco CMX.
Step 2 Click **PRESENCE ANALYTICS**.

Step 3 Click the **PDF Report** icon.

Step 4 Enter notes for the PDF report, if any.

Step 5 Enter the email address (optional) of the recipient. If there are multiple recipients for the report, separate the email addresses using a comma.

Step 6 Click **Submit**.

If you want to schedule the PDF report to a future date, check the **Schedule** check box and enter the Schedule parameters such as **Start From** (date and time) and **Frequency** (**Daily** or **Weekly**), and then click **Schedule**.

Managing Reports

The **Presence Analytics** service enables you to manage the scheduled and generated reports. In addition, you can customize the logo that appears on the generated PDF reports.

The **Reports** window contains the following areas:

- **Report Logo**—Enables you to upload an image file that you can use as a logo for your PDF report.
- **Scheduled Reports**—Enables you to modify or delete a report that is already scheduled (email or PDF).
- **Generated PDF Reports**—Enables you to download or delete a generated PDF report.

Procedure

- To upload a logo for your report, perform the following steps:
  a) Log in to Cisco CMX.
  b) Click **PRESENCE ANALYTICS** > **Manage**.
  c) Click **Reports**.
  d) In the **Report Logo** area, click **Browse** and then choose the image file that you want upload as the report logo.
  e) Click **Upload**.
- To edit or delete a scheduled report, perform the following steps:
  a) Log in to Cisco CMX.
  b) Click **PRESENCE ANALYTICS** > **Manage**.
  c) Click **Reports**.
  d) In the **Scheduled Reports** area, under the **Link** column, click either **Edit** or **Delete**.

  If you choose to edit a scheduled report, the existing schedule details are displayed in the **EDIT SCHEDULED REPORT** window, where you can make the necessary changes.
- To download or delete a generated PDF report, perform the following steps:
  a) Log in to Cisco CMX.
  b) Click **PRESENCE ANALYTICS** > **Manage**.
  c) Click **Reports**.
  d) In the **Generated Reports** area, under the **Link** column, click either **Download** or **Delete**.

Specifying Filter Parameters

The **Filter Parameters** tab allows you to exclude data from a specific SSID, MAC address, or defined duration.

Procedure

Step 1 Log in to Cisco CMX.
Step 2 Choose **PRESENCE ANALYTICS** > **Manage** > **Filters**.
Step 3 Check the **Enable Exclusion Filters** check box to exclude data.
Step 4 Click **Save**.

Enabling a Global Site

Enabling a Global site combines all the existing data from all the individual sites into a single large site so that you can view the data for all the sites at once. You must provide a time zone for the global site, which will override all individual site time zones. All the analysis will be in context of the time zone defined for the global site.

Procedure

Step 1 Log in to Cisco CMX.
Step 2 Choose **PRESENCE ANALYTICS** > **Manage** > **Global Sites**.
Step 3 Check the **Enable Global Site** check box.
Step 4 Specify **Site Name**, **Address**, and **Time Zone**.
Step 5 Click **Save**.

Creating a Site Group

Site groups allow you to combine information from multiple sites for analysis, for example, all the sites in the same time zone.

Procedure

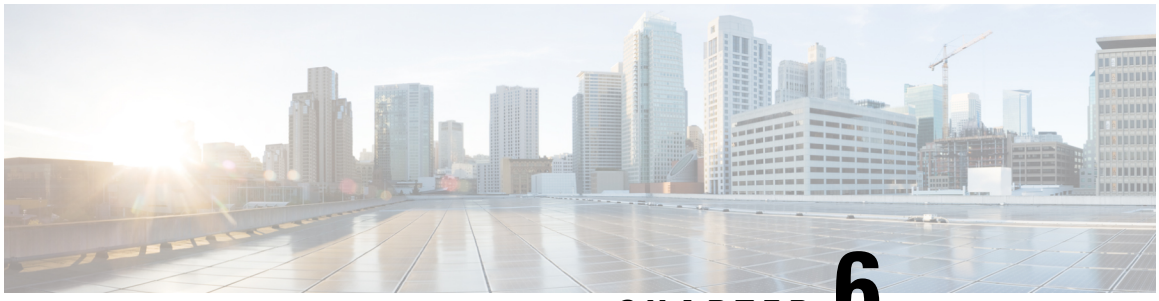
Step 1 Log in to Cisco CMX.
Step 2 Choose **PRESENCE ANALYTICS** > **Manage** > **Site Groups**.
Step 3 Click **Create Group**.
Step 4 Specify **Group Name**, **Address**, **Timezone**, and **Sites**.

Step 5 Click **Save**.

Changing the Presence Analytics Theme

Procedure

Step 1 Log in to Cisco CMX.
Step 2 Click **PRESENCE ANALYTICS**.
Step 3 Click the **Themes** icon.
Step 4 Choose your desired theme.



CHAPTER 6

Managing Cisco CMX Configuration

Overview of the Manage Service

The Cisco Connected Mobile Experiences (Cisco CMX) **MANAGE** service comprises the following tabs, which help you perform a variety of tasks to effectively manage the Cisco CMX configuration, including, but not restricted to those listed here:

- **Locations**—Enables you to manage and add location zones and tags. For more information, see Managing Perimeters and Zones on Location Maps, on page 160.
- **Licenses**—Enables you to manage and add licenses. For more information, see Managing Licenses, on page 166.
- **Users**—Enables you to manage and add users. For more information, see Managing Users, on page 169.
- **Notifications**—Enables you to manage and add email and HTTP notifications. For more information, see Managing Notifications from Applications, on page 171.
- **Cloud Apps**—Enables you to manage Cisco CMX Cloud service. For more information, see Managing the Cisco CMX Cloud Apps, on page 181.

Note All the Manage service tasks can be performed only by users with corresponding user roles. For information on user roles, see User Roles, on page 169.

Managing Perimeters and Zones on Location Maps

A perimeter is an all-inclusive zone where clients are always inside of this. The individual zones are inside the perimeter.

Note In Cisco CMX Release 10.2.3, the ability to create and delete a perimeter on location maps is no longer available.

Viewing Campus, Building, Floor, and Zone Details

Procedure

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

Step 2 Choose **MANAGE** > **Locations**.

Step 3 In the left pane of the window that is displayed, click **Campus, Building, Floor,** or **Zone** depending on the area you want to view.
Items corresponding to the area selected are displayed as boxes.

Step 4 Click the curved arrow at the top-right corner of each item box to view details pertaining to that item.
This opens the **Zone Editor** map view, displaying a floor map.

Note The curved arrow at the top-right corner of a floor box is called the **Go to map view** arrow. This arrow is available on the box of items at any level. For example, for a building, this opens the first floor. For a campus, this opens the first floor of the first building. You can then switch to other buildings and floors in that campus.

Adding a Campus Address

When you import maps from Cisco Prime Infrastructure, the campus addresses are not imported automatically. You must set them manually in the **Locations** tab.

Before you begin

Ensure that you successfully import maps from Cisco Prime Infrastructure and you can view the imported map hierarchy under the **Detect and Locate** service.

Procedure

Step 1 In Cisco CMX, choose **Manage** > **Locations**.

Step 2 In the left pane of the window that is displayed, click **Campus**.

The **Campus Item** panel is displayed.

Step 3 In the **Address** field, enter a valid address. You can choose the right address from the drop-down list that is displayed.

Step 4 Click **Enter** to save the address.

Step 5 Navigate to **Detect & Locate** tab.

The campus address is displayed on the world map in the **Activity Map** window.

Managing Tags

You can add tags to a campus, building, floor, or zone.

Procedure

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

Step 2 Choose **MANAGE** > **Locations**.

Step 3 From the right panel, choose the item for which you want to add the tag.

Step 4 Click the **Tag** icon at the top-right corner of the window.

The **Location Tag Manager** window is displayed with available tags.

Step 5 In the **Create New Tag** field, enter a new name for the tag and press **Enter**.

Step 6 (Optionaly) Click on any existing tag to see all the geo items that are tagged against it.

Creating an Inclusion or Exclusion Region

The Create Inclusion/Exclusion feature allows you to create inclusion and exclusion regions on a floor.

- Inclusion regions define areas within a floor where wireless devices will be either inside or snapped on the boundary (due to weak coverage). There will be one inclusion region per floor only. When there is no inclusion region defined in the floor maps, Cisco CMX creates a default inclusion region that is the same as the floor dimension. We recommend having one inclusion region on a floor to correctly bound the clients on floor area.
- Exclusion regions define areas within a floor which are inside an inclusion region. In an exclusion region, wireless devices will be ignored. There could be multiple exclusion regions per floor.

Defining inclusion and exclusion regions can help you focus Cisco CMX processing to just those areas of the map where you want to manage your wireless devices, and ignore others.

Procedure

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

Step 2 Choose **Manage** > **Locations**.

Step 3 In the left pane, click **Floor**.

Step 4 To go to the map view of the floor, click the arrow on the top right of the floor tile view. The **Zone Editor** window is displayed with a list of icons to the right.

Step 5 To add a new inclusion region:

a) Click the + icon to create an inclusion region on the map. If you already have an inclusion region, creating a new inclusion region will overwrite the existing region.

b) Double-click to finish creating the inclusion area. The inclusion region is displayed in green.

c) In the **Create a Inclusion** dialog box, click **Add**.

To add an exclusion region, click the – icon and draw the exclusion area on the inclusion area.

Creating a Perimeter

Procedure

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

Step 2 Choose **MANAGE** > **Locations**.

Step 3 In the left pane of the window that is displayed, click **Zone**.

The zone is used for the analytics purpose.

The **Zone Item** boxes are displayed.

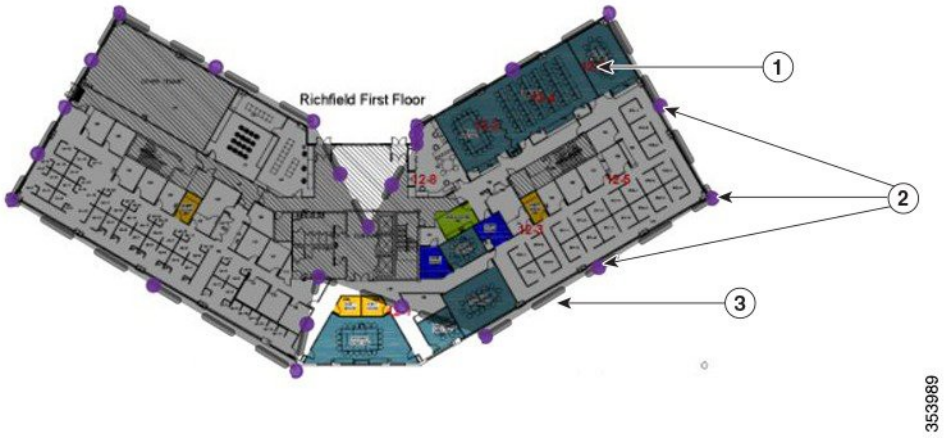
Step 4 Click the Subzone in the corresponding zone.

Step 5 In the **Zone Editor** window, click the **CREATE A PERIMETER**  icon.
The cursor changes to a drawing tool.

Step 6 Click each point that you want to designate as a vertex of the perimeter. Double-click the last vertex point to complete marking the vertices of the perimeter and closing the perimeter.
When you double-click the last vertex point, the **CREATE A PERIMETER** dialog box opens.

Step 7 Click **Add** to add this perimeter to the floor.

Figure 18: A Perimeter and its Vertices



1	Dark gray area indicating an area encircled by the perimeter.	**3**	Dark gray bar indicating the perimeter.
2	Purple indicating vertices of the perimeter.		

Deleting a Perimeter

Procedure

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

Step 2 Choose **MANAGE** > **Locations**.

Step 3 In the left pane of the window that is displayed, click **Zone**.
The **Zone Item** boxes are displayed.

Step 4 Click the Subzone in the corresponding zone.

Step 5 In the **Zone Editor** window, click the **Edit Perimeter** icon.

Step 6 Click inside the perimeter to be deleted.
The perimeter will be highlighted in gray.

Step 7 Click the **Trash** icon.

Step 8 In the **DELETE PERIMETER** confirmation dialog box, click **Confirm** to delete the perimeter.

Editing a Perimeter

Procedure

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

Step 2 Choose **MANAGE** > **Locations**.

Step 3 In the left pane of the window that is displayed, click **Zone**.
The **Zone Item** boxes are displayed.

Step 4 Click the Subzone in the corresponding zone.

Step 5 In the **Zone Editor** window, click the **Edit Perimeter** icon.

Step 6 Click inside the perimeter that is to be edited.
The perimeter will be highlighted in gray and the vertices in purple.

Step 7 Drag the purple vertices to modify the shape of the perimeter.

Step 8 After you have the required shape, click outside the perimeter. This saves the new shape.

Creating a Zone

Procedure

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

Step 2 Choose **MANAGE** > **Locations**.

Step 3 In the left pane of the window that is displayed, click **Zone**.
The **Zone Item** boxes are displayed.

Step 4 Click the Subzone in the corresponding zone.

Step 5 In the **Zone Editor** window, click the **Draw Polygon Zone** icon.
The cursor will change to a drawing tool.

Step 6 Click each point that you want to designate as a vertex of the perimeter. Double-click the last vertex point to complete marking the vertices of the perimeter and for closing the perimeter see the figure below.
When you double-click the last vertex point, the **CREATE A NEW ZONE** dialog box is displayed.

Step 7 Click **Add** to add this zone to the corresponding floor.
An Item pane pertaining to this zone is displayed on the right side of the window. You can add existing tags from the drop-down list, or add a new tag.

Note Zones cannot be outside the floor map and they cannot overlap. Overlapping zones can be created using Cisco Prime Infrastructure.

Figure 19: A Zone and its Vertices

1	A zone named Lab.	**3**	Purple indicating vertices of the zone.
2	Gray bar indicating the perimeter.	**4**	Other zones on the map.

Deleting a Zone

Procedure

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

Step 2 Choose **MANAGE** > **Locations**.

Step 3 In the left pane of the window that is displayed, navigate to the zone that you want to delete.

Step 4 Click the **Trash** icon.
The **DELETE ZONE** confirmation dialog box is displayed.

Step 5 Click **Confirm**.

Editing a Zone

Procedure

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

Step 2 Choose **MANAGE** > **Locations**.

Step 3 In the left pane of the window that is displayed, click **Zone**.
The **Zone Item** boxes are displayed.

Step 4 Click the Subzone in the corresponding zone.

Step 5 In the **Zone Editor** window, click the **Gear** icon to view the zone editing options.

Step 6 To change the shape of the zone, use the **Pencil** icon to reshape the zone by moving the vertices.
The **DELETE ZONE** confirmation dialog box is displayed.

Step 7 To move the zone, use the drag tool, denoted by the **Hand** icon, to drag the zone around. Click the **Hand** icon, move the cursor to the center of the zone, where it will change to an **Arrow** icon. You can then drag the zone.

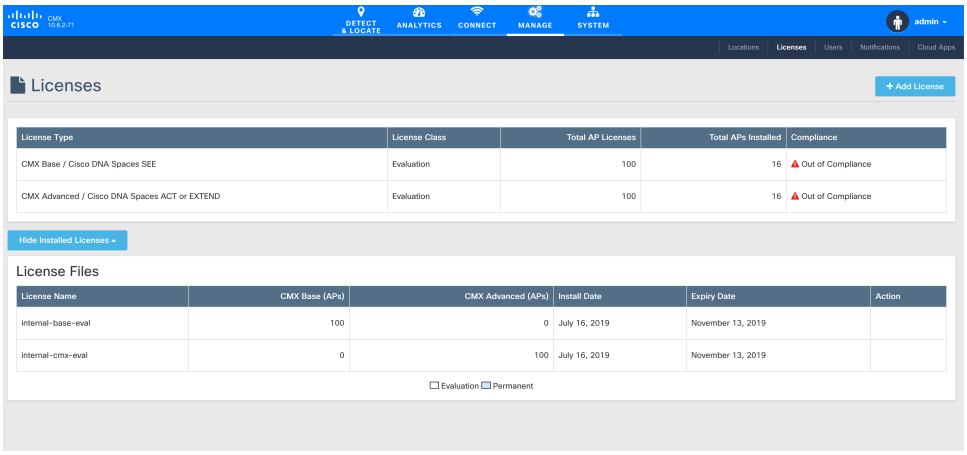
Step 8 Click outside the zone to save your changes.

Note Zones cannot be outside the floor map and they cannot overlap. Overlapping zones can be created using Cisco Prime Infrastructure.

Managing Licenses

To view the list of licenses that your Cisco CMX system has, log in to Cisco CMX and choose **MANAGE** > **Licenses**. The list of licenses is displayed in the **Licenses** window.

Figure 20: Licenses Window



Cisco CMX has the following license models:

- CMX Default: Includes access to **Cloud Apps** (for enabling connection to Cloud applications) and **License** (for Base or Advanced License installation) features, **MANAGE** and **SYSTEM** services, and sending Northbound notifications.
- CMX Base License: Includes RSSI Location Calculation, GUI access to **DETECT**, **MANAGE**, and **SYSTEM** services. It supports Permanent and Term licenses.
- CMX Advanced: Includes CMX Base features, Angle of arrival, **CONNECT**, **PRESENCE ANALYTICS**, and **LOCATION ANALYTICS** services, provides access to Partner Stream, and to the complete Cisco CMX GUI. It supports Permanent and Term licenses.

Note The Cisco CMX Base License no longer provides access to Cisco CMX Hyperlocation or Partner Stream. The Cisco CMX Advanced License is required to access these services. Cisco CMX Hyperlocation, Cisco CMX Connect, Cisco CMX Advance Location services migrated from Cisco CMX Base License to Cisco CMX Advance license will continue to work after upgrade from Cisco CMX 10.3.x release. However, an alert is generated every 24 hours for license upgrade. A new Cisco CMX installation will require a Cisco CMX Advance license.

For information about the licenses required to operate Cisco CMX, see the Cisco CMX 10 Ordering and Licensing Guide.

Note

- Cisco CMX Release 10.3 supports High Availability. For more information, see Enabling High Availability for Cisco CMX, on page 210.
- Cisco CMX comes with a 120-day full-functionality evaluation license. All the access points (APs) connected to Cisco CMX must be licensed.
- CMX Evaluation licenses are not synchronized between Cisco CMX High Availability (HA) pairs. Once the evaluation license expires on the primary server, Cisco CMX HA will not invoke failover to the secondary server. You must add a permanent license to make the HA setup functional.
- Cisco CMX permanent licenses will be synchronized between the primary and secondary servers in the CMX HA pair. You need not upload the permanent licenses on the secondary server.

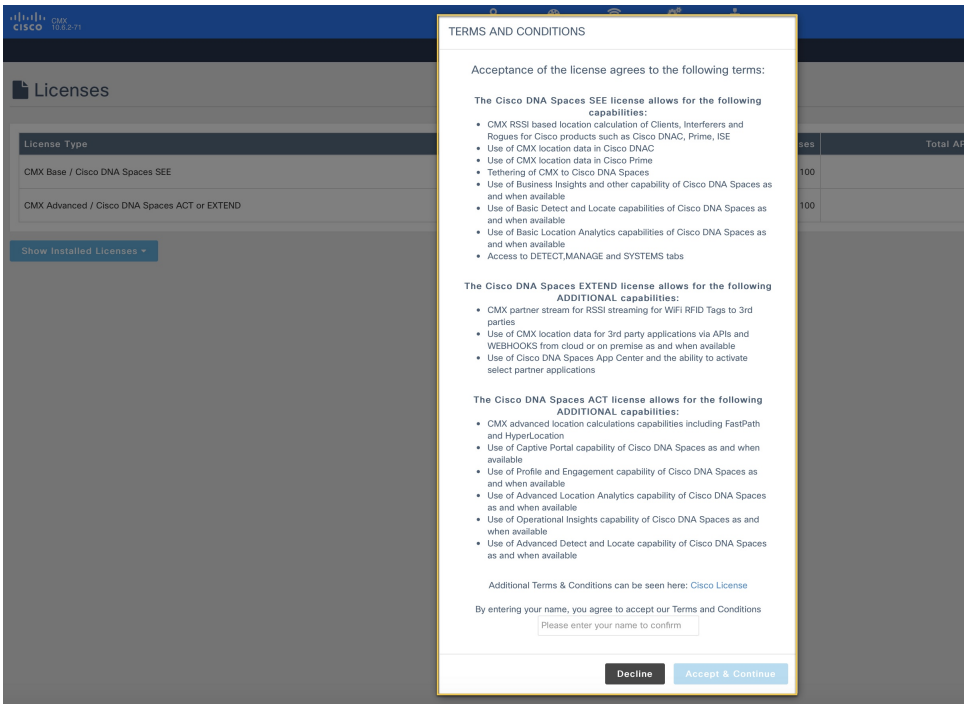
Add a License

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **MANAGE** > **Licenses**.

Step 3 Click **Add License**. The **TERMS AND CONDITIONS** dialog box is dispalyed.



Step 4 To accept the terms and conditions, enter your name, and then click **Accept & Continue**.

When you accept and proceed to install a certificate, a dialog box is displyed with a message indicating that you can use only the Analytics or Location features.

The **UPLOAD LICENSE** dialog box is displayed.

Step 5 Click **Browse** to select the corresponding license file, and then click **Upload**. Ensure that you to select a license file with the .lic extension.

Note Cisco CMX uses license files with the .lic extension. This file is made available when you place an order for any of the Cisco CMX per Access Point SKUs, for example, *Cisco DNA Spaces EXTEND*.

The license file is available as part of your licensing package and will be attached to an email from licensing. Extract the .lic file to your system and upload to Cisco CMX when adding a new license.

Step 6 In the **Licenses** window, click **See Installed Licenses** to view the list of installed licenses. You can view the **License Name**, **CMX Base (APs)**, **CMX Advanced (APs)**, **Install Date**, and **Expiry Date** for the insatlled licenses.

Delete a License

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **MANAGE** > **Licenses**.

Step 3 In the **Licenses** window, click **See Installed Licenses** to view the list of installed licenses.

Step 4 In the **Action** column adjacent to the license you want to delete, click **Delete**.

Note Note that only nonevaluation type licenses can be deleted.

The **DELETE LICENSE** dialog box is displayed.

Step 5 Click **Delete License** to proceed with the deletion.

Managing Users

Cisco Connected Mobile Experiences (Cisco CMX) is shipped with a default admin user account and password. An admin user can add, edit, and delete other users.

Adding a User

Procedure

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

Step 2 Choose **MANAGE** > **Users**.

The **Users** window, where all the current users are listed, is displayed.

Step 3 Click **+ New User** at the bottom of the table.
The **ADD NEW USER** dialog box is displayed.

Step 4 Enter the details and select one or more roles for the user from the **Roles** drop-down list.
For information about the roles available for selection, see User Roles, on page 169.

Note The password for the new user must be mimimum of eight characters.

Step 5 Click **Submit**.

User Roles

Your Cisco Connected Mobile Experiences (Cisco CMX) system comes with the following services, depending on whether or not you have the license for that service:

- **SYSTEM** service (included with Cisco CMX base license)
- **MANAGE** service (included with Cisco CMX base license)
- **DETECT & LOCATE** service (included with Cisco CMX base license)
- **CONNECT** service (included with Cisco CMX base license)
- **ANALYTICS** service (provided only with Cisco CMX advanced license; not included with Cisco CMX base license)

When setting up users in Cisco CMX, you can select one or more roles for each user. Each role provides access privileges to one or more services, provided your license includes those services.

See the table below for a description of the access privileges associated with each role.

Table 14: User Roles and Associated Access Privileges

Role	Allows
Admin	Read/Write access to all the services
System	Read/Write access to the service
Manage	Read/Write access to the service
Location	Read/Write access to the service
Analytics	Read/Write access to the service
Connect	Read/Write access to the service
Connect Experiences	• Read/Write access to Connect Experiences in the **CONNECT & ENGAGE** service • Read-only access to all the settings in the **CONNECT & ENGAGE** service • No access to the Dashboard in the **CONNECT & ENGAGE** service
Read Only	Read-only access to all the services

Note

- A user can be allocated the System, Manage, Location, Analytics, and Connect roles. This allows the user to function like an admin user. Such nonadmin users can be deleted by admin users, but not vice-versa.
- Only an admin user can delete another admin user.
- An admin or Connect user has both read/write access to the Policy Plans. However, Connect Experience users only have Read access to the Policy plans page.

Changing the Default Admin Password

Procedure

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

Step 2 Choose **MANAGE** > **Users**.
The **Users** window, where new users can be added and the roles of existing users modified, is displayed.

Step 3 Click **Edit** in the **Actions** column adjacent the admin user.
This opens the **EDIT USER** dialog box for that admin user.

Step 4 Change the default factory-shipped admin password.

Step 5 Click **Submit**.

Editing User Information

Procedure

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

Step 2 Choose **MANAGE** > **Users** .
The **Users** window, where all the current users are listed, is displayed.

Step 3 Click **Edit** in the **Actions** column adjacent the user whose details you want to edit.
The **EDIT USER** dialog box is displayed.

Step 4 Edit the details of the user. Note that the username cannot be edited.
For information about user roles, see User Roles, on page 169.

Step 5 Click **Submit**.

Deleting a User

Procedure

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

Step 2 Choose **MANAGE** > **Users**.

Step 3 Click **Delete** in the **Actions** column adjacent the user whose details you want to delete.
The **DELETE USER** confirmation dialog box is displayed.

Step 4 Click **Delete User** to proceed with the deletion.

Managing Notifications from Applications

You can set up notifications for your own applications and for third-party applications. The Notifications feature supports the following:

- HTTP receiver
- MAC address scrambling, which is enabled by default
- Two message formats, JSON and XML
- Alerts
- Network configuration change notification
- REST notification over HTTPS

The following sections describe the notifications-related tasks that you can perform:

Create a New Notification

Procedure

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

Step 2 Choose **MANAGE** > **Notifications**.
The **Notifications** window is displayed.

Step 3 Click **New Notification**.
The **CREATE NEW NOTIFICATION** dialog box is displayed.

Figure 21: Create New Notification

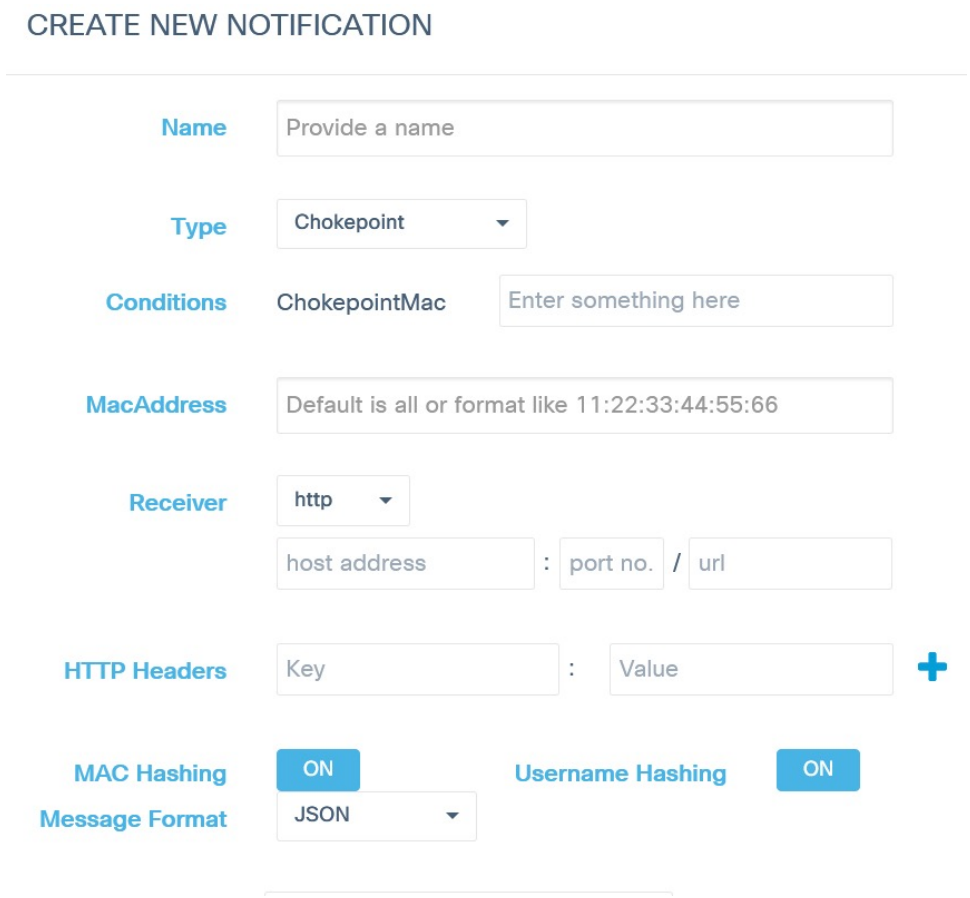
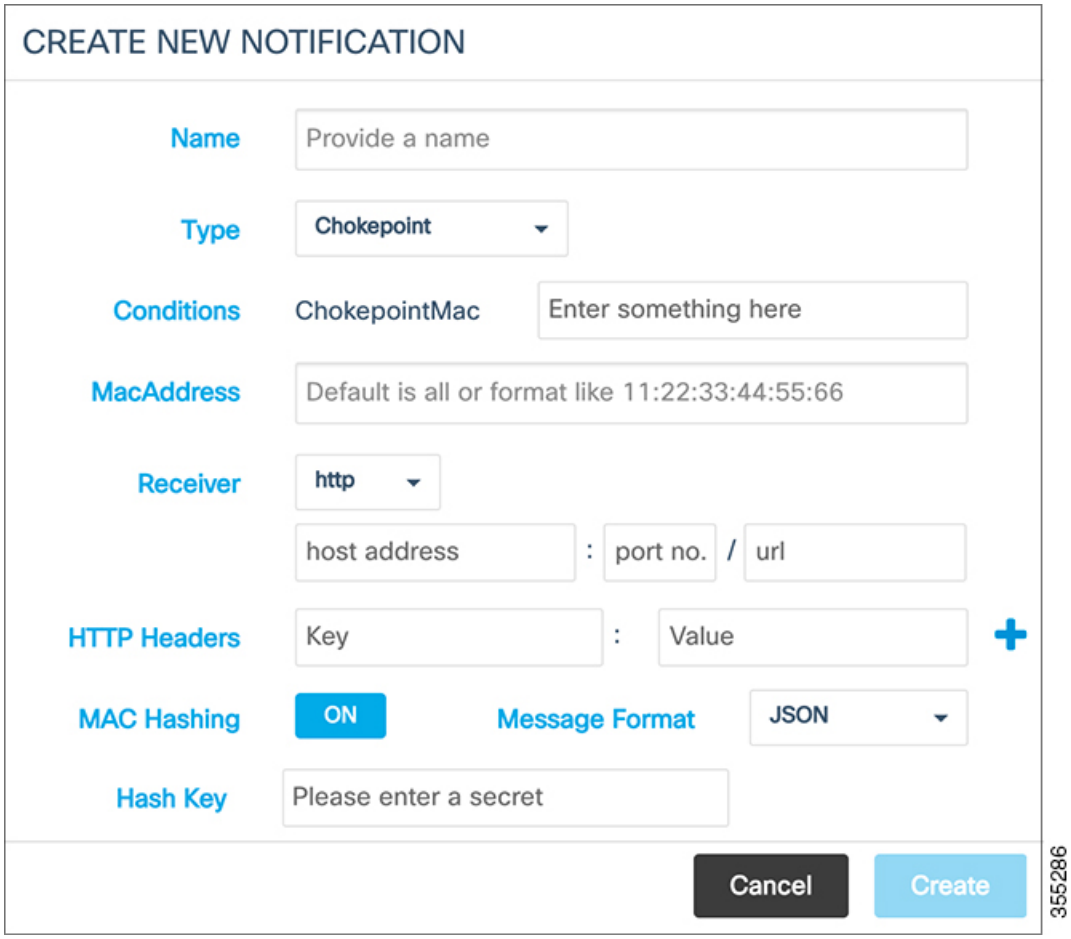


Figure 22: Create New Notification



Step 4 Enter the following parameters to configure the new notification:

- **Name**: Enter a name for the new notification name.
- **Type**: From the **Type** drop-down list, choose the notification type.

