

Cisco CMX Configuration Guide, Release 11.1.1

First Published: 2025-11-28

Last Modified: 2026-08-14

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface xi

Audience xi

Conventions xi

Related Documentation xii

Communications, services, and additional information xii

Cisco Bug Search Tool xiii

Documentation feedback xiii

CHAPTER 1

Get Started with Cisco CMX 1

Getting Started 1

Introduction to Cisco Connected Mobile Experiences 1

Overview of Cisco CMX Services 1

Cisco CMX Feature Parity 3

Installing Cisco CMX 11.1.1 4

What's New in Cisco CMX Release 11.1.1 5

CSL AlmaLinux Upgrade Cisco CMX 11.1.1 8

Migrate data to Cisco CMX Release 11.1.1 8

Wireless Controller and Wi-Fi Client Support 10

Generate Root Password 10

Using the Evaluation License 10

Logging In to the Cisco CMX User Interface 11

Configuring SSO Authentication in Cisco CMX 12

Importing Maps and Cisco Wireless Controllers 16

Exporting Cisco Prime Infrastructure Maps 16

Copying the Exported Maps 16

Importing Maps 16

Adding Controllers 17
Import Controllers using CLI 18
Enabling or Disabling Cisco CMX Services 20
Installing Certificates in Cisco CMX 20
Installing a Self-Signed Certificate 20
Installing a CA-Signed Certificate 21
OCSP Support for Certificates 24
Wildcard Certificate Support for Cisco CMX 24
Installing a CA-Signed Certificate for High Availability in Cisco CMX 24
Adding Users and Managing Roles 25
Using the Cisco CMX Setup Assistant 25
REST APIs Version 3 Support in Cisco CMX 26
Supporting Active Clients Version 3 API 26
Getting APIs 27
Restricted CLI 27
Encrypting Cisco CMX Connection to Remote Syslog Server Using IPSec Protocol 28
About Cisco CMX Integration with Cisco Catalyst Center 29
Create Cisco CMX Settings 29
Remote HTTPS Server Support for Windows OS 31
Support for Proxy with Basic Authentication 32
External Endpoint Connect 32

CHAPTER 2 **The Cisco CMX Detect and Locate Service 33**
Overview of the Detect and Locate Service 33
Initial Configurations 33
Viewing or Tracking Devices 34
Enhanced Associated Clients Tracking 39
Viewing Device Details 40
Customizing Client Refresh Rates 40
Customizing Device Views Using Filters 41
Adding and Deleting Filters 41
Searching for a Device 42
Client Playback 43
Data Privacy 43

CMX Grouping 45
Enabling Cisco Hyperlocation and FastLocate in Cisco CMX 47
Hyperlocation Mixed Mode Support 49
Running Hyperlocation Diagnostics 51
View Hyperlocation Groupings 59
Controlling the Probing Client Expiry Time 63
Supported Access Points for Cisco CMX 10.5 Location Features with Cisco WLC 8.7 64
Measuring Client Location Accuracy Using the Location Accuracy Test 65
Analyzing Location Accuracy Results 69
Understanding Client Diagnostics 70
Analyzing Location Accuracy Log Files 72
Location Accuracy for Hyperlocation Deployments 74
Accuracy Testing 75
Testing accuracy using GUI 77
Testing accuracy using CLI 79
Understanding the test results 81

CHAPTER 3 **The Cisco CMX Analytics Service** 85
Overview of the Analytics Service 85
The Analytics Dashboard 85
Accessing the Analytics Dashboard 86
Filtering the Data Displayed in the Analytics Dashboard 86
Viewing a Device Count and Average Dwell Time Report 87
Analytics Reports 88
Creating and Managing Customized Reports 89
Create a Custom Report 89
Edit a Report 91
Configure Custom Time Ranges for an Analytics Report 91
Delete a Customized Report 93
Creating an Analytics Report Based on Associated or Probing Only Devices 93
Viewing Global Alerts for Critical Services 94
Customized Widgets 94
The Visitors Widget 94
The Dwell Time Widget 95

The Wi-Fi Adoption Widget 96
The Dwell Time Breakdown Widget 97
Creating Customized Widgets 99
Create a Realtime Report 100
Performing Heatmap Analysis 100
Set SSID Filter Parameters for Analytics Service 101
Disable Cisco CMX Analytics Service (CLI) 102

CHAPTER 4 **Managing Cisco CMX Configuration** 105
Overview of the Manage Service 105
Managing Perimeters and Zones on Location Maps 106
Viewing Campus, Building, Floor, and Zone Details 106
Adding a Campus Address 106
Managing Tags 107
Creating an Inclusion or Exclusion Region 107
Creating a Perimeter 108
Deleting a Perimeter 109
Editing a Perimeter 110
Creating a Zone 110
Deleting a Zone 111
Editing a Zone 112
Managing Licenses 112
Add a License 114
Delete a License 115
Managing Users 116
Adding a User 116
User Roles 116
Changing the Default Admin Password 117
Editing User Information 118
Deleting a User 118
View Active User Sessions 118
Managing Notifications from Applications 119
Create a New Notification 120
Making Changes to Notifications 123

Enabling and Disabling a Notification 123
Editing a Notification 123
Viewing Northbound Notifications 124
Viewing Northbound Notification Attributes 124
Managing Proxy Settings for Notifications 126
Deleting a Notification 128
Managing the Cisco CMX Cloud Apps 129
Creating and Retrieving the Token Using Cisco CMX Tethering 132
Polling Access Point Information Using NMSP 136
Setting Up Outbound Proxy 136
Setting Up Outbound Proxy in HA-Enabled Setup 137
Configuring Basic CMX Settings 137
Root User Changes 138

CHAPTER 5 **Managing Cisco CMX System Settings** 139
Overview of the System Service 139
Viewing the Overall System Health 139
Understanding the Node Table 141
Understanding the System Update Table 141
Understanding the Coverage Details Table 142
Understanding Smart License 143
Understanding the Controllers Table 143
Managing Dashboard Settings 144
Setting Device-Tracking Parameters 144
Setting Filtering Parameters 146
Setting Location Calculation Parameters 147
Setting Data Privacy 149
Setting Data Retention Parameters 151
Configuring the Mail Server for Notifications 152
Importing Maps and Controllers into Cisco CMX 153
Importing Maps and Adding Controllers 154
Importing Maps from Cisco Catalyst Center 156
Upgrading Cisco CMX 157
Enabling High Availability for Cisco CMX 158

Pre-requisites for High Availability 159
SSH Login Failure Issue 160
Enabling High Availability for Cisco CMX Using the Web UI 160
Enabling High Availability Using CLI 161
High Availability State Information 162
Replacing a Cisco CMX High Availability Unit 162
High Availability Synchronization with Cisco MSE 163
Smart License 164
Set Up Smart License on Cisco CMX with High Availability 166
Set Up Smart License on Cisco CMX (GUI) 167
Set Up Smart License on Cisco CMX (CLI) 169
Configure Smart License 170
Troubleshoot Smart License 172
Viewing Live System Alerts 174
Viewing Patterns 174
Understanding the Metrics Tab 175
Viewing System Summary Metrics 176
Viewing System Summary Metrics Using the Dashboard 176
Viewing CMX Node Metrics 177
Viewing CMX Node Metrics Using the Dashboard 177
Viewing Database Metrics 178
Viewing Database Metrics Using the Dashboard 178
Viewing Cache Metrics 178
Viewing Cache Metrics Using the Dashboard 179
Viewing Location Metrics 179
Viewing Location Metrics Using the Dashboard 180
Viewing Analytics Notification Metrics 180
Viewing Analytics Notification Metrics Using the Dashbaord 181
Viewing Presence Metrics 181

CHAPTER 6 **FIPS, CC, and UCAPL Support in Cisco CMX** 183
FIPS Mode Requirements 185
Authentication Requirements 185
Log in Requirements 185

Password Requirements 185
Protocol Requirements 185
UCAPL Mode Requirements 185
Authentication Requirements 186
Log in Requirements 186
Password Requirements 186
Protocol Requirements 186
Setting up FIPS or UCAPL Mode Correctly 187
Choosing an Encryption Key Type 188
Creating a Certificate Signing Request 188
Viewing Stored Certificates 190
Validating Mutual Certificate During NMSP Connection in FIPS Mode 191
Verifying FIPS Readiness 192
Enabling and Managing FIPS Mode 193
Configuring Notification Listener in FIPS Mode 194
Enabling and Managing UCAPL Mode 195
Enabling Logging in UCAPL mode 195
Logging HTTP Headers 195
Logging File Access 196
Validating Client Certificates 196
Setting Up a UCAPL Automatic Backup 197
Working with the Certificate Revocation List 198
Manual Import of CRL 198
Disk Wipeout 199

CHAPTER 7 **Performing Administrative Tasks** 201
Cisco CMX User Accounts 201
Unlocking Users 202
Setting Strong Password Authentication 203
Password Recovery 205
Resetting Cisco CMX GUI Administrator Password 208
Resetting Root Password - Cisco CMX Release 10.4 and Earlier with CentOS 6.0 208
Resetting Password - Cisco CMX Release 10.6 and Later with CentOS 7.0 209
Setting Up External Server Authentication 209

Configuring Cisco CMX Users in the External Authentication Server 211
Configuring an External Authentication Server in Cisco CMX 211
Configuring an External AAA Server with Cisco CMX 212
Displaying External Authentication Server Settings 213
Deleting External Authentication Server Settings 213
Manage AAA users for SSH Access 214
Log in to SSH as AAA User 215
Setting Up Audit Logging 215
Performing Scheduled Backup for Cisco CMX 218
Performing Manual Backup for Cisco CMX 218
Increasing the Hard Disk Space 220
Restoring Data 221
Encrypting the CMX /opt Directory 223
Display a Login Banner 225
Managing NTP Servers 226
Configuring Authenticated NTP Server 226
Configuring Unauthenticated NTP Server 229
Updating Auntenticated NTP Server Parameters 229
Troubleshooting Cisco CMX Server Shutdown Problems 230

APPENDIX A **Guidelines for Managing Maps in Cisco CMX** 231
Create a Map Using Cisco Prime Infrastructure 234
Delete a Map Using Cisco Prime Infrastructure 234
Move an Access Point Between Maps Using Cisco Prime Infrastructure 235
Export a Map Using Cisco Prime Infrastructure 239
Import New and Modified Maps to Cisco CMX 240

APPENDIX B **Guidelines for Managing Zones in Cisco CMX** 243

APPENDIX C **Cisco CMX Alerts** 247

APPENDIX D **Cisco CMX Network Protocols and Port Matrix** 259



Preface

- Audience, on page xi
- Conventions, on page xi
- Related Documentation, on page xii
- Communications, services, and additional information, on page xii

Audience

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

Cisco CMX is the on-premise location service that is provided as part of the Cisco Spaces overall location as a platform service.

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.
[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.

Convention	Indication
<>	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 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 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 CMX Rest APIs, see:

  https://developer.cisco.com/docs/cisco-cmx-v11-0-0/.
- For more information about Cisco Spaces, see Cisco Spaces support page.

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.

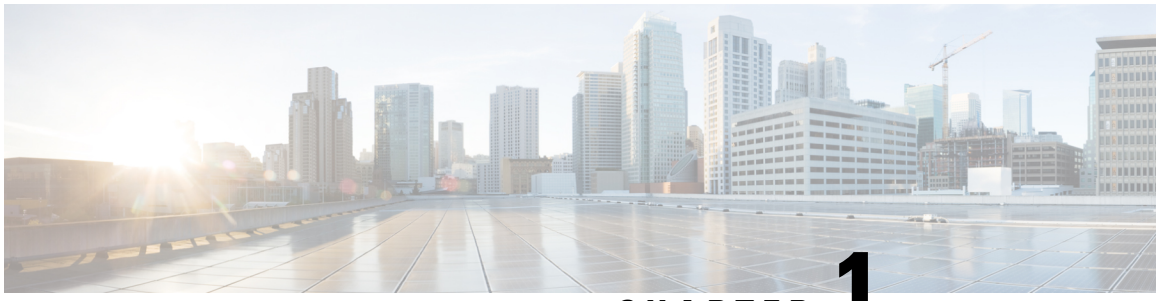
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

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.



CHAPTER 1

Get Started with Cisco CMX

• Getting Started, on page 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 Spaces.

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

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

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

Overview of Cisco CMX Services

Cisco CMX enables you to access the following services:

- **DETECT & LOCATE**: The Detect & Locate service uses the data provided by Cisco WLCs to calculate the X,Y location (based on 0,0 at the top left hand side of the map) of wireless devices that are detected by the access points that support the wireless LAN (WLAN) to a high degree of precision (generally +/-5 to 7 meters, 90% of the time with standard location technologies and +/- 3 meters, 50% of the time with Hyperlocation technologies). Given the proper physical environment with access points deployed in accordance with Cisco best practices for a location ready environment. The CMX GUI will be able to display the physical location of:
  - Associated Wireless Devices (shown as green dots in default view)

- Unassociated Wireless Devices (shown as red dots in default view)
- RF Interferers (Lightning icon)
- Access Points (Circles)
- Rogue Access Points
- Rogue Clients
- Active Wi-fi RFID Tags (Tag icon)

The background map can display:

- Inclusion and Exclusion Zones imported from Cisco Prime Infrastructure
- Analytics Zones created in Cisco CMX
- Thick Walls
- GPS Markers

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

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

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

For more information, see Overview of the Detect and Locate Service, on page 33.

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

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

  - Device count
  - Dwell time
  - Dwell time breakdown
  - Associated User Report

  For more information, see The Cisco CMX Analytics Service, on page 85.

- **MANAGE**: This service enables you to manage licenses, users, zones, beacons, and notifications. For more information, see Overview of the Manage Service, on page 105.

- **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 139.

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

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

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

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

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

To restart Cisco CMX services, follow these steps:

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

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

Cisco CMX Feature Parity

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

Table 2: Feature Parity

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

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

Installing Cisco CMX 11.1.1

Run the **cmxos upgrade** command to perform an inline upgrade from Cisco CMX Release 11.1.0 to Cisco CMX Release 11.1.1. After the upgrade, you must reboot the system. This reboot is necessary because the Linux Kernel upgrades during the process.

After the upgrade is complete, run the **cmxos reboot** command if the system does not prompt to do so. Many Linux packages upgrade during this process, so the Cisco CMX upgrade might take longer to finish.

You can only upgrade from Cisco CMX Release 11.1.0. This is a limitation from Almalinux, which allows OS upgrades only from version 8.10 to 9.6.

Cisco CMX Release 11.1.1 does not support inline upgrade from Cisco CMX Release 10.6.3-146 or earlier.

For more information about installing Cisco CMX, see Cisco Mobility Services Engine Virtual Appliance Installation Guide for Cisco CMX Release 11.1.1.

Upgrade process

If you are upgrading from Cisco CMX Release 11.0.0-154 or Cisco CMX Release 11.0.1-129, perform a **cmxos upgrade**. First, upgrade to Cisco CMX Release 11.1.0, and then upgrade to Cisco CMX Release 11.1.1.

Note With Cisco CMX Release 11.1.1, the Almalinux version is upgraded to to 9.6. The Almalinux upgrade path only allows upgrades from 8.10 to 9.x. Therefore, a direct upgrade from Cisco CMX Release 11.0.0 or Cisco CMX Release 11.0.1 is not possible for this release.

Table 3: Upgrade path

From Release	To Release	Upgrade Method
CMX 11.0.0-154	CMX Release 11.1.1	To upgrade, follow these steps: 1. Run the **cmxos upgrade** command and upgrade to CMX 11.1.0. 2. Run the **cmxos upgrade** command and upgrade to CMX 11.1.1.
CMX 11.0.1-129	CMX Release 11.1.1	To upgrade, follow these steps: 1. Run the **cmxos upgrade** command and upgrade to CMX 11.1.0. 2. Run the **cmxos upgrade** command and upgrade to CMX 11.1.1.
CMX 11.1.0-21	CMX Release 11.1.1	To upgrade, run the **cmxos upgrade** command.