  For a description of the available notification types, see the table below. When specifying the details, note that:

  - If a location hierarchy is selected, the hierarchy will be the specific area filter for that notification.
  - If a MAC address is entered, the MAC address will be a filter for that notification.

Table 15: Notification Types

Notification Type	Used for
Absence	Generating a notification when a client is undetected for more than 15 minutes.
Area Change	Generating a notification when a device changes its location between campuses, buildings, or floors.

Notification Type	Used for
Association	Generating a notification when a client is associated or unassociated.
Battery Life	As part of RFID telemetry, Cisco CMX receives battery information which are of type **Low**, **Medium**, and **Normal**. Depending on the condition(s) set in the notification rule, notifications are generated for tags reporting similar battery status. **Note** This notification is applicable for RFID tag only.
Chokepoint	As part of RFID telemetry, Cisco CMX receives chokepoint details when a tag encounters it. A notification is generated when Cisco CMX detects an encountered mac that matches the chokepoint mac from notification rule. **Note** This notification is applicable for RFID tag only.
Emergency	As part of RFID telemetry, Cisco CMX receives event information which are of type **Any**, **Unknown**, **Panic Button**, **Detached**, and **Tampering**. Depending on the condition(s) set in the notification rule, notifications are generated for tags reporting similar events. **Note** This notification is applicable for RFID tag only.
In/Out	Generating a notification when a device is detected as moving into or moving out of a specific area in the location hierarchy.
Location Update	Generating a notification when a device's location is being recalculated. The Location Update notification is based on the RSSI from the different APs that detect the device.
Movement	Generating a notification when a device moves more than a specified distance.
Network Design Changed	Generating a notification when maps are changed.

- **Conditions**: Depending on the notification type selected, the **Conditions** parameters are displayed. Enter the required conditions for the new notification.

Note

- For some notifications types such as **Association**, **Absence**, and so on, you must provide **Device Type** as a condition parameter. The **Device Type** field on the **Create New Notification** window provides these options: **All**, **RFID Tag**, **Client**, **BLE Tag**, and **Interferer**. For notification types **Area Change**, **In/Out**, **Location Update**, and **Movement**, the **Device Type** condition has the following additional options: **Rogue Client** and **Rogue AP**.
- For the **In/Out** notification type, if the **In** option is selected in the **Condition** field, this warning message is displayed: *Please make sure to add 'Out' condition with same Hierarchy*. Conversely, if the **Out** option is selected in the **Condition** field, this warning message is displayed: *Please make sure to add 'In' condition with same Hierarchy*.
- For the **Location Update**, **In/Out**, and **Movement** notification type, choose the device status from the **Status** drop-down list. The association status for the client device are **All**, **Probing Only**, and **Associated**. This condition helps to filter the clients by their association status and sends notifications only for the filtered subset of client devices.
- For the **Location Update** notification, Cisco CMX provides a new **Status** option for the **Client** device type. Use this option to filter notifications to either associated or probing devices. If the **Status** option is not selected, the default option **(All)** is considered, and then notifications are sent for both associated and probing clients.
- For the **Location Update** notification with device type as **BLE tag**, Cisco CMX will receive details such as UUID, Major, Minor fields in the payload.
- To view In/Out notification details for all locations, we recommend that you configure seperate In/Out notifictions for each hierarchy created in the **Activity Map** window.
- For the notification type **Battery Life**, the conditions **All** and **Any** indicates the same battery life status. You can either select **All** or **Any** to incule all available battery life statues conditions to create the notification.
- For the notification type **Emergency**, the conditions **All** and **Any** indicates the same emergency status condition. You can either select **All** or **Any** to incule all condition types to create the notification.

- **MacAddress**: Enter the MAC address. The defaul is **all**.
- **Receiver**: From the **Receiver** drop-down list, choose the receiver type as **HTTP**, **HTTPS**, or **Email**. For HTTP and HTTPS receiver, you must provide the host address, port number, and url.

  Note When FIPS mode is enabled in Cisco CMX and the receiver is selected as **HTTPS**, you must import a CA certificate corresponding to that receiver. Use the **Browse** field to import CA certificate which is signed with northbound notification receiver's server certificate.

  The imported CA certificate is used to validate receiver's certificate when Cisco CMX tries to establish TLS connection to the receiver to send notifications to it.

  If northbound notification receivers were added prior to enabling FIPS mode in Cisco CMX, you must edit individual northbound notification receiver and then import CA certificate or remove and add the northbound notification receiver again.

- **HTTP Headers**: Enter the HTTP header inputs for **Key** and **Value**. Click the plus icon to add more custom HTTP headers to the notification. You can add a maximum of three custom HTTP headers.

  Note HTTP headers are manadatory for northbound notifications to connect to third party services.

- **MAC Hashing**: Click to disable the MAC hashing. By default, MAC hashing is enabled.
- **Message Format**: From the **Message Format** drop-down list, choose the format as **JASON** or **XML**.
- **Salt**: Enter a secret hash key.

Step 5 Click **Create**. The new notification is created and displayed in the Notifications window.

Making Changes to Notifications

Note If you are a non-admin user, you can make changes to only those notifications that were created by you. A non-admin user cannot make changes to notifications created by other users.

The following are the changes that you can make to notifications:

Enabling and Disabling a Notification

When a notification is created, it is enabled by default.

Procedure

- To disable a notification, in the **NOTIFICATIONS** window, under the **Status** column adjacent the notification, click **Enabled**.
  The label changes to **Disabled** and the notification is disabled.
- To enable a notification, in the **NOTIFICATIONS** window, under the **Status** column adjacent the notification, click **Disabled**.
  The label changes to **Enabled** and the notification is enabled.

Editing a Notification

Procedure

Step 1 To edit a notification, in the **NOTIFICATIONS** window, under the **Actions** column adjacent the notification, click **Edit**.
The **EDIT NOTIFICATION** dialog box is displayed.

Step 2 Edit the details of the notification, as required.

Note You cannot edit the name of the notification.

Viewing Northbound Notifications

You can now view northbound notifications from the Cisco CMX UI and CLI. Cisco CMX does not support authentication for Northbound notifications.

To view Northbound Notifications:

Procedure

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

Step 2 **Choose Manage > Notifications**.

Step 3 Under the **Actions** column for an existing notification, click **Details** to view additional information about the notification.

You can also view the northbound notification details in the Edit Notifications window. Optionally, from the CLI, use the **cmxctl metrics notification** command to view the northbound notifications.

Viewing Northbound Notification Attributes

The following table lists the Northbound Notification attributes:

Table 16: Northbound Notification

Type	Description
Notification Type	What type of notification this output describes (For example, locationupdate)
Subscription Name	The name of the notification created in CMX (user provided)
Event ID	Unique for notification identification per event
Location Map Hierarchy	The Hierarchy string that shows campus, building, floor, and zone (if applicable)
Location Coordinate	XY location for the device
Geo Coordinate	GPS location for device, if GPS markers are set
Confidence Factor	Represents a square box of where the client should be, lower means better location accuracy
AP Mac Address	The AP that the client is connected to
Associated	Shows if this device is associated or not
Username	The username of this Associated client if using 802.11x
IP address	If this client is associated, what IP address(es) are assigned to it, can include IPv4 and IPv6 addresses
SSID	The SSID of the client is Associated
Band	802.11 band the device is it connected to
Floor Id	Long value representing hieracrchy, would not use

Type	Description
Floor Ref Id	New to 10.3.1, represents a long for what hierarchy it is on (Floor Id might be rounded if the number is large enough due to a conversion from long to double), only is filled in for location update, recommended for use
Entity	What type of device is it, Client (normal devices), RFID Tag (these are devices that send a chirp on an interval), Interferers (Devices that are connected to APs or are APs that aren't on the network controlled by a controller on this CMX)
Device Id	MAC address of device
Last Seen	Timestamp of packet last received from controller for this device
Raw Location	-
Area Global Id List	-
Tag Vendor Data	For RFID tags, information that was encoded in packets we received like battery life or something like that.
Manufacturer	Based on the first half of the MAC address of this device
Timestamp	When the notification is generated
status	Refers to what the status of the device is - IDLE(0), AAA_PENDING(1), AUTHENTICATED(2), ASSOCIATED(3), POWERSAVE(4), DISASSOCIATED(5), TO_BE_DELETED(6), PROBING(7), BLACK_LISTED(8), WAIT_AUTHENTICATED(256), WAIT_ASSOCIATED(257);

Type	Description

rssiEntries	Displays the Access Points information used for determining the location of the device.
	<pre>"rssiEntries": [
	{
	"apMacAddress": "6c:8b:d3:ef:d4:60",
	"band": "IEEE_802_11_B",
	"slot": 2,
	"antennaIndex": 0,
	"rssi": -55,
	"lastHeardSecs": 7
	},
	{
	"apMacAddress": "6c:8b:d3:b2:ba:60",
	"band": "IEEE_802_11_B",
	"slot": 2,
	"antennaIndex": 0,
	"rssi": -69,
	"lastHeardSecs": 2
	}
	]</pre>

Managing Proxy Settings for Notifications

In Cisco CMX, configure proxy settings for notifications that need to pass through specific proxy when sending notification to client devices. If proxy is set in Cisco CMX, you need to set the **no_proxy** variable for all notification addresses that need not go through the proxy.

Procedure

Step 1 To verify the current proxy settings, run the **cmxos sysproxy show** command.
The following is a sample output:

```
[cmxadmin@cmx-nortech ~]$ cmxos sysproxy show
USE_PROXY=1
HTTP_PROXY_URL=""
HTTPS_PROXY_URL=http://proxy.esl.cisco.com:80
FTP_PROXY_URL=""
NO_PROXY_LIST=192.0.2.1
```

Note The proxy variable required for CMX notifications is the HTTPS_PROXY_URL.If this variable is set and you are not getting the notification, follow the below steps to configure the no_proxy variable.

Step 2 To set the **no_proxy** variable, run the **sysproxy no_proxy** *host name*: *port* command, wherein the host name is domain associated with your host machine IP address, for example, **cmxos sysproxy no_proxy** 192.0.2.1:8000

To find out the domain name, run the **host** *ip addresss* command and identify the domain name pointer value.

If you have multiple domain values, enter all of them as comma seperated no_proxy values in the command, for example, **cmxos sysproxy no_proxy** *no_proxy_value1*, *no_proxy_value2*: *port number*.

For example, **cmxos sysproxy no_proxy** 192.0.2.1,example.com:8000

Step 3 Run the following commands to restart the agent and location services.**cmxctl agent restartcmxctl location restart**.

The notifications will be send to your client devices as per the notification type configuration. If the notificqation listener is outside the Cisco firewall, set proxy using the **cmxos sysproxy http_proxy** command. If the notification listener is within Cisco firewall, use the **cmxos sysproxy no_proxy** command to add all IP addresses that do not require a proxy setting.

The following table lists the commands used for setting proxy:

Table 17: Cisco CMX Proxy Setting Commands

Scenario	Cisco CMX Proxy Command	Cisco WSA Proxy Version	Squid Version - By default, uses web socket connection method.	McAfee Web Gateway Version
Northbound notifications with listener inside Cisco Firewall	**cmxos sysproxy no_proxy** *192.0.2.1*	Proxy is not used	Proxy is not used	Proxy is not used
Northbound notifications with external listener in AWS cloud (outside of Cisco firewall) To send to the cloud use the following: http://ip address:9094/api/v1/notify To check the cloud instance use the following REST API: http://ip address:9094/api/v1/notifications	**cmxos sysproxy http_proxy** *<hostname>:<port_number>* For example, **cmxos sysproxy http_proxy** *example.com:80/* **cmxctl agent restart** **cmxctl location restart**	Yes	Yes	Yes
BLE (HTTPS, web socket: defaults, supports HTTP as well)	**cmxos sysproxy https_proxy***<hostname>:<port_number>* For example, **cmxos sysproxy http_proxy** *example.com:80/* **cmxctl agent restart** **cmxctl location restart**	Yes	Yes	Yes

Scenario	Cisco CMX Proxy Command	Cisco WSA Proxy Version	Squid Version - By default, uses web socket connection method.	McAfee Web Gateway Version
Connect (SMS & FB) (HTTP & HTTPS)	**cmxos sysproxy https_proxy***<hostname>:<port_number>* For example, **cmxos sysproxy http_proxy** *example.com:80/* **cmxctl agent restart** **cmxctl location restart**	Yes	Yes	Yes

Deleting a Notification

Caution A notification delete action takes effect immediately without a delete confirmation dialog box being displayed.

Procedure

To delete a notification, in the **NOTIFICATIONS** window, in the **Actions** column adjacent the notification, click **Delete**. The notification is immediately deleted.

Managing the Cisco CMX Cloud Apps

Cisco CMX helps you to calculate the location of connected devices. This location information can be shared with various other CMX apps that are available as cloud services. Most of these cloud services are configured using a set of Northbound notifications from Cisco CMX to the Cisco CMX application hosted on the cloud.

Note An outbound proxy is required for connecting to the Cisco CMX applications. To set the up outbound proxy, see Setting Up Outbound Proxy, on page 189.

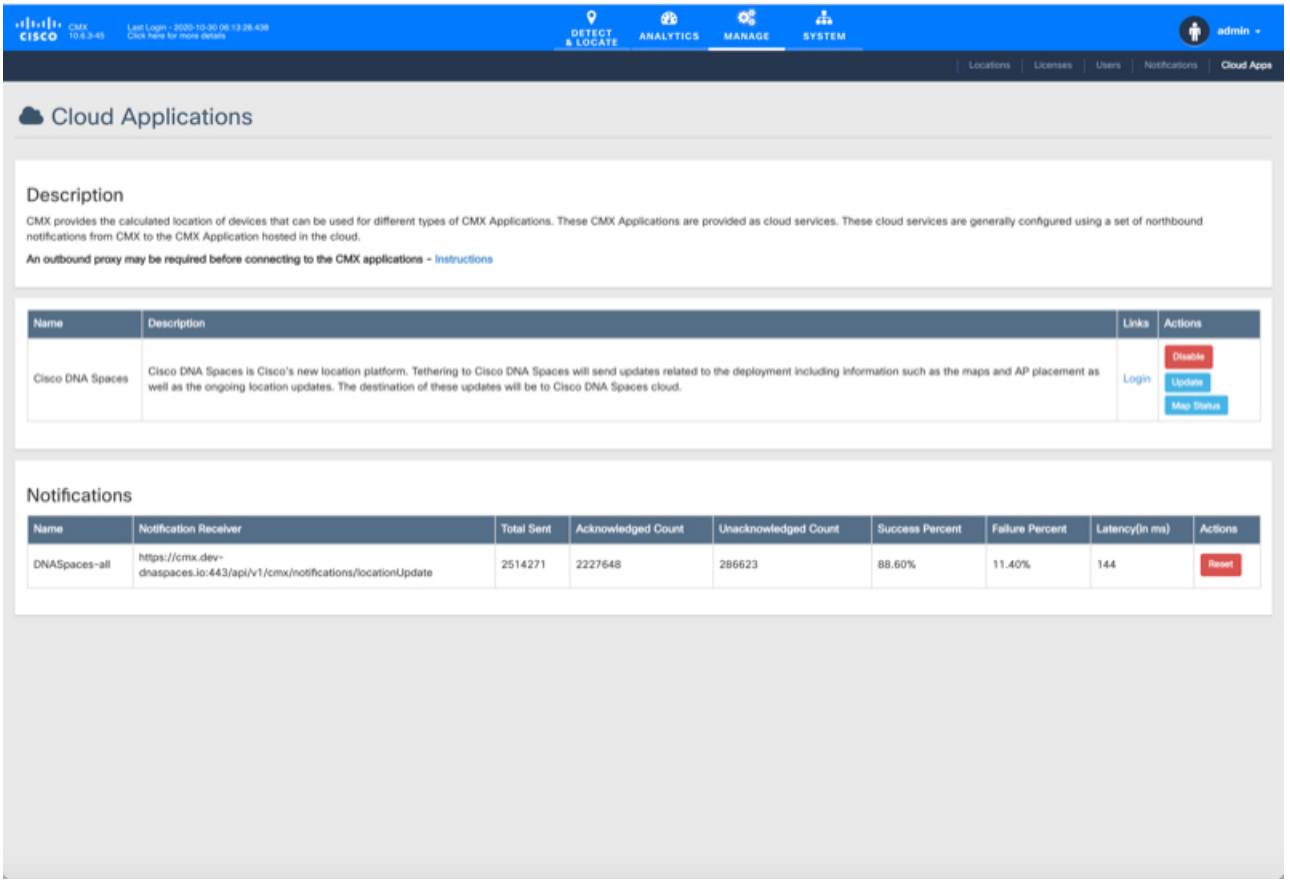
Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **MANAGE** > **Cloud Apps**.

The **Cloud Application** window displays the cloud application name, description, documentation links, web interface login links, and the enable and disable options for the cloud apps.

Figure 23: Cloud Apps



Step 3 Manage cloud apps using the available options. The cloud apps that are available are:

- **Cisco DNA Spaces**—A single, scalable, reliable location platform that leverages the existing wireless investments to digitize spaces, including people and things. 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.
- **Cisco Operational Insights**—A cloud-based solution to manage assets within a location. This solution helps operationalize and benefit from a better understanding of assets within an environment.

  Note If you have already enabled Cisco DNA Spaces, then you need not enable Cisco Operational Insights.

- **Cisco BLE Management**—A comprehensive resource for detecting and monitoring BLE beacons or tags as well as managing CCX BLE devices within your network.

  For deployment scenarios using Catalyst 9800 Wireless Controller, you need to allow Cisco CMX to poll AP information over NMSP. For more information, see Polling Access Point Information Using NMSP, on page 189.

Step 4 Use the options available in the **Links** and **Actions** colum to access documentaion and connect with the required cloud app:

- **Documentation**—Click to access the documentation for the corresponding Cloud App.
- **Login**—Click to log in to the required cloud app.
- **Enable**— To enable a cloud app, click the **Enable** option in the **Actions** column for the required cloud app. After you enable the cloud app, you will be able to view the **Update** or **Disable** options.

  Note If you enable a cloud app through **Manage > Cloud Apps**, Cisco CMX continues to send notifications to the cloud app even though the Cisco CMX license has expired. However, if you enable a cloud app from **Manage > Notification**, Cisco CMX stops sending notifications to the cloud app if the Cisco CMX license is expired.

To enable Cisco DNA Spaces, follow these steps:

Note To enable the **Cisco DNA Spaces** service, you must have a Cisco DNA Spaces account. **Cisco DNA Spaces** uses location data to gain insights into the behavior of people and things in any place with wireless connectivity – such as retail, hospitality, healthcare, carpeted enterprise, and higher education allowing you to make informed business decisions, optimize operations, and improve experiences.

Note that for a set of 60k clients and 50k RFID tags, system needs around 10 Mbps line between Cisco CMX and Cisco DNA Spaces Cloud.

a) In the **Actions** column, click **Enable**.
b) In the dialog box that is displayed, enter the token to enable **Cisco DNA Spaces**.

The token can be obtained from **Cisco DNA Spaces** dashboard. You must create a new Cisco CMX wireless network and retrieve the token. For more information, see Creating and Retrieving the Token Using Cisco CMX Tethering, on page 184.

c) Check the **Sync Zones** check box to automatically synchronize zone information from Cisco CMX to Cisco DNA Spaces. This option is enabled by default.

Note After you import the maps, you can use the **Manage** services to update maps, edit zones or exclusion regions and these changes are automatically reflected in Cisco DNA Spaces. To achieve this enhanced tethering feature, you must configure the proxy settings to Cisco CMX with **HTTPS**.

d) Click **Save**.

After a successful connectivity is established between Cisco CMX and Cisco DNA Spaces, you can use the **Map Sync** feature to push maps from Cisco Maps to Cisco DNA Spaces.

Cisco CMX auto sync maps to Cisco DNA Spaces whenever a new map is uploaded or existing map is updated. We recommend that you use the **Map Sync** option when there is some error or discrepancy between both system.

To enable Cisco BLE Management, for example, follow these steps:

a) In the **Actions** column, click **Enable**.

Note To enable the **Cisco BLE Management** service, you must have a Cisco BLE Management account.

b) In the dialog box that is displayed, enter the token number to enable **Cisco BLE Management**.

The token to enable Cisco BLE Management can be obtained from the **Cisco BLE Management** service available in Cisco DNA Spaces. In the **Cisco BLE Management**, use the **Setup** tab to generate token.

c) Click **Save & Enable**.

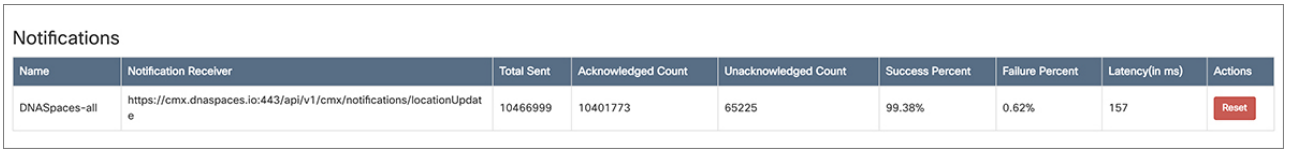
We recommend that you verify the outbound proxy configuration, Cisco WLC 8.7, and Cisco 4800 APs setup to successfully complete the cloud app enabling process.

Note

- For more information about enabling **Cisco Operational Insights**, see the *Operational Insight Configuration* Guide. To get an Operational Insights cloud account and support regarding the **Cisco Operational Insights** service, contact opinsights-support@external.cisco.com.
- If you have already enabled Cisco DNA Spaces, then you need not enable Cisco Operational Insights.
- If you are an existing **Cisco Operational Insights** customer who has upgraded from Cisco CMX 10.4 to 10.5, and choose to enable **Cisco Operational Insights**, it is been observed that redundant notifications are created and duplicate events are sent to the **Operational Insights** cloud app. As a workaround, we recommend that you enable **Cisco Operational Insights** using the token received from **Cisco Operational Insights** location engine and perform an update to **Cisco Operational Insights** using the same token and save your changes.
- Observe the Notifications table to ensure that notifications with the name **operational-insights-tag** and **operational-insights-client** are deleted.

Step 5 Use the **Notifications** section to view the notification name, receiver details, total number of notifications sent, acknowledged notification count, unacknowledged notification count, success percent, failure percent, and latency.

Figure 24: Cloud Apps Notification



Note

- 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.
- To reset a notification, click the **Reset** option in the **Actions** column against each notification.

Creating and Retrieving the Token Using Cisco CMX Tethering

Use the Cisco DNA Spaces dashboard to create a new wireless network for Cisco CMX. A token is generated for each Cisco CMX wireless network that is added to Cisco DNA Spaces. Cisco CMX requires these tokens to manage Cisco DNA Spaces. To generate a token, you must first create a Cisco CMX wireless network using the Cisco DNA Spaces dashboard.

To create a Cisco CMX wireless network in Cisco DNA Spaces, and to retrieve the token, perform the following steps:

Procedure

Step 1 Log in to Cisco DNA Spaces.

Step 2 In the **Cisco DNA Spaces** dashboard, choose **Setup** > **Wireless Networks**.

Step 3 In the **Get your wireless network connected with Cisco DNA Spaces** area, click **Add New**.

The **Connect your wireless network** window is displayed two options - **Cisco AireOS/Catalyst** and **Cisco Meraki**.

Step 4 Click **Select** for **Cisco AireOS/Catalyst**.

Step 5 In the window that is dispalyed, click **Select** for **Via CMX On-Prem**.

The **Connect your wireless network** window is displayed two options - **10.5 and below** and **10.6 or later**.

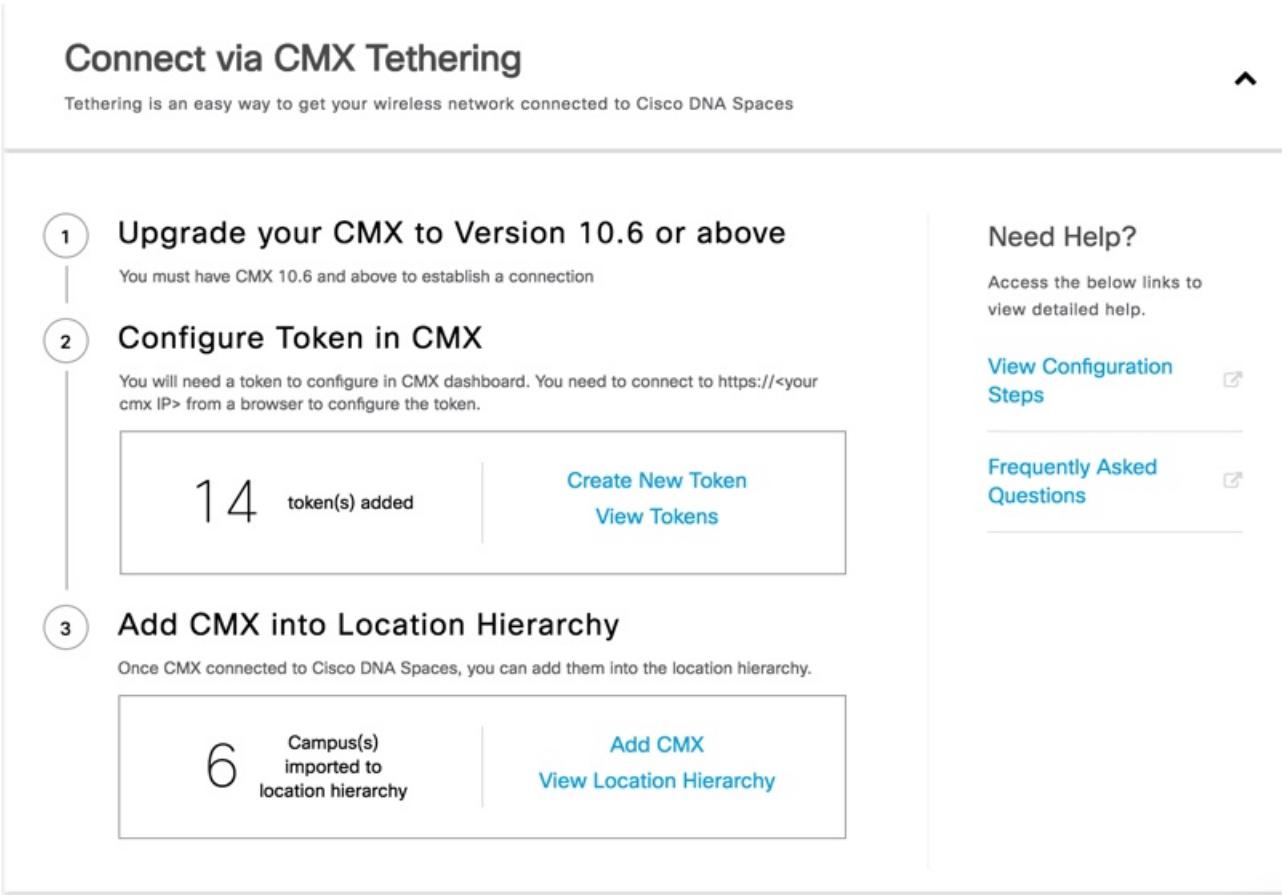
Step 6 Click **Select** for **10.6 or later**.