What's New in Cisco CMX Release 11.1.1

This section provides a brief introduction to the new features and enhancements introduced in Cisco CMX Release 11.1.1:

- **AlmaLinux CSL upgrade**: Upgraded from AlmaLinux 8.10 to AlmaLinux 9.6 along with vulnerabilities fixes to various components.

  For more information, see CSL AlmaLinux Upgrade Cisco CMX 11.1.1, on page 8.

- **Data migration**: Data migration is supported from Cisco CMX Release 10.6.3-146 to Cisco CMX Release 11.1.1.

  For more information, see Data Migration.

- **Audit Logging Enhancements**:
  - **Comprehensive Action Logging**: Actions performed on Cisco CMX through CLI, UI, and API interfaces are now logged to the local syslog for improved auditability and system monitoring.
  - **Audit Message Format Update**: Audit messages now utilize a new colon-separated (:) format for improved readability and structured log parsing.

    Audit messages now include these new fields apart from existing fields:
    - IP address from where the user is logged in
    - Module in the Cisco CMX system where the audit message is generated (for example, Location/Configuration)

    - Location in the Cisco CMX system where the audit message is generated (source file/script or referring URL in case of API related audit log)

  - **Audit Message Log Level**: Audit log messages have log level from one to three, one being lowest (and default) and three being the highest. You can modify the log level to generate desired level of logs.
  - **Audit Logging View and Filter**: Run the **cmxctl config audit view** command to filter and view logs of specific modules.

- **Support for two Remote Syslog servers**: This release introduces support for two new remote syslog servers to collect and store system event logs generated by the Cisco CMX system. You can configure up to two remote syslog servers using the **cmxctl config audit settings** command in Cisco CMX. This allows CMX logs to be transmitted to two different syslog servers. Both TLS and IPSEC protocols are supported for communication with these remote syslog servers. However, both servers must be configured to use the same protocol simultaneously—either both use TLS or both use IPSEC.
- **Support for two Unauthenticated NTP Server**: This release supports configuration of up to two unauthenticated NTP servers in Cisco CMX using the **cmxos ntp type** command by selecting the "unauthenticated" type.
- **User Session Management**: This release includes enhancements to improves session management by providing administrators with greater visibility and control over user sessions in the Cisco CMX environment. On the Cisco CMX UI, administrators can now view a list of active user sessions, including both GUI and SSH sessions.
- **SSH Multi-Factor Authentication (SSH MFA) for External Authentication Server**: This release extends the External Authentication Server feature in Cisco CMX to allow SSH access for AAA/RADIUS users, complementing the existing support for GUI access. With this enhancement, AAA/RADIUS users can log in to the CMX SSH terminal using multi-factor authentication (MFA) that involves user certificates and RADIUS server authentication. Use the **cmxctl config authserver settings** command to configure SSH MFA.
- **Certificate Management: Support for 2048-bit RSA key**: This release supports configuring the RSA key length for Cisco CMX certificates to enhance security flexibility. When generating new certificates—whether self-signed or CA-signed—administrators can select the RSA key length to be either 2048 bits or 4096 bits, with 4096 bits set as the default. Use the **cmxctl config certs keytype** command to configure and select **RSA** as the key type.
- Firewall updates: This release introduces conditional opening of port 4242, which is used for High Availability (HA) in Cisco CMX. By default, port 4242 remains closed and is only opened in these scenarios:
  - When a CMX server with the Primary role is converted to the Secondary role using the **cmxha secondary convert** command.
  - When High Availability is enabled on the Primary CMX using the **cmxha config enable** command.
  - When the **cmxha web enable** command is executed by the cmxadmin user on a CMX server with either Primary or Secondary role.
- **HTTP/2 Support on port 4242**: This release allows the HTTP/2 protocol on port 4242 when UCAPL mode is enabled using the **cmxctl config fips ucaplmode enable** command. When UCAPL mode is disabled, port 4242 continues to support the HTTP/1.1 protocol.

- **Password Policy updates**: This release allows all GUI user passwords to include all printable special characters, including whitespace. However, the backslash character (\) is explicitly not allowed in the password.
- **License Type Updates**: This release introduces updates to the Cisco CMX license names.
  - Cisco CMX Essentials (formerly called Cisco CMX Base) is now inlcuded in Cisco Spaces Essentials.
  - Cisco CMX Advantage (formerly called Cisco CMX Advanced) is now inlcuded in Cisco Spaces Advanatge.



Note DNA Advantage customers with a Cisco Spaces Extend license continue to have access to Cisco CMX Essentials (formerly known as Cisco CMX Base) along with CMX Partner Stream capability.

- **Inclusion Zone updates**: This release supports a new parameter in feature flag: **location.perimetercheckon.floorutil**. The default value is **false**.
  - This flag controls how CMX determines whether a client is inside or outside the inclusion zone.
  - When set to **true**, CMX uses floor perimeter coordinates for detection. When set to **false**, CMX uses the legacy method (up to release 11.1.0) based on rails and region information.
  - It is recommended to keep this flag set to **false** unless Maps show clients outside the inclusion zone or outside the floor map.
- **Component upgrades**: This release supports these component version updates:
  - csm-toolkit: Version 1.19.2
  - ciscossl: Version 1.1.1zb.7.2.593
  - ciscossh: Version 1.18.80 (OpenSSH_10.0p2)
  - nodejs: Version 22.16.0
  - npm: Version 10.9.2
  - PostgreSQL: Version 16.9
- **Patch merges**: This release supports these patch merges:
  - cmx-patch-rel-20250902-11.1.0-1
    - cmx-cmxpartner-cli-fix-patch-11.1.0-1
    - cmx-notification-deletion-fix-patch-11.1.0-1
  - cmx-fix-cassandra-perm-patch-11.0.1-1
  - cmx-fix-diag-perm-patch-11.0.1-1
- **Critical issues fixes**: Includes critical bug fixes.

CSL AlmaLinux Upgrade Cisco CMX 11.1.1

To address multiple vulnerabilities found in previous Cisco CMX Releases 11.x.x, upgrade AlmaLinux from version 8.10 to 9.6.

If the upgrade is from Cisco CMX Release 11.1.0 or Cisco CMX Release 11.1.1, perform a system reboot after the upgrade. This system reboot is required for the changes in the Linux Kernel. Run the **cmxos reboot** command after the upgrade if not prompted at the end of the upgrade process.

The Almalinux upgrade path is only available from 8.10 to 9.x, which is why a direct upgrade from Cisco CMX 11.0.0 or CMX 11.0.1 will not be allowed for this release.

Upgrade is allowed only from Cisco CMX Release 11.1.0. This is a known limitation from Almalinux that OS can be upgraded only from 8.10 to 9.6.

An error message might display during the "salt call" process. Disregard these messages as the upgrade process will not be affected. To verify the upgrade status, open another terminal to Cisco CMX and check the upgrade log progress using `tail -f /opt/cmx/var/log/salt-upgrade.log`.

```
** Running salt-call
Error processing line 1 of /opt/saltstack/salt/lib/python3.10/site-packages/relenv.pth:

   Traceback (most recent call last):
File "/opt/saltstack/salt/lib/python3.10/site.py", line 186, in addpackage
   exec(line)
File "<string>", line 1, in <module>
File "/opt/saltstack/salt/lib/python3.10/site-packages/relenv/runtime.py", line 774, in
bootstrap
   setup_openssl()
File "/opt/saltstack/salt/lib/python3.10/site-packages/relenv/runtime.py", line 703, in
setup_openssl
   _, directory = proc.stdout.split(":")
   ValueError: too many values to unpack (expected 2)
```

When you upgrade to Cisco CMX Release 11.1.1, the system upgrades the CSL version from 8.10 to 9.6. This upgrade processes several hundred system packages during the CMX upgrade. Therefore, the upgrade takes longer to complete and the screen may not display much activity for some time.

Open another terminal to CMX and check the upgrade log progress using:

```
tail -f /opt/cmx/var/log/salt-upgrade.log
```

Migrate data to Cisco CMX Release 11.1.1

Migrate configuration and data from Cisco CMX Release 10.6.3-146 to Cisco CMX Release 11.1.1 to ensure continued access to historical data and system settings on the updated release platform.

Cisco CMX Release 11.1.1 supports data migration from Cisco CMX Release 10.6.3-146 to the latest Cisco CMX Release 11.1.1.

Data migration or inline upgrade from releases earlier than Cisco CMX Release 10.6.3-146 is not supported.

This data migration process applies when upgrading Cisco CMX from release 10.6.3-146 to 11.1.1. It requires specific verification and preparation steps to maintain data integrity, minimize downtime, and support optional high availability configurations.

Before you begin

Before starting the data migration, verify that the system date is correct in both Cisco CMX.

Note If you are migrating from a Cisco CMX release earlier than 10.6.3 to 11.x, do not copy older certificates, even if the certificates remain valid. The purpose fields of CMX Server certificates have changed in 11.x, so old certificates do not work when High Availability is enabled.

Instead, new CMX certificates should be generated either as self-signed or CA-signed for CMX services and High Availability to work correctly.

Follow these steps to migrate data.

Procedure

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

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

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

a) To verify the Cisco CMX Release, run the **cmxctl version** command.
b) Install the patch: cmx-11-migration-readiness-patch. For more information, see *README.txt* text file.
c) To create a backup file on Cisco CMX Release 10.6.3-146, run the **cmxos backup --path /home/cmxadmin --include_onlydatabase,cache,cassandra,floormaps** command.

If High Availability is configured on Cisco CMX Release 10.6.3, create backup from the primary box only.

Step 3 On the Cisco CMX server running the image version of Cisco CMX Release 11.1.1-111, run the following commands:

Note
We recommend that you execute the steps when the Cisco CMX is in standalone mode (Day 0 (initial) configuration). After restoring the data, continue with High Availability pairing if required.

If High Availability was paired without restoring the previous data, restore the data only in primary. The data transfer from the primary server to the secondary server is handled internally.

a) To stop the monit service, run the **cmxos monit stop** command.
b) To stop all Cisco CMX services, run the **cmxctl stop –a** command. This is mandatory as the restore fails during the cache services restart.
c) To restore backup on Cisco CMX Release 11.1.1-111 instance, (before pairing the High Availability), run the **cmxos restore** *--file /home/cmxadmin/cmx_backup.tar.gz --include_only database,cache,cassandra,floormaps --ignore_licenses* command.

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

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

The data migration from previous Cisco CMX Release is complete.

Wireless Controller and Wi-Fi Client Support

Cisco CMX Release 11.1.0 supports the new message IDs (associated with Wi-Fi 7 client) along with the old message IDs for backward compatibility with the Cisco Catalyst 9800 Series Wireless Controller.

Cisco CMX Release 11.1.0 supports Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.15.2 or later releases.

Note For Cisco CMX Release 10.6.3-146, a separate patch will be available to support the new message IDs.

Generate Root Password

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

Procedure

Step 1 Log in to the Cisco CMX CLI as cmxadmin user.

Step 2 To generate a root challenge text, run the **cmxctl users get-root-challenge** command.

The root challenge text is valid for 30 minutes.

Step 3 To get the root login key, open a case with Cisco's Support Services Technical Assistance Center (TAC).

Step 4 To generate a new password, run the **cmxctl users enable-root** command.

Step 5 Enter the token generated by the cloud support team and the new password.

By default, the root access is disabled within six hours.

Step 6 (Optional) To manually disable the root access login, run the **cmxctl users disable-root** command.

Using the Evaluation License

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

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

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

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

- For two weeks before the evaluation license expires, a daily alert is displayed on the Cisco CMX **System > Alerts** window.
- An alert email is sent if you have configured email settings.
- An alert is displayed when you log in to Cisco CMX.

To add a license, click **Add new license** from the alert. You can also add a license from the Cisco CMX **Manage** > **Licenses** window. For information about adding permanent licenses, see Managing Licenses, on page 112.

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

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

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

Logging In to the Cisco CMX User Interface

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

Before you begin

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

Procedure

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

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

The Cisco CMX user interface displays the Login window. If SSO is enabled in Cisco CMX, **Sign in with SSO** option is displayed. For more information about configuring SSO, see Configuring SSO Authentication in Cisco CMX, on page 12.

Step 3 Enter your username and password.

Note

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

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

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

- The default username is admin and the default password is admin.
- The default global session timeout for Cisco CMX GUI is 30 minutes. This is the absolute session timeout which works from the session establishment time to the session end time irrespective of whether the session remain active on Cisco CMX.
- If a Cisco CMX CLI or GUI user account is inactive for 60 days or more, the account is locked. A Cisco CMX admin user (cmxadmin) can unlock the account and use the applicable command:
  - **cmxctl users unlock gui <userID>** command to unlock the user's Cisco CMX GUI account.
  - **cmxctl users unlock cli <userID>** command to unlock the user's Cisco CMX CLI account.

  If the Cisco CMX admin user account is locked out, the admin user must connect directly to the console and use the applicable command: **cmxctl users unlock gui <userID>** or **cmxctl users unlock cli <userID>**.
- You can use the **cmxctl config auth settings** command to set the expiration period for the password. The default expiration period is 9999 days.

Configuring SSO Authentication in Cisco CMX

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



Note

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

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

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

The following is a list of prerequistes for configuring SSO:

- Cisco CMX integrated with SAML 2.0 framework
- IDP with SAML 2.0 support
- Cisco CMX with proxy confgured to reach IDP endpoint

The following is a list of limitations while configuring SSO:

- Only a cmxadmin user can manage SSO configurations. Ensure that you disable SSO before you log in to Cisco CMX.
- A user with cmxadmin or admin role is exempted from the SSO authentication while logging in to Cisco CMX.
- Ensure that you configure the SSO settings everytime when you install or generate a new server certificate on Cisco CMX.
- SSO authentication is not applicable for Web Installer, SSH login, and HA 4242 port login and for API Server user management and API Docs.

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

Procedure

Step 1 To setup proxy settings on Cisco CMX, run the following command:

cmxos sysproxy

Step 2 To restart agent, run the following command:

cmxctl agent restart

Step 3 To restart Cisco CMX services, run the following commands:

- **cmxctl stop**
- **cmxctl start**

Step 4 To configure SSO on Cisco CMX, run the following command:

cmxctl config sso configure

Note

- After you run this command, you need to confirm if you want to perform a check on Cisco CMX database for users with username assigned to them. You will also get a prompt to confirm what role to assign to a user in case a user does not exist in Cisco CMX or if database lookup for a role is not allowed.
- Ensure that you have IDP metadata XML file available to download on Cisco CMX. You can download the IDP 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 the IDP metadata file from https://%3Cadfs-server-name%3E/FederationMetadata/2007-06/FederationMetadata.xml
- If you are unable to download the IDP file, you must provide related information such as SSO endpoint URL for 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 SP metadata file.
- The type of **NameIDFormat** used by Cisco CMX is email Address. Cisco CMX will use **emailAddress** returned in SAML resposne.
- Cisco CMX requires firstname, lastname, email address field information from IDP in SAML response. Cisco CMX will extract the username from email address by stripping the @domain part from email address. For

example, if email address is xyz@abc.com, Cisco CMX will strip @abc.com out and use **xyz** as username for SSO user.

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

  We recommend that you remove the **X509 Cert parsed** from SP Metadata File on ADFS as it will result in the 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, login credentials are not prompted and user is logged in automatically. This is because the IDP session is still valid and not yet expired. As a work around, you will have to close the browser window every time you logout of Cisco CMX.