Prerequisites for Cisco CMX Tethering is displayed. You must have Cisco WLC version 8.0 and above and Cisco CMX 10.6 and later.

Step 7 Click **Customize Setup**.

A **Connect via Cisco CMX Tethering** network bar is displayed in the **Wireless Networks** window.

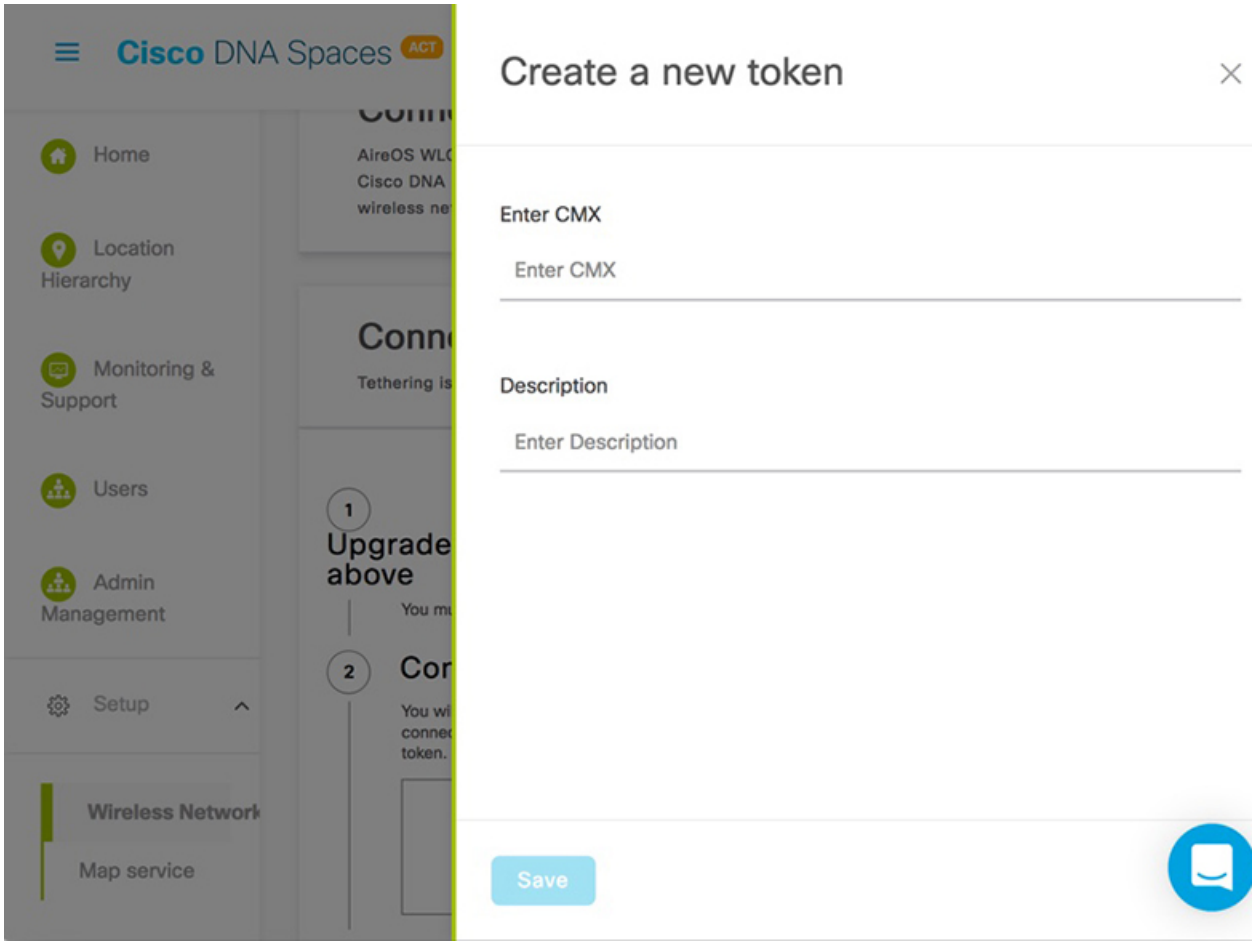
Figure 25: Connect via CMX Tethering Network Bar



Step 8 Click the drop down arrow at the far right of the **Connect via Cisco CMX Tethering** network bar.

Step 9 To add a new Cisco CMX Tethering token, click **Create New Token** that is displayed as **Step 2**.
The **Create New Token** window is displayed.

Figure 26: Create Cisco CMX Token



Note

- A token is mandatory to connect and configure Cisco DNA Spaces from Cisco CMX dashboard.
- You must connect to https://<your cmx IP> from any browser to configure the token.

Alternatively, in the Cisco DNA Spaces dashboard, you can also click the **Wi-Fi** icon at the top-right of the window, and then click **Wireless Network Status** to add a Cisco CMX wireless network. In the **Wireless Network Status** window that is displayed, click **Cisco CMX** from the left panel.

Step 10 In the **Create a new token** window that is displayed, enter a new name and description for the Cisco CMX network connector.

Step 11 Click **Save**.

Step 12 Click **View Tokens** to display the Cisco CMX Tethering tokens.

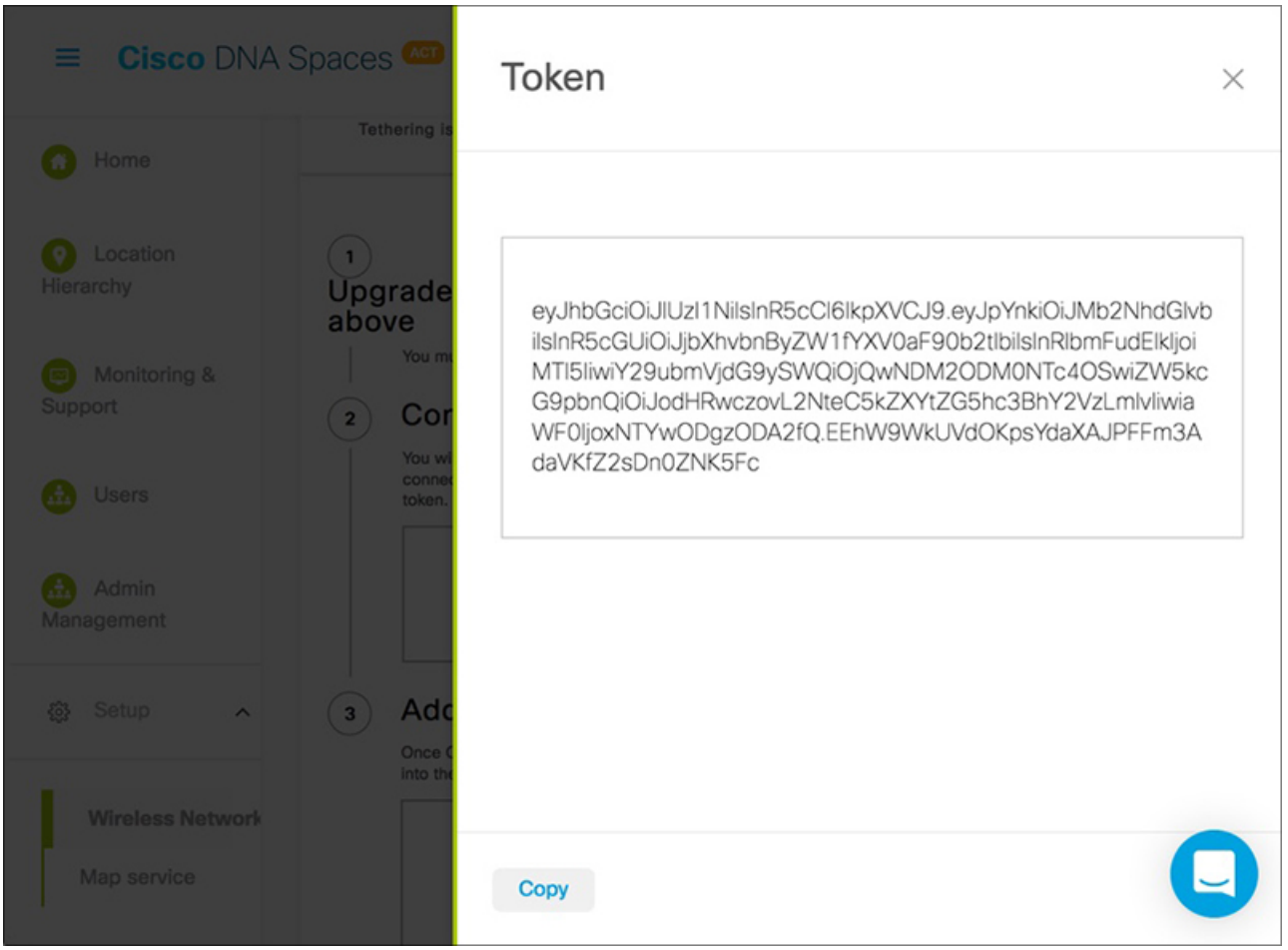
The newly added token is listed on the **Cisco Tethering Tokens** window. A Cisco CMX wireless network is shown as active after its establishes connection with Cisco DNA Spaces. You can also view the first heard and last heard timestamp details in this window.

Step 13 In the **Cisco Tethering Tokens** window, click the **View Access Token** icon adjacent to the token you added.

Step 14 In the dialog box that is displayed, enter your Cisco DNA Spaces login credentials, and click **Submit**.

The token is displayed.

Figure 27: Token



Step 15 Click **Copy** to copy the token. Use this token to enable Cisco DNA Spaces in Cisco CMX under **Manage** > **Cloud Applications** tab.

After Cisco CMX is connected to Cisco DNA Spaces, follow steps 16-19 to add Cisco CMX into the location hierarchy using the Cisco DNA Spaces dashboard.

Step 16 In the **Connect via CMX Tethering** network bar, click **Add CMX**.

Step 17 Choose a location where you want to import Cisco CMX and click **Next**.

Step 18 In the **Display Name** field, add a new name.

Step 19 Choose the sites you want to import and click **Import**.

The selected campuses, buildings, and floors are imported into the location hierarchy.

Click **View Location Hierarchy** to view already added Cisco CMX.

Polling Access Point Information Using NMSP

If your network deployment has Catalyst 9800 Wireless Controller, you need to allow Cisco CMX to poll AP information over NMSP. This is a one time procedure and the configuration will be saved across Cisco CMX service restarts and software upgrades. If you want to poll AP information, use the following commands:

Procedure

Step 1 Connect to Cisco CMX through the console.

Step 2 Run the **cmxctl config featureflags configuration.apimport false** command to disable api import.

Step 3 Run the **cmxctl agent restart** command to restart the CMX agent.

Step 4 Run the **cmxctl configuration stop** command to stop Cisco CMX configuration.

Step 5 Run the **cmxctl configuration start** command to restart the configurations.

Step 6 Run the **cmxctl nmsplb stop** command to stop the Load Balancer service used for NMSP messages to Location services.

Step 7 Run the **cmxctl nmsplb start** command to restart the Load Balancer service used for NMSP messages.

Setting Up Outbound Proxy

If your Cisco CMX on-premise setup requires a forward proxy for internet access, you must configure the proxy and restart your Cisco CMX services. Proxy setting is mandatory if Cisco CMX wants to communicate with cloud. For example, Cisco BLE Management requires the HTTP_PROXY and HTTPS_PROXY environment variables to be set as proxy, and the NO_PROXY environment variable set as local host.

Procedure

Step 1 Connect to Cisco CMX via SSH.

Step 2 To set up a proxy, run the following commands in the same sequence:

a. **cmxos sysproxy proxy** *http://<proxy><port #>*

b. **cmxos sysproxy proxy** *https://<proxy><port #>*

c. **cmxos sysproxy no_proxy localhost,127.0.0.1,company.com**

Step 3 To stop and restart the agent and Cisco CMX services, run the following commands in the same sequence:

a. **cmxos stop -a**

b. **cmxctl agent start**

c. **cmxctl start**

Setting Up Outbound Proxy in HA-Enabled Setup

To set up outbound proxy in an HA-enabled setup, follow these steps:

Procedure

Step 1 Connect to Cisco CMX via SSH.

Step 2 To set up a proxy, run the **cmxos sysproxy show** command on the primary server.

Step 3 To ensure that the no_proxy list is configured, run the **NO_PROXY_LIST=localhost** *127.0.0.1,primary-ip,secondary-ip* command.

Step 4 If no_proxy is not set or is configured incorrectly, run the **cmxos sysproxy no_proxy localhost** *127.0.0.1,primary-ip,secondary-ip* command to set the no_proxy list. Ensure that you replace the *primary-ip* and *secondary-ip* with the primary and secondary IP address of the HA setup.

Step 5 Log out of the Cisco CMX services, and log in again.

Step 6 To view the proxy settings in the environment, run the **env | grep -i proxy** command.

Step 7 To view the proxy settings on the secondary server, run the **cmxos sysproxy show** command. We recommend that you wait for five minutes to reflect the proxy settings on secondary.

Step 8 To view the proxy settings in the environment of the secondary server, run the **env | grep -i proxy** command.

Step 9 To restart the Cisco CMX services, run the **cmxctl agent restart**.

Customizing Verticals

Customizing a vertical means changing the names of the entities in your vertical based on your business. You can optimize your vertical by customizing it to meet your specific needs. Customizing includes naming the hierarchy of your vertical, association of icons, building a tag library, and specifying tag locations.

Procedure

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

Step 2 Choose **MANAGE** > **Verticalization**.
The Verticalization window is displayed with a list of the supported verticals.

Step 3 Choose a vertical by clicking the icon corresponding to that vertical.
The customized widgets available for the chosen vertical are displayed.

Step 4 Click **Run Setup Wizard**.
The setup wizard displays the steps required to optimize the vertical and complete the customization.

Step 5 Click **Get Started**.
The Hierarchy Configuration window is displayed.

Step 6 Configure the hierarchy levels of your vertical. Follow the instructions on the Hierarachy Configuration window to configure hierarchy levels for Campus, Building, Floor, and Zone and select an icon. If you approve of the default hierarchy name and the associated icon, click **Skip Step**.

Step 7 Click **Continue**.

Step 8 Tags are used to categorize locations and devices. Click **Continue** to configure tagging.

Step 9 Depending on the vertical you select, the tags specific to that vertical are listed. Select the tags you want to create by clicking the button corresponding to that tag. The setup wizard creates the tags. Click **Continue**.

Step 10 Location tags can be applied to specific locations based on your hierarchy. The setup wizard iterates through the hierarchies in your vertical. Select the hierarchies that you want to tag by clicking the corresponding name. The right pane lists the Zone item name and a list of tags to choose from. Select the tags that are applicable to the Zone. Click **Continue**.

Step 11 Click **Create a Report**.
The **Analytics Reports** window is displayed with the list of customized wizards for your vertical.

Configuring Basic CMX Settings

The GUI allows you to set up maps, Cisco WLC, and mail server.

Procedure

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

Step 2 Click **SYSTEM**.
The **SETUP ASSISTANT** window is displayed.

Step 3 Click **Next** to set up the **New UI Password**.
The **Maps and Controllers** window is displayed.

Step 4 Choose either **Default** or the **Advanced** option.

- In the **Default** window, provide Cisco Prime Infrastructure credentials such as **`Username`**, **`Password`**, and **`IP Address`**, and click **Import Controllers and Maps**. This imports the Controllers and maps from Cisco Prime Infrastructure.
- In the **Advanced** window, provide the map and Cisco WLC information, and click **Next**.

Note If the **Override** checkbox is checked, the import will override the existing entries.

Step 5 In the **Mail Server** window that is displayed, enter the corresponding details.

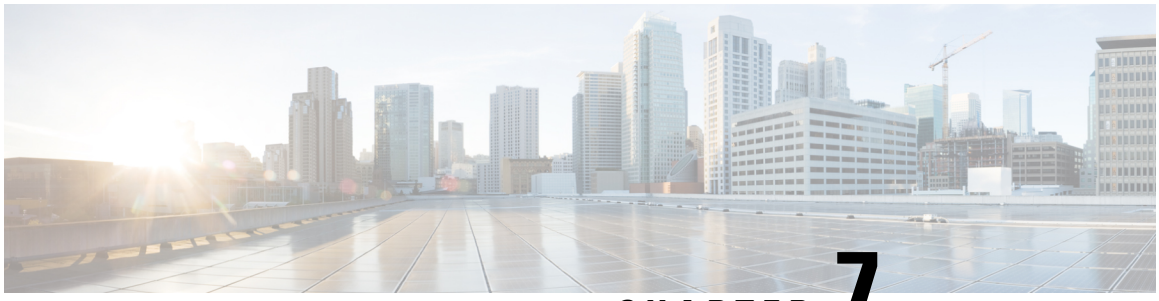
Step 6 Click **Next** to complete the configuration.

Root User Changes

In releases prior to Cisco CMX 10.2, all the processes used the root user role. This has been changed in Cisco CMX 10.2 by introducing two new user roles: cmx and cmxadmin. The cmx user is a no-login user who owns all the processes, except postgres. The cmxadmin is the primary user who performs all the administrative tasks.

The root user is not disabled; this user can still be used for installation and debugging. You cannot directly log in to root through SSH or console. First you have log in as cmxadmin and then issue the **su** command to go to the root user level.

Caution Do not use the root user account; unless explicitly directed to do so by the Cisco Technical Assistance Center team.



CHAPTER 7

Managing Cisco CMX System Settings

Overview of the System Service

The Cisco CMX **System** service comprises the following tabs, which help you perform a variety of system-related tasks, including, but not restricted to, those listed here:

- **Dashboard**—Enables you to have an overall view of the system.
- **Alerts** —Enables you to view live alerts.
- **Patterns**—Enables you to detect patterns of various criteria, such as Client Count, CPU Usage, Memory Usage, and so on.
- **Metrics**—Enables you to view system metrics.

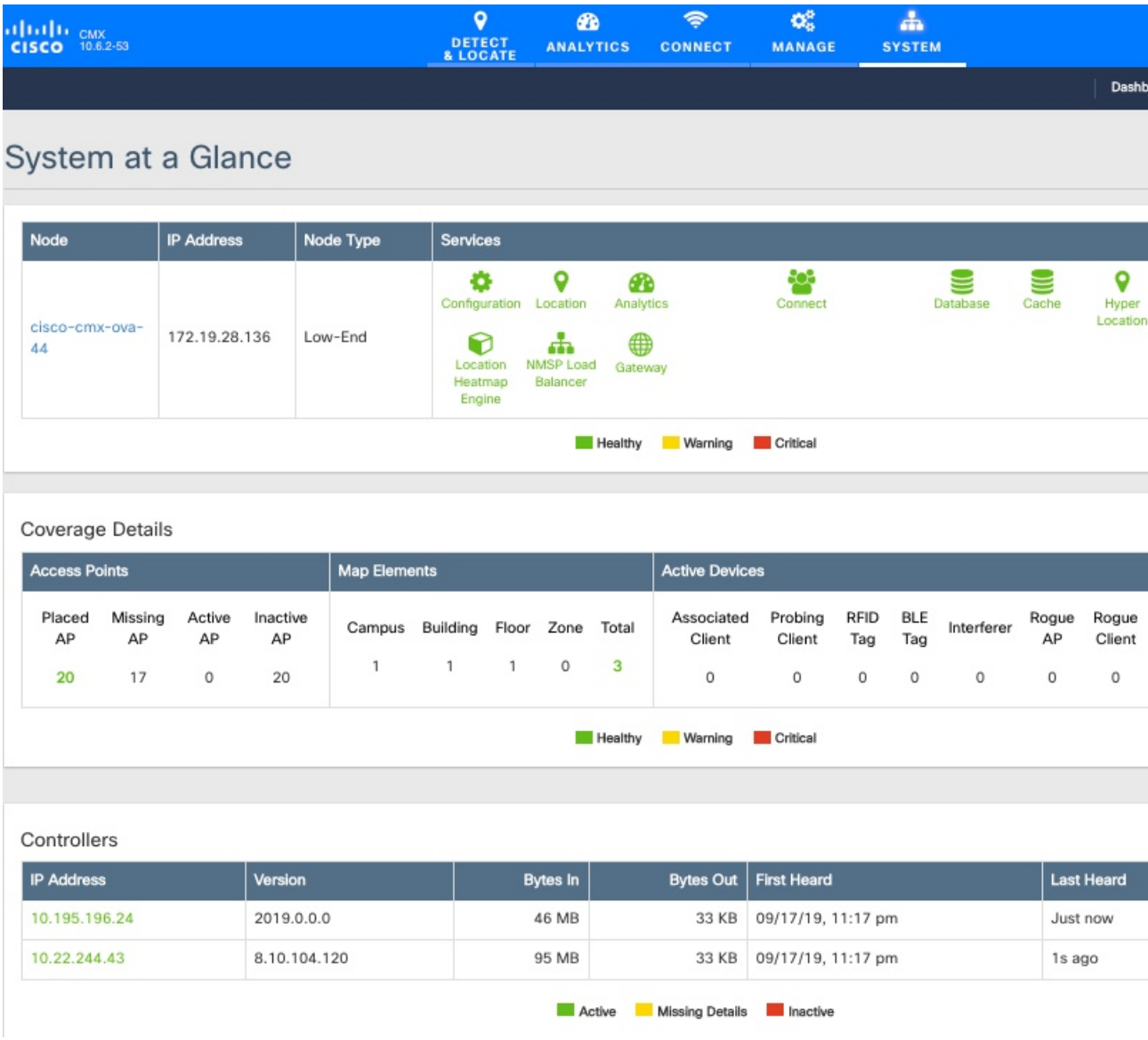
Viewing the Overall System Health

Procedure

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

Step 2 Choose **System** > **Dashboard**.

The **System at a Glance** window (see the image below) is displayed.



Step 3 View the following sections:

- Node Table. For details, see Understanding the Node Table, on page 195.
- Coverage Details Table. For details, see Understanding the Coverage Details Table, on page 195.
- High Availability Table.
- Controllers Table. For details, see Understanding the Controllers Table, on page 196.

Understanding the Node Table

The **Node** table in the **System at a Glance** window displays the following Cisco CMX node information:

- **Node**—Lists all the associated Cisco CMX nodes.
  - Click a node name to view its metrics. See Viewing CMX Node Metrics, on page 217.
- **IP Address**—Shows the IP address of the Cisco CMX node.
- **Node Type**—Shows the type of the Cisco CMX node.
- **Services**—Lists all the services for each Cisco CMX node.
  - The colors of the icons pertaining to these services indicate the status of these services. Ensure that the services are in green color; this indicate a healthy status.
  - Click a service icon to view the corresponding service or system metrics.
- **Memory**—Shows the load on the memory, in percentage.
  - Click it to view the **Live Alerts** window. See Viewing Live System Alerts, on page 215.
- **CPU**—Shows the load on the CPU, in percentage.
  - Click it to view the **Live Alerts** window. See Viewing Live System Alerts, on page 215.

Understanding the Coverage Details Table

The **Coverage Details** table in the **System at a Glance** window displays the following information:

- **Access Points**—Shows the number of access points placed on Cisco CMX map.
  - **Placed AP**—Shows the total count of access points placed on Cisco CMX map.
  - **Missing AP**—Shows the number of access point which has sent location details but not found on the map. This could impact the accuracy of the location.
  - **Active AP**—Shows the number of active access points. This helps to troubleshoot and determine if there are access points that are not placed on Cisco CMX map. An AP is considered as active when Cisco CMX receives RSSI measurements for clients and tags from the AP. An AP will remain in active status until midnight and post midnight all AP status (such as Active / Missing / Inactive) are flushed out. Depending on the Cisco CMX map and RSSI measurements AP status will be readjusted. Note that the AP status will also be readjusted when you import a map on Cisco CMX.
  - **Inactive AP**—Shows the number of inactive access points. By default all APs are in inactive status when you add a Cisco Prime Infrastructure map. After a controller is added and Cisco CMX starts receiving RSSI measurements, an AP is considered as active.
- **Map Elements**—Shows the number of elements available on Cisco CMX map.
  - **Campus**—Shows the number of campuses in Cisco CMX.

- **Building**—Shows the total number of buildings in Cisco CMX.
- **Floor**—Shows the total number of floors in Cisco CMX.
- **Zone**—Shows the total number of zones in Cisco CMX.
- **Total**—Shows the summation of all the previous elements. This is the total elements in Cisco CMX .

- **Active Devices**—Shows the number of active devices available on Cisco CMX map.
  - **Associated Client**—Shows the number of associated clients.
  - **Probing Client**—Shows the number of probing clients.
  - **RFID Tag**—Shows the number of active RFID tags.
  - **Interferer**—Shows the number of interferers.
  - **Rogue AP**—Shows the number of rogue access points.
  - **Rogue Client**—Shows the number of rogue clients.
  - **BLE Tags**—Shows the number of bluetooth devices.
  - **Total**—Shows the summation of all the previous devices.
- **System Time**—Shows the current system time with the time zone set as on Cisco CMX system .

Understanding the Controllers Table

The **Controllers** table in the **System at a Glance** window lists the controllers that are sending Network Mobility Services Protocol (NMSP) data to Cisco CMX.

The table displays the following details for each Cisco controller:

- **IP Address**: The color of the table border to the left of each IP address indicates whether the controller is active or not.
- **Version**: Controller software version. Cisco CMX must have the latest controller password to display the correct controller version.
- **Bytes In and Bytes Out**: Number of bytes received from and sent to the controller.
- **First Heard**: Number of seconds since the first communication received from the controller.
- **Last Herad**: Number of seconds since a communication was received from the controller.
- **Action**: Allows you to modify the details of an existing controller or delete an existing controller. Click **Edit** to edit the controller details in the Edit Controller window. Click the plus icon to view the **Controllers and Map Setup** tab details in the **Settings** window.

Note

- Click the plus icon to add new controllers. The **SETTINGS** window is displayed with **Import from Cisco Prime** tab. For more information about adding controllers, see Importing Maps and Controllers into Cisco CMX, on page 206.
- Active contollers are shown in green. Inactive contorllers are shown in red. Controllers with missing SNMP or SSH credentials are also shown in yellow.

Managing Dashboard Settings

The **Settings** option in the **System at a Glance** window enables you to manage the configurations and other settings related to the **Cisco CMX System** service.

Setting Device-Tracking Parameters

Procedure

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

Step 2 Choose **System** > **Dashboard**.
The **System at a Glance** window is displayed.

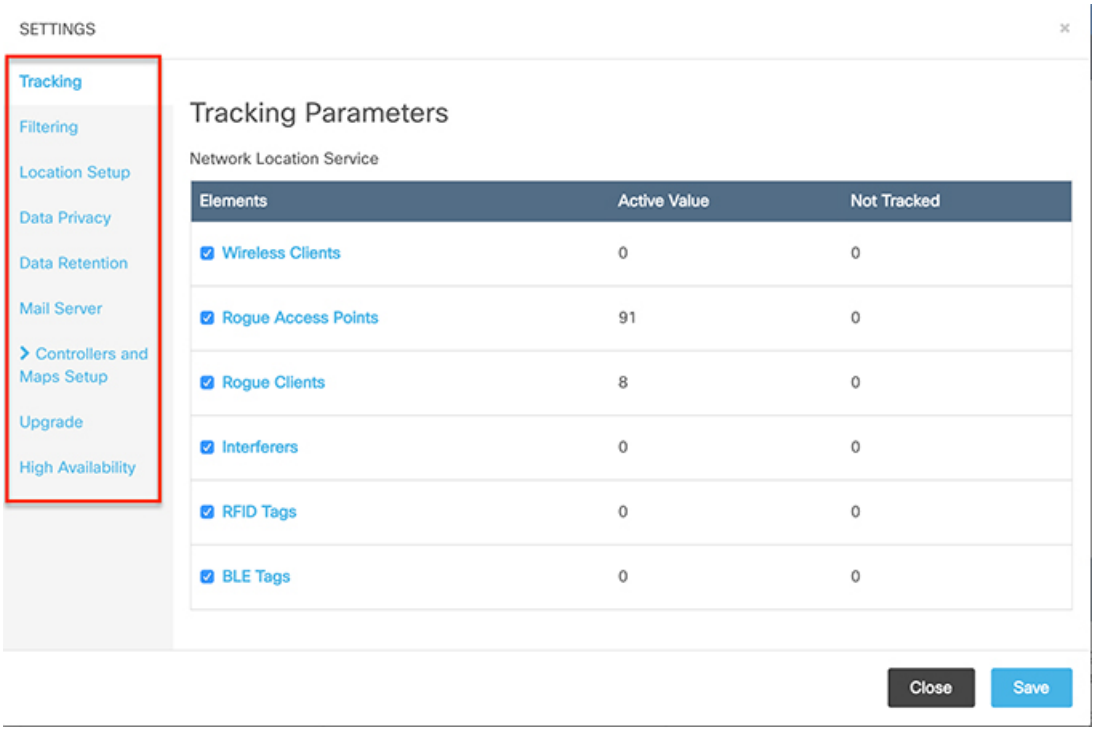
Step 3 Click **Settings** at the top-right corner of the window.

The **SETTINGS** window is displayed.

Note By default, the **Tracking Parameters** tab is displayed.

Step 4 In the **Elements** column, check the check box of the device that you want to select for tracking.

Figure 28: Tracking Parameters



Only the elements selected here will be tracked by the Network Location service and will appear on the **Activity Map** window.

The following elements are available for tracking:

- Wireless Clients
- Rogue Access Points
- Rogue Clients
- Interferers
- RFID Tags
- BLE Tags

Note

- BLE-capable APs are discovered by Cisco Prime Infrastructure. Use Cisco Prime Infrastructure to place the APs on the maps and export the maps. Cisco CMX utilizes the map file exported from Cisco Prime Infrastructure.
- BLE beacons are detected in 2 ways:
  - **Clean air over NMSP**—To enable this tracking method, check the **Interferers** option. You require Cisco WLC with software Release 8.0.115.0 or later for this method.
  - **Fast path over UDP**—To enable this tracking method, check the **BLE Beacons** option. You require Cisco WLC with software Release 8.6.1.146 or later for this method.
- BLE tags are supported on high-end appliance only.

Step 5 Click **Save**.

Setting Filtering Parameters

Procedure

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

Step 2 Choose **System > Dashboard**.
The **System at a Glance** window is displayed.

Step 3 Click **Settings** at the top-right corner of the window.

The **SETTINGS** window is displayed.

Step 4 In the left pane, click **Filtering**.

Here, you can configure the following filtering parameters:

- **Duty Cycle Cutoff (Interferer)**: This is a percentage value. Interferers with a Duty Cycle that is less than the specified cutoff will not be tracked.
- **Severity Cutoff (Interferer)**: This numeric value represents percentage of time. Interferers must be seen on the network before Cisco CMX starts tracking them. Sometimes, interferers are very short lived with **Duty Cycle** as 0% and overwhelms Cisco CMX. This filter helps Cisco CMX to discard such short lived interferers as they come and go. The default value is 10 which means that the interferer must be seen 10% of the time in the network before Cisco CMX starts processing it.

  Note Cisco CMX will process interferers only when the **Duty Cycle** and **Severity Cutoff** filters are satisfactory. Interferer must be reported with DutyCycle 10% or above and Severity value 1 or above. Interferes that do not follow this criteria would be moved to the category **Not Tracked** under **System > Settings > Tracking** option.

- **RSSI Cutoff (Probing Only Clients)**: This is the radio signal strength cutoff for filtering. The default is -85 dBm.
- **Exclude Probing Only Clients**: Check this check box to filter out clients that are only probing. This is the best effort to stop detecting probing clients. However, a small percentage of probing clients may appear for short duration. So this should not be considered as complete probing client removal from the system. If you check this option, the **Probing Client Filtering** service is enabled on Cisco WLC 8.7 or later, and then Cisco CMX will not receive any probing client information.
- **Enable Location MAC Filtering**: Check this check box to filter out specific MAC addresses. For example, you can use this to filter out MAC addresses of employees' devices. After checking this, you can either specify a MAC address that you want to allow or disallow, or choose to allow, disallow, or delete previously entered MAC addresses.
- **Enable Location SSID Filtering**: Check this check box so that the Location service excludes all visitor devices associated to a particular SSID.

  a. Click **Enable SSID Filtering**.

b. Click **Select SSID**, and select a particular **SSID**. If no SSIDs appear in the list, make sure that a Cisco WLC is active, and then click **Fetch SSIDs** to refresh the list.

Note

- With Cisco CMX Release 10.5.1 or later, Cisco CMX relies on WLC notification (INFO messages) to populate the SSID list. For all earlier Cisco CMX releases, this was achieved using SNMP polling.
- Cisco CMX would clear the blocked SSID's every midnight (as part of midnight cleanup job) and require the blocked clients to be reported again from the blocked SSID's. So you may see the blocked clients being tracked again past midnight. If you want Cisco CMX to not clear the blocked SSID's by midnight job, then set the **featureflags location.filteredssidscleanupatmidnight** configuration as **false**. Run the following commands to configure:
  1. To set featureflag location parameters, run the following command **cmxctl config featureflags location.filteredssidscleanupatmidnight false**
  2. To restart Cisco CMX agents, run the following command **cmxctl agent restart**
  3. To stop and start the location and NMSP, run the following commands **cmxctl location stop; cmxctl nmsplb stop** and **cmxctl location start; cmxctl nmsplb start**

c. Click **Filter SSID** to add the selected SSID to the filter list.

Step 5 Click **Save**.

Setting Location Calculation Parameters

Procedure

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

Step 2 Choose **System > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 Click **Settings** at the top-right corner of the window.

The **SETTINGS** dialog box is displayed.

Step 4 In the left pane, click **Location Setup**.

Here, you can configure the following **Location Calculation Parameters**:

- **Enable OW Location**—Check this check box to enable the use of Outer Walls (obstacles) for location calculation. The Calibration model includes information regarding the Walls. This setting controls whether the CMX should honor the walls while calculating the heatmaps or not.
- **Enable Location Filtering**—Check this check box if you want the system to use previous location estimates for estimating the current location. This parameter will be applied only for client location

calculation. Enabling this parameter reduces location jitter for stationary clients and improves location tracking for mobile clients. This parameter is enabled by default.

- **Use Default Heatmaps for Non Cisco Antennas**—Check this check box to enable the usage of default heat maps for non-Cisco antennae during location calculation.
- **Chokepoint Usage**—Check this check box to enable the usage of chokepoint proximity to determine the location of a device. This applies only to Cisco-compatible tags that are capable of reporting chokepoint proximity. This parameter is enabled by default.
- **Enable Hyperlocation/FastLocate/BLE Management**—Check this check box to enable hyperlocation, fastlocate, and BLE management in Cisco CMX.

  Note This option will not be displayed if the system is not a large OVA installation. Hyperlocation requires a high end system to run and if run on lower system the option is hidden. For high end system (20 vCPU) and Bare metal (3365), Hyperlocation option is enabled by default and displayed in the GUI. For standard (16 vCPU) and low end system (8 vCPU), Hyperlocation option is hidden.

- **Optimize Latency**—Check this check box to enable latency optimization. If you enable this option, Cisco CMX enables faster location computation over less data affecting accuracy due to not using the fully available data for computation. By default, this option is not enbaled. If not enabled, Cisco CMX will provide location updates at default intervals computed over full available data. If you check this option, the **Relative discard RSSI time** and **Relative discard AoA time** values will be changed to 30. You will not be able to edit these values. We recommend you to enable this option only if recommended by Cisco.
- **Use Chokepoints for Interfloor conflicts**—Use this drop-down list to specify the frequency to determine the correct floor during interfloor conflicts.
- **Chokepoint Out of Range Timeout (secs)**—After a Cisco-compatible tag leaves a chokepoint proximity range, RSSI information will be used again to determine the location only after this timeout value is exceeded. Specify a timeout value, in seconds, accordingly.
- **Relative discard RSSI time (secs)**—Enter the time, in seconds, after which the RSSI measurement should be considered obsolete and discarded from use in location calculations. This time is from the most recent RSSI sample, and not an absolute time. For example, if this value is set to 3 minutes, and two samples are received at 10 minutes and 12 minutes, both the samples will be retained. However, an additional sample received at 15 minutes will be discarded. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.
- **Relative discard AoA time**—Enter the time, in secondsß, after which the AoA mesaurement should be considered as obsolete and discarded from use in location calculations. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.
- **Absolute discard RSSI time**—Enter the time, in minutes, after which the RSSI measurement should be considered obsolete and discarded from use in location calculations regardless of the most recent sample. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.
- **RSSI cutoff**—Enter the RSSI cutoff value, in dBm, at which you want the server to discard AP measurements. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.

You can also set the following **Movement Detection Parameters**:

- **Individual RSSI change threshold**—Enter a threshold, in dBm, beyond which you want individual RSSI movement recalculation to be triggered. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.
- **Aggregated RSSI change threshold**—Specify the Aggregated RSSI movement recalculation trigger threshold. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.
- **Many new RSSI change percentage threshold**—Specify the trigger threshold recalculation (as a percentage) for many new RSSI changes. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support. This parameter indicates the threshold for comparing against the aggregated APs value. This compariosn will help you to decide whether the location computation is required.
- **Many missing RSSI percentage**—Specify the trigger threshold recalculation (as a percentage) for many missing RSSI changes. We recommend that you do not modify this parameter without the guidance of Cisco Technical Support.

Step 5 Click **Save**.

Setting Data Privacy

The EU General Data Protection Regulation (GDPR) places the onus on organizations to be more accountable for data protection and deploy appropriate security controls. MAC address hashing is one of the requirements for GDPR compliance.

Cisco CMX is a system that enables organizations locate wireless clients. To identify these clients, Cisco CMX uses the MAC address of the corresponding wireless devices. In the content of the GDPR, the MAC address or IP address of the wireless clients are considered as personal identifiable information (PII). Cisco CMX stores location information in multiple ways and processes it to generate analytics data. In the context of the GDPR, Cisco CMX acts as a data controller as well as a data processor.

Attention Consult your legal department and your GDPR data privacy officer to achieve a Cisco CMX configuration that is compliant with your requirements.

The Setting Data Privacy feature prevents personally identifiable information (MAC address) from being directly accessed. Using a salted hashing algorithm, the MAC address for a particular user is transformed to a hashed value. You cannot recover the original MAC address from the hashed value. You can change the salt value for a particular date or range of dates. If the salt value is not set for a particular date, the salt value from the preceding date or date range is used. If a salt value is not set, the hash function does not use salt in the hashing algorithm.

Procedure

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

Step 2 Choose **System > Dashboard**.
The **System at a Glance** window is displayed.

Step 3 Click **Settings** at the top-right corner of the window.

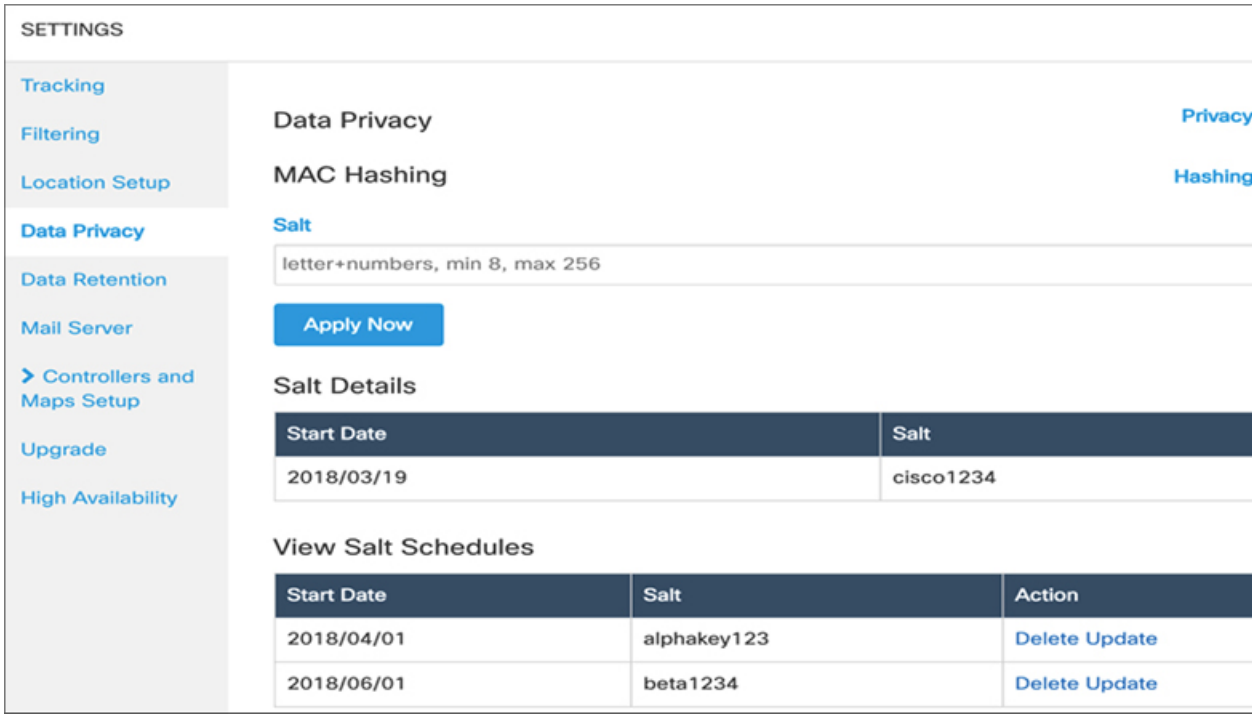
The **SETTINGS** window is displayed.

Step 4 In the left pane, click **Data Privacy**.

Step 5 To enable data privacy, set **Privacy** to **On**.

Step 6 To enable MAC hashing, set **MAC Hashing** to **On**.

Figure 29: MAC Hashing



Note When you enable Data Privacy and MAC Hashing, Cisco CMX generates dashboard alerts and email notifications. Ensure that you set up a mail server configuration to receive notifications.

Step 7 In the **Salt** field, enter a value. This is the alphanumeric value used for hashing on the real MAC address.

Step 8 Click **Apply Now**. You can apply salt for the current date or a future date. The new salt details are displayed in the **Salt Details** section. If you are adding salt for the first time, the salt is applied for the current date. You also can add a salt for a future date.

Step 9 In the **Salt Details** section, view the following:

- **Start Date**—Displays the date on which salt was applied first.
- **Salt**—Displays the salt value.

Step 10 In the **View Salt Schedules** section, click the eye icon to view the following:

- **Start Date**—Displays the date on which salt was applied first.
- **Salt**—Displays the salt value.

- **Action**—Click **Update** to open the **Update Salt** dialog box and update the salt details. Click **Delete** to delete the salt details.

Step 11 To add salt for a future date, click the plus icon.

The **Add Future Salt Schedule** dialog box is displayed.

Step 12 In the **Add Future Salt Schedule** dialog box, enter the **Salt** details and the **Start Date** in mm/dd/yyyy format, and click **Add**.

Step 13 In the **Subscription Details** section, view the following:

- **Category**—Displays the list of categories.
- **Active Value**—Displays the active value.
- **Action**—Click **Add** to open the **Add Opt-In Device** dialog box and add the device MAC address. Click **Delete** to delete the category details.

Step 14 In the **Device MAC Address** field, enter the MAC address that you want to hash.

Step 15 Click **Hash**.

The hashed MAC address is displayed in the **Hash MAC Address** field.

Step 16 Click **Save** to save the data privacy settings.

Setting Data Retention Parameters

Data Retention is a part of Data Privacy feature. Data Retention configurations help Cisco CMX to retain data such as location history, analytics data, and so on.

Procedure

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

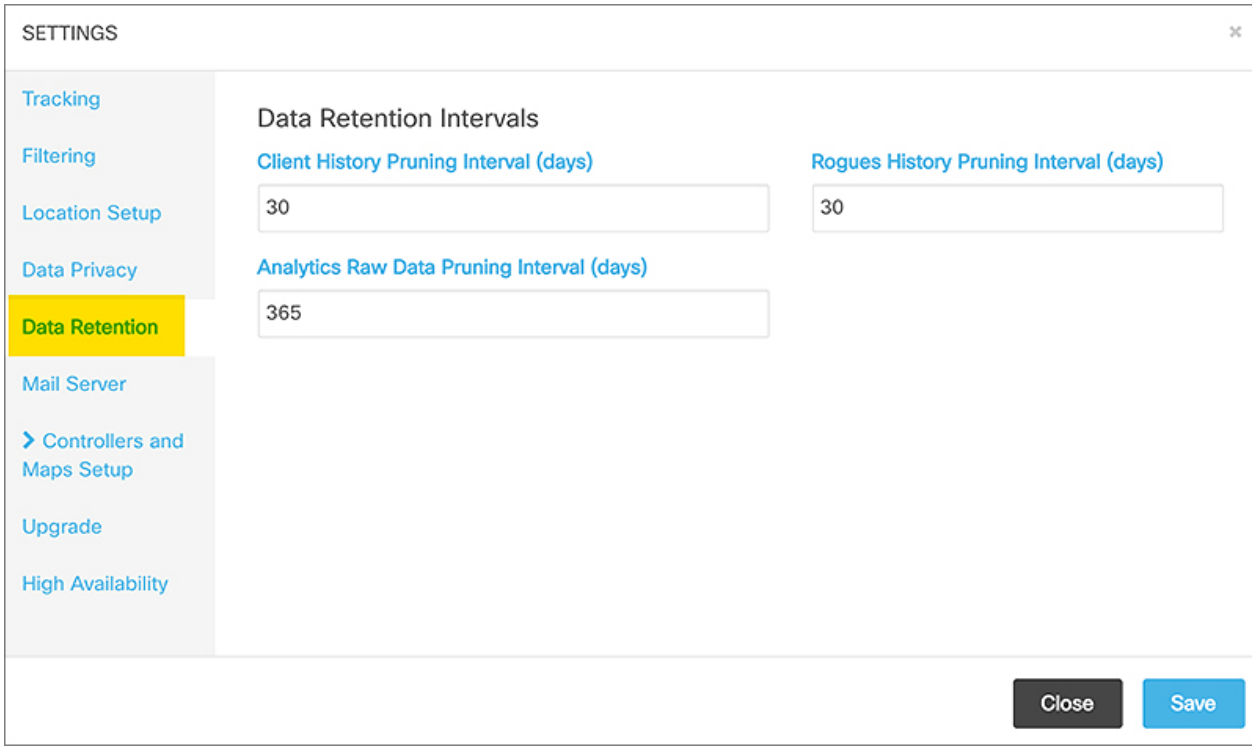
Step 2 Choose **System** > **Dashboard**.
The **System at a Glance** window is displayed.

Step 3 Click **Settings** at the top-right corner of the window.

The **SETTINGS** window is displayed.

Step 4 In the left pane, click **Data Retention**.

Figure 30: Data Retention



Step 5 In the **Client History Pruning Interval (days)** field, enter the interval value, in days. The default value is 30 days.

Step 6 In the **Rogues History Pruning Interval (days)** field, enter the interval value, in days. The default value is 30 days.

Step 7 In the **Analytics Raw Data Pruning Interval (days)** field, enter the interval value, in days. The default value is 365 days.

Step 8 Click **Save**.

Configuring the Mail Server for Notifications

Procedure

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

Step 2 Choose **System > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 Click **Settings** at the top-right corner of the window.

The **Settings** dialog box is displayed.

Step 4 In the left pane, click **Mail Server**.

Here, you can configure the following:

- **From Email Address**—Email address of the mail server host.
- **To Email Address**—Enter the email addresses to which the notifications should be sent. You can add multiple email addresses sepearted using the delimiters comma, semi-colon, and space.
- **Server**—Mail server URL.
- **Port**—Port number for the mails. The default is port 25.
- **Authentication**—Option to enable or disable email authentication.
- **SSL**—Option to enable or disable email security with Secure Sockets Layer (SSL) to prevent third parties from potentially viewing your email messages.
- **TLS**—Option to enable or disable email secured with Transport Layer Security (TLS).

Step 5 To test your settings, click **Save and Test Settings**.

Step 6 Enter the email address and then click **Send e-mail**.

Step 7 Click **Save** to save your settings if the test is successful.

Importing Maps and Controllers into Cisco CMX

Note (CSCvf77237, CSCvf93122) (related to CSCvf21552) The following are considerations when using Cisco Prime Infrastructure:

- Cisco Prime Infrastructure Release 3.2 supports either Cisco CMX or Cisco MSE, but it does not support both at the same time.
- Only data is synchronized between Cisco Prime Infrastructure and Cisco CMX. Changes to maps are not synchronized.
- Addresses are not imported from Cisco Prime Infrastructure. You must set the address of the campus manually on Cisco CMX. For more information, see Adding a Campus Address, on page 160.

To import maps and controllers directly from Cisco Prime Infrastructure, do the following:

Before you begin

Ensure that while exporting maps from Prime, check the **Include Calibration Information** option. Cisco CMX will not be able to compute the location for network elements (Clients/ Interferers / Tags) for maps having no calibration information.

Import operation for map archive files will fail if **Include Calibration Information** option is not selected in the Prime Infrastructure while importing maps. While importing maps, ,the upload utility validates if the calibration model is available for each floor in the given maps archive file. If not available, map import will fail with an error message: 'Calibration model is missing in the uploaded map archive. Please select the option 'Include Calibration Information' on Prime Infrastructure GUI while exporting maps archive.

Procedure

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

Step 2 Choose **System > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 Click **Settings** at the top-right corner of the window.

Step 4 Choose the **Controllers and Maps Setup** > **Import** tab, and enter the following parameters:

a) **Username**—Username of the Cisco Prime Infrastructure server.

b) **Password**—Password of the Cisco Prime Infrastructure server.

c) **IP Address**—IP address of the Cisco Prime Infrastructure server. Ensure that the SNMP community string is properly configured in Cisco Prime Infrastructure.

- To save the Cisco Prime Infrastructure credentials, check the **Save Cisco Prime Credentials** check box.
- To override the existing maps that currently exist in Cisco CMX while importing, check the **Delete & replace existing maps & analytics data** check box.
- If you import a map with a new campus, you need not check the **Delete & replace existing zones** check box. Cisco CMX will automatically process all the zones added in the map.
- If you reimport an existing map, ensure that you check the **Delete & replace existing zones** check box. If you check the **Delete & replace existing zones** check box, the existing zones in Cisco CMX will be replaced by zones that you import from Cisco Prime Infrastructure.
- To override the existing zones that currently exist in Cisco CMX while importing, check the **Delete & replace existing zones** check box.

Note We recommend exporting updated maps only from Cisco Prime Infrastructure. In addition, when importing updated maps to Cisco CMX, make sure the **Delete & replace existing maps & analytics data** check box and the **Delete & replace existing zones** check box are unchecked.

Step 5 Click **Import Controllers and Maps**.

Step 6 Click **Save**.

Importing Maps and Adding Controllers

You can manually import maps and add Cisco Wireless Controllers into Cisco CMX using the web interface.

Procedure

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

Step 2 Choose **System > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 Click **Settings** at the top-right corner of the window.

Step 4 Choose the **Conrollers and Maps Setup > Advanced** > tab.

Step 5 To manually import a map, perform the following:

a) Under the **Maps** area, click **Browse**.

The File Upload dialog box is displayed.

Note

- If you check the **Delete & replace existing maps & analytics data** check box , the maps existing in Cisco CMX will be replaced by the maps that you import from Cisco Prime Infrastructure. Existing zones are also removed when you override the maps.
- If you import a map with a new campus, you need not check the **Delete & replace existing zones** check box. Cisco CMX will automatically process all the zones added in the map.
- If you reimport an existing map, ensure that you check the **Delete & replace existing zones** check box.

  If you check the **Delete & replace existing zones** check box, the existing zones in Cisco CMX will be replaced by zones that you import from Cisco Prime Infrastructure.

Ensure that while exporting maps from Prime, check the **Include Calibration Information** option. Cisco CMX will not be able to compute the location for network elements (Clients/ Interferers / Tags) for maps having no calibration information.

b) Navigate to the location of the map file, select the map file, and then click **Open**.

c) Click **Upload**.

d) Click **Save**.

Step 6 To import a Cisco WLC, configure the following parameters under the **Controllers** area:

a) **Controller type**—Choose from **Cisco WLC** or **Unified WLC**.

b) **IP address / Hostname**—IP address or hostname of the controller.

c) **Controller Version**—(Optional) Software version of the controller.

d) **Applicable Services**—Check the CAS check box if Context Aware Service (CAS) is applicable.

e) **Controller SNMP version**—Choose from **v1**, **v2c**, or **v3**.

f) **Controller SNMP Write Community**—Enter the controller SNMP write Community string. The default is *private*.

g) Click **Add Controller**.

Note

-
- 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, on page 196.
- If you are adding Unified WLC, ensure that SSH is enabled on the controller before adding it to Cisco CMX.

Step 7 Click **Save**.

Importing Maps from Cisco DNA Center

Cisco CMX allows you to import maps from Cisco DNA Center. When you import a map from Cisco DNA Center to Cisco CMX, all elements of map data is imported to Cisco CMX in the same manner when you import maps from Cisco Prime Infrastructure, such as access points information, floor images, calibration model/antenna patterns, inclusion/exclusion region, GPS markers, zones and so on.

In Cisco DNA Center, the **Network Hierarchy** tab under **Design** helps you to create network hierarchy and apply them to different areas of the organization. When you add maps using **Network Hierarchy**, map data can have nested campus/site structure. For example, under Global map, you can add U.S.A as a site and can add San Jose and RTP as sub-sites.

When you import maps in Cisco CMX, the map utility imports map data following a simple three element structure: "**Campus > Building(s) > Floor(s)**". However, when you import maps from Cisco DNA Center, map data pushed to Cisco CMX can include nested campus/site structure. For example, "**US>CA>SJC>Milpitas>CiscoBuilding24>FirstFloor**" which is different from the typical three element structure "**Milpitas>CiscoBuilding10>FirstFloor**" as in Cisco CMX.

When you import maps from Cisco DNA Center to Cisco CMX, Cisco CMX will only import the sites/campuses with a building element. For an imported map, if the **Network Hierarchy** on Cisco DNA Center is **US>CA>SJC>Milpitas>CiscoBuilding24>FirstFloor**, Cisco CMX will only show partial **Network Hierarchy** that is **Milpitas>CiscoBuilding24>FirstFloor**. However, Cisco CMX maintains a list of the parent elements in the database as **US>CA>SJC** and this information is only displayed in the API response and Northbound Notification messages, but not on the Cisco CMX GUI.

In Cisco CMX, you can view the Network Hierarchy using the following three options:

1. REST API version 1 (HTTP GET /api/location/v1/<element-type>/)
2. REST API version 3 (HTTP GET /api/location/v3/clients/)
3. Northbound Notification messages

Following are the limitations when you import maps from Cisco DNA Center **Network Hierarachy**:

- Cisco CMX does not import the address and latitude/longitude of the sites from the Cisco DNA Center.
- No limitation for the number of nested sites. Cisco DNA Center allows you to create a maximum of four nested sites. As the number of nested sites increase, the **locationMapHierarchy** or **mapHierarchyString** attribute value will also increase accordingly.
- It is not recommended to have duplicate site names. When map data is imported from Cisco DNA Center with the Network Hierarchy: **US>CA>SJC>Campus-One>CiscoBuilding24>FirstFloor** and **US>CA>RTP>Campus-One>CiscoBuilding24>FirstFloor**, Cisco CMXwill overwrite the parent list of **Campus-One** from **US>CA>SJC** to **US>CA>RTP** which is the last incoming parent list for that campus.

Upgrading Cisco CMX

After you install Cisco CMX 10.2, future upgrades can be performed via the Cisco CMX GUI or by using the **cmxos upgrade** CLI command and the .cmx file, for example, cmxos upgrade <**CISCO_CMX$$$.cmx**>, while logged in as cmxadmin.

To upgrade Cisco CMX to a future release using the GUI, perform the following task:

Procedure

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

Step 2 Choose **System > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 Click **Settings** at the top-right corner of the window.

Step 4 In the **SETTINGS** dialog box, click the **Upgrade** tab and then click **Upgrade**.

Step 5 Either choose a local .cmx file or point to the URL of the .cmx file

Before selecting the local file option, ensure that the .cmx file is available on the machine from which access to the web GUI is being made.

The upgrade process involves the following tasks:

a. The .cmx file is copied to /opt/image/newimage.

b. The **cmxos upgrade** command is executed in the background:

- Services are stopped
- New files are copied and configured
- Services are restarted

What to do next

For more information about upgrading Cisco CMX using CLI, see Upgrading Cisco CMX Using CLI.

Enabling High Availability for Cisco CMX

High Availability (HA) is a simple and reliable failover mechanism. It helps Cisco CMX host and support multiple mobility applications seamlessly without any interruption.

The definition of servers described in this section are as follows:

- **Active Server**—The Cisco CMX server that is actively serving traffic from the controllers. The virtual IP address (VIP) for the HA pair should point to the current active server. The VIP address is optional.
- **Primary Server**—The Cisco CMX server that will be initially active in the HA pair.
- **Secondary Server**—The CMX server that will be the backup or standby server in the HA pair.

Cisco CMX HA requires two servers. The primary server acts as the active Cisco CMX server. Cisco CMX server can use virtual IP addresses too. The primary Cisco CMX server is installed by selecting the Location or Presence node type. In an active HA deployment, data on the primary server will be continuously synchronized with the secondary server. If the primary server encounters any issues, the secondary server will take over the responsibility as the active server.

Install Cisco CMX Release 10.3.x on both the servers. From the web installer, choose either **Presence** or **Location** as the node type. Both the servers should have the same node type. After installation completes,

each server is considered a standalone server and has the primary HA role. HA requires both primary and secondary servers, the role for one server needs to change. To change the HA role of a server from primary to secondary, use the **cmxha secondary convert** command in cmxadmin mode.

The Cisco CMX HA Admin interface is hosted on Cisco CMX port 4242 and can be accessed using http://*cmx_ip_address*:4242/. Log in to the web interface using *cmxadmin* as user ID and the password configured for cmxadmin during the primary and secondary server installation. This Cisco CMX HA Admin interface is different from the regular Cisco CMX interface that can be accessed at http://*cmx_ip_address*. Use the Cisco CMX HA Admin interface specifically monitoring and managing HA.

Every active Cisco CMX instance is backed by another (inactive) instance. The second CMX instance is not active until the failover procedure is initiated, either manually or automatically.

Initial HA configuration is dependent on data size. For example, for 5 GB of data, initial configuration could take up to 1 hour to complete. The average time for a failover condition is 7 minutes, depending on your systems. The failback time is dependent on the amount of data to resynchronize. For example, for 5 GB of data, the expected time for failback to complete is 1.5 hours.

You can enable HA by using either Cisco CMX web UI or CLI.

If your Cisco CMX setup with HA requires a forward proxy for internet access, you must configure the proxy and restart your Cisco CMX services. For more information about setting up outbound proxy, see Setting Up Outbound Proxy in HA-Enabled Setup, on page 190.

Note We recommend that you use the Cisco CMX web UI for HA configuration.