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

The following is a sample of SP metadata XML file:

```
<?xml version="1.0"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:
metadata" validUntil="2019-08-15T20:23:26Z" cacheDuration="PT604800S"
entityID="https://10.30.114.196/login/" ID="ONELOGIN_78ca24a0-8e9c-4fc9-b258-688e07354084">
<md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing"><ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data><ds:X509Certificate>MIIFhDCCA2ygAwIBAgIEXUiZADANBgkqhkiG9w0BAQsFADBMMQswCQYDVQQGEwJV
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 Catalyst Center, ensure that none of these reserved names are used in the Maps elements. If this recommendation is not followed, maps on Cisco CMX may not function well and you will see the campus, building, floor hierarchy incorrectly from the parent child relationship.

Copying the Exported Maps

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

Importing Maps

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

When you import maps, they are appended to the existing ones in Cisco CMX. When Cisco CMX finds that a campus whose name already exists in Cisco CMX has a different UID in the import map file, Cisco CMX performs a map sync operation under this campus if the override option is set to **Yes**. For more information about importing maps, see Importing Maps and Controllers into Cisco CMX, on page 153.

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

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

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

Note

- Cisco CMX does not support auto-synchronization of map updates from Cisco Prime Infrastructure. We recommend that you perform a manual synchronization in Cisco CMX to get the latest map updates from Cisco Prime Infrastructure.
- After upgrading to Cisco CMX Release 10.6.3, the Cisco Prime Infrastructure stops displaying clients on the Cisco Prime Infrastructure map. This is due to the deprecation of V1 and V2 client API calls in Cisco CMX Release 10.6.3. Cisco Prime Infrastructure Release 3.8 and older versions use V1and V2 API calls to CMA to get the client information and hence it fails. To work around this issue, in the Cisco Prime Infrastructure Release 3.9, there is an option to specify the Cisco CMX V3 API credentials while adding Cisco CMX in Cisco Prime Infrastructure and thus Cisco CMX Release 10.6.3 works with Cisco Prime Infrastructure Release 3.9.

Adding Controllers

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

- **AireOS**: Provide SNMP RW credentials for the AireOS WLCs after you import them to successfully add them to Cisco CMX.
- **Catalyst 9800**: Provide SSH credentials and enable password details.

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

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

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

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

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

Note Using the **cmxctl config controllers import [FILE]** command to add controllers via a CSV file may fail if the CSV file format is incorrect. To address this issue, add the controllers using the GUI.

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 153.

Note

- Cisco CMX does not support Cisco Catalyst 9800 Series Wireless Controllers with special characters > or # in the message-of-the-day (MOTD) banner.
- After adding controllers, you must verfiy if the controller status is up and running. Using the CLI, you can run the command **cmxctl config controllers show** to display the list of controllers with the status. An **Active** status indicates an established connection.
- To validate the controller status using user interface, you need to navigate to the **System** tab. The controllers list is displayed in the tab and the new controller should appear in green. For more information, see Understanding the Controllers Table, on page 143.

Import Controllers using CLI

Cisco CMX accepts three options for importing a controller via CLI using a CSV file:

- **AireOS SNMP v2**: [AireOS WLC, ipAddress, wlcver [Blank allowed], snmpVersion, snmpWriteCommunity]

  Example: WLC,1.2.3.4,,v2c,testCommunity

- **AireOS SNMP v3**: [AireOS WLC, ipAddress, wlcver [Blank allowed], 'v3', username, authType, authPassword, privType, privPassword]

  Example: WLC, 1.2.3.4,,v3,username,hmacsha,authPasswordauthPassword!,aescfb128,privPasswordprivPassword!

- **9800/IOS-XE**: [Catalyst (IOS-XE) WLC, ipAddress, version [Blank allowed], telnet username, telnet password, telnet enablePassword]

  Example: Catalyst (IOS-XE) WLC, 1.2.3.4,,admin,Cisco123!,Cisco123!

Note The **authType** options are hmacmd5 or hmacsha, and the **privType** options are des or aescfb128. These parameters are mandatory and case-sensitive.

Follow these steps to import controllers using Cisco CMX CLI.

Before you begin

You can add controllers via Cisco CMX CLI using CSV file.

Procedure

Step 1 Open the terminal.

Step 2 To initiate the controller import process, run the **cmxctl config controllers import** command.
A window displays prompting you to specify the import type. The options available are: [PI/FILE] (PI, FILE) [FILE].

Step 3 Choose the import type as **FILE** (CSV file import)and enter the option as **`FILE`**.

Step 4 Enter the path to the CSV file containing the controller details. For example, **`/home/cmxadmin/SampleControllerAdd.csv`**.

Step 5 Verify if the CSV file contains the controller details in the specified format. Each line in the CSV file should follow one of these three formats:

- **AireOS WLC:** WLC, ipAddress, wlcver [Blank allowed], snmpVersion, snmpWriteCommunity
- **Catalyst (IOS-XE) WLC:** Catalyst (IOS-XE) WLC, ipAddress, version [Blank allowed], username, password, enablePassword
- **AireOS WLC (v3 SNMP):** WLC, ipAddress, wlcver [Blank allowed], 'v3', username, authType, authPassword, privType, privPassword

For example,

WLC,10.10.10.1,7.4.121.0,v2c,private

WLC,10.10.10.3,,v3,admin,hmacmd5,pass,des,pass

WLC,10.10.10.4,,v3,admin,hmacsha,pass,aescfb128,pass

Catalyst (IOS-XE) WLC,10.10.10.2,,admin,admin,admin

Note

- Importing Controllers using the CSV file with the command **cmxctl config controllers import** [FILE] may fail if the correct format is not followed. For example, you might get the following errors:
  - Error: Invalid value: Invalid number of columns in row
  - Error: Invalid value: Unsupported controller type in row
  - _csv.Error: iterator should return strings, not bytes
- Leave the Controller version blank. Cisco CMX fetches this information from Controller.
- Use **WLC** for AireOS and **Catalyst (IOS-XE) WLC** for 9800/IOS-XE. These parameters are essential for Cisco CMX to identify the controller type.
- If some controllers are unreachable via SNMP (AireOS) or SSH (9800/IOS-XE), the import may fail.

After the CSV file is processed, a confirmation message is displayed indicating that the controller is added successfully.

Enabling or Disabling Cisco CMX Services

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

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

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

Installing Certificates in Cisco CMX

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

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

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

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

- TLS Web Server Authentication
- TLS Web Client Authentication

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

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

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

Installing a Self-Signed Certificate

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

Procedure

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

Step 2 Run the following commands:

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

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

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

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

Note
When a Cisco CMX instance with a self-signed certificate is added in Catalyst Center, the Cisco CMX IP address must be added in the Subject Alternative Name (SAN) IP address. In the Cisco CMX Release 11.1.0, a new command is introduced to add the SAN IP in the self-signed certificates.

Step 3 To add the SAN IP address in the self-signed certificates:

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

b. To install the new certificates, run the **cmxctl config certs installnewcerts--add-ip-san** command.

c. To apply the certificate changes, restart the Cisco CMX services.

Step 4 Press **Enter** to restart the Cisco CMX services.

Step 5 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.

OCSP Support for Certificates

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

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

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

Wildcard Certificate Support for Cisco CMX

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

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

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

Before you begin

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

Procedure

Step 1 Install CA-signed certificates on primary server.

a) To clear current certificates, run the **cmxctl config certs clear** command.
b) To generate Certificate Signing Request (CSR), run the **cmxctl config certs createcsr** command
c) On Cisco CMX server, run the **cmxctl config certs importcacert** command to import CA certificate.
d) To import server certificate and private key (combined into single file), run the **cmxctl config certs importservercert** command.

Note
For more information, see Installing a CA-Signed Certificate, on page 21.

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

Note
- If **Secondary CMX** is selected during the initial web installation, then entire CMX services are not installed and the **cmxctl config certs** commands are not available to install CA-signed certificates. As a workaround, use the **cmxos seccerts** commands to clear, create a CSR, import a CA certificate, or

import a server certificate. The commands are exactly same as corresponding keyword options under the **cmxctl config certs** command.

- If Cisco CMX was installed as primary server and then converted to a secondary server using the **cmxha secondary convert** command, use the cmxctl config certs command to install the secondary server certificates.
- Ensure that both primary and secondary certificates are signed by the same Certification Authority.

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

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

Step 4 Enable HA pairing.

Adding Users and Managing Roles

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

The following list displays the types of users:

- Admin users—An admin user can access all the services and functionalities (based on the license type) of Cisco CMX.
- Others—An admin user can create other users and assign roles to them.

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

- System
- Manage
- Analytics
- Read Only
- Location
- Admin

For more information about the creation of users and assignment of roles, see Managing Users, on page 116.

Using the Cisco CMX Setup Assistant

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

REST APIs Version 3 Support in Cisco CMX

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

- Wi-Fi Tags
- Rogue Clients
- Rogue Access Points (AP)
- Interferers

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

Supporting Active Clients Version 3 API

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

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

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

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

Active Clients v3 API supports these additional parameters:

- mapHierarchy
- manufacturuer
- macAddressSearch
- associated/probing

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

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

Getting APIs

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

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

Note

- The apiserver must be running on Cisco CMX before the API call is initiated.
- For support in using APIs, including the GitHub version of API Version 3, contact the Cisco DevNet Community at: https://developer.cisco.com/site/cmx-mobility-services/.

Restricted CLI

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

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

Table 4: Linux Commands Allowed in the Restricted CLI

Command	Description
cat	Prints file contents.
cp	Copies file.
df	Prints the file system disk space usage.
du	Prints the file space usage.
grep	Prints the lines matching a pattern.
ifconfig	Displays the network interface configuration.
ls	Lists the directory contents.
nslookup	Queries the internet name servers.
passwd	Changes the cmxadmin password.
ping	Sends Internet Control Message Protocol (ICMP) echo requests to network device.
pwd	Prints the current or working directory.

Command	Description
route	Displays the routing table.
rm	Removes the files.
scp	Secures the remote copy files.
sftp	Secures file transfer.
ssh	Use Secure Shell (SSH) to connect with the client.
tail	Outputs the last part of a file.
top	Displays the Linux process.
wget	Network downloader

Encrypting Cisco CMX Connection to Remote Syslog Server Using IPSec Protocol

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

Before you begin

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

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

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

Procedure

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

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

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

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

```
[cmxadmin@cmx]# cmxctl config ipsec authtype
Current IPSec Auth Type = PUBKEY
Do you want to change it? (y/n) [n]: y
```

```
Select IPSec Auth Type: (PUBKEY/PSK) [PUBKEY]: PSK
IPSec auth type changed to PSK.
IPSec is configured with PSK : nIXRjNrMiNzcKj7yVZ0Nod5IzxUyO9XZ
Configuring ipsec ....
In primary
Stopping strongSwan IPsec...
Starting strongSwan 5.6.2 IPsec [starter]...
```

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

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

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

About Cisco CMX Integration with Cisco Catalyst Center

Cisco Catalyst Center (formerly known as 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 Catalyst 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 Catalyst Center, see the *Catalyst Center User Guide* at:

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

Note Cisco CMX should be anonymized for security purposes.

Create Cisco CMX Settings

Procedure

Step 1 In the Cisco Catalyst 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, Catalyst 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 Catalyst 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 Catalyst 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 Catalyst 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 Catalyst Center Maps API to list the clients on the floor: `curl -k -u <user>:<password> -X GET /api/v1/dna-maps-service/domains/<floor group id>/clients?associated=true`

Remote HTTPS Server Support for Windows OS

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

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

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

Procedure

Step 1 Choose **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

Step 2 Click **HTTP Response Headers**.

Step 3 In the Actions panel, click **Add**.

Step 4 In the Add Custom HTTP Response Headers dialog box, enter the value: **`2 Value: max-age=31536000`**.

Step 5 Confirm the changes and close **IIS Manager**.

Step 6 To redirect users to visitors to the HTTPS URL, follow these steps:

a) Open the **IIS Manager**.
b) Click **HTTP Redirect**.
c) Check the **Redirect** check-box.
d) Enter the target URL (HTTPS).
e) Set the status to Permanent Redirect (301).

What to do next

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

Support for Proxy with Basic Authentication

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

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

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

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

External Endpoint Connect

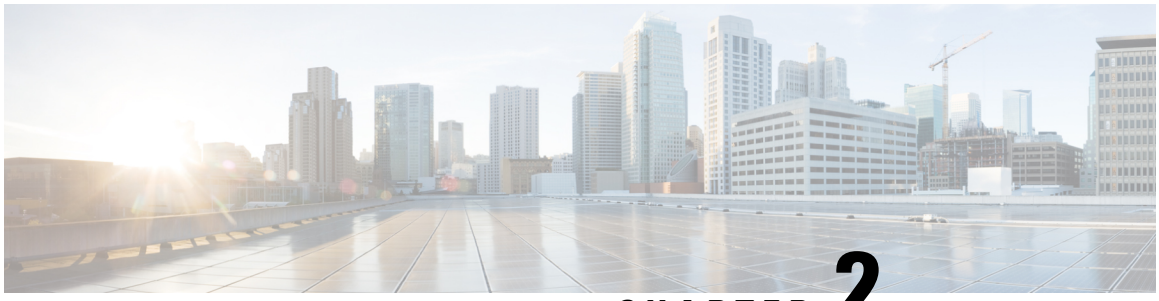
Ensure that the firewall permits outbound HTTP and HTTPS connections to the required external endpoints.

Table 5: External Endpoints

Service/API	Endpoint URL	Purpose	CMX Module/Feature	Connection Type