The High-Availability feature on Cisco CMX is part of the Cisco CMX Base license, which you would install on the primary HA server. The secondary HA server automatically receives a copy of the Cisco CMX license during sync up. There is no HA-specific license to install.

Tip Cisco CMX High Availability documentation is embedded in the product. From the Cisco CMX user interface, choose **Documentation** from the drop-down list on the top-right corner.

Pre-requisites for HA

- Both the primary and the secondary server should be of the same size and the same type (VM or physical appliance).
- Both the primary and the secondary server should have the same Cisco CMX version.
- Both the primary and the secondary server should be connected on the same subnet.
- Both the primary and the secondary server should be connected on the same subnet if Layer 2 HA is required.
- Both the primary and the secondary server should be IP connected with delay of less then 250ms if Layer 3 HA is used.
- From Cisco CMX release 10.6.2, NTP server settings must be configured on both Primary and Secondary server instance before HA pairing starts. We recommend that you use the same NTP server on both Primary and Secondary. As a Cisco CMX admin you can also use a dedicated NTP for Primary and Secondary.

Enabling High Availability for Cisco CMX Using the Web UI

Procedure

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

Step 2 Choose **System > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 Click **Settings** at the top-right corner of the window.

The **Settings** dialog box is displayed.

Step 4 Click the **High Availability** tab.

Step 5 Configure the following parameters:

- **Secondary IP Address**—Enter the IP address of the secondary server. The primary server will be continuously synchronized with the secondary server. If the primary server encounters any issues, the secondary server will take over the responsibility as the active server.
- **Secondary Password**—Enter the password for the *cmxadmin* user on the secondary server.
- **Use Virtual IP Address**— By default, this option is checked. (If you do not check this option, the **Virtual IP Address** field is dimmed, and this address will not be used for HA configuration.)

  If you decide to retain the default, enter the corresponding virtual IP address.
- **Virtual IP Address**—(Optional) Enter the virtual IP address for the HA pair if the **Use Virtual IP Address** check box is checked. .
- **Failover Type**—From the **Failover Type** drop-down list, choose **Auto** or **Manual**.

  Note
  - If you choose **Auto**, Cisco CMX automatically fail over to the secondary server when a serious issue is detected.
  - We recommend that you run the **cmxha failover** command on the primary active Cisco CMX appliance to verify automatic failover configuration.
  - You must not use the **cmxos shutdown**if the failover configuration is automatic.
  - If you choose **Manual**, manual intervention is required to initiate failover from the web interface or command line. The failure will be reported via a notification, but no action will be taken.

- **Notification Email Address**— Enter the email address to which HA notifications are to be sent. You can add multiple email addresses.

Step 6 To enable HA, click **Enable**.

Cisco CMX will verify the HA settings and start enabling HA between the primary and secondary servers.

NTP server settings must be configured on both Primary and Secondary server instance before HA pairing starts. Use the **cmxos ntp type** command to configure the NTP server.

```
[cmxadmin@server]# cmxos ntp type
Current NTP Type = <Not Set>
```

```
Select NTP Type [1] Unauthenticated, [2] Authenticated or [3] Skip [3]: 1

Changing the NTP Type = Unauthenticated
Please enter the NTP server name (blank for no NTP server) []: ntp.xyz.com
Setting ntp server ntp.xyz.com
```

Step 7 Click **Save**.

The initial synchronization of the primary and the secondary server takes time and the **System at a Glance** window displays the state as **Primary Syncing** while the synchronization is in progress. After the synchronization is complete, the primary server will be in the state **Primary Active** state. Also, after synchronization, an informational alert is generated in Cisco CMX and an email is sent to the addresses that have been provided, indicating that HA is enabled and synchronized successfully.

Tip Click the **Help** link in the top-right corner of the **Settings** dialog box to launch the HA online help. For more information about the HA installation process, see http://*cmx_server*/docs/ha/.

Enabling High Availability Using CLI

Procedure

Step 1 To enable HA using CLI, run the **cmxha config enable** command.

Step 2 Follow the command prompt and enter the HA parameters.

The HA options are similar to the ones available in Cisco CMX Web UI:

```
$ cmxha config enable

Are you sure you wish to enable high availability? [y/N]: y
Please enter secondary IP address: 192.0.2.250
Please enter the cmxadmin user password for secondary:
Do you wish to use a virtual IP address? [y/N]: y
Please enter the virtual IP address: 192.0.2.251
Please enter failover type [manual|automatic]: automatic
Please enter an email address(es) for notifications (Use space, comma or semicolon to
separate): email@cisco.com
Attempting to configure high availability with server: 192.0.2.250
Configuring primary server for HA
Configuring secondary server for HA
.....................................................................
Synchronizing Postgres data from primary to secondary
.........
Synchronizing Cassandra data from primary to secondary
.....................
Syncing primary files to secondary
Successfully started high availability. Primary is syncing with secondary.
```

High Availability State Information

The HA nodes are expected to be in the following states:

Table 18: HA State Information

Configuration Description	Node State
CMX HA is not configured. Two different standalone boxes and they are not paired.	Primary is not configured. Secondary is not configured.
Pairing has just started and system is attempting to synchronize data from the primary server to secondary server.	Primary is synchronizing. Secondary is synchronizing.
CMX HA is established, and Primary is actively synchronizing with the secondary server. Primary is serving in master role and secondary is in backup role.	Primary is active. Secondary is active.
The system has failed over to the secondary and the secondary is serving.	Primary failover is active. Secondary failover is active.

Replacing a Cisco CMX High Availability Unit

If you want to replace a failed primary server, follow the steps:

Procedure

Step 1 Perform a backup from the secondary HA server considering primary server is down.

Step 2 To disable HA, run the following command:

cmxha config disable

Note We recommend that before you disable HA ensure that all the services are up and running on the secondary server. After disabling HA, the secondary server will continue to serve and all the services on the secondary will be up and running.

Step 3 To convert the current secondary server into primary server, run the following command:

cmxha primary convert

Step 4 Replace the primary Cisco CMX box.

Step 5 Install the required SSL certificates on the new Cisco CMX box. For more information, see Installing Certificates in Cisco CMX. Certificates can be only installed on a primary server.

Step 6 Configure the new Cisco CMX box as a secondary server.

As part of synchronization, license will be automatically copied from active server.

Step 7 To enable HA configuration, run the following command:

cmxha config enable

High Availability Synchronization with Cisco MSE

High Availability synchronization with Cisco MSE 8.0.150.x and older versions is reporting a failure at 10% due to oracle certification validation issue. Cisco MSE exchanges Oracle Database Certificate between primary and secondary Cisco MSE. The validity of the Oracle Database Certificate is 10 years and once the validity of the certificate expires, Cisco MSE displays an error: ORA-29024: Certificate validation failure.

This certificate validation issue is not seen on standalone Cisco MSE. The primary MSE health-mointor.log displays the error: ORA-29024: Certificate validation failure, only when you pair HA. We recommend to install the patch on all Cisco MSE HA pairs as the validity of oracle certificate expired on 29 July 2021. This issue is not experienced with an existing working HA immediately, however, you will encounter this issue when you perform a HA pair setup again in future.

We recommend that you follow these steps to apply the patch:

Procedure

Step 1 Download the patch from the following path: http://172.19.35.252/mse8-releases/patches/oracle-cert-patch.tar.gz.

Step 2 Copy the patch under */root*.

README file and script to install the patch is available in this location.

Step 3 Follow the installation instructions in the README file.

Viewing Live System Alerts

Procedure

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

Step 2 Choose **System** > **Alerts**.

Step 3 In the **Live Alerts** window that is displayed, sort the alerts **By Severity, By Node,** or **By Service** using the drop-down list at the top-right corner.

To dismiss an alert, in the **Actions** column adjacent the corresponding node name, click the **Dismiss** icon.

Viewing Patterns

The **Patterns** window shows the pattern of a specific feature, such as client count, unique devices, and so on over the week for a selected time period. For example, if you select client count for the last 1 month, it shows which days or times of the week had the most client counts in the last 1 month. The larger dots indicates a larger count for the specific feature. You can hover cursor over the dots to interpret the pattern details.

- **Client Count**—Displays the total devices seen at a given time.

- **Location Calculation Time**—Displays the average amount of time, in milliseconds, taken by the Location algorithm, to calculate a client's location.
- **CPU Usage**—Displays the percentage of used CPU on a per-node basis.
- **Memory Usage**—Displays the percentage of used memory on a per-node basis.
- **Redis Connections Received**—Displays the total number of connections received by the cache service.
- **Locally Administered MAC count**—Displays the total number of iOS devices.

Note In Cisco CMX Release 10.2.3:

- The following pattern details are no longer available: Incoming Rate, Dropped Notifications, and NMSP LB Read Operations.
- In the **Select Criteria** drop-down list, the **iOS8 Devices** option is renamed to **Locally Administered MAC count**.

To view patterns:

Procedure

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

Step 2 Choose **SYSTEM > Patterns**.

The **Patterns** window is displayed.

Step 3 From the **Select Criteria** drop-down list, choose the criteria for which you want to view pattern data.

Step 4 From the **Select Date Range** drop-down list, choose the time frame for the criteria pattern.

Note By default, the pattern data is displayed for the last one week for all the nodes in the cluster. You can view the average for the days from Monday to Sunday at all times for the selected time frame.

Step 5 Optionally, from the **Select Server** drop-down list, choose the Cisco CMX node for which you want pattern data to be displayed. By default, the pattern data for all the Cisco CMX nodes in a cluster is displayed.

Understanding the Metrics Tab

The **Metrics** tab in the Cisco CMX System service enables you to view system metrics, database metrics, cache metrics, location metrics, and analytics notification mertics. Metrics information related to the following criterias are displayed:

- System Summary
- Node Mertics
- Database Metrics

- Cache Mertics
- Location Metrics
- Analytics Notification Metrics

Viewing System Summary Metrics

The **System Summary Metrics** window displays the following information:

- **Number of Active Clients**
- **Number of NMSP messages processed by the system per second, in the last one minute**
- **Overall CPU usage metrics**
- **Overall memory usage metrics**
- **Overall disk usage metrics**

Procedure

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

Step 2 Choose **SYSTEM > Metrics**.

The **System Summary** tab in the left pane is selected by default, and the corresponding details are displayed.

Viewing System Summary Metrics Using the Dashboard

Alternatively, to view the System Summary metrics from the Dashboard:

Procedure

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

Step 2 Choose **SYSTEM > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 In the **Services** column, click the **Configuration, Location Heatmap Engine, NMSP Load Balancer,** or **Proxy** icon to view the corresponding **System Summary** metrics.

Note Hover your cursor over the metrics and graphs for descriptions and details.

Viewing CMX Node Metrics

The **CMX Node Metrics** window for a Cisco CMX node displays the following information:

- **Number of active clients**
- **Location latency time**
- **Number of incoming and outgoing NMSP messages**
- **Number of Controllers**
- **CPU uesage metrics for each service**
- **Memory usage metrics for each service**
- **Disk IO metrics**
- **Disk usage metrics**
- **redis-iops**
- **jdbc-iops**
- **redis-errors**
- **jdbc-errors**

To view the Node metrics for a Cisco CMX node:

Procedure

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

Step 2 Choose **SYSTEM > Metrics**.

Step 3 In the left pane, click a Cisco CMX node name to view the metrics for that node.

Viewing CMX Node Metrics Using the Dashboard

Alternatively, to view the node metrics from the Dashboard:

Procedure

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

Step 2 Choose **SYSTEM > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 In the **Node** column, click a Cisco CMX node name to view the metric details for that node.

Note Hover your cursor over the metrics and graphs for descriptions and details.

Viewing Database Metrics

The **Database Metrics** window displays the following metrics:

- **Databse Size**—Shows the active memory used by the Cassandra and Postgres database.

To view the Database metrics:

Procedure

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

Step 2 Choose **SYSTEM > Metrics**.

Step 3 In the left pane, click **Database Metrics**.

Note Hover your cursor over the Database metrics graph for descriptions and details regarding the database usage.

Viewing Database Metrics Using the Dashboard

Alternatively, to view the database metrics from the Dashboard:

Procedure

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

Step 2 Choose **SYSTEM > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 In the **Services** column, click the **Database** icon.

Note Hover your cursor over the metrics and graphs for descriptions and details.

Viewing Cache Metrics

The **Cache Metrics** window displays the following metrics:

- **Blocked connections**—Shows the number of clients pending on a blocking call to finish.
- **Connected clients**—Shows the number of client connections in use.
- **Used memory**—Shows the total number of bytes allocated by Redis using its allocator .
- **Evicted keys**—Shows the number of evicted keys due to maxmemory limit.

To view the Cache metrics:

Procedure

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

Step 2 Choose **SYSTEM > Metrics**.

Step 3 In the left menu, click **Cache Metrics**.

Viewing Cache Metrics Using the Dashboard

Alternatively, to view the Cache metrics from the Dashboard:

Procedure

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

Step 2 Choose **SYSTEM > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 In the **Services** column, click the **Cache** icon.

Note Hover your cursor over the metrics and graphs for descriptions and details.

Viewing Location Metrics

The **Location Metrics** window displays the following metrics for each Cisco CMX node:

- **Location Counts**—The total computations done per second.
- **Location Times**—The location calculation time includes the mathematical portion of the location computation, and in most cases, is about 10 to 20 milliseconds. The location latency is the total time of latency computation from when the message comes from NMSPLB, to location, aggregation, creating cache, and calculation.
- **Location and Nmsplb Location and Nmsplb**—The rate of Network Mobility Service Protocol (NMSP) messages coming in to the NMSPLB.
- **Hyperlocation Rates**—The rate of incoming hyperlocation messages.
- **Location Computation**—The chart for location computation.

To view the Location metrics:

Procedure

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

Step 2 Choose **SYSTEM > Metrics**.

Step 3 In the left pane, click **Location Metrics**.

Viewing Location Metrics Using the Dashboard

Alternatively, to view the Location metrics from the Dashboard:

Procedure

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

Step 2 Choose **SYSTEM > Dashboard**.

The **System at a Glance** window is displayed.

Step 3 In the **Services** column, click the **Location** icon.

Note Hover your cursor over the metrics and graphs for descriptions and details.

Viewing Analytics Notification Metrics

The **Analytics Notification Metrics** window shows the most important performance indicators relating to the Analytics service. A notification is sent from the Location service to the Analytics service when significant movement is detected from a device. Each notification contains an update on the location of a single device.

The Analytics Notification Metrics window displays the following metrics for each Cisco CMX node:

- **Notification processing time**—The average time taken to process an incoming notification. This time will depend on a number of factors, but most notably, the size of the network, that is, the number of buildings, floors, zones, tags, and so on. This metric is relatively stable although you can expect peaks when the system is starting up.
- **Notification queue size**—The size of the queue for incoming notifications, which are queued before being processed. Depending on the system load, the Location service will send the notifications in batches. Therefore, you can always expect a queue of size greater than 0. This mechanism may also result in a very irregular graph at some zoom levels, that is, one with many ups and downs. This is the expected behavior. The queue size is expected to rise when the incoming rate increases. If it continues to grow, you will begin to see dropped notifications in the Notification dropped rate metric
- **Notification dropped rate**—The size of the queue for incoming notifications is limited. Hence, if the queue gets too big, notifications will be rejected. The **Notification dropped rate** graph shows how many notifications are rejected per second. Ideally, you require this chart to show a flat line of 0. If it does not show 0, you should consider adding another server to the cluster for running the Analytics service. This will distribute the load over the two servers.
- **Notification incoming rate**—This is the number of notifications received by the Analytics service per second. This trend should roughly equal the client count, that is, the more clients are detected by the Location service, the more notifications are expected. However, the trend is also influenced by the clients' movement rates because notifications are only sent when the location of a device changes.

To view the Analytics Notification metrics:

Procedure

Step 1 Log in to Cisco Mobile Connected Experiences (Cisco CMX).
Step 2 Choose **SYSTEM > Metrics**.
Step 3 In the left pane, click **Analytics Notification Metrics**.

Viewing Analytics Notification Metrics Using the Dashbaord

Alternatively, to view the Analytics Notification metrics from the Dashboard:

Procedure

Step 1 Log in to Cisco Mobile Connected Experiences (Cisco CMX).
Step 2 Choose **SYSTEM > Dashboard** .

The **System at a Glance** window is displayed.

Step 3 In the **Services** column, click the **Analytics** icon.

Note Hover your cursor over the metrics and graphs for descriptions and details.

Viewing Presence Metrics

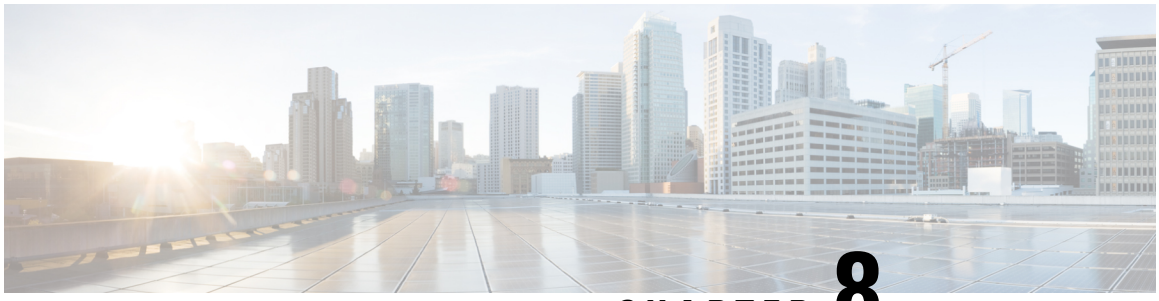
The **Presence Metrics** window displays the following metrics:

- **Presence Counts**
- **Presence Rates**

To view the Presence metrics:

Procedure

Step 1 Log in to Cisco Mobile Connected Experiences (Cisco CMX).
Step 2 Choose **SYSTEM > Metrics**.
Step 3 In the left pane, click **Presence Metrics**.



CHAPTER 8

Performing Administrative Tasks

This chapter describes how to perform administrative tasks using Cisco CMX. Users who are assigned administration privileges can perform administrative tasks.

Cisco CMX User Accounts

Prior to Cisco CMX 10.2 all Cisco CMX processes ran under the Linux root user account. Cisco CMX 10.2 introduces two new user accounts (cmx and cmxadmin) to prevent any potential risks and secure the system.

- root—Root user account. Users should not use this account.

Note The password of the root account is now being set and maintained by the system owners, and no longer has a default password configured. This way, the account is still available for special-case installation and tackling debugging issues, and the root user will be owned by the end-user. Password recovery is accomplished through the use of the single user login process. For more information see Resetting Password - Cisco CMX Release 10.6 and Later with CentOS 7.0, on page 228.

- cmx—A no login account that now owns all the CMX processes with the exception of postgress.

- cmxadmin—Primary account used for the performance of all administrative tasks using CLI. User will *sudo* from this account to perform tasks requiring root-level access. This account is used to upgrade Cisco CMX 10.2 to a future release using GUI.
- admin—Admin user account for configuring maps, and Cisco WLCs, and restart services using Cisco CMX Web UI.
- normal user accounts—User-defined accounts.

Note From Cisco CMX Release 10.5.0, you must install the root patch to access root user account. For more information about transferring and installing patches, see Transferring and installing patches on CMX 10.6 and above.

Unlocking Users

You can unlock CMX access for a command line interface (CLI) or graphical user interface (GUI) user after they have been locked out, using the **cmxctl users unlock** command. For caveats and full details, refer to 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

Before you begin

You must have root access credentials to modify these settings.

Procedure

Step 1 Connect to CMX via SSH.

Step 2

Step 3 Enter one of the following commands to unlock a CMX user:

- **cmxctl users unlock cli** *username* to unlock a CLI user.
- **cmxctl users unlock gui** *username* to unlock a GUI user.

The user can log in again from the user interface you unlocked.

Setting Strong Password Authentication

You can enable strong password authentication with or without enabling FIPS or UCAPL mode. If you do plan to enable FIPS or UCAPL, set the correct minimums for that mode.

Before you begin

You must have CMX root user credentials to modify these settings.

If FIPS or UCAPL is enabled, you must connect directly from the console, or access the console through VMware VSphere client.

Procedure

Step 1 Connect to CMX via SSH.

Step 2 Enter the **cmxctl config auth settings** command to set password authentication settings.

Step 3 Respond to the following prompts:

Prompt	Action
Enable strong password [yes / no] [yes]:	Enable strong password authentication. Default is yes. UCAPL: Yes. **Note** If **Enable strong password** is set to **Yes**, you can extend the password upto 127 characters. However, we recommend you to ensure that password should have minimum one lower case, one upper case, one digit and a special character.
Minimum password length [8-20] [8]:	Set minimum password length. Range is 8-20 characters. Default is 8 characters. CMX default: 8 characters.
Maximum password lifetime [1-9999] [9999]:	Duration after which password will expire. You must change password before the password expires. Range is 1-9999 days. CMX default: 9999 days. characters.

Prompt	Action
Password Expiry Warning Period [1-30] [14]:	Password expiry warning period duration. Range is 1-30 days. CMX default: 14 days. characters. **Note** If the password of Cisco CMX user is going to expire within the duration specified, then a warning message is displayed about the password expiry immediately following the login. On the Cisco CMX GUI, an alert window is displayed showing when the password is going to expire. If you are logging into Cisco CMX using SSH and the Cisco CMX CLI account for which the password is going to expire within the specified warning period, a warning message is printed just after the login successful message and before the command prompt. If password is already expired, then you will be redirected to change the password immediately after the login.
Unsuccessful login attempts before account lock [3-5] [3]:	Set the number of times a user can attempt to login before they are locked out for 30 minutes. Range is 3-5. Default is 3. CMX default: Not required.
Fail interval in minutes [1-120] [15] :	Set the fail interval time in minutes. Range is 1-120. Default is 15. Fail interval time is automatically set to 15 minutes when UCPAL mode is enabled.
Account lockout interval in minutes [1-120] [30] :	Set the account locakout interval time in minutes. Range is 1-120. Default is 30.
Set session timeout in minutes [1-720] [30] :	Set the number of minutes a user can be inactive on the system before CMX times out. Range is 10-120 minutes. There is no default session timeout. CMX default: Not required.

Cisco CMX then restarts its authorization services.

Resetting Cisco CMX GUI Administrator Password

The GUI admin user password can be reset to the default of admin from the Cisco MSE CLI using the following command:

cmxctl users passwd username

Note You should know the cmxadmin user password for CLI access. If you do not know the current cmxadmin password, follow the guidelines to reset the root password. For more information, see and Resetting Root Password - Cisco CMX Release 10.4 and Earlier with CentOS 6.0, on page 227 and Resetting Password - Cisco CMX Release 10.6 and Later with CentOS 7.0, on page 228.

Resetting Root Password - Cisco CMX Release 10.4 and Earlier with CentOS 6.0

Cisco CMX uses a single user mode to reset the root/cmxadmin user passwords.

To enter into the single user mode you require:

- A (non-SSH) console connection to the Cisco Mobility Services Engine (Cisco MSE).
- A power-cycle of the Cisco MSE appliance

For Cisco CMX Release 10.4 and below with CentOS 6.0 operating system to reset the root or cmxadmin password, perform the following tasks:

Procedure

Step 1 Establish console access.

Step 2 Power on the Cisco MSE.

Step 3 Press the Up arrow key within 6 seconds of the first text appearing on window.

Step 4 When the GRUB menu is displayed:

a) Verify if the first entry is highlighted.
b) Press the **e** key to edit.

Step 5 Use the Down arrow key to highlight the entry that begins with the word *kernel*.

a) Press the **e** key to edit the entry.
b) Press the space bar, type the word **single**, and then press Enter.
c) Press the **b** key to boot the selected entry.

Step 6 After the system boots and you are at the # prompt:

a) Enter **passwd** <*username*> and press Enter.
b) When prompted, enter the new password for the user (root/cmxadmin) and press Enter.
c) Re-enter the password to verify.

Step 7 Type **reload** and press **Enter** to reboot the system and load the Cisco CMX services.

Resetting Password - Cisco CMX Release 10.6 and Later with CentOS 7.0

To recover a password, console access is mandatory. Console access can be a VM console or a physical console depending on the type of appliance used in the deployment.

Procedure

Step 1 Establish console access.

Step 2 Break the boot sequence on the GRUB screen.

Step 3 Choose the entry for the **Rescue** mode and then press the e.key to edit.

If prompted for username or password, enter the credentials as username: **root** password: **password** (not the configured root password).

Step 4 In the code, navigate to the line **linux16** and remove the last 2 parameters for **rhgb** and **quiet**.

Step 5 Add **rd.break enforcing=0** in the same **linux16** line.

Step 6 Press **Ctrl+X** to restart with the new parameters. After the system reboots, you are at the **switch_root:/**# prompt.

Step 7 Use the **# mount -o remount,rw /sysroot** command to mount the partition in read/write mode.

Step 8 Use **# chroot /sysroot** option to change the filesystem root.

Step 9 Use the **# passwd** command and enter the new root password.

Step 10 Use the **# mount -o remount,ro /** command to re-mount the partition in read-only mode.

Step 11 Enter the **exit** command twice to reboot the system and load the Cisco CMX services. The root password is successfully reset.

Setting Up Audit Logging

You can enable remote logging of system events, and specify which syslog events you want to log and view.

Before you begin

You must have CMX root user credentials to modify these settings.

Procedure

Step 1 Connect to CMX via SSH.

Step 2 Enter the **cmxctl config audit settings** command.

Step 3 Respond to the following prompts. **`Enter`** selects the prompt default, shown in [brackets].

Prompt	Action
Enable or Disable Remote Syslogging [Enable / Disable] [Enable]:	Choose whether CMX should log system events. Options are Enable or Disable, and defaults to enable.
If logs size goes beyond 1 gb, drop or overwrite messages? [drop / overwrite] [overwrite]	Select CMX behavior when log size exceeds 1 gigabyte. Options are drop and overwrite, and defaults to overwrite.
Please enter rsyslog port [514]:	Optional. Enter the port number of a remote syslog server if you want to enable remote audit logging. The default is port number 514.
Please enter rsyslog DNS:	Optional. If your system uses a domain name server (DNS) for authentication, enter the DNS address here. There is no default. For example, *yoursyslogserver.yourco.com*
Please enter the email IDs (comma separated) for mail alerts:	List email IDs which need to receive important email alerts about audit logging.

A confirmation message displays.

```
Remote Audit Logging = Enabled
```

Step 4 Select the events you want CMX to log. Yes logs all events. No prompts you to select the event types you want to log, and confirms the update.

```
Show all logs [yes/no] [yes]: no
Enter day [today(1)/yesterday(2)/last week(3)/last month(4)/all(5)] [5]:
Enter event type [MGMT_EVENT(1)/CONN_EVENT(2)/AUTH_EVENT(3)/CONF_EVENT(4)/ALL(5) [5]:
Enter identity [root(1)/admin(2)/all(3)] [3]:
Enter status [success(1)/failure(2)/all(3) [3]:

Settings saved.
```

CMX then restarts the affected loggers.

Example

This example shows how to log everything except Connection, Management, and Misc events.

```
[root@server]# cmxctl config audit settings enable

Enable or Disable Audit Logging [Enable / Disable] [Enable]:enable
If logs size goes beyond lgb, drop or overwrite messages? [drop / overwrite]
[overwrite]:overwrite
Please enter rsyslog IP: 168.172.1.20
Please enter rsyslog port [514]: 514
Please enter rsyslog DNS: sls1296@wowco.com
Please enter the email IDs (comma separated) for mail alerts: email@example.com

Remote Audit Logging = Enabled

Please select the events to be logged
All Events [yes/no] [yes]: no
Connection Events [yes/no] [yes]:no
```

```
Management Events [yes/no] [yes]:no
Auth Events [yes/no] [yes]:
Configuration Events [yes/no] [yes]:
Security Configuration Events [yes/no] [yes]:
Security Events [yes/no] [yes]:
Misc Events [yes/no] [yes]:no
Settings saved.
```

Performing Scheduled Backup for Cisco CMX

You can use SSH File Transfer Protocol (SFTP) or Secure copy protocol (SCP) commands for backing up and restoring data on Cisco CMX 10.x. We recommend you to follow the below best practice for data backup automation.

Note Cisco CMX does not support File Transfer Protocol (FTP) commands for managing data.

Procedure

To schedule a Cisco CMX backup capability, run the **cmxos backupsched** command.

For more information, see the Cisco CMX command reference guide.

Performing Manual Backup for Cisco CMX

After you install and run Cisco CMX successfully, you can take a backup to avoid losing any data.

You may lose data on your CMX server, if:

- The hard disk in your CMX server fails
- The data on your CMX server is corrupted while upgrading

Therefore, backing up your data enables you to restore it to the original state. You can back up data on either /tmp or /opt partition. The /tmp folder is allocated 25 GB storage.

If Cisco CMX contains huge amount of saved data, the backup operation will take up extra disk space. In that case, you can consider the following:

- Back up to an external drive if there is not enough space on the Cisco CMX server. You can perform this operation by plugging in a removable hard disk or a mounted hard disk.
- After the backup operation, move the backup file (using scp) to a different server and remove it from the Cisco CMX server.

You can backup data such as location history, current client location, floor maps, and licenses.

Note We recommend that you backup database, floormaps, license and setup components to be compliant with General Data Protection Regulation (GDPR).

The following components are included in the backup:

- Database—Stores configuration data, such as, maps, controllers, location, and aggregated analytics data.
- Cache—Stores analytics repeat visits.
- Cassandra—Stores location history data and analytics raw visits.
- Influxdb—Stores metrics data for systems.
- Consul—Stores Consul configurations.
- Floormaps—Stores floor images for UI display.
- Licenses—Stores Cisco CMX license information.
- Setup—Stores CMX setup data.
- Conf—Stores node configurations.