OpenStreetMap Nominatim	nominatim.openstreetmap.org/reverse and /search	Forward geocoding only (converts addresses to coordinates)	Location Services—Address Resolution	Client-side (browser)
Cisco Spaces	dnaspaces.cisco.com	Portal access for DNA Spaces integration	Admin Portal—External Link	User-initiated
Cisco Smart Licensing	cisco.com/software/smartaccounts	License management and registration	System Settings—License Section	User-initiated

Note

- OpenStreetMap is a public service and does not require authentication.
- Ensure that the firewall permits outbound HTTP and HTTPS connections to these endpoints.
- Cisco portal links are user-initiated only; no automatic connections are made.



CHAPTER 2

The Cisco CMX Detect and Locate Service

- Overview of the Detect and Locate Service, on page 33
- Initial Configurations, on page 33
- Viewing or Tracking Devices, on page 34
- Enhanced Associated Clients Tracking, on page 39
- Viewing Device Details, on page 40
- Customizing Client Refresh Rates, on page 40
- Customizing Device Views Using Filters, on page 41
- Adding and Deleting Filters, on page 41
- Searching for a Device, on page 42
- Client Playback, on page 43
- Data Privacy, on page 43
- CMX Grouping, on page 45
- Enabling Cisco Hyperlocation and FastLocate in Cisco CMX, on page 47
- Controlling the Probing Client Expiry Time, on page 63
- Supported Access Points for Cisco CMX 10.5 Location Features with Cisco WLC 8.7, on page 64
- Measuring Client Location Accuracy Using the Location Accuracy Test, on page 65

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 and Wi-Fi interferers.

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 16.
- Add controllers—For information about concept, see Adding Controllers, on page 17.

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

World Map

The World Map requires an active internet connection on the client machine to retrieve map data from an external map service. If internet access is unavailable or the service is blocked, the map background may appear blank or fail to load.

Viewing or Tracking Devices

Procedure

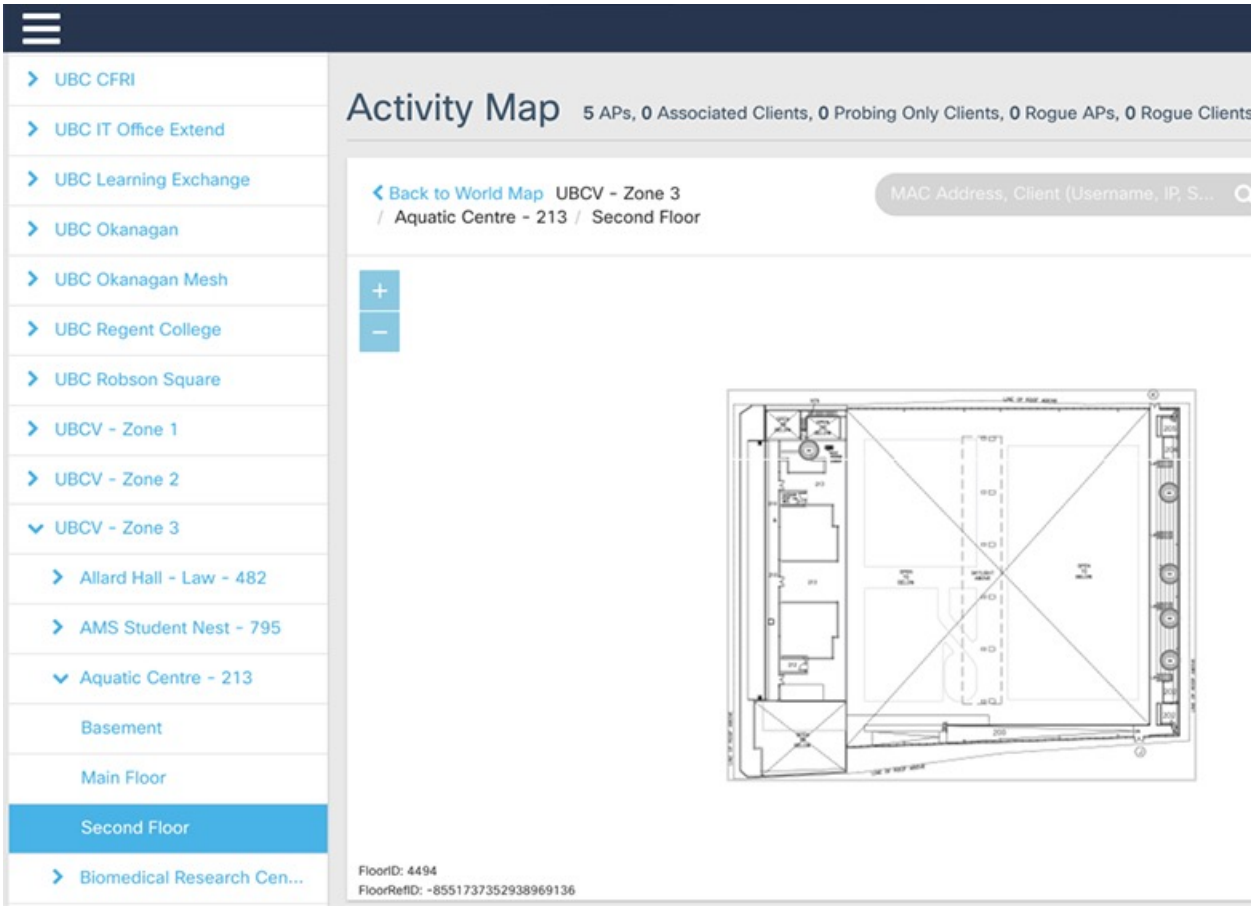
Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).

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 2000. If t
    connected clients are displayed, again up to a maximum of 2000 (see the figure below). However, if the nu
    also exceeds 2000, no clients are displayed. In such a scenario, we recommend that you use the Analytics servi



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

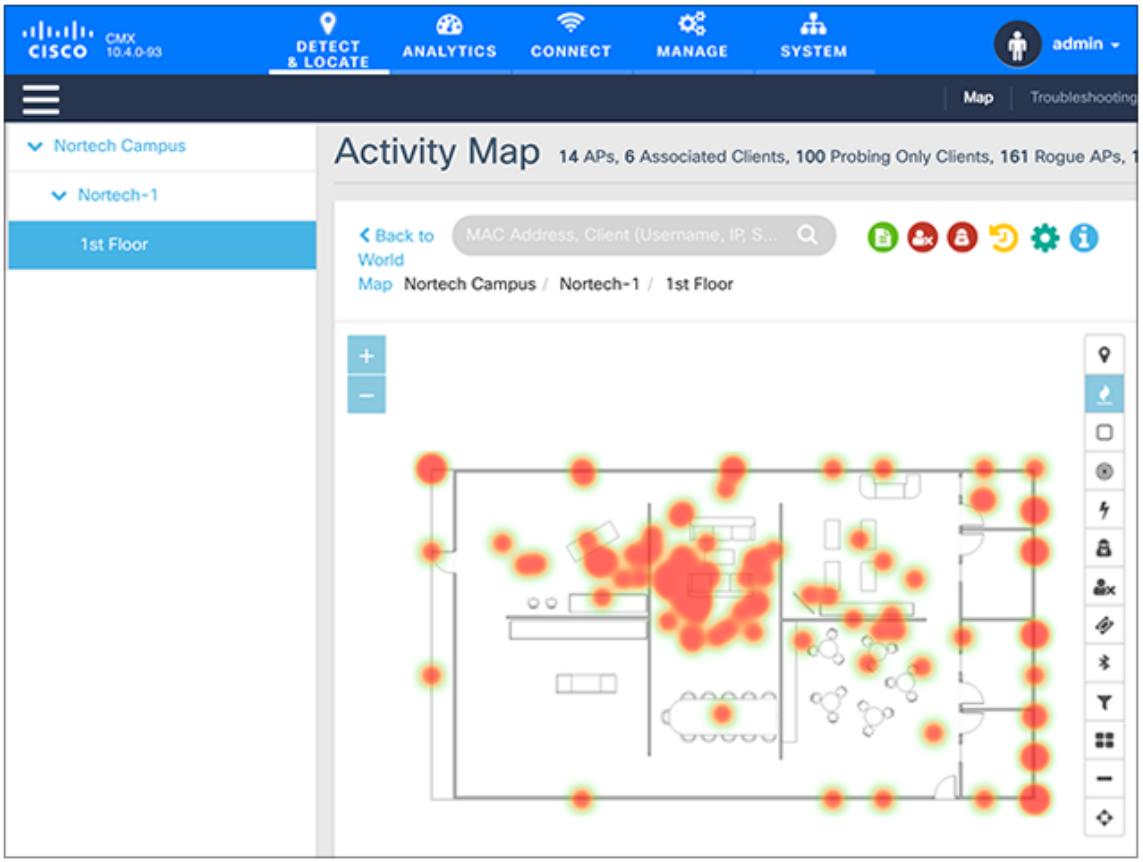
  This behavior depends on the phone usage and for such inactive, sleeping devices, Cisco CMX would not show

- Cisco CMX needs the WIFI devices to send RSSI probe messages to have the very first location available. Aft WIFI devices are expected to send regular updates to Cisco CMX so that Cisco CMX maintains the device stat status displays as active on the controller. However they are not sending any RSSI probe messages and hence C non-locatable devices. Such devices are not considered as active devices on Cisco CMX and is discarded.

- 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 that are not p 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 146. 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 144.

- **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 42.

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 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 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.

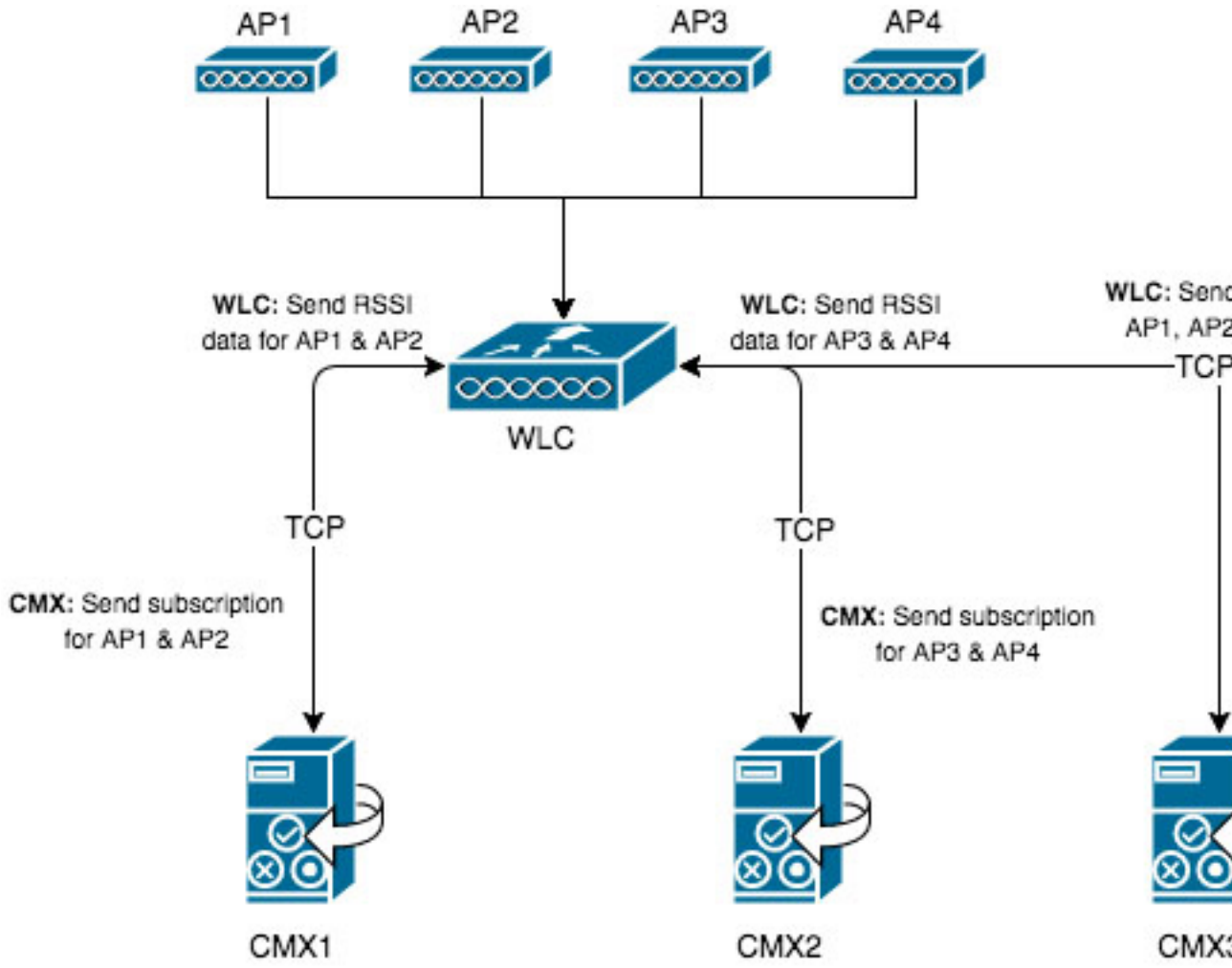
The performance of Cisco CMX can be optimized in the following ways:

- 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.

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).

The following Wi-Fi6 access points support Cisco FastLocate:

- Cisco Aironet 9120 Series Access Points
- Cisco Aironet 9130 Series Access Points

The following access points support Cisco FastLocate:

- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points

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 45.
- 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** 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

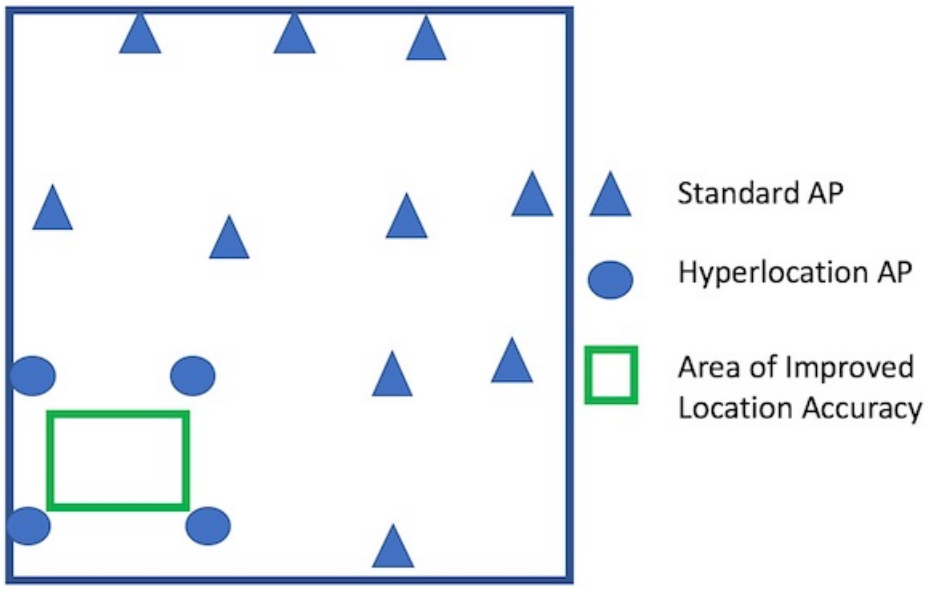
Hyperlocation groups are formed consisting both hyperlocation and regular access points. The floor mode is decided when generating the hyperlocation group. There following are the three supported modes:

- 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.

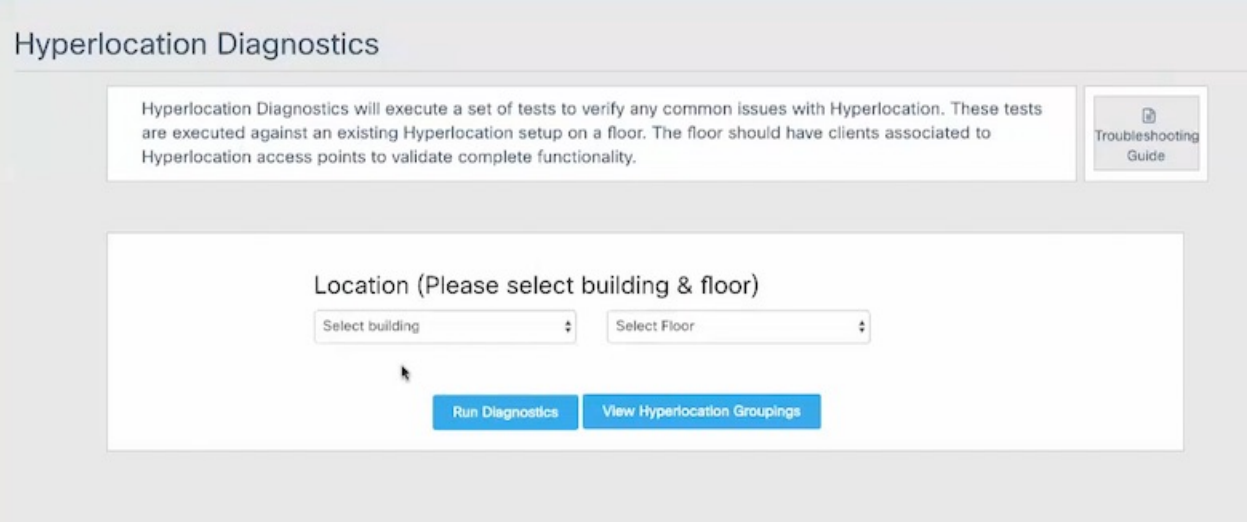
Hyperlocation Diagnostics executes a set of tests to verify any common issues with Hyperlocation. These tests are executed against an existing Hyperlocation setup on a floor. The floor should have clients associated to Hyperlocation access points to validate complete functionality.

Procedure

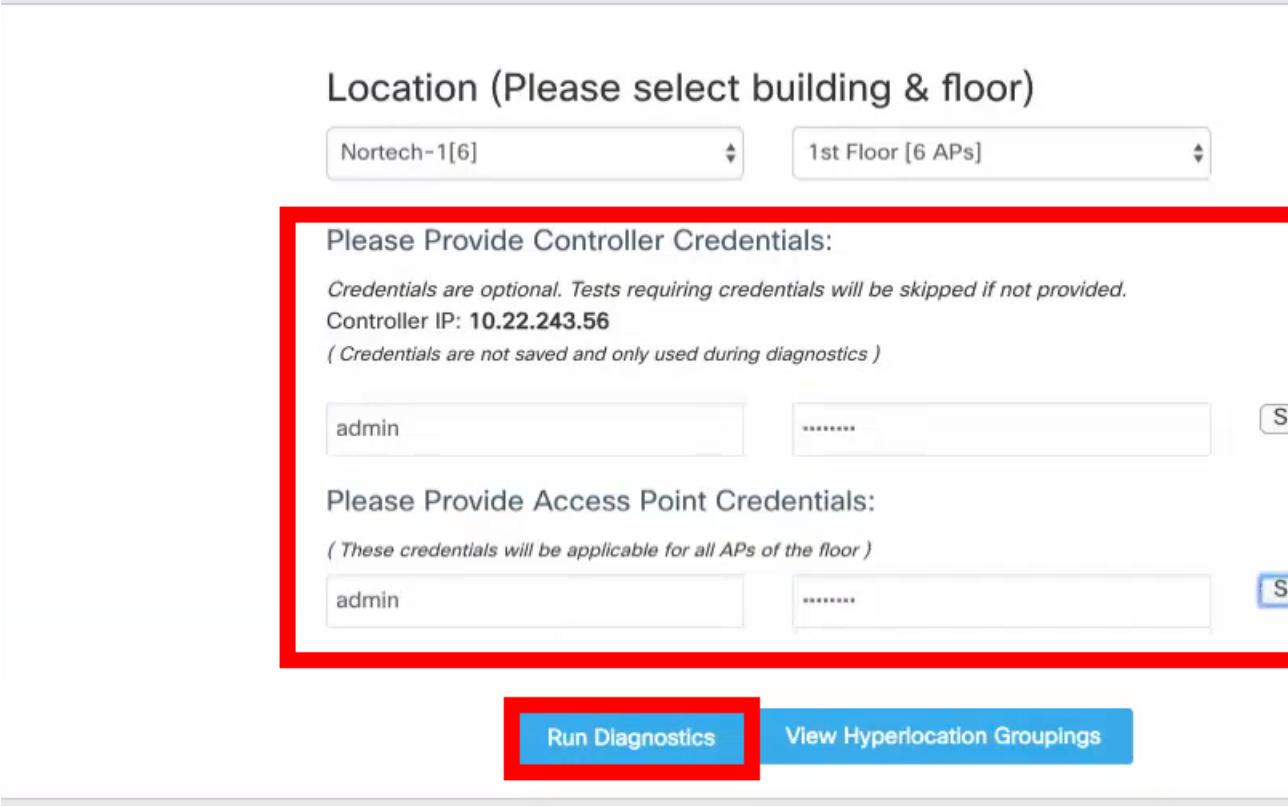
Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX) either as an admin user or a user with Location role.

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.

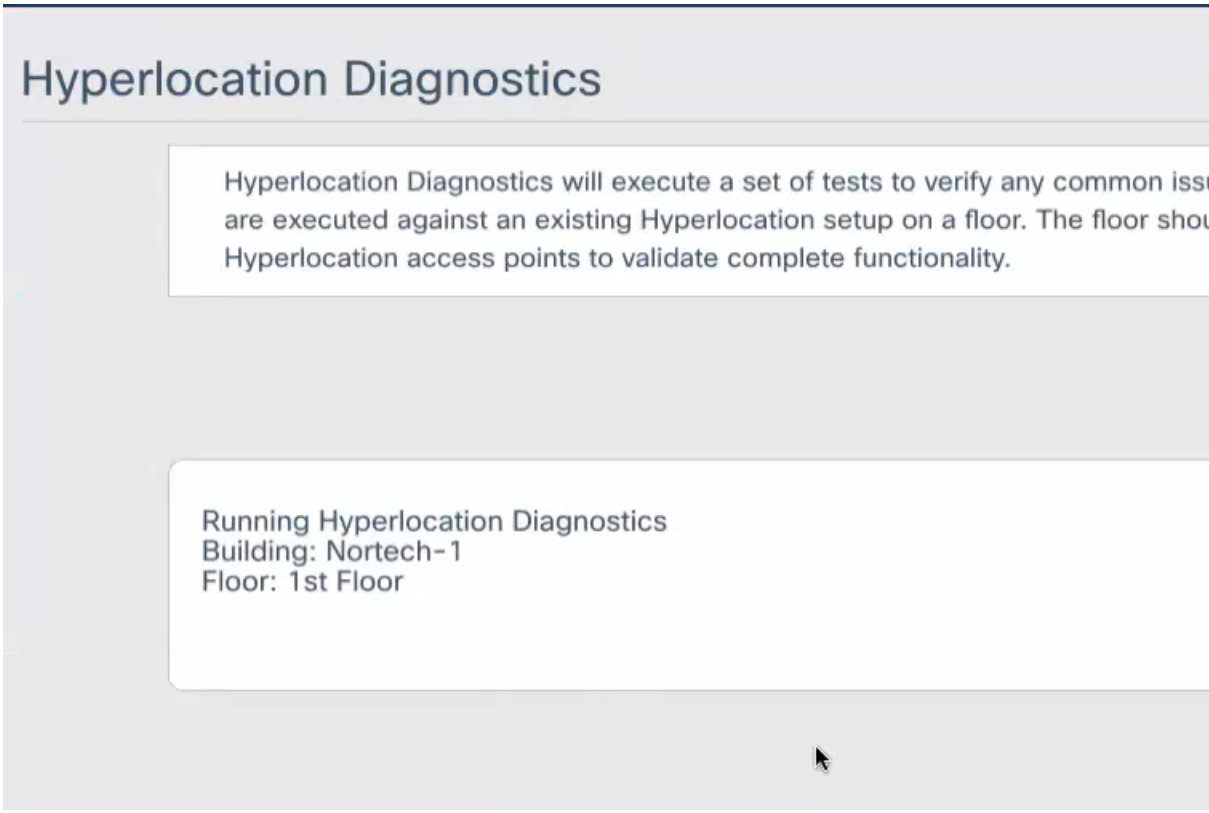


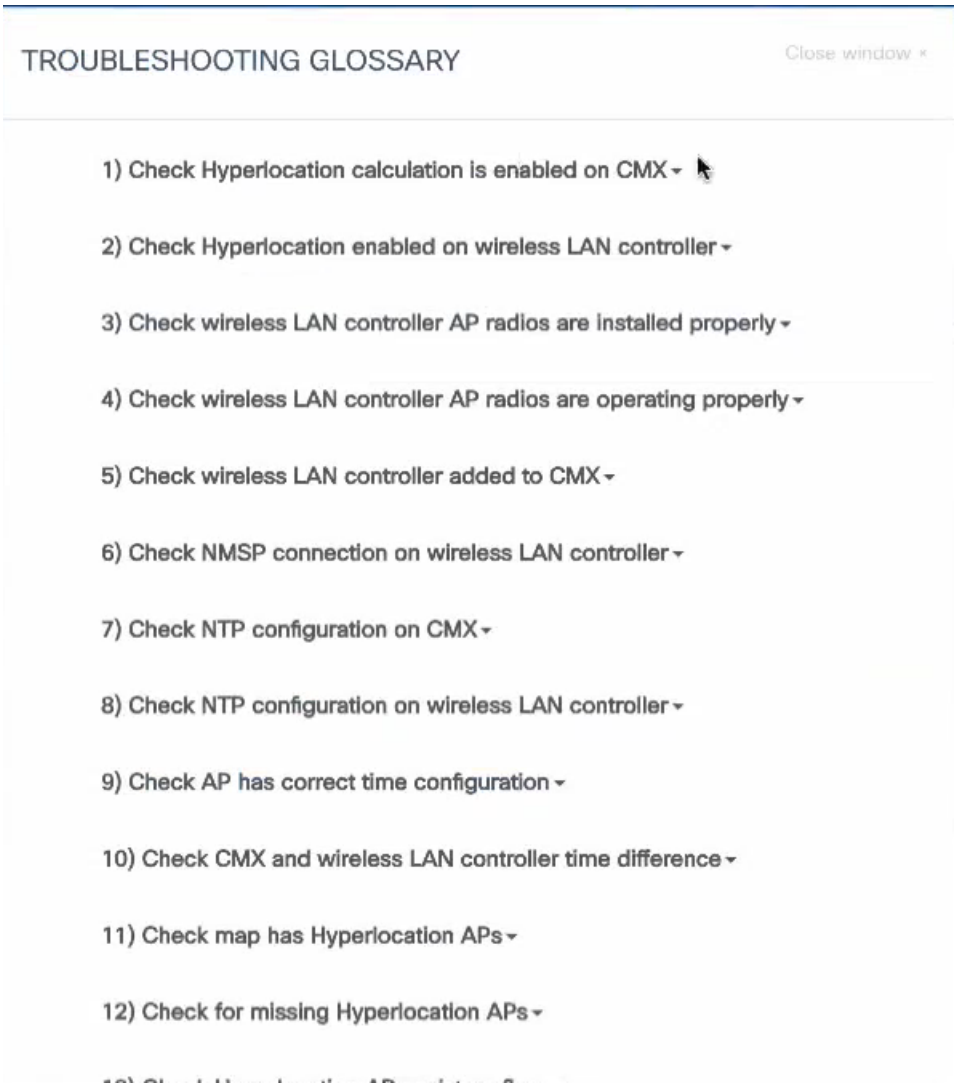
Step 3 (Optional) Add the details and credentials of a controller and an access point for a more detailed report.



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

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

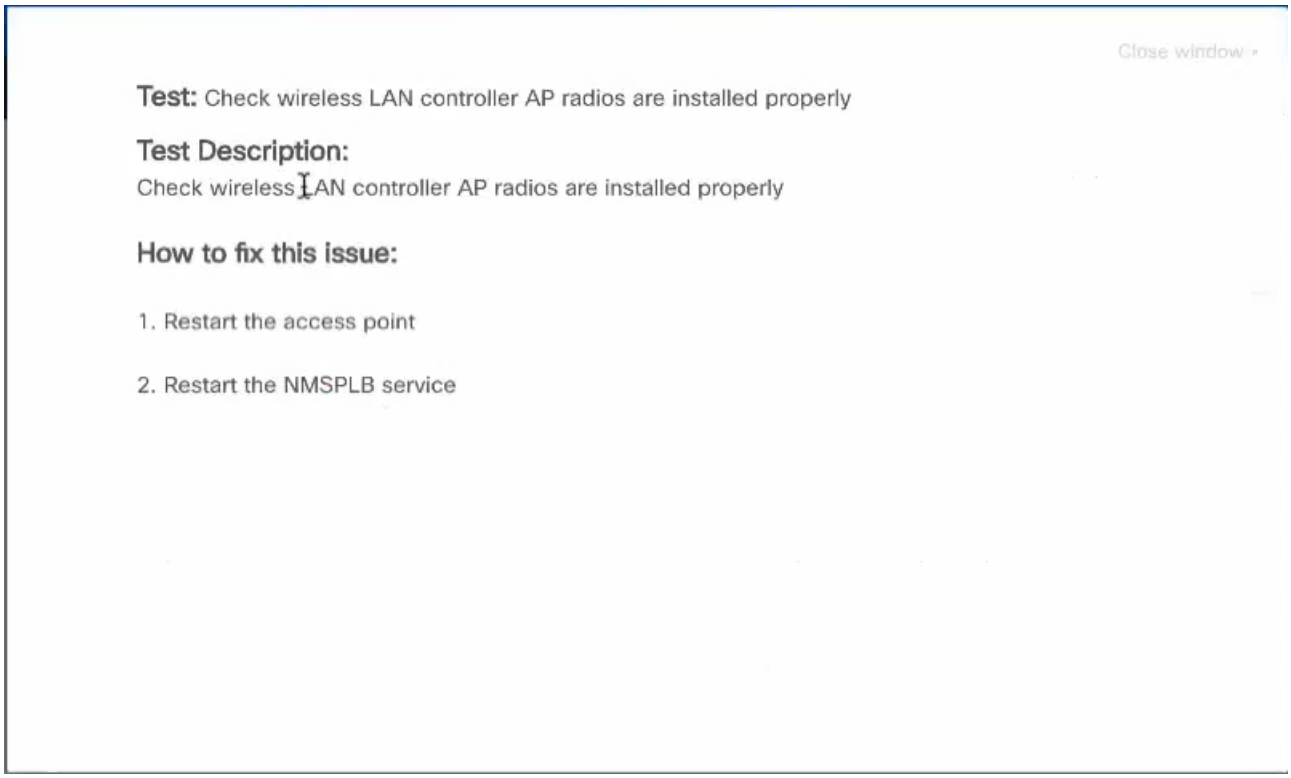

Hyperlocation Diagnostics
Hyperlocation Diagnostics will execute a set of tests to verify any common issu
are executed against an existing Hyperlocation setup on a floor. The floor shou
Hyperlocation access points to validate complete functionality.
Running Hyperlocation Diagnostics
Building: Nortech-1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