Procedure

To perform a backup operation, run the **cmxos backup** command using the cmxadmin (non-root user) account.

You can include the -i (for example, cmxos backup -i database) parameter with the backup so that you can choose the components that you want to include in the backup.

The other backup options available are:

- **--all**—Include influxdb in the backup. The default is without influxdb and only includes postgres and Cassandra data.
- **--path**—Specify a location for the backup file. The default location is /tmp.
- **--online**—Perform the backup without stopping cmx services.
- **--offline**—Stop cmx services first and then perform the backup.

Note
- The destination directory for backup file requires rwx permission. When you specify a backup directory other than /tmp, ensure that the directory has "r/w/x" permission by user:cmx.
- If High Availability is enabled on Cisco CMX, online backup is supported only on primary and not secondary. If High Availability is disabled, online and offline backups are supported on both primary and secondary.

The following is a sample output from the **cmxos backup** command:

```
[cmxadmin@test ~]$ cmxos backup
Please enter the path for backup file [/tmp]: /tmp
[17:01:30] Preparing for backup...
Data size 287388806
Available disk space 139165282304
```

```
Pre-backup took: 0.0118758678436 seconds
['database', 'cache', 'cassandra', 'influxdb', 'consul', 'floormaps', 'licenses' , 'setup',
 'conf']
[17:01:30] Backup Database...
Backup database took: 1.15777993202 seconds
[17:01:32] Backup Cache...
Backup cache took: 0.383176088333 seconds
[17:01:32] Backup Cassandra...
Backup Cassandra DB took: 2.99715185165 seconds
[17:01:35] Backup InfluxDb...
Backup Influx DB took: 0.0846002101898 seconds
[17:01:35] Backup Consul...
Backup Consul took: 0.0185141563416 seconds
[17:01:35] Backup Floormaps...
Backup floor maps took: 0.000938892364502 seconds
[17:01:35] Backup licenses...
Backup licenses took: 0.000122785568237 seconds
[17:01:35] Backup setup...
Backup setup took: 0.000464200973511 seconds
[17:01:35] Backup node configuration...
Backup configuration took: 0.476609945297 seconds
[17:01:35] Creating tar file..
Post backup took: 16.3115179539 seconds
[17:01:52] Done Backup. Created backup file
/tmp/cmx_backup_test.cisco.com_2015_07_28_17_01.tar.gz
[cmxadmin@test ~]$
```

What to do next

You can automate the backing up process. For more information, see Performing Scheduled Backup for Cisco CMX, on page 230.

Increasing the Hard Disk Space

You can increase the hard disk space if your Virtual Machine that runs Cisco CMX is run out of disk space for backup.

Procedure

Step 1 Stop all the Cisco CMX services by entering the following commands:

cmxctl stop

cmxctl stop -a

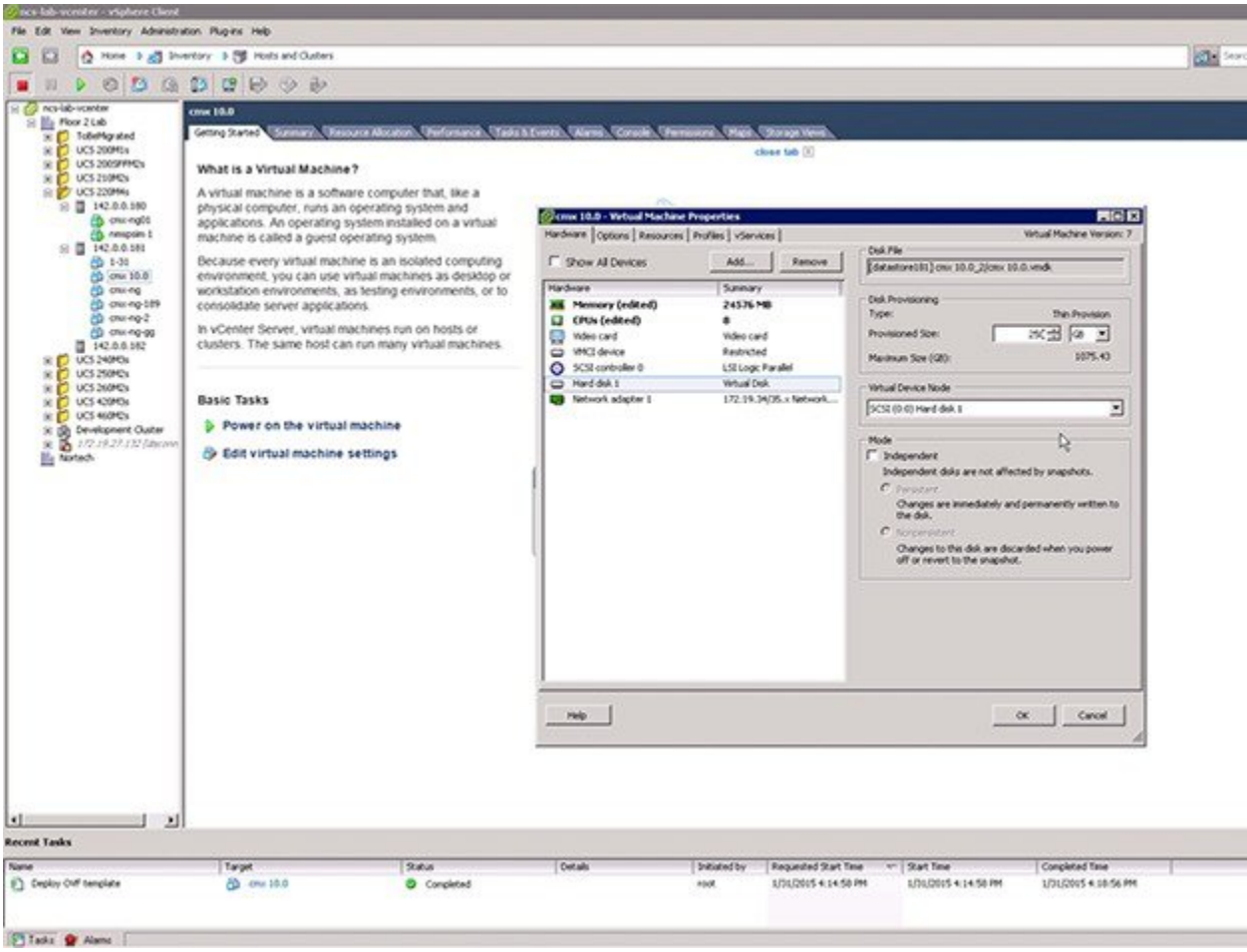
Step 2 Shutdown the virtual machine by entering the following command:

Shutdown –h now

Step 3 Edit the virtual machine settings and increase the hard disk space.

Note You cannot increase the hard disk space if the virtual machine was ever restored from snapshot.

Figure 31: Virtual Machine Settings



Step 4 Reboot the virtual machine.

After performing these steps, you can back up Cisco CMX.

You can enter the **cmxctl status** command to verify the status of CMX services. If any of the services is not running, you may need to restart it by entering the **cmxctl restart** <*service name*> command.

Restoring Data

After the backup, you can save the backup file in a safe location. If required, you can restore from this location.

To restore data, the Cisco CMX server must have free disk space which is 4 times the size of the backup file. If there is not enough disk space in the Cisco CMX server, you must increase the disk space. For more information, see Increasing the Hard Disk Space.

Note

- The restore of backup data on a third-party server is not allowed.
- Restoring Cisco CMX data must be done on a device that has the same local time as the device from which the data is collected.
- Otherwise, you will not be able to correctly access the analytics data. In addition, the data will result in errors or zero values on reports.

Procedure

To restore the data, enter the **cmxos restore** command using the cmxadmin (non-root user) account.

You can include the -i (for example, cmxos restore -i database) parameter with the **restore** command so that you can choose the components that you want to restore.

The following is a sample output from the **cmxos restore** command:

```
[cmxadmin@cmx~]# cmxos restore
Please enter the backup file path: /tmp/cmx_backup_test.cisco.com_2015_07_28_17_01.tar.gz
Please enter the path for untar backup file [/tmp]: /tmp
[17:08:54] Preparing for restore...
Restore size 27866720
Available disk space in /tmp is 139137040384
Available disk space is 139424529077
[17:08:54] Untarring backup file...
[17:08:55] Stopping all services...
Pre restore took: 26.4669179916 seconds
[17:09:21] Restoring Database...
Created database mse
Running command /usr/bin/sudo -u postgres  pg_restore -d mse -Fc
/tmp/cmx_backup_test.cisco.com_2015_07_28_17_01/postgres/mse.dump
Restored database mse
Restarting database...
Restore database took: 18.3071520329 seconds
[17:09:39] Restoring Cache...
Stopping cache_6383...
Restarting cache_6383...
Stopping cache_6380...
Restarting cache_6380...
..............
Stopping cache_6382...
Restarting cache_6382...
Stopping cache_6379...
Restarting cache_6379...
Stopping cache_6381...
Restarting cache_6381...
Stopping cache_6378...
Restarting cache_6378...
Restore Cache took: 46.7663149834 seconds
[17:10:26] Restoring Cassandra...
Stopping Cassandra...
Starting casandra
Creating cassandra scehma
..............
Restore Cassandra took: 29.5983269215 seconds
[17:10:56] Restoring Influxdb...
Stopping Influxdb...
```

```
Restarting Influxdb...
Restore Influx DB took: 13.9934449196 seconds
[17:11:10] Restoring consul...
Restore Consul took: 0.761927843094 seconds
[17:11:10] Restoring floormaps...
Restore floor maps took: 0.0269021987915 seconds
[17:11:10] Restoring licenses...
Restore licenses took: 0.00019907951355 seconds
[17:11:10] Restoring setup...
Restore setup took: 0.000532150268555 seconds
[17:11:10] Running Post Restore Tasks...
[17:11:10] Migrating Schemas...
[17:11:11] Migrating Cassandra schemas...
[17:11:12] Restarting all services...
stopping cassandra
Post restore took: 6.64956212044 seconds
[17:11:17] Starting all services...
..............
[17:12:45] Done
$
```

Encrypting the CMX /opt Directory

You can elect to encrypt CMX data in one of two ways:

- **CMX installation.** You have the option to encrypt the `/opt` partition of the disk as part of the installation process, or to skip it. Refer to *Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX, release 10.5* for more details.
- The **cmxos encryptdisk** command. You have the option to run the encryption command after installation. The following task uses this option. Refer to *Cisco CMX Command Reference, release 10.5* for more details.

Note We recommend that you enable encryption at installation, or as soon as possible afterward. The encryption process requires time proportional to the amount of data present on the `/opt` partition.

Important Encryption cannot be disabled or undone. It requires someone with root access credentials to manually enter the encrypted disk passphrase from the command line each time the device is rebooted or powered up.

Before you begin

You must have CMX root user credentials to modify these settings.

Procedure

Step 1 Connect to CMX via SSH, or through the console if FIPS or UCAPL is enabled.

Step 2 Enter the **cmxos encryptdisk** command.

Step 3 At each of the following prompts, enter **y** to stop CMX and backup your data, or **N** to cancel. Data backup could take some time.

```
Have you closed all SSH sessions to this CMX? [y/N]:y
Are you sure you want to encrypt the /opt partition of the disk ? [y/N]:y

Checking disk space requirements for backing up /opt folder...
Looks Good.

Proceed with stopping all CMX services? [y/N]:y

Backing up /opt folder into /var ...
tar backup done.
Press Enter key to enter rescue mode and begin the encryption.
```

Step 4 Press **Enter** to continue. This process can take some time.

```
Shredding /opt ...
Shread: List of deleted folders
Shread: List of deleted folders
Shread: List of deleted folders
...
Formatting /opt ...

You will be prompted to set a passphrase for encrypted disk /opt.
Choose a passphrase, Enter and Verify it.

Note:
On every boot / power up, you will be prompted for this passphrase.
System will continue only if this passphrase is correct.
```

Step 5 Respond to the following prompt. If you enter **YES**, encryption is irreversable.

```
WARNING!
========
This will overwrite data on /dir/your_cmx/opt irrevocably.
Are you sure? (Type uppercase yes): YES
```

Step 6 Follow the prompts to select and confirm the encrypted disk passphrase.

```
Enter passphrase:
Verify passphrase:
Command successful.

Opening /opt ...
Enter passphrase for /dir/your_cmx/opt:
```

At this point, the encryption process begins in earnest. This process can take some time.

Step 7 When the process completes, press **Enter** at the prompt to reboot the disk.

```
Encryption of /opt is complete.

System will reboot now.
Upon (every) restart, when prompted to enter passphrase for /opt partition,
enter the passphrase you just set.

Press Enter to continue with reboot
```

Step 8 Once the system reboots, enter the encrypted disk passphrase at the prompt.

```
Please enter passphrase for disk device_name_opt on /opt!:
```

Step 9 Log into Cisco CMX command line.

Display a Login Banner

You can create a banner that displays when users log into CMX.

Before you begin

You must have CMX root user credentials to modify these settings.

Procedure

Step 1 Connect to CMX via SSH.

Step 2 Enter the **cmxctl config banner edit** command.

If there is an existing banner, CMX displays the text [within brackets]. If none, the brackets are empty.

Step 3 Enter the banner text:

a) Type the text you want to display, and press **Enter**.

b) On the second line, type a period, and press **Enter**.

Your new banner will display the next time a user logs in from a browser or from the command line.

Note Use the **cmxctl config banner show** command to display the login banner.

Use the **cmxctl config banner disable** to disable the login banner.

For more information about the **cmxctl config banner** command, see https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_command/cmxcli106.html.

Example

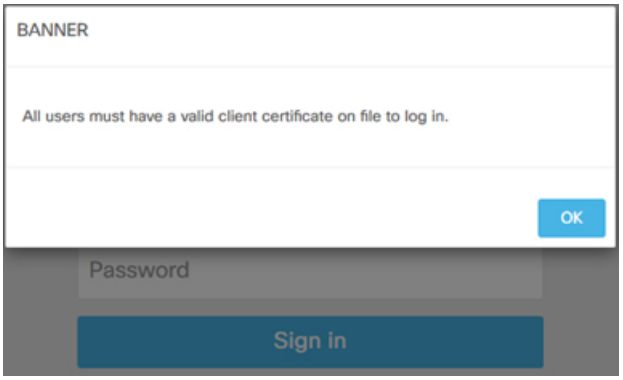
This example creates the following login banner: "All users must have a valid client certificate on file to log in."

```
Current Login Banner = []
Enter text to be displayed as login banner. Enter a single period on a line to
terminate.

All users must have a valid client certificate on file to log in.
.
starting /usr/sbin/sshd... \c
done.
```

When you opened CMX in a browser, you would see something similar to this:

Figure 32: Example of a login banner from a browser



Logging in from the command line, you would see something similar to this:

```
login as: cmxadmin
All users must have a valid client certificate on file to log in.
cmxadmin@192.168.1.20's password:
```

Managing NTP Servers

You can set up multiple Network Time Protocol (**NTP**) servers in Cisco CMX. You can add 2 types of NTP servers in Cisco CMX – unauthenticated NTP Server and and authenticated. You can add either a single unauthenticated NTP server or add up to 2 authenticated NTP servers.

Configuring Authenticated NTP Server

Before you begin

You need to decide on a local password for CMX's NTP client.

Procedure

Step 1 On NTP Server, run the **ntp-keygen -e -c RSA-SHA1 -p <server_password> -q <client_password>** command to export an IFF Key. Note that you must use the local password of the CMX NTP client for executing this command.

The command output is displayed as follows:

```
[cmxadmin@cmx]# ntp-keygen -e -c RSA-SHA1 -p <server_password> -q <client_password>
Using OpenSSL version OpenSSL 1.0.1e-fips 11 Feb 2013
Using host test group ntpserver
Using host key ntpkey_RSAhost_ntpserver.3747444855
Using host key as sign key
Using IFF keys ntpkey_IFFkey_ntpserver.37474448555
Writing IFF parameters ntpkey_iffpar_ntpserver.3747444855 to stdout
# ntpkey_iffpar_ntpserver.3747444855
# Mon Oct  1 21:54:15 2018

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

```
MIG0AgEAMIGpBgcqhkjOOAQBMIGdAkEAvi39ekol/VjRa5J8D329KUY+U6V63XBE
6xOFGlSFIii/3j87ZEy5U7M6aJte8N0RFrR/HNdXl2HUAsEPyYXjmwIVALVEPtki
j4NB7b7lDgq7VWwhIcwDAkEAnMdvYaA4AA4DCeiszaTecVAtRnuZlajE8r7+hq64
hR+/ircsjjICmrgCdJXrgv+NDRi6L48LBGHyCbrsK5TiNAQDAgEB
-----END PRIVATE KEY-----
Writing IFF keys ntpkey_iffkey_ntpserver.3747444855 to stdout
# ntpkey_iffkey_ntpserver.3747444855
# Mon Oct  1 21:54:15 2018

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIH9MEAGCSqGSIb3DQEFDTAzMBsGCSqGSIb3DQEFDDAOBAj8r+RVOkTclgICCAAw
FAYIKoZIhvcNAwcECGQosPZ3xNr9BIG4AozI6FFAlP1M+O9JI3SA+iDmamB7ONwl
iXzmVJgspncg5NXwU3AJYxhNHvRN+/ENWdiUev3vRcCdvFHOF5HDiAHYSx0OTtQE
749FmolxuWq+Fsy6KDDH+EmcgKOEjFtnNu7z7Y7dBeGlrFxBnctAtbyhjzZVMnCf
jIwaSyySquA38OlMii7LEuCVuUBzJvcOjLHqVOpIphZUUnMPs9+cthzlIC3HChGB
nYHFkDVUvuLIcRiUDILb/g==
-----END ENCRYPTED PRIVATE KEY-----
```

Step 2 From the command output, copy or export the the ENCRYPTED PRIVATE KEY block along with preceding 2 comment lines into a file.

Step 3 SCP the file to Cisco CMX server.

Step 4 Connect to CMX command line either from a console, or from a VMWare vSphere console.

Step 5 To delete all the NTP configurations, run the **cmxos ntp clear** command.

Step 6 To configure authenticated NTP server, run the **cmxos ntp type** command, followed by the IP addresses of the NTP server.

```
[cmxadmin@cmx]$ cmxos ntp type
Current NTP Type = <Not Set>
Select NTP Type [1] Unauthenticated, [2] Authenticated or [3] Skip [3]: 2

Changing the NTP Type = Authenticated
Enter local password:
Repeat for confirmation:
Password changed and host key/cert file generated successfully.

Enter hostname / IP for NTP Server #1 (blank to skip) []: 172.19.28.54
Please enter complete path of exported IFF (encrypted) key file: /tmp/iffkey
Checking if server 172.19.28.54 is reachable ...
OK
Key file successfully saved as ntpkey_iffkey_cmx-vmdev334.3747444855
NTP Server added successfully

Enter hostname / IP for NTP Server #2 (blank to skip) []:
```

Step 7 Repeat step 6 to add the second NTP server.

Note that you need to wait for a few minutes for the NTP servers to sysnchronize.

Step 8 (Optional) To verify the status of the NTP server configuration, run the **cmxos ntp status** command. Add **`--verbose`** to get detailed status.

```
[cmxadmin@cmx]# cmxos ntp status
NTP Type = Authenticated
Status   = Synchronized

[cmxadmin@cmx-vmdev281 ~]$ cmxos ntp status --verbose
NTP Type = Authenticated
Status   = Synchronized

synchronised to NTP server (1.2.3.4) at stratum 3
   time correct to within 990 ms
```

```
   polling server every 64 s

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*1.2.3.4              1.8.8.5     2 u   46   64   37    0.585   10.659   8.258

ind assid status  conf reach auth condition  last_event cnt
===========================================================
  1  4891  f63a   yes   yes   ok   sys.peer    sys_peer  3
```

Note If you want to change NTP type from unauthenticated to authenticated or vice versa, you can change it using following commands:

a. Run the **cmxos ntp clear** command to clear current NTP settings.

b. Run the **cmxos ntp type** command to select appropriate type.

Configuring Unauthenticated NTP Server

To add unauthenticated NTP server, follow these steps:

Procedure

Step 1 Connect to CMX command line either from a console, or from a VMWare vSphere console.

Step 2 To delete all the NTP configurations, run the **cmxos ntp clear** command.

Step 3 To configure unauthenticated NTP server, run the **cmxos ntp type** command, followed by the IP addresses of the NTP server.

Step 4 (Optional) To verify the status of the NTP server configuration, run the **cmxos ntp status** command.

Updating Auntenticated NTP Server Parameters

To update configured authenticated NTP server parameters, follow the steps:

Procedure

Step 1 To change the local password and set a new password, run the **cmxos ntp auth password** command.

1. If you want to change the local password, execute cmxos ntp auth password command and set the new password

```
[cmxadmin@cmx]# cmxos ntp auth password
Enter local password:
Repeat for confirmation:
Password changed and host key/cert file generated successfully.
[cmxadmin@cmx-vmdev282 ~]$
```

Step 2 To add/delete NTP server details, run the **cmxos ntp auth servers** command.

```
[cmxadmin@cmx]# cmxos ntp auth servers

Server 1 is already configured with IP 1.2.3.4

Do you want to (1) Edit (2) Delete (3) Skip ? [1]: 3
Enter hostname / IP for NTP Server #2 (blank to skip) []: 1.2.3.5
Please enter complete path of exported IFF (encrypted) key file: /tmp/iffkey2
Checking if server 1.2.3.5 is reachable ...
OK
Key file successfully saved as ntpkey_iffkey_ntpserver2.3747444855
NTP Server added successfully

NTP Service restarted successfully
```

Note If you need to restart NTP service, run the **cmxos ntp restart** command. It will restart NTP daemon. Run **cmxos ntp status** command to check the NTP status. You can add **--verbose** option to the command if you want detailed output.