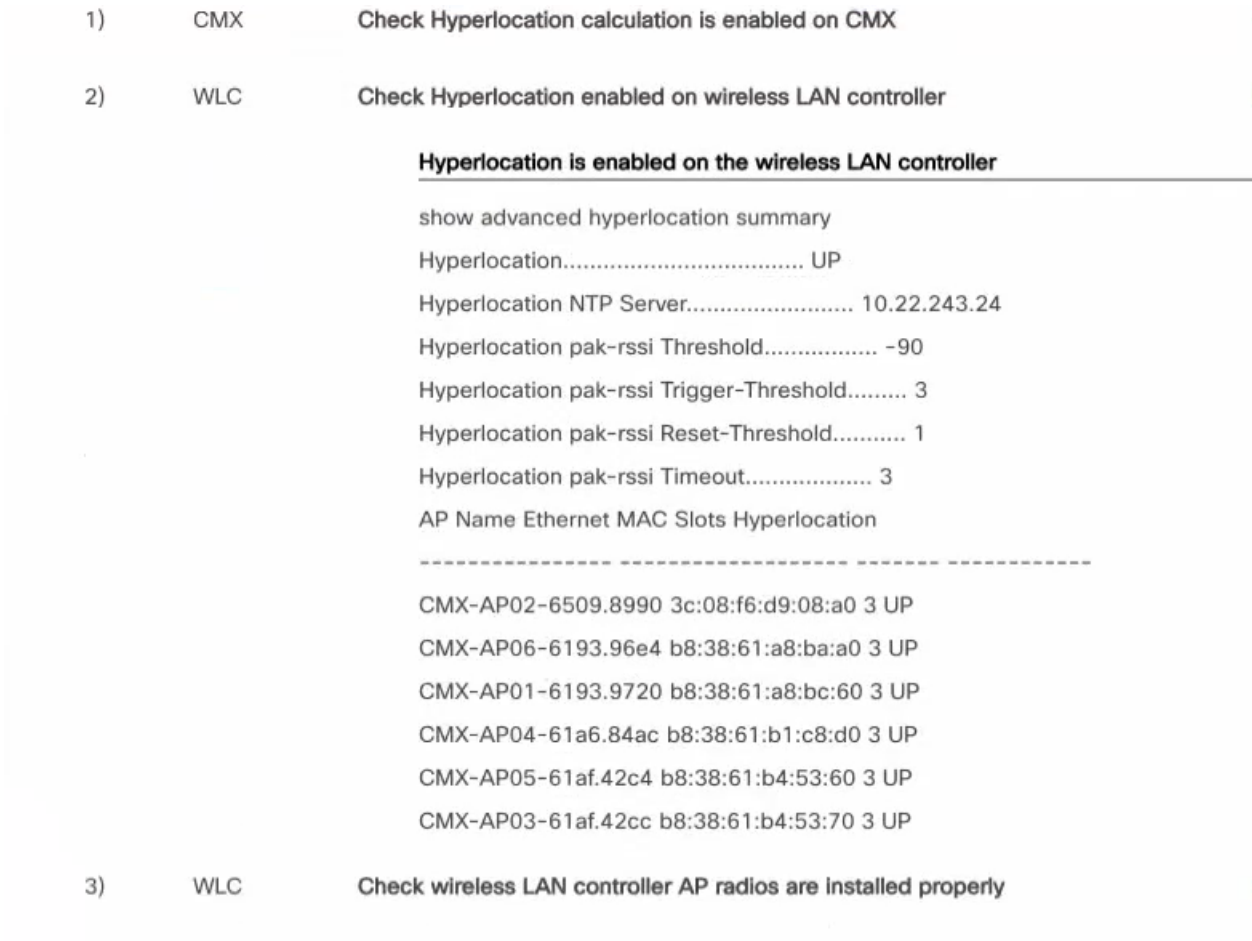
Step 5 Observe a sample test result. The Test Type indicates which deployment component is being tested, and it can be CMX, WLC, or AP.

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

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	Pas
2)	WLC	Check Hyperlocation enabled on wireless LAN controller	Pas

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	Fail

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

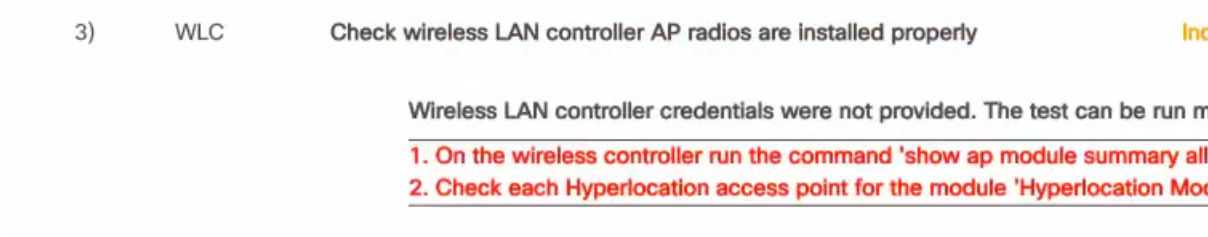
Message count after 10 second interval 1700348

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

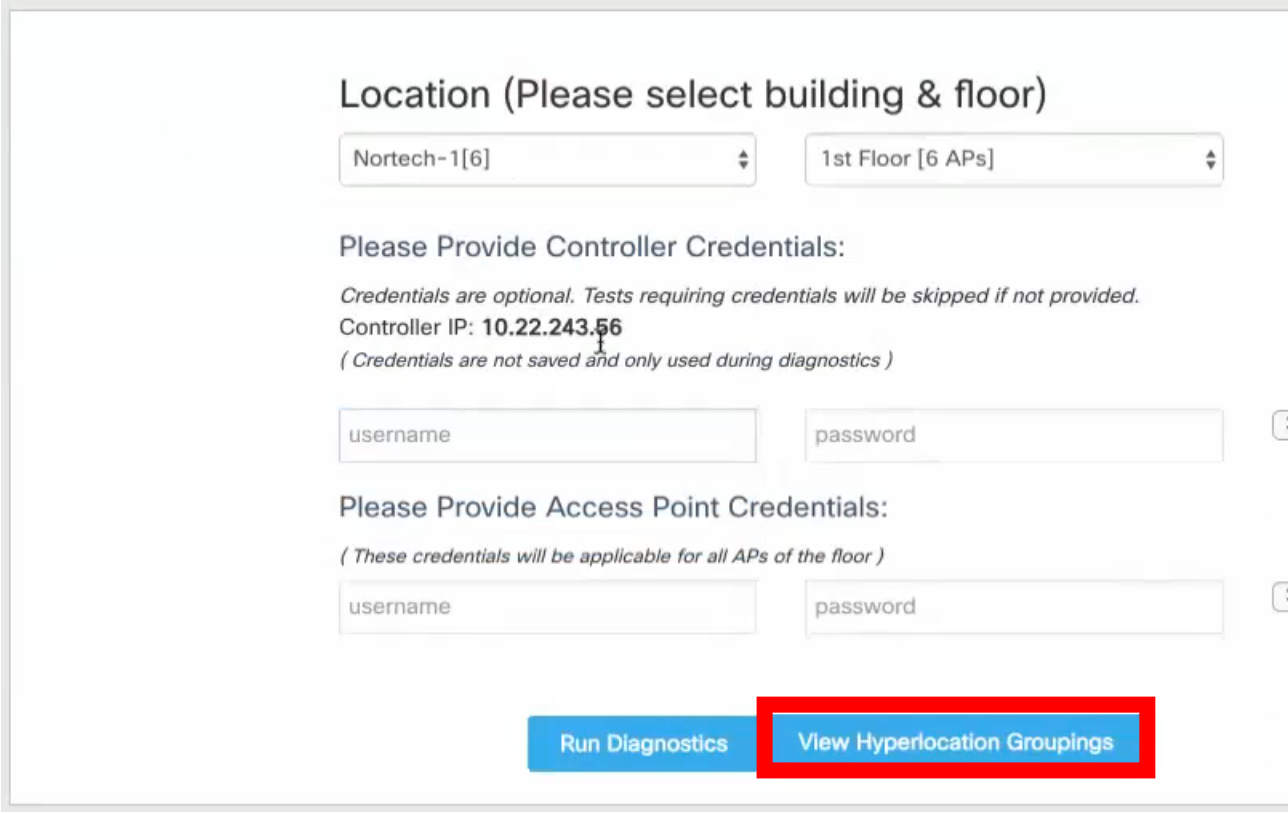
The Hyperlocation deployment calculates location in the following manner. During the time period of a slot, the respective primary emits bar packets. Bar responses are sent by client devices in the vicinity. The subordinates access point listen to these response packets. The primary and subordinates 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

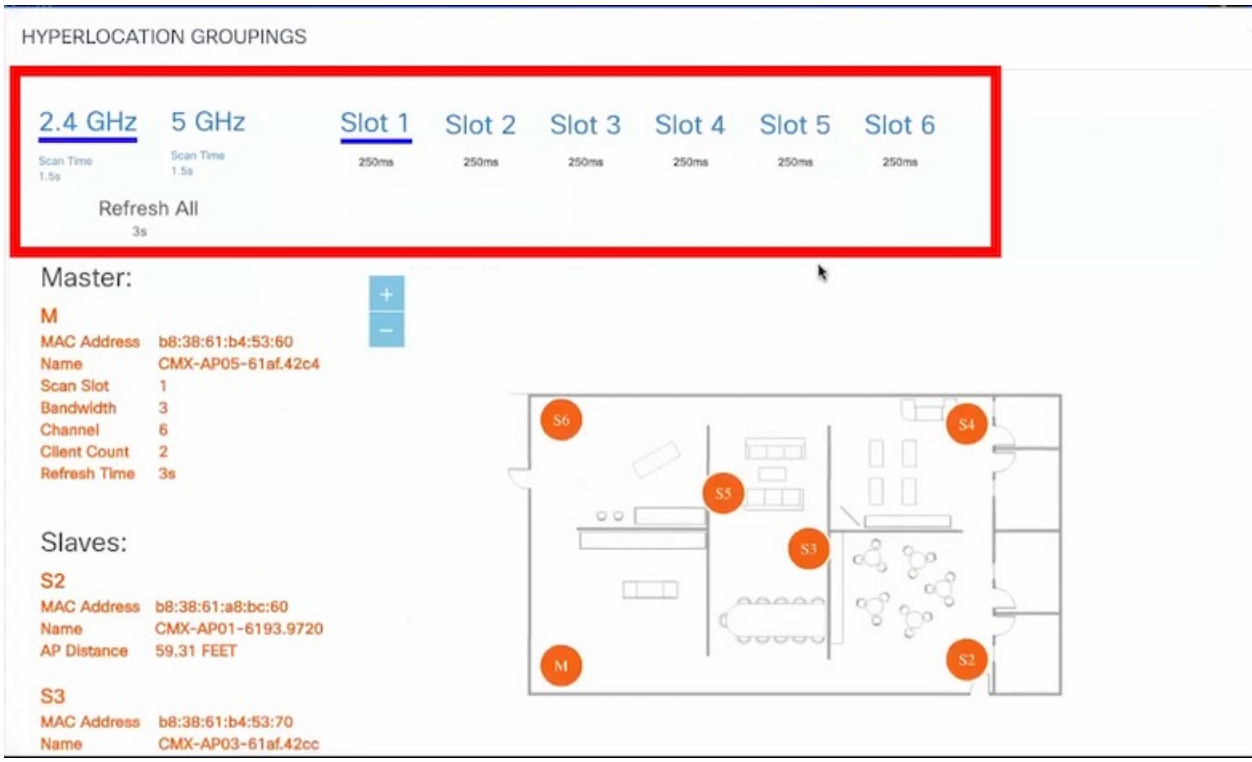
Step 1 Open the CMX Dashboard, **Detect and Locate>Troubleshooting**. As this is a floor-level test, select a building and floor. Note that only floors with hyperlocation access points are populated here.

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

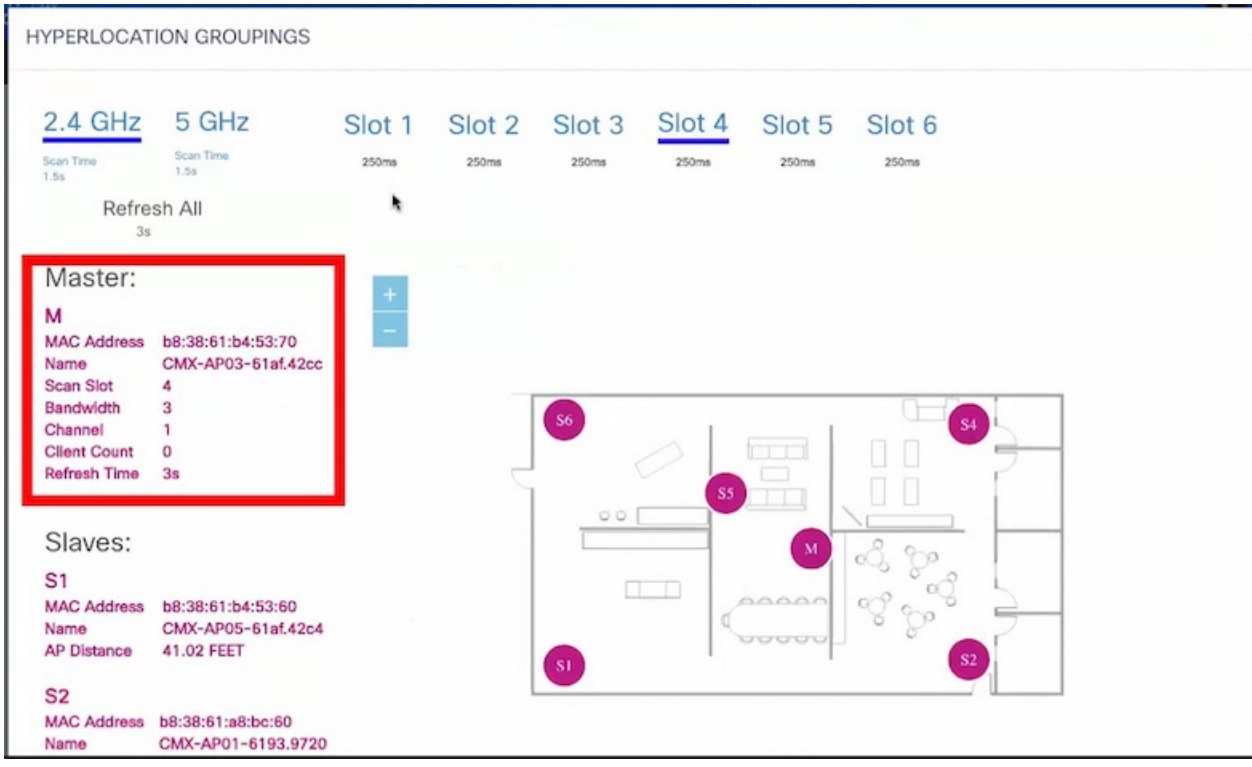
Note
You can observe that each slot has an allocated time which is listed below the slot. There are also two frequency bands, 2.4 and 5 GHz, each with scan times. Scan time is the total time allocated to scan every slot of a band at least once. Since there are two such bands, 2.4 and 5 GHz, the total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



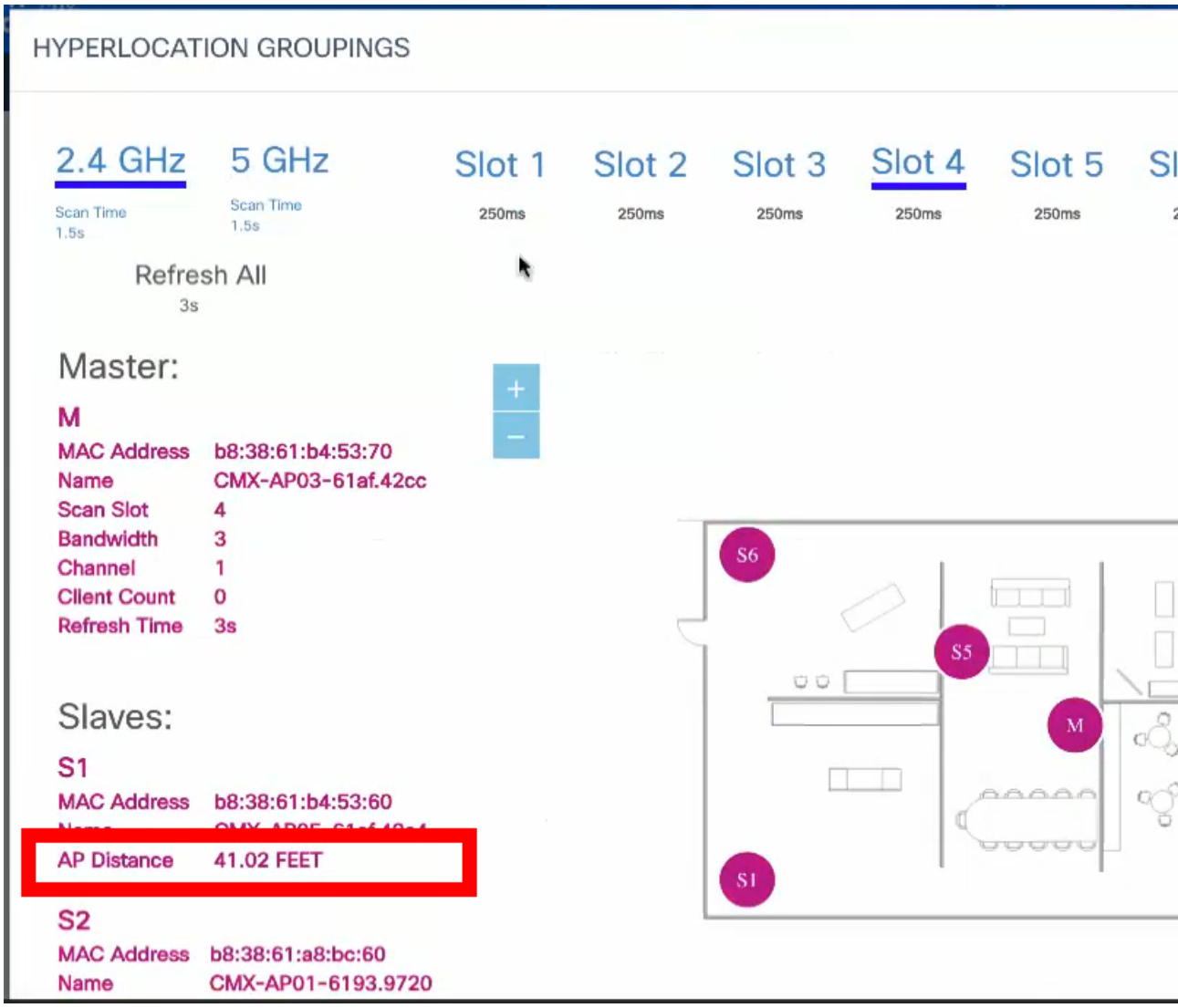
Step 3 Click a frequency band, and select a slot. You can observe the primary access point for the site marked by M, and the subordinates marked by S. You can also change the primary to a more appropriate one in this page.



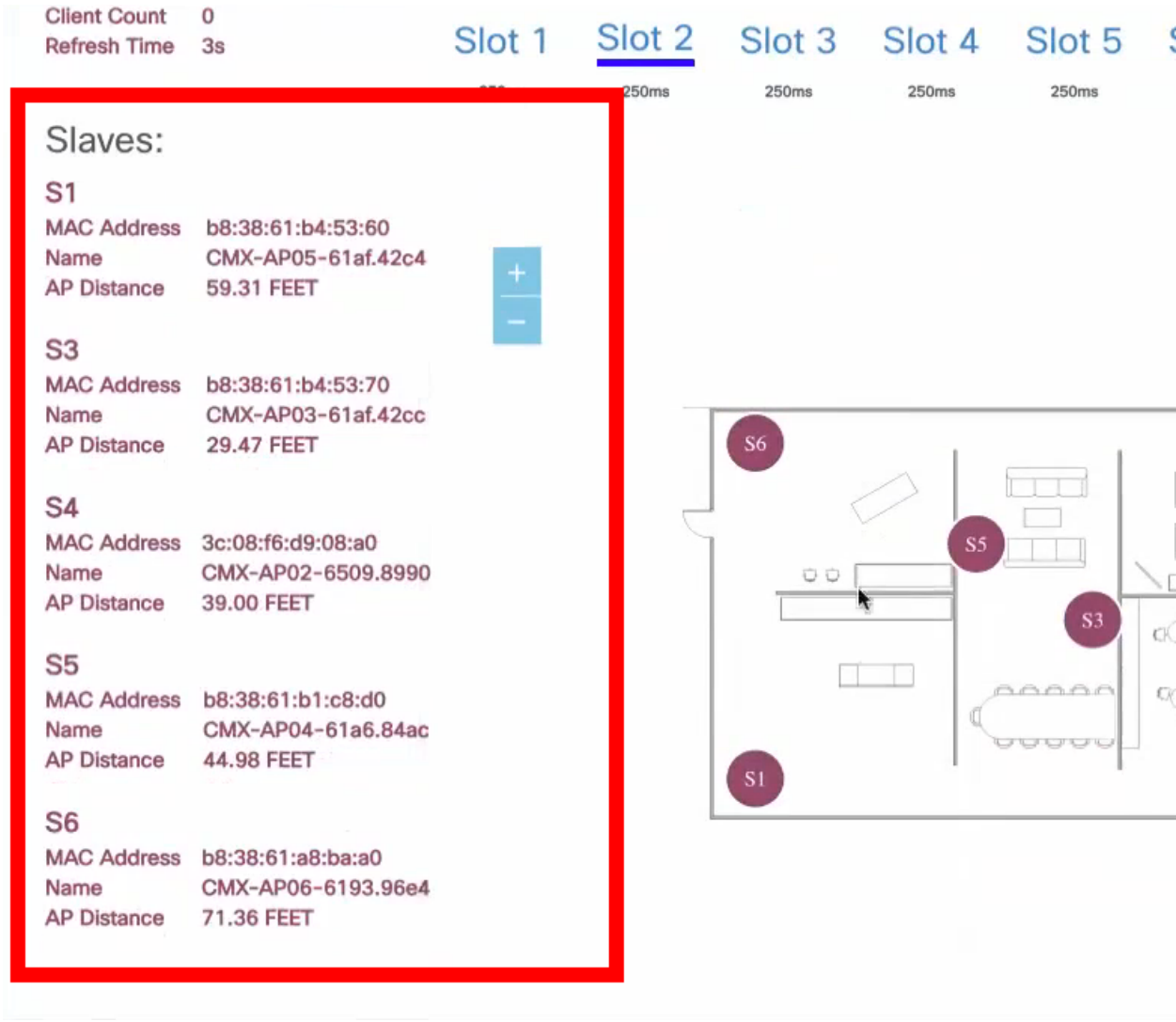
Step 4 Observe details of the primary access point of a slot, like bandwidth, channel and client count.



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 An administrator user should not change the sensitive parameters without Cisco's instructions and contact Cisco TAC or BU escalation to decide the appropriate operation.

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 6: 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

Location Feature	Supported Marvel-Based Cheetah Access Points	Supported Cisco IOS Access Points (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)	
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 or RFID Tag. In this task, we will choose a client.

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



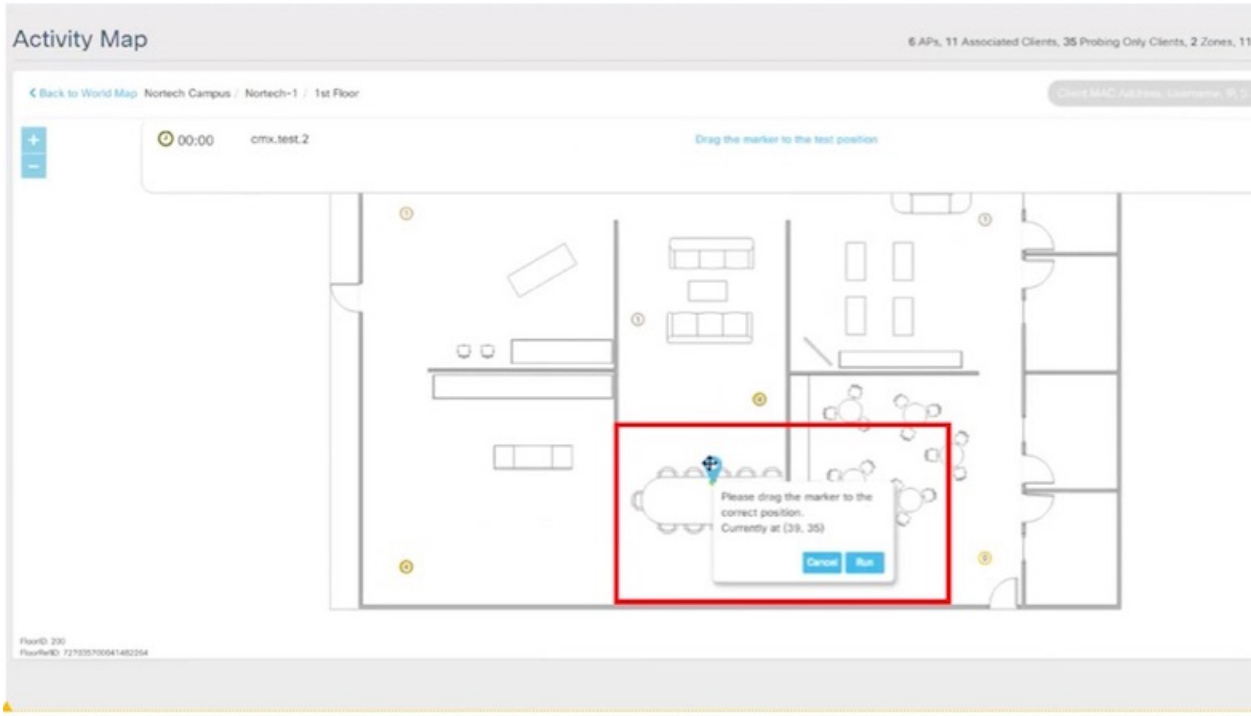