```
[cmxadmin@cmx]# cmxos ntp restart
NTP Service restarted successfully
```

Troubleshooting Cisco CMX Server Shutdown Problems

The Cisco CMX server shuts down all the services when disk space usage reaches 85 percent. If you encounter this issue, create additional disk space on your Cisco CMX server by deleting unnecessary files, if any, from the server. Run the cmxos clean find/normal command to find unnecessary files and delete it to free some disk space.

After you have sufficient space, you can choose to restart your Cisco CMX server by running the **cmxctl start –a** command, if required.

Performing Periodic Maintenance for Cisco CMX

We recommend that you schedule a maintenance window every two months to perform Cisco CMX software restart (system, application services). This periodic maintenance can be performed on both HA and standalone setups. It will take up to 5 mins and help Cisco CMX to reclaim system resources yielding better performance. From the operations perspective this would result in scheduled downtime of approximately 30 mins per year.

Note 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, follow the steps

Procedure

Step 1 To shut down a Cisco CMX service, run the following command:

cmxctl stop -a

Step 2 To kill services, run the following command:

cmxos kill

Step 3 To restart agent, run the following command:

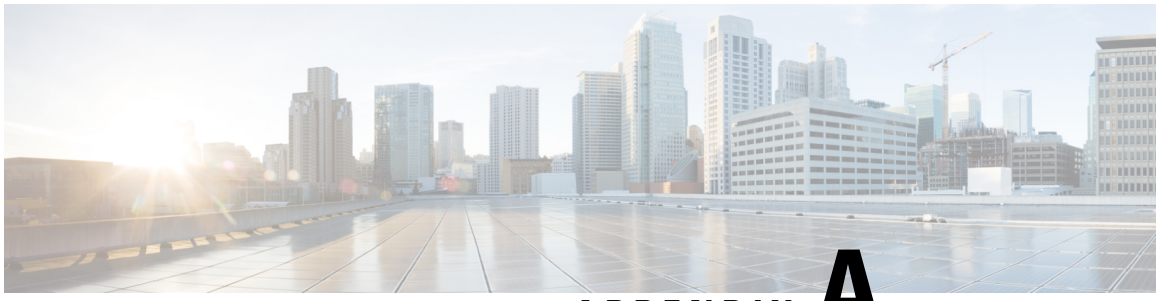
cmxctl agent restart

Step 4 To restart a Cisco CMX service, run the following command:

cmxctl start

Step 5 To start Cisco CMX API server, run the following command:

cmxos apiserver start



APPENDIX A

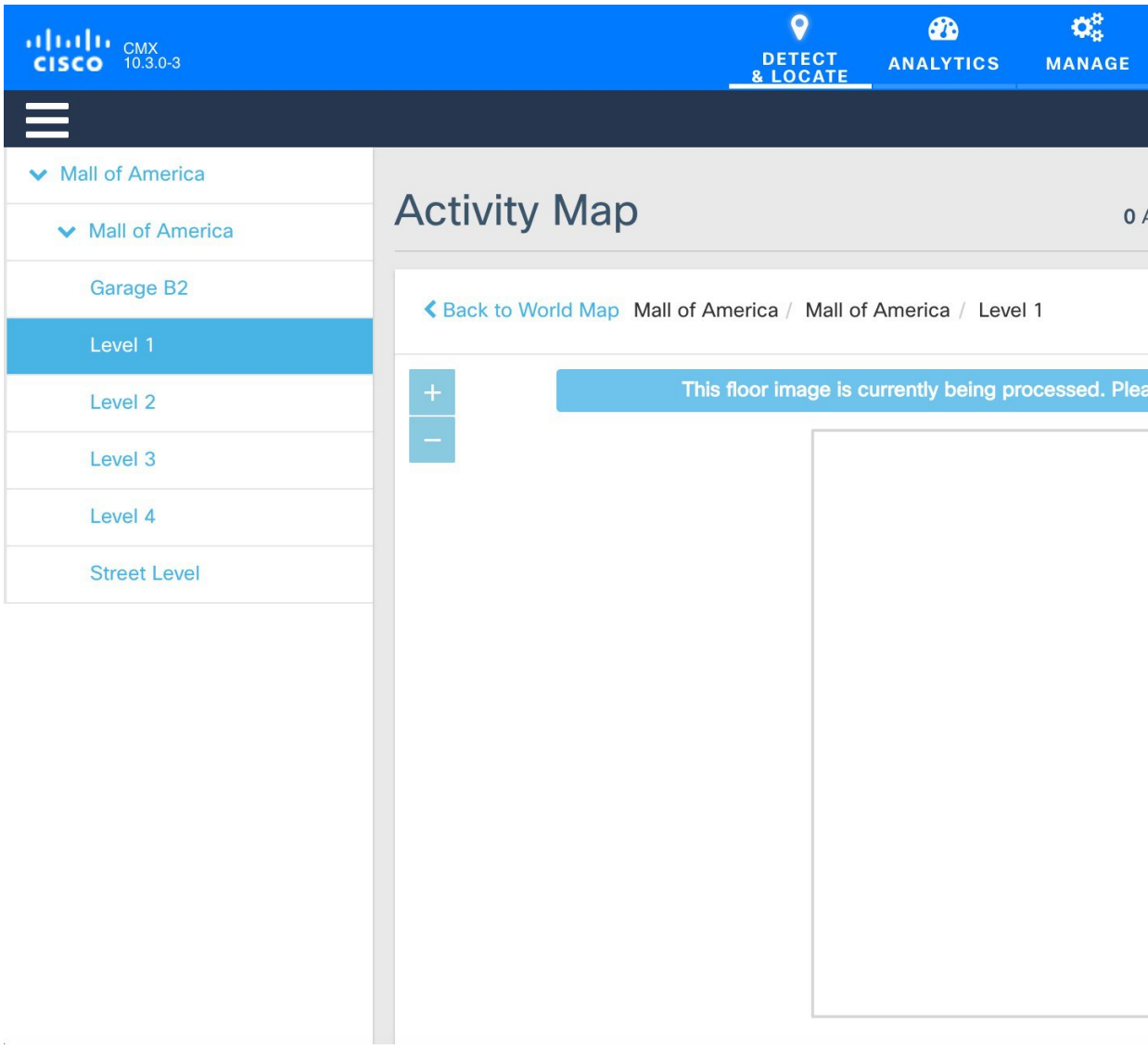
Guidelines for Managing Maps in Cisco CMX

We recommend that you use the following guidelines to effectively manage the maps on Cisco CMX. These guidelines are based on frequently asked questions about map import/update scenarios and will help avoid typical mistakes while importing/updating maps on Cisco CMX.

- You can import maps from Cisco DNA Center. Refer to Importing maps from Cisco DNA Center.
- Map uploads into Cisco CMX are best performed outside of business hours (or when Cisco CMX system activity is low), after 9PM is recommended. There are no hard and fast rules though. Maps import involves significant amount of processing to update the Database and processing floor images based on the size of floor image.
- Decide on an update window of 30 minutes for uploading maps to Cisco CMX. For a typical floor image, Cisco CMX can take up to 15 seconds per image to complete processing and show the floor image on Cisco CMX GUI. A typical map of a Campus with 100 floors may take up to 30 minutes to complete image processing background jobs. If the image processing in progress, The GUI will show an information message saying 'This floor image is currently being processed. Please refresh the page after a few moments

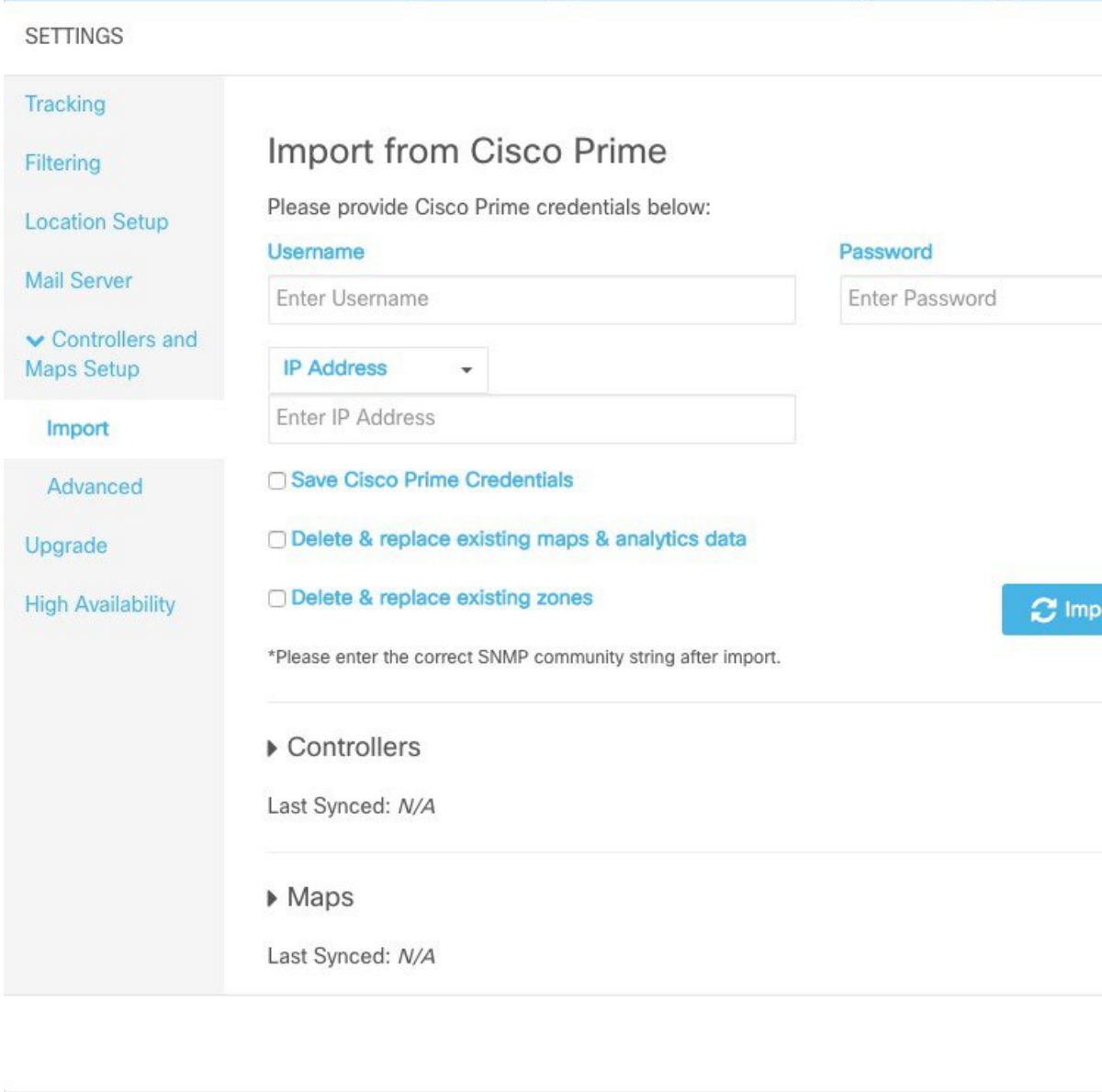
Guidelines for Managing Maps in Cisco CMX

to view the image'.



- Create and update the zones using Cisco CMX GUI map editor. All other map edit operations are to be performed using Prime Infrastructure.
- An AP can only be associated with a single floor map in Prime. If you are planning to move APs from one floor to another, you want to disassociate them from existing floor-map in Prime so that they can be associated to new floor-map in Prime. (Please refer to 'Typical map import issues: Case 2' for troubleshooting steps.)
- To expand a map to cover a larger area, create a new map in Prime and move APs to the new map from older map. You also want to make sure that the older floor is deleted from Prime and Cisco CMX before the new floor map is imported on Cisco CMX.
- Avoid doing bulk map import/exports. Export individual maps changes from Prime Infrastructure and import into Cisco CMX. For large set of maps, Its not recommended to use 'Import from Cisco Prime' option (shown in the picture) as this will sync all maps from Prime to Cisco CMX that may put significant

amount of load on the system.



- Create a Map Using Cisco Prime Infrastructure, on page 245
- Delete a Map Using Cisco Prime Infrastructure, on page 246
- Move an Access Point Between Maps Using Cisco Prime Infrastructure, on page 247
- Export a Map Using Cisco Prime Infrastructure, on page 250
- Import New and Modified Maps to Cisco CMX, on page 251

Create a Map Using Cisco Prime Infrastructure

To create a map using Cisco Prime Infrastructure, see the "Using Wireless Maps" chapter in the Cisco Prime Infrastructure 3.1 User Guide.

Delete a Map Using Cisco Prime Infrastructure

Procedure

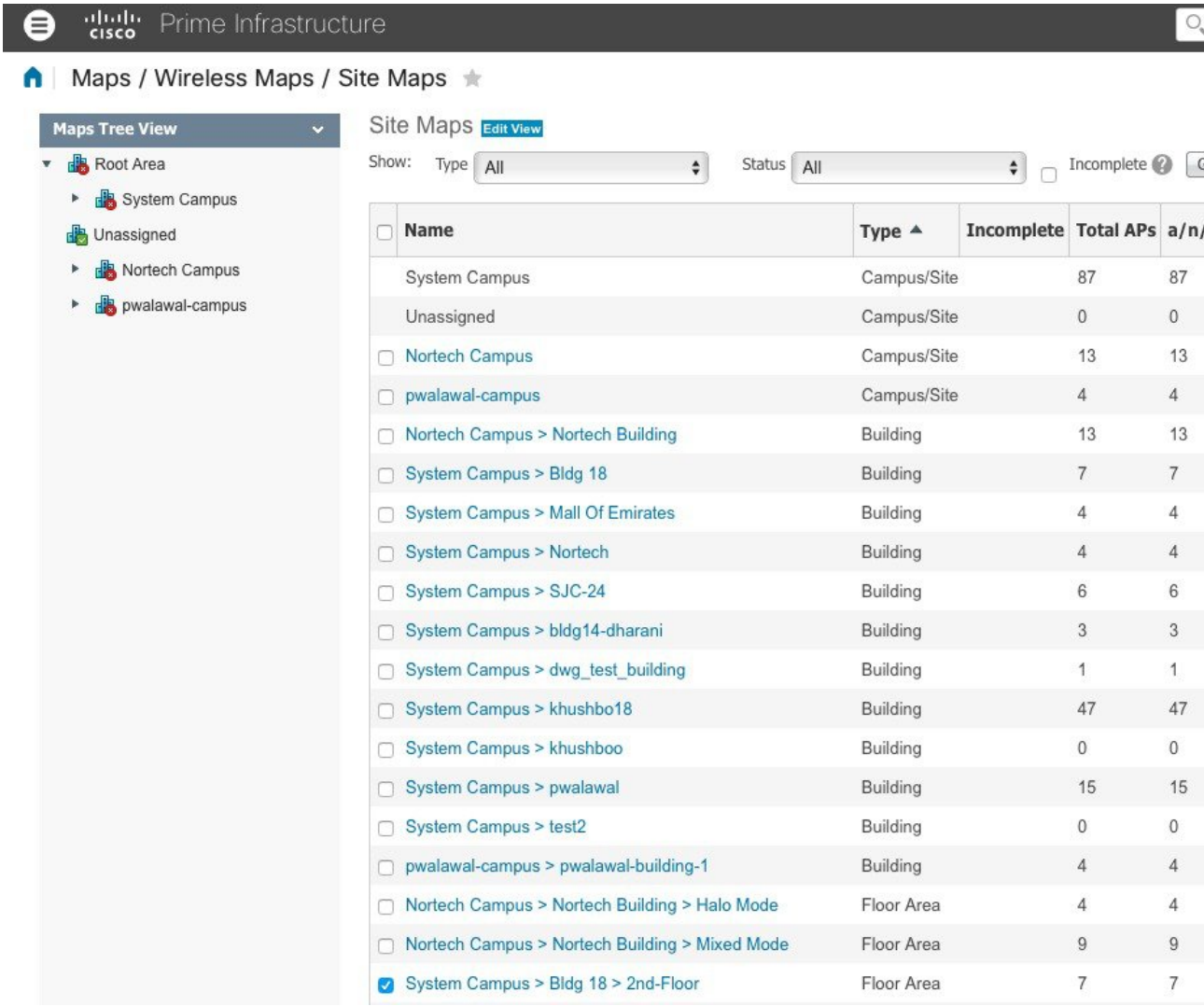
Step 1 Log in to Cisco Prime Infrastructure.

Step 2 Click the **Open/Close** navigation icon (above the Home icon on top left hand side).

Step 3 Choose **Maps > Site Maps**.

Step 4 From the **Select a command** drop-down list, choose **Delete**.

Step 5 Select the checkbox of the individual map you wish to delete and click **Go** (next to the **Select a command** drop-down).



Move an Access Point Between Maps Using Cisco Prime Infrastructure

Procedure

Step 1 Log in to Cisco Prime Infrastructure.

Step 2 Click on Open/Close navigation icon (above the Home icon on top left hand side).

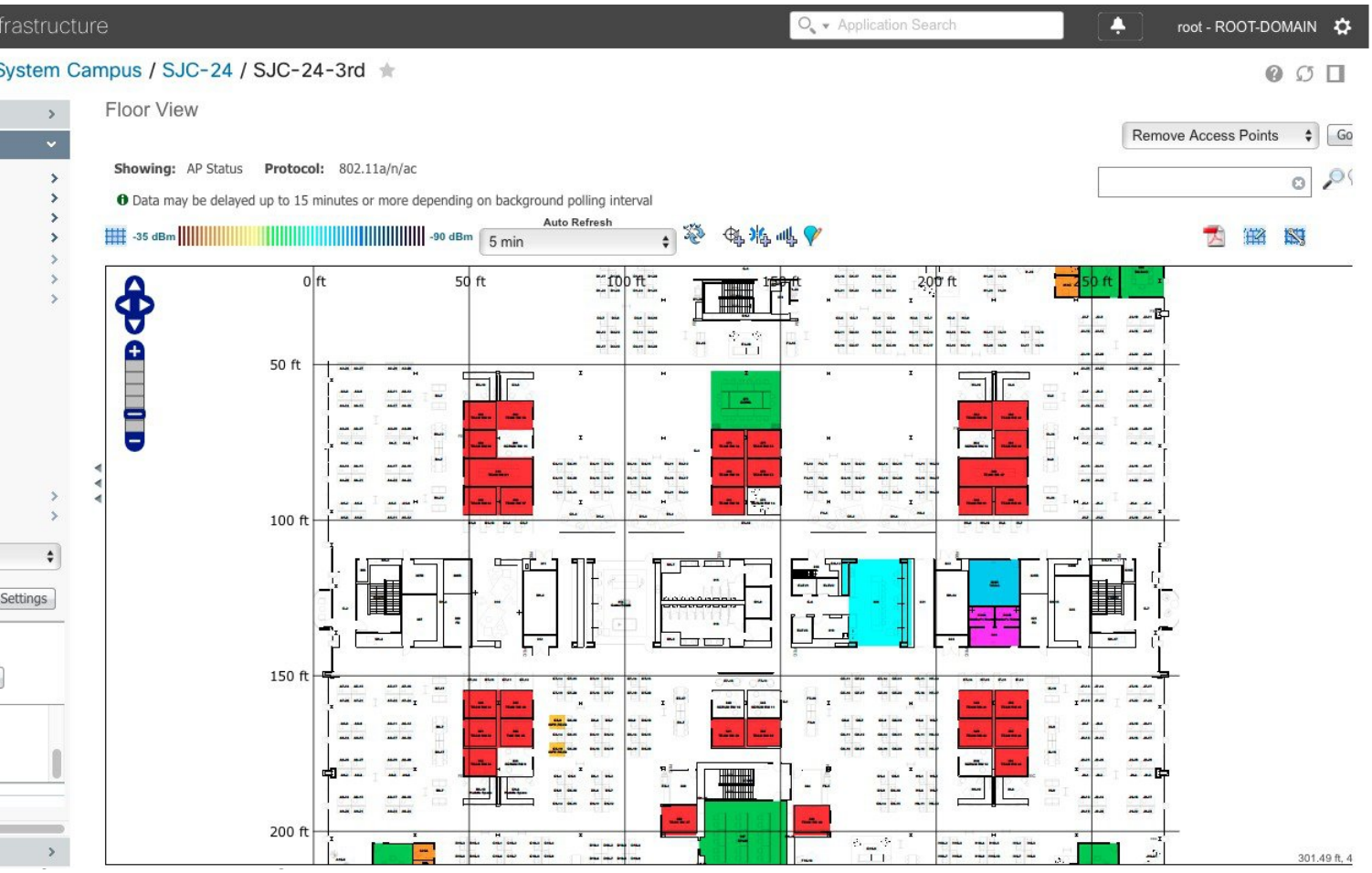
Step 3 Choose **Maps > Site Maps**.

Step 4 From the **Select a command** drop-down list, choose **Floor Area**.

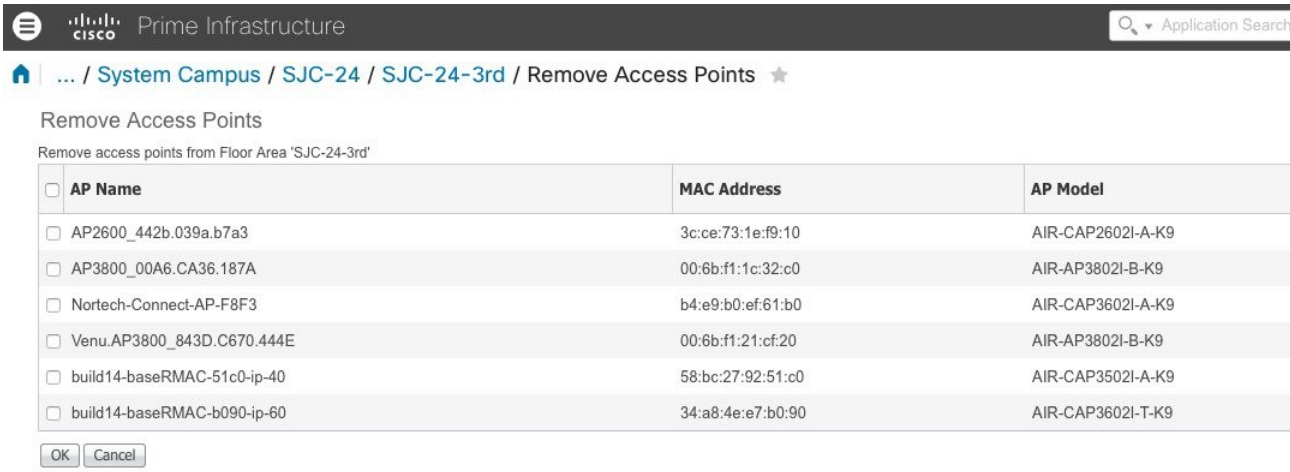
Step 5 Click **Go**.

Step 6 Click on the floor Area from which you want to release the AP. The **Floor View** window is displayed.

Step 7 From the **Select a command** drop-down list, choose **Remove Access**

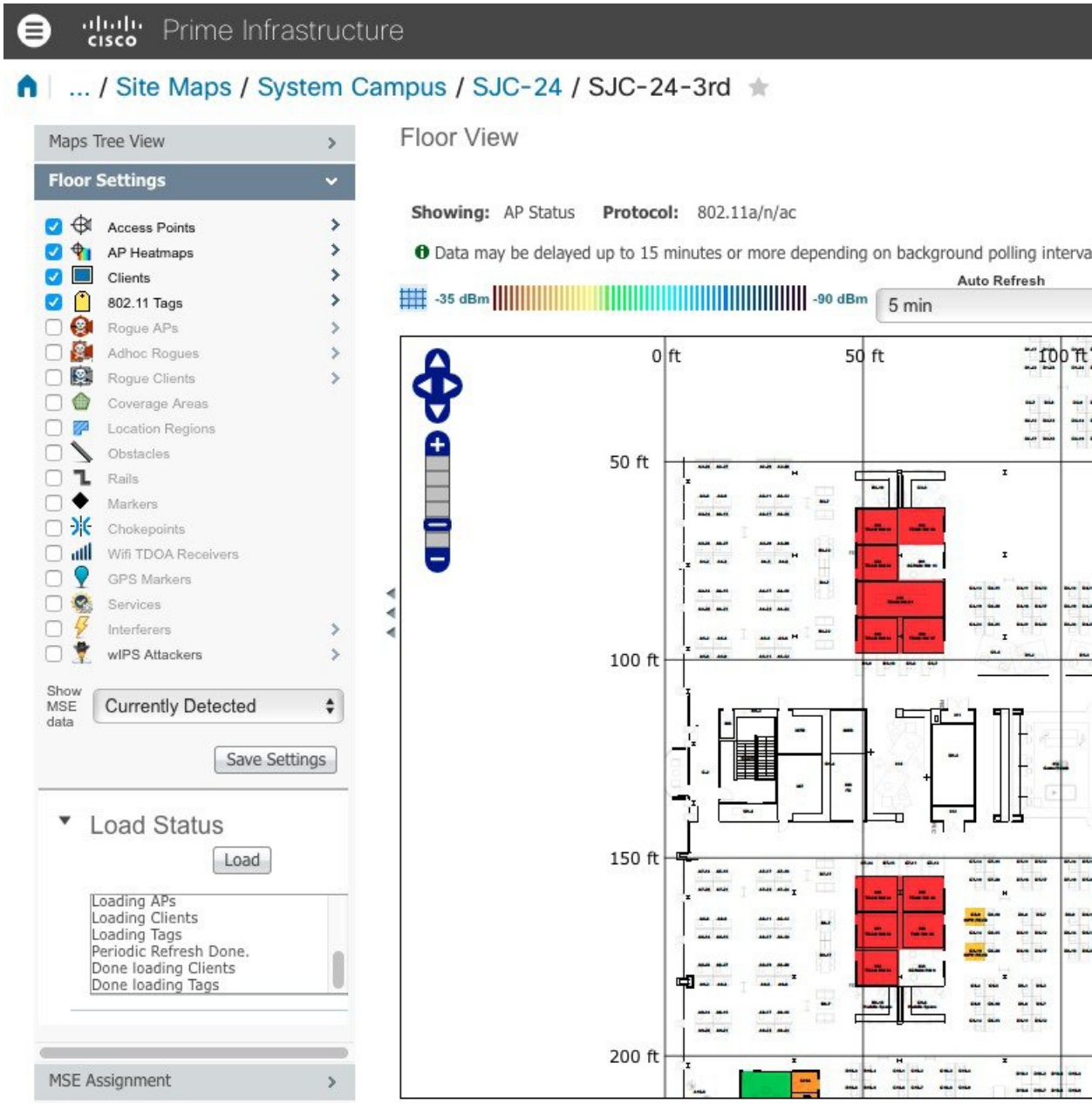


Step 8 Select the AP to be deleted and click **OK**.

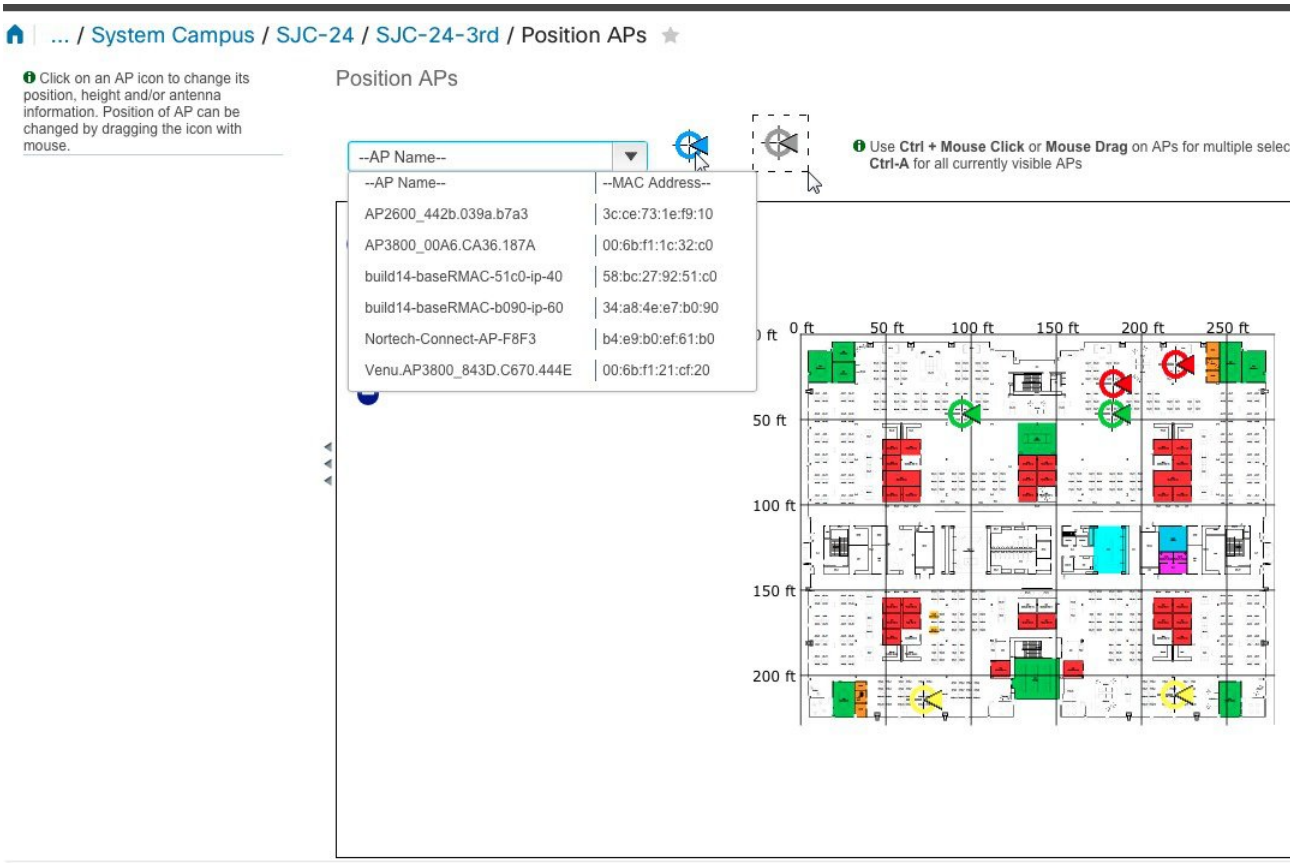


Guidelines for Managing Maps in Cisco CMX

Step 9 Click **Position AP** icon (before the delete icon) to place APs on the map.



Step 10 From the **AP Name** drop-down list, choose the AP and place it to the correct location on the map.



Export a Map Using Cisco Prime Infrastructure

Procedure

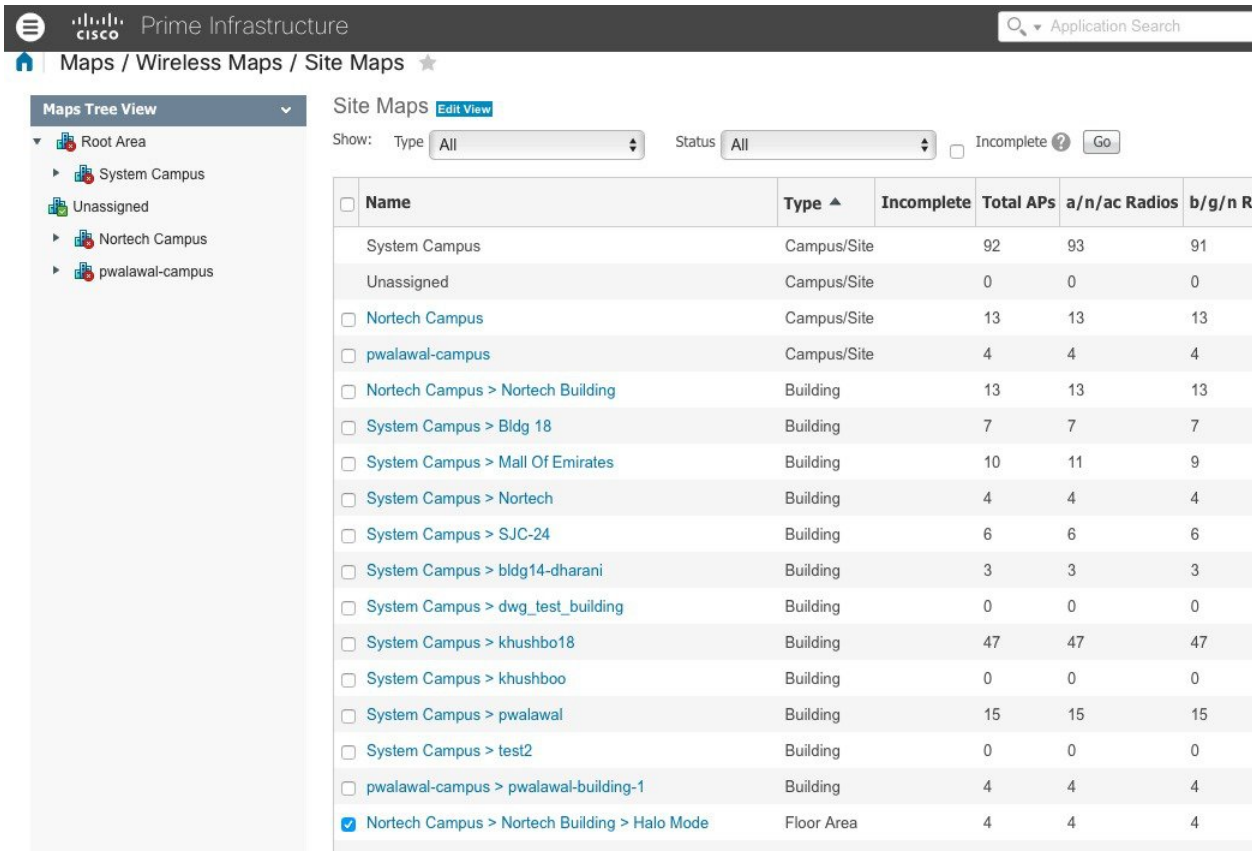
Step 1 Log in to Cisco Prime Infrastructure.

Step 2 Click on Open/Close navigation icon (above the Home icon on top left hand side).

Step 3 Choose **Maps > Site Maps**.

Step 4 From the **Select a command** drop-down list, choose **Export Maps**.

Step 5 Check the checkbox of the individual map you wish to export .

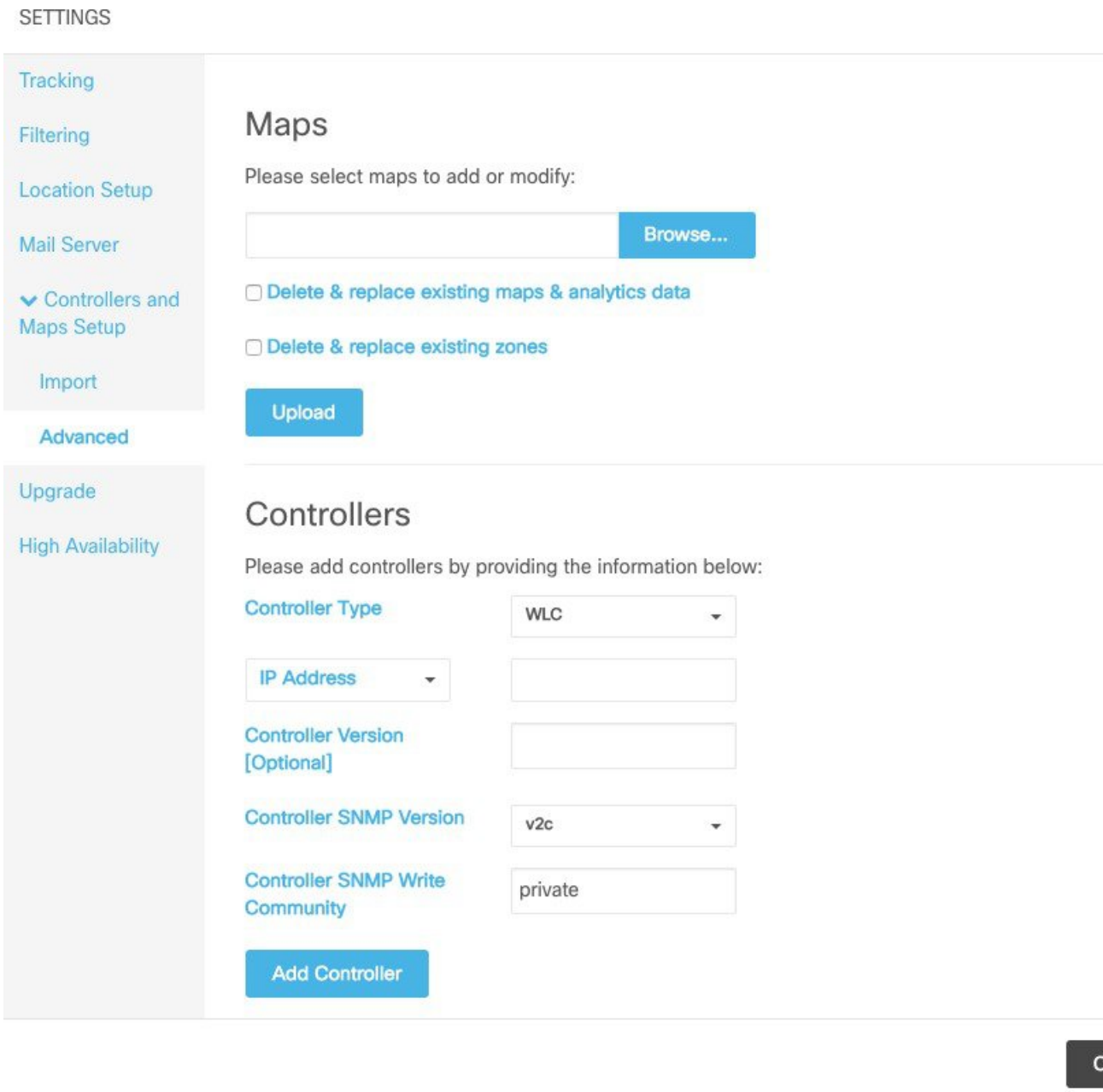


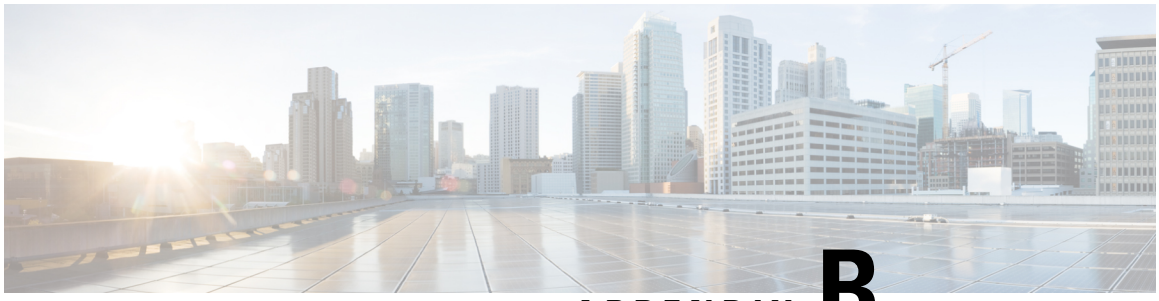
Step 6 Click **Go**.

Import New and Modified Maps to Cisco CMX

Navigate to Cisco CMX UI Advanced import option below (select System - Settings - Controllers and Maps Setup - Advanced), leave both checkboxes unchecked shown below. Browse to the maps file to be imported, select **Upload**.

Guidelines for Managing Maps in Cisco CMX





APPENDIX B

Guidelines for Managing Zones in Cisco CMX

For more information about managing zones, see Managing Perimeters and Zones on Location Maps, on page 160.

Common issues related to map import:

Case 1: Clients not detected, Heatmap generation failed

Initial Observations

A customer is using the 10.3.0-19 build and CMX is not detecting Clients / Tags. After debugging it was found that there are no heatmaps generated on CMX and the location computations are failing. Matlab-engine logs show a message 'No floors present in model info, heatmaps will not be computed'.

What went wrong?

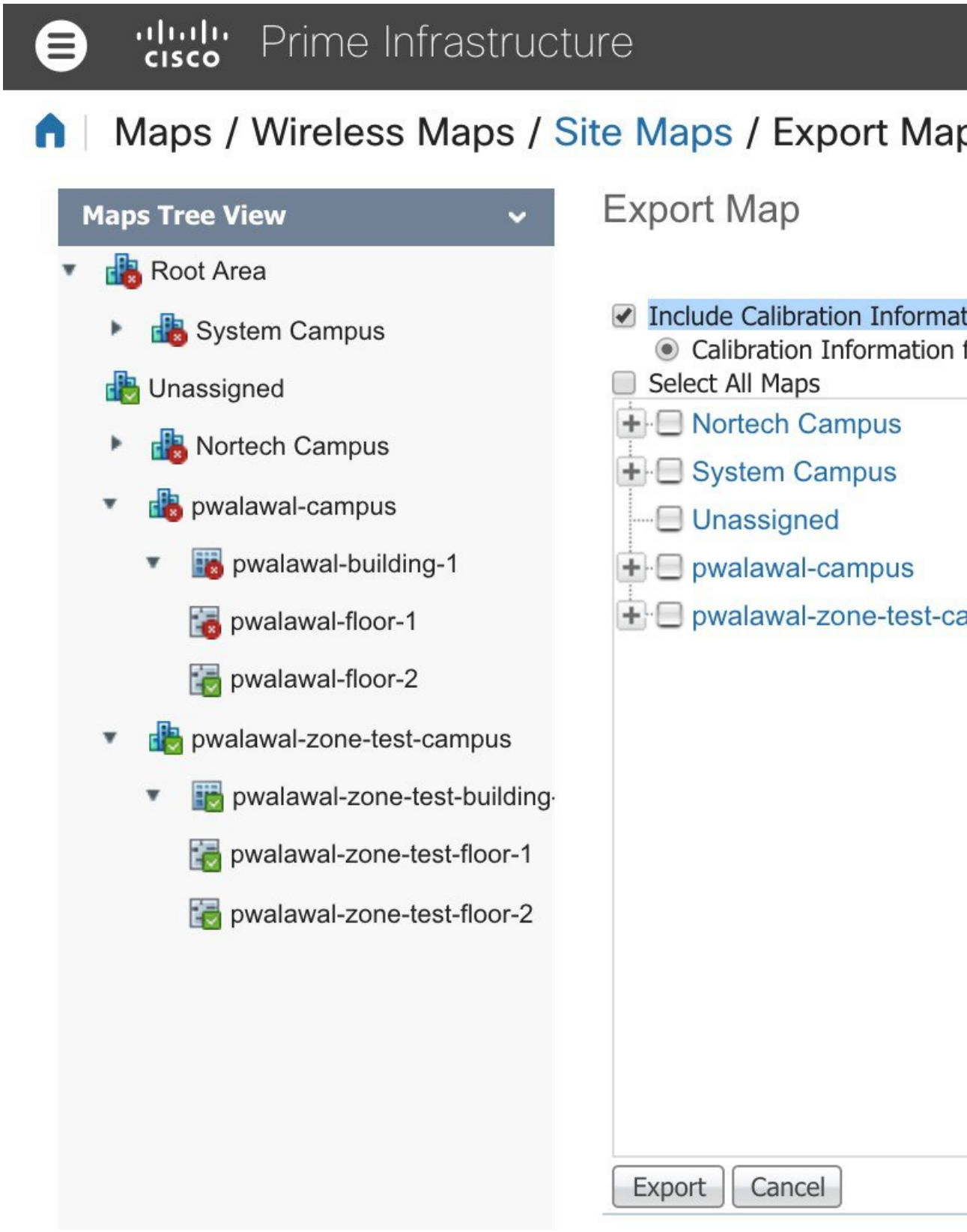
While exporting maps from Prime Infrastructure, Calibration model information was not included in the exported map file.

How to fix it?

Calibration model information is a vital piece of data linked to a floor-map on CMX. Client detection, Location computation and heatmap generation depends on Calibration model information.

When we export Maps from Cisco Prime Infrastructure, there is an option **Include Calibration Information** which is selected by default. While exporting maps, We want to make sure that this option is checked all the time.

Guidelines for Managing Zones in Cisco CMX



Case 2: The 'Access point' shows up on two floor-maps.

Initial Observations

The customer moved the Access points from Floor-X to Floor-Y on Prime Infrastructure and delete Floor-Y from Prime Infrastructure. Then they imported only 'Floor-X' on CMX. Now CMX shows same set of APs on both 'Floor-X' and 'Floor-Y'.

What went wrong?

When the APs were moved from Floor-X to Floor-Y and Floor-Y was deleted, A deleted operation for 'Floor-Y' was not executed on CMX. Unless user chooses the option 'Delete & replace existing maps & analytics data' while importing the maps, The entire map hierarchy will not be overwritten. If the option 'Delete & replace existing maps & analytics data' is not selected, CMX will only update the floors present in the uploaded map archive (i.e. Floor-X in this case).

How to fix it?

Before re-importing 'Floor-X', you want to make sure that 'Floor-Y' is deleted from CMX so that the APs linked to 'Floor-Y' are also deleted. This can be done via CMX CLI command as follows.

1. ssh to CMX as cmxadmin user.
2. List the floors and identify the floor from which the APs are moved.

```
[cmxadmin@cmx-prod opt]# cmxctl config maps floors
+-------------------------------------------+---------------------+--------------------+
| Floor Name | Location Floor ID | Analytics Floor ID |
+-------------------------------------------+---------------------+--------------------+
| Mall of America>Mall of America>Garage B2 | -60xxxxxxxxxxxxxxxx | 52 |
+-------------------------------------------+---------------------+--------------------+
| Mall of America>Mall of America>Level 1 | -604xxxxxxxxxxxxxxx | 53 |
+-------------------------------------------+---------------------+--------------------+
```

3. Execute delete floormap command for the identified floor so that The APs linked to that floor are deleted form CMX.

```
[cmxadmin@cmx-prod opt]# cmxctl config maps delete
Please enter the hierarchy to be deleted
(campus-name>building-name>floor-name): Mall of
America>Mall of America>Level 1
Confirm delete hierarchy:
Mall+of+America%3EMall+of+America%3ELevel+1 ? [y/N]: y
Hierarchy Mall+of+America%3EMall+of+America%3ELevel+1
deleted.
[cmxadmin@cmx-prod opt]#
```

4. Make sure that the floor is deleted by listing the floors.

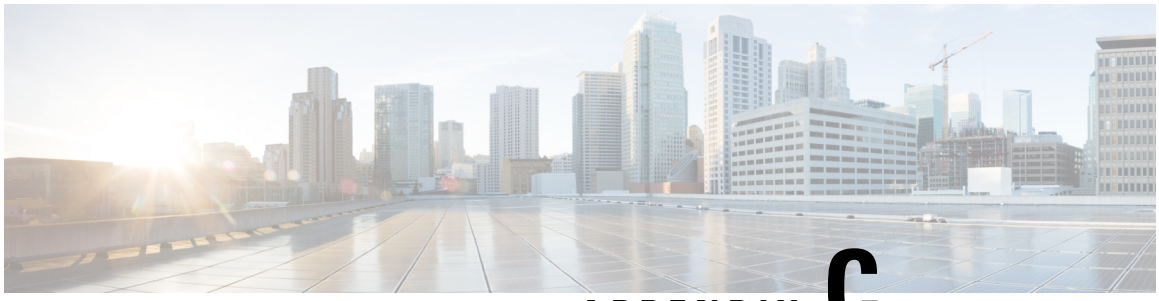
```
[cmxadmin@cmx-prod opt]# cmxctl config maps floors
+-------------------------------------------+---------------------+--------------------+

| Floor Name | Location Floor ID | Analytics Floor ID |
+-------------------------------------------+---------------------+--------------------+

| Mall of America>Mall of America>Garage B2 |
-60xxxxxxxxxxxxxxxx | 52 |
+-------------------------------------------+---------------------+--------------------+
```

5. Export only 'Floor-X' from Prime Infrastructure and Import the maps file on CMX so that new APs are now added to 'Floor-X'.

6. Go to CMX GUI on 'Detect and Locate' page and observe the floor-maps. 'Floor-X' should have the new set of APs on it.



APPENDIX C

Cisco CMX Alerts

Cisco CMX alerts can be of different level of severity. For critical alerts, there is an immediate impact on Cisco CMX and as a customer you should take necessary steps to resolve. Else, you will be risking losing data, for example, if a controller is down,you will not be able to retrieve data for any floor/access point that the controller manages.

As a customer, you can only resolve the obvious alerts such as controller not working. Most of the other alerts either indicate an undersized Cisco CMX or a critical failure in Cisco CMX. Both these cases would require intervention from Cisco CMX technical experts. You can use some of the **cmxos** and **cmxctl** commands to fix these critical failures. We recommend that you seek Cisco CMX technical help for troubleshooting.

Cisco CMX Alert	Description	Possible Solution
CPU_USAGE	Displayed when your CPU exceeds 80% on a Cisco CMX box.	Upgrade to a bigger Cisco CMX box.
MEMORY_USAGE	This alert is displayed when the memory usage is high.	Reduce the load on the Cisco CMX. Probably need a bigger CMX. Support should be able to figure that out.
SERVICE_STATUS	Displayed when a Cisco CMX service is crashed.	We recommend that you call the support.
DATA_PROCESSING_STATUS	Displayed when the Analytics service is slowing down.	Reduce load.
NMSP_CONNECTION_STATUS	Displayed when the Controller goes down for some reason.	Troubleshoot for a probable networking issue.
OUT_OF_MEMORY	Not used in Cisco CMX.	NA.
QUEUE_FULL	Not used in Cisco CMX.	NA
ARRAY_INDEX_OUT_OF_BOUND	Not used in Cisco CMX	NA

Cisco CMX Alert	Description	Possible Solution
BEACON_STATUS	Not supported	NA
BEACON_MOVEMENT	Not supported	NA
DISK_USAGE	Displayed when the Hard drive is getting full.	Run the cmx cleanup tool or remove unnecessary load from the hard drive.
AWIPS_LICENSE	Not used in Cisco CMX	NA
NMSP_MSG_RATE_EXCEEDED	Displayed when the system is getting too many NMSP messages for its box type.	We recommend that you either get a bigger box or clear unwanted clients by removing a controller or a map.
LOCATION_OVERLOADED	Critical alert that is not expected to happen.	NA
EVAL_LICENSE_EXPIRY	Displayed after the built in license expired after 120 days.	We recommend that you buy and activate a new Cisco CMX license.
AP_CONTROLLER_FETCH_STATUS	Displayed if SNMP information from the controller cannot be fetched.	Provide Cisco CMX with valid SNMP credentials.
SSID_CONTROLLER_FETCH_STATUS	Same as AP Controller.	NA
MAP_IMPORT_ERROR	Displayed if maps are not imported successfully during the import process from Cisco Prime Infrastructure.	We recommend that you contact support to re-import maps from Cisco Prime Infrastructure.
ANALYTICS_MISMATCH	Displayed if Analytics sanity test is failed.	We recommend that you call the Cisco support.
HETERARCHY_SIZE_LIMIT_EXCEEDED	Displayed if maps/aps/zones numbers exceed their limit for the corresponding Cisco CMX service type.	This might affect Cisco CMX performance. We recommend that you either reduce the number of elements or move them to a larger Cisco CMX box.

Cisco CMX Alert	Description	Possible Solution
mem_usage	Displayed once the memory usage is above 80%. This is a critical error.	Consider upgrading hardware or VM specs.
SERVER_STATUS	Displayed after the High Availability is successfully disabled. The Primary server is no longer syncing with secondary server.	This is an informational alert, and no action required.
SERVER_STATUS	Displayed when attempting to failback from secondary server to primary server: 192.168.99.110.	This is an informational alert, and no action required.
UNIQUE_DEVICE_EXCEEDED	Two alerts will be generated on Cisco CMX. First warning alert is generated when the number of unique devices seen in a particular day reaches 90% of allowed limit for that Cisco CMX. The second critical alert is generated when the number of unique devices seen in that day exceeds the allowed limit for that Cisco CMX.	This alert indicates that Cisco CMX is having heavy load than allowed in a day and this could lead to performance issue on Cisco CMX. One of the possible solution will be to lower the traffic using filtering parameters such as **Disable Probing Clients** or split the traffic among multiple Cisco CMX.

Monit Email	Customer Action
1m Load avg. above 3	No action required.
1m Load avg. recovered	No action required.
5m Load avg. above 3	No action required.
5m Load avg. recovered	No action required.
15m Load avg. above 2	No action required.
15m Load avg. recovered	No action required.

Monit Email	Customer Action
Adminui service is down	Run the **cmxos adminui start** command.
Agent service is down	Run the **cmxctl agent start** command.
Analytics service is down	Run the **cmxctl analytics start** command.
Analytics service recovered	No action required.
cache_6378 service is down	Run the **cmxctl cache_6378 start** command.
cache_6378 service recovered	No action required.
cache_6379 service is down	Run the **cmxctl cache_6379 start** command.
cache_6379 service recovered	No action required.
cache_6380 service is down	Run the **cmxctl cache_6380 start** command.
cache_6380 service recovered	No action required.
cache_6381 service is down	Run the **cmxctl cache_6381 start** command.
cache_6381 service recovered	No action required.
cache_6382 service is down	Run the **cmxctl cache_6382 start** command.
cache_6382 service recovered	No action required.
cache_6383 service is down	Run the **cmxctl cache_6383 start** command.
cache_6383 service recovered	No action required.
cache_6385 service is down	Run the **cmxctl cache_6385 start** command.
cache_6385 service recovered	No action required.
cassandra service is down	Run the **cmxctl cassandra start** command.
cassandra service recovered	No action required.
Collectd service is down	No action required.
Collectd service is up	No action required.
Confd service is down	Run the **cmxctl confd start** command.
Confd service is up	No action required.
configuration service is down	Run the **cmxctl configuration start** command.
configuration service recovered	No action required.
Consul Service is down	Run the **cmxctl consul start** command.
Disk usage is above 80%	Remove files. Add storage.

Monit Email	Customer Action
Disk usage recovered	No action required.
DNSMasq service is down	No action required.
File Descriptors are above bounds	No action required.
File Descriptors recovered	No action required.
File system	
HAProxy service is down	Run the **cmxctl haproxy start** command.
HAProxy service is up	No action required.
hyperlocation service is down	Run the **cmxctl hyperlocation start** command.
hyperlocation service recovered	No action required.
Influxdb service is down	Run the **cmxctl influxdb start** command.
Influxdb service is up	No action required.
Inode usage is above 80%	Remove files.
Inode usage recovered	No action required.
Load	Suggested actions to lessen the load: • Create fewer notifications • Run fewer reports • Remove some WLCs • Upgrade system.
location service is down	Run the **cmxctl location start** command.
location service recovered	No action required.
matlabengine service is down	Run the **cmxctl matlabengine start** command.
matlabengine service recovered	No action required.
Memory usage is above 80%	Restart the system during a quiet period. Upgrade system.
Memory usage recovered	No action required.
Monit instance changed	None. Informational.
nmsplb service is down	Run the **cmxctl nmsplb start** command.
nmsplb service recovered	No action required.

Monit Email	Customer Action
Port 5432 is not responding	Run the **cmxctl database stop** and **cmxctl database start** command.
Port 5432 is responding	No action required.
Port 6378 is not responding	Run the **cmxctl cache_6378 stop** and **cmxctl cache_6378 start** command.
Port 6378 responding	No action required.
Port 6379 is not responding	Run the **cmxctl cache_6379 stop** and **cmxctl cache_6379 start** command.
Port 6379 responding	No action required.
Port 6380 is not responding	Run the **cmxctl cache_6380 stop** and **cmxctl cache_6380 start** command.
Port 6380 responding	No action required.
Port 6381 is not responding	Run the **cmxctl cache_6381 stop** and **cmxctl cache_6381 start** command.
Port 6381 responding	No action required.
Port 6382 is not responding	Run the **cmxctl cache_6382 stop** and **cmxctl cache_6382 start** command.
Port 6382 responding	No action required.
Port 6383 is not responding	Run the **cmxctl cache_6383 stop** and **cmxctl cache_6383 start** command.
Port 6383 responding	No action required.
Port 6385 is not responding	Run the **cmxctl cache_6385 stop** and **cmxctl cache_6385 start** command.
Port 6385 responding	No action required.
Port 6511 is not responding	Run the **cmxctl hyperlocation stop** and **cmxctl hyperlocation start** command.
Port 6512 responding	No action required.
Port 6531 is not responding	Run the **cmxctl location stop** and **cmxctl location start** command.
Port 6531 responding	No action required.
Port 6532 is not responding	Run the **cmxctl location stop** and **cmxctl location start** command.

Monit Email	Customer Action
Port 6532 responding	No action required.
Port 6541 is not responding	Run the **cmxctl analytics stop** and **cmxctl analytics start** command.
Port 6541 responding	No action required.
Port 6542 is not responding	Run the **cmxctl analytics stop** and **cmxctl analytics start** command.
Port 6542 responding	No action required.
Port 6551 is not responding	Run the **cmxctl configuration stop** and **cmxctl configuration start** command.
Port 6551 responding	No action required.
Port 6552 is not responding	Run the **cmxctl configuration stop** and **cmxctl configuration start** command.
Port 6552 responding	No action required.
Port 6571 is not responding	Run the **cmxctl nmsplb stop** and **cmxctl nmsplb start** command.
Port 6571 responding	No action required.
Port 6572 is not responding	Run the **cmxctl nmsplb stop** and **cmxctl nmsplb start** command.
Port 6572 responding	No action required.
Port 6581 is not responding	Run the **cmxctl matlabengine stop** and **cmxctl matlabengine start** command.
Port 6581 is responding	No action required.
Port 6582 is not responding	Run the **cmxctl matlabengine stop** and **cmxctl matlabengine start** command.
Port 6582 is responding	No action required.
Port 9042 is not responding	Run the **cmxctl cassandra stop** and **cmxctl cassandra start** command.
Port 9042 is responding	No action required.
postgres service is down	Run the **cmxctl database start** command.
postgres service is up	No action required.
qlesspy service is down	Run the **cmxctl qlesspy start** command.
qlesspy service recovered	No action required.

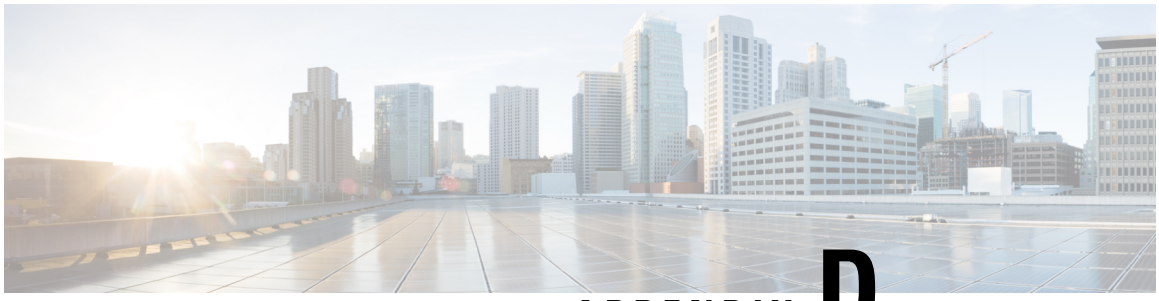
Monit Email	Customer Action
Socket 5432 is not responding	Run the **cmxctl database stop** and **cmxctl database start** command.
Socket 5432 is responding	No action required.
Swap usage is above 80%	Increase swap space or reduce memory usage.
Swap usage recovered	No action required.
SYS CPU usage is above 60%	No action required.
SYS CPU usage recovered	No action required.
The analytics service is not reporting health	Run the **cmxctl analytics stop** and **cmxctl analytics start** command.
The analytics service reporting health	No action required.
The configuration service is not reporting health	Run the **cmxctl configuration stop** and **cmxctl configuration start** command.
The configuration service reporting health	No action required.
The hyperlocation service is not reporting health	Run the **cmxctl hyperlocation stop** and **cmxctl hyperlocation start** command.
The hyperlocation service reporting health	No action required.
The location service is not reporting health	Run the **cmxctl location stop** and **cmxctl location start** command.
The location service reporting health	No action required.
The matlabengine service is not reporting health	Run the **cmxctl matlabengine stop** and **cmxctl matlabengine start** command.
The matlabengine service reporting health	No action required.
The nmsplb service is not reporting health	Run the **cmxctl nmsplb stop** and **cmxctl nmsplb start** command.
The nmsplb service reporting health	No action required.
USR CPU usage is above 80%	No action required.
USR CPU usage recovered	No action required.
WAIT CPU usage is above 60%	No action required.
WAIT CPU usage recovered	No action required.
Memory usage is above 80%	Restart the system during a quiet period. Upgrade system.

Monit Email	Customer Action
Memory usage recovered	No action required.
Swap usage is above 80%	Increase swap space or reduce memory usage.
File system	
Disk usage is above 80%	Remove files. Add storage.
Disk usage recovered	No action required.
Inode usage is above 80%	Remove files.
Inode usage recovered	No action required.
File Descriptors are above bounds	Restart the system.
File Descriptors recovered	No action required.
ocation service is down	Run the **cmxctl location start** command.
location service recovered	No action required.
Port 6531 is not responding	Run the **cmxctl location stop** and **cmxctl location start** command.
Port 6531 responding	No action required.
Port 6532 is not responding	Run the **cmxctl location stop** and **cmxctl location start** command.
Port 6532 responding	No action required.
The location service is not reporting health	Run the **cmxctl location stop** and **cmxctl location start** command.
The location service reporting health	No action required.
matlabengine service is down	Run the **cmxctl matlabengine start** command.
matlabengine service recovered	No action required.
Port 6581 is not responding	Run the **cmxctl matlabengine stop** and **cmxctl matlabengine start** command.
Port 6581 responding	No action required.
Port 6582 is not responding	Run the **cmxctl matlabengine stop** and **cmxctl matlabengine start** command.
Port 6582 responding	No action required.

Monit Email	Customer Action
The matlabengine service is not reporting health	Run the **cmxctl matlabengine stop** and **cmxctl matlabengine start** command.
The matlabengine service reporting health	No action required.
nmsplb service is down	Run the **cmxctl nmsplb start** command.
nmsplb service recovered	No action required.
Port 6571 is not responding	Run the **cmxctl nmsplb stop** and **cmxctl nmsplb start** command.
Port 6572 responding	No action required.
The nmsplb service is not reporting health	Run the **cmxctl nmsplb stop** and **cmxctl nmsplb start** command.
The nmsplb service reporting health	No action required.
postgres service is down	Run the **cmxctl database start** command.
postgres service is up	No action required.
Socket 5432 is not responding	Run the **cmxctl database stop** and **cmxctl database start** command.
Socket 5432 is responding	No action required.
Port 5432 is not responding	Run the **cmxctl database stop** and **cmxctl database start** command.
Port 5432 is responding	No action required.
qlesspy service is down	Run the **cmxctl qlesspy start** command.
qlesspy service recovered	No action required.
cache_6378 service is down	Run the **cmxctl cache_6378 start** command.
cache_6378 service recovered	No action required.
Port 6378 is not responding	Run the **cmxctl cache_6378 stop** and **cmxctl cache_6378 start** command.
Port 6378 responding	No action required.
cache_6379 service is down	Run the **cmxctl cache_6379 start** command.
cache_6379 service recovered	No action required.
Port 6379 is not responding	Run the **cmxctl cache_6379 stop** and **cmxctl cache_6379 start** command.
Port 6379 responding	No action required.

Monit Email	Customer Action
cache_6380 service is down	Run the **cmxctl cache_6380 start** command.
cache_6380 service recovered	No action required.
Port 6380 is not responding	Run the **cmxctl cache_6380 stop** and **cmxctl cache_6380 start** command.
Port 6380 responding	No action required.
cache_6381 service is down	Run the **cmxctl cache_6381 start** command.
cache_6381 service recovered	No action required.
Port 6381 is not responding	Run the **cmxctl cache_6381 stop** and **cmxctl cache_6381 start** command.
Port 6381 responding	No action required.
cache_6382 service is down	Run the **cmxctl cache_6382 start** command.
cache_6382 service recovered	No action required.
Port 6382 is not responding	Run the **cmxctl cache_6382 stop** and **cmxctl cache_6382 start** command.
Port 6382 responding	No action required.
cache_6383 service is down	Run the **cmxctl cache_6383 start** command.
cache_6383 service recovered	No action required.
Port 6383 is not responding	Run the **cmxctl cache_6383 stop** and **cmxctl cache_6383 start** command.
Port 6383 responding	No action required.
cache_6385 service is down	Run the **cmxctl cache_6385 start** command.
cache_6385 service recovered	No action required.
Port 6385 is not responding	Run the **cmxctl cache_6385 stop** and **cmxctl cache_6385 start** command.
Port 6385 responding	No action required.

Cisco CMX Alerts



APPENDIX D

Cisco CMX Network Protocols and Port Matrix

The following table lists the ports that Cisco CMX uses for communicating with wireless clients, controllers, Cisco Prime Infrastructure, and mail servers:

Table 19: Cisco CMX Network Protocols and Port Matrix

Source Device	Destination Device	Protocol	Destination Port	Description
Cisco CMX	NMSP on WLC	TCP	16113	-
Cisco CMX	SNMP on WLC	UDP	161/162	-
Cisco CMX	NTP Server	UDP	123	-
Cisco CMX	DNS Server	-	53	-
Cisco CMX	Mail Server	TCP	25	-
Cisco CMX	Internet	-	80/443	Used to pull down images of world map and validate addresses
Web	CMX HTTPS	TCP	443	Used to manage and administer Cisco CMX
Cisco CMX CLI via SSH	CMX Management	-	22	-
Web	CMX Management	-	1984	Used to upgrade Cisco CMX
HTTPS	Clients	TCP	443	-
HTTP	Clients	TCP	80	-

Table 20: HA Port Information

HA Ports	Description
7000, 7001, 9042	Cassandrs database
6378 through 6385	Redis
4242	High availability REST and web service. An HTTPS protocol using REST to communicate between the CMX HA
22	SSH port and used to synchronize files between servers

Table 21: Cassandra Database

Cassandra Database	Protocol
7000	TCP
7001	TCP
9042	SSL Communication

Table 22: Cisco CMX Communication With Other Cisco Devices

Component	Application	Direction	Protocol	Destination Port
Cisco CMX	Cisco Wireless Controller	Out	SSH	22
Cisco CMX	Cisco Wireless Controller	Out	SNMP	161
Cisco CMX	Cisco Wireless Controller	In/Out	NMSP	16113
Cisco CMX	Cisco DNA Spaces	In/Out	HTTPS	443
Cisco CMX	Cisco DNA Center	In/Out	SSH/HTTPS	443
Cisco CMX	Cisco Prime Infrastructure	In	HTTPS	443

INDEX

E