The **Client** dialog box is displayed.

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.

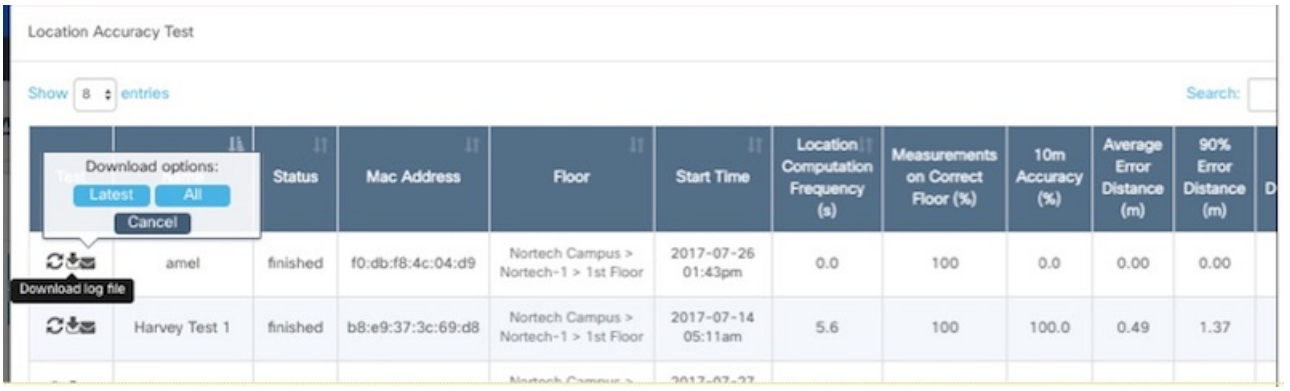
A dialog box, showing 10 m accuracy and Average Error Distance is displayed.





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.

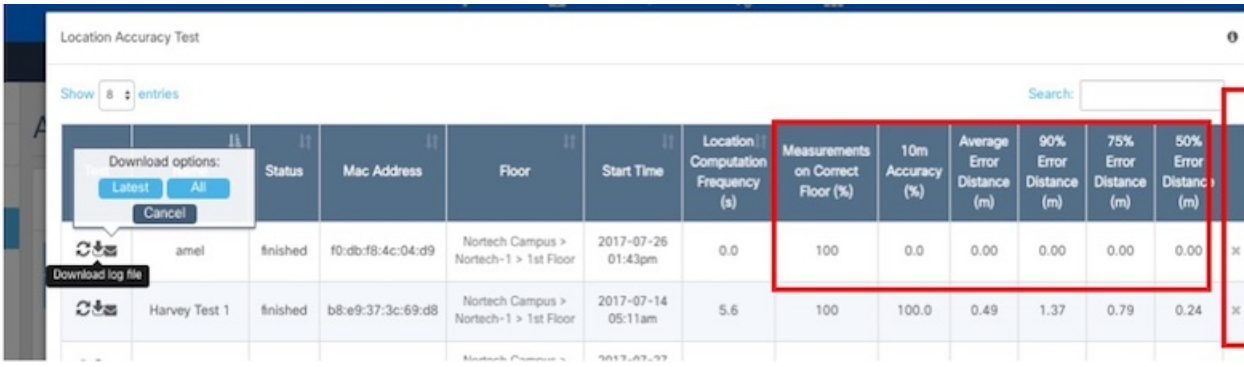


The test results displayed indicate that for 100% of the time, Cisco CMX locates the client within this many meters from where the client is actually located.

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:



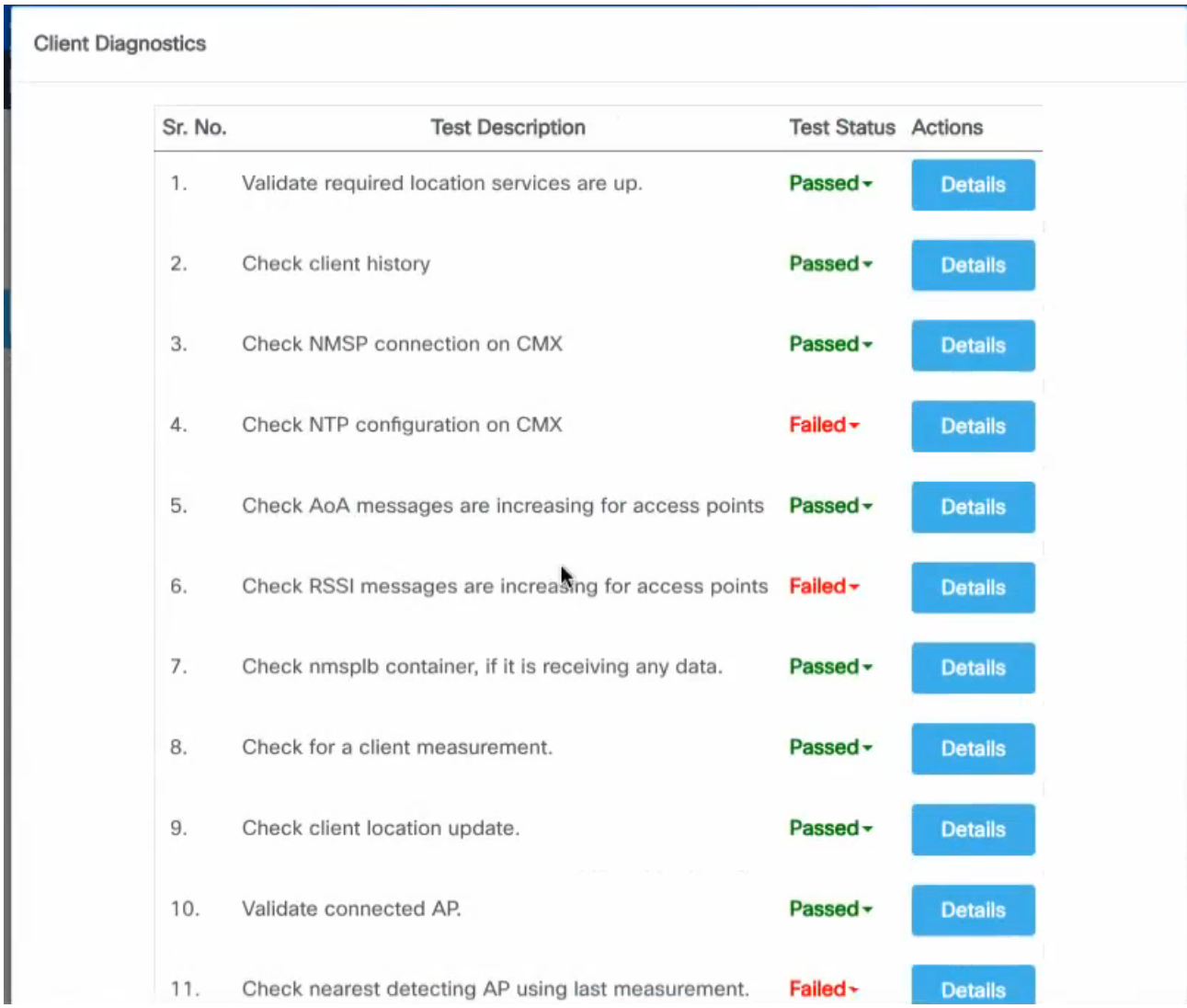
Ensure that **Measurements on Correct Floor** should be at 100%. This is an indicator of whether the client has been detected by the access points on the same floor, and not on a different floor. You can delete the test and the corresponding log files using the cross buttons here.

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.



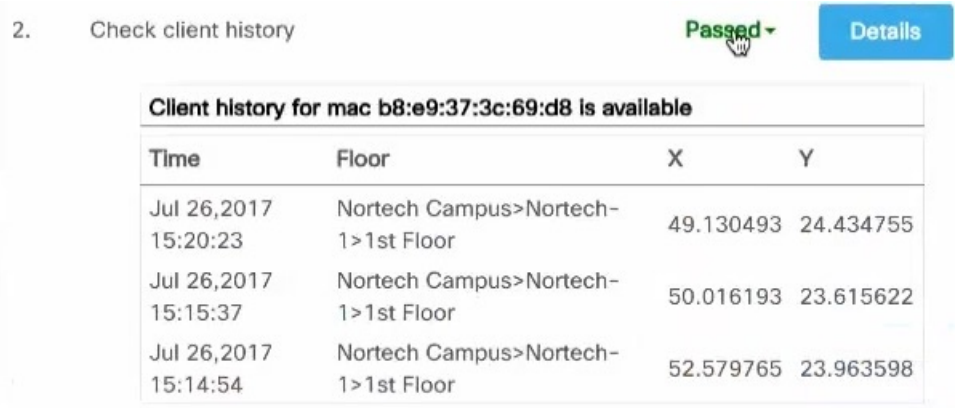
Below is a sample test report.



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

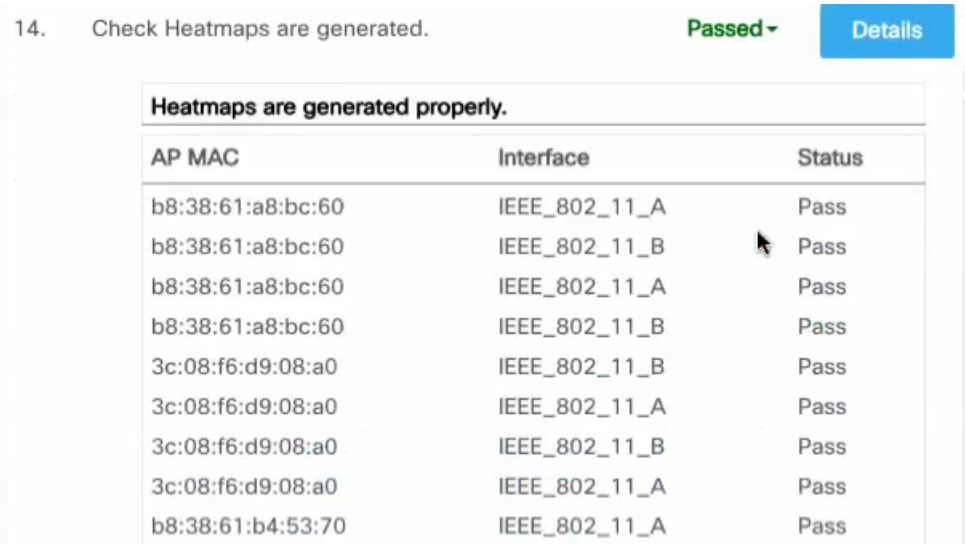


2. Check client history — Passed — Details

Client history for mac b8:e9:37:3c:69:d8 is available

Time	Floor	X	Y
Jul 26,2017 15:20:23	Nortech Campus>Nortech-1>1st Floor	49.130493	24.434755
Jul 26,2017 15:15:37	Nortech Campus>Nortech-1>1st Floor	50.016193	23.615622
Jul 26,2017 15:14:54	Nortech Campus>Nortech-1>1st Floor	52.579765	23.963598

Figure 4: Sample Output: Check Heatmaps are generated

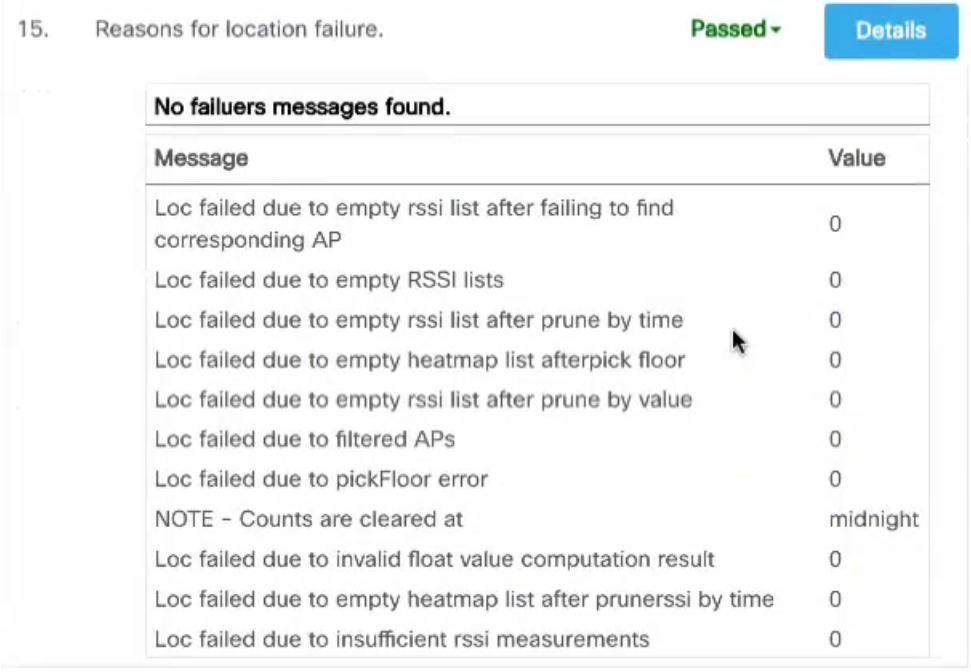


14. Check Heatmaps are generated. — Passed — Details

Heatmaps are generated properly.

AP MAC	Interface	Status
b8:38:61:a8:bc:60	IEEE_802_11_A	Pass
b8:38:61:a8:bc:60	IEEE_802_11_B	Pass
b8:38:61:a8:bc:60	IEEE_802_11_A	Pass
b8:38:61:a8:bc:60	IEEE_802_11_B	Pass
3c:08:f6:d9:08:a0	IEEE_802_11_B	Pass
3c:08:f6:d9:08:a0	IEEE_802_11_A	Pass
3c:08:f6:d9:08:a0	IEEE_802_11_B	Pass
3c:08:f6:d9:08:a0	IEEE_802_11_A	Pass
b8:38:61:b4:53:70	IEEE_802_11_A	Pass

Figure 5: Sample Output: Reasons for location failure

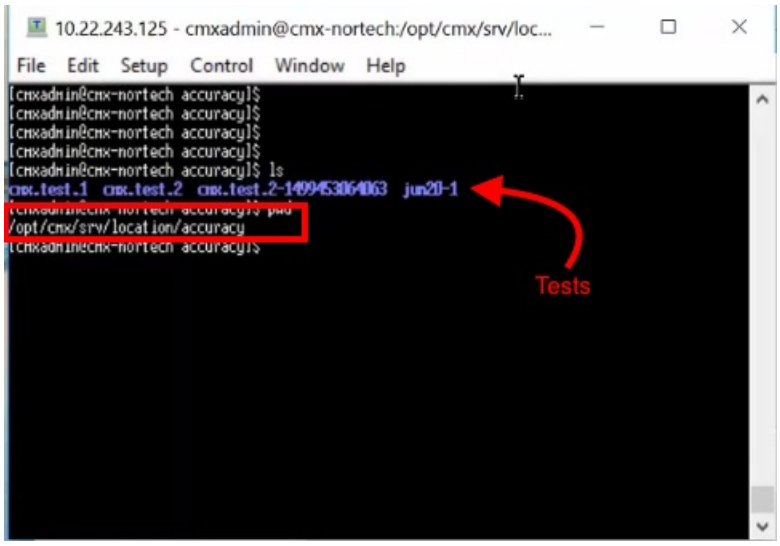


Analyzing Location Accuracy Log Files

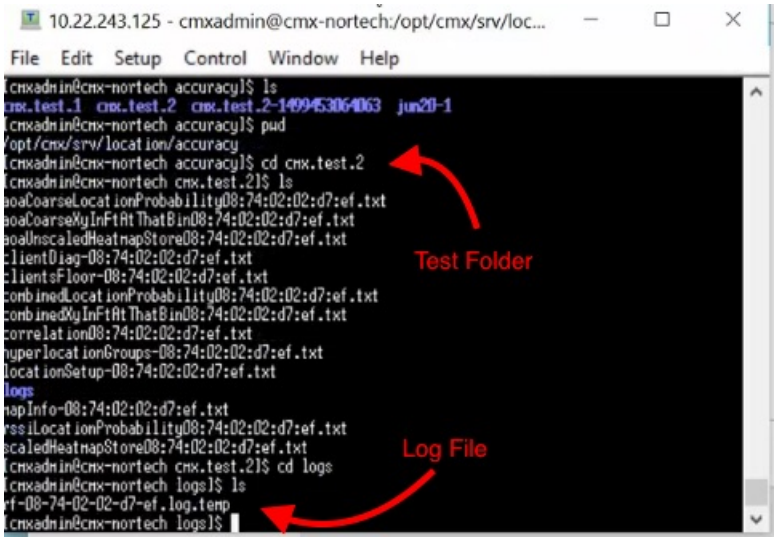
This task analyzes the Location Accuracy log files stored in `/opt/cmx/srv/location/accuracy`.

Procedure

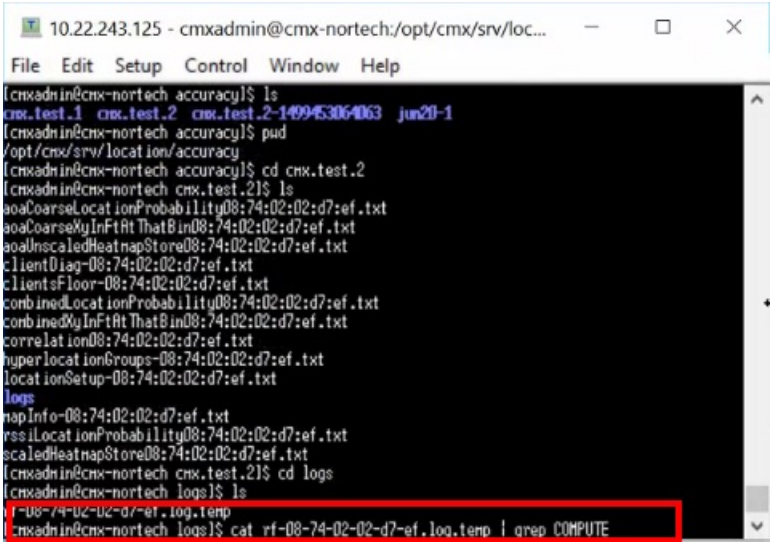
Step 1 Telnet into the CMX box and navigate to the `/opt/cmx/srv/location/accuracy` directory where location accuracy results are stored by default.



Step 2 Navigate to the folder named after your test.



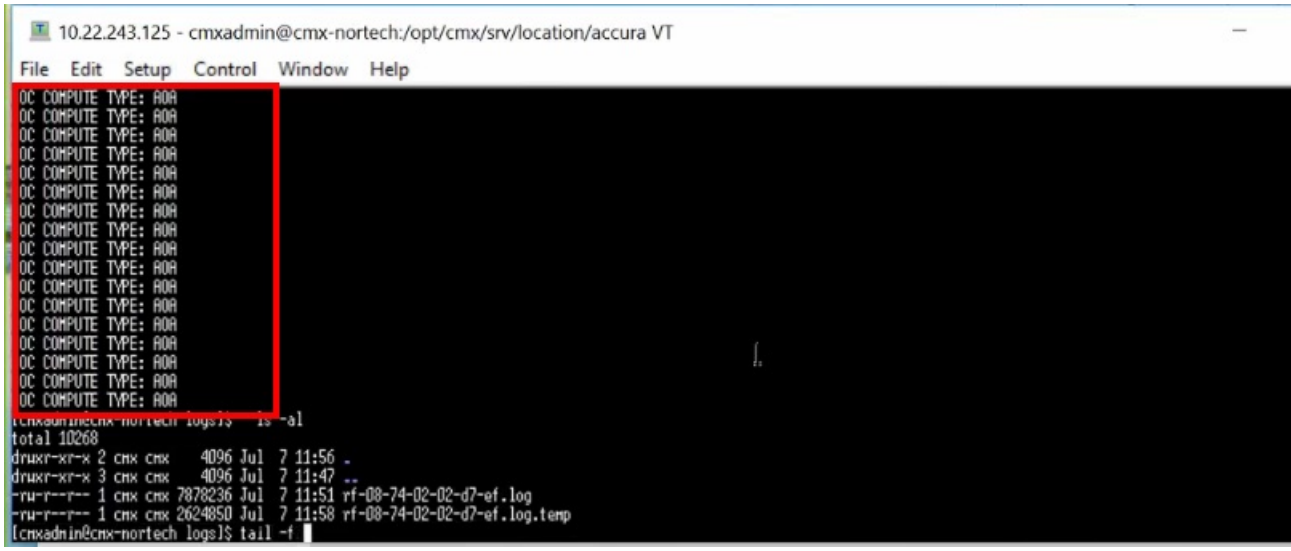
Step 3 Navigate into the `logs` folder, where the log files are stored.



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.

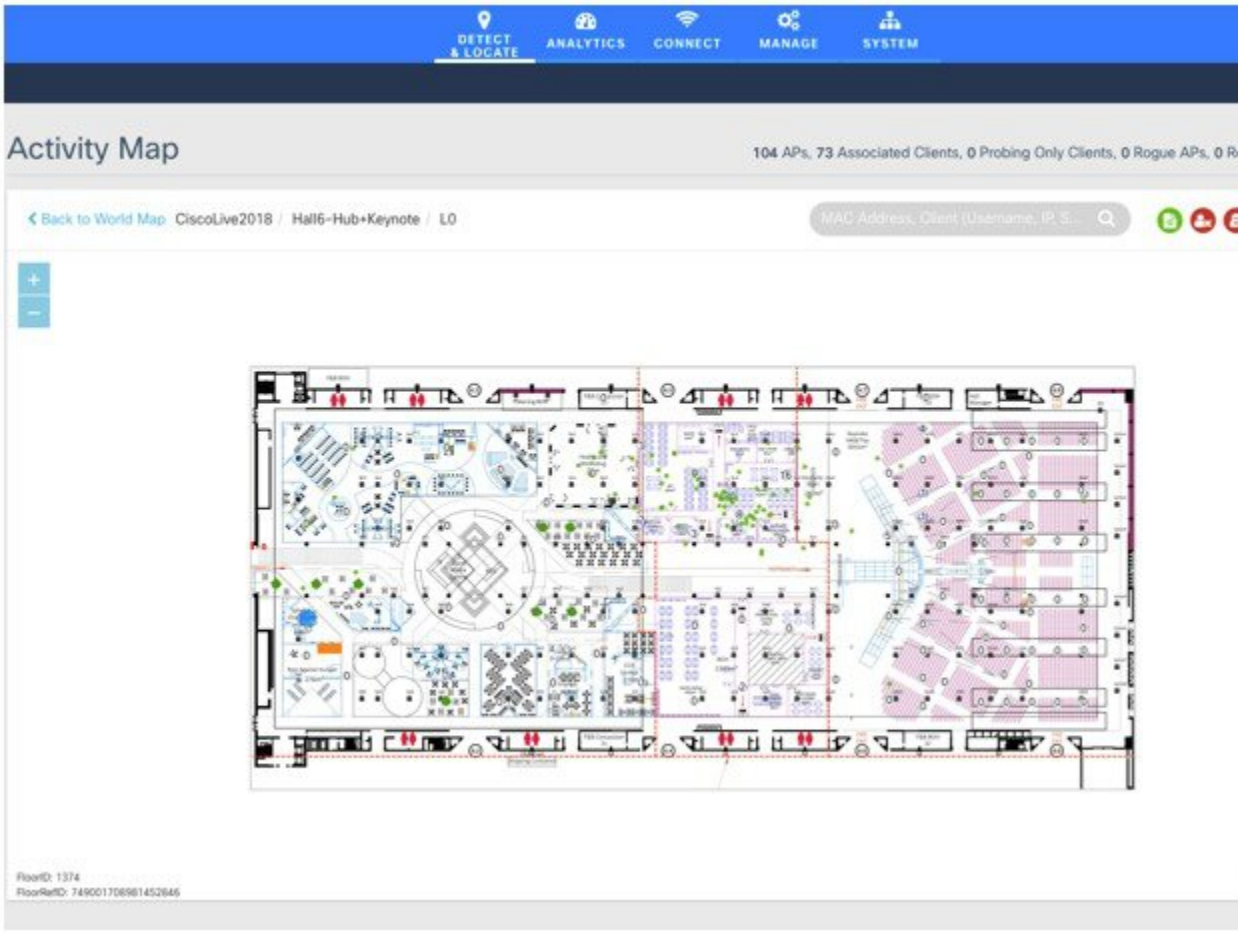
Figure 7: GUI accuracy testing

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 Ty
+-------------------+-------+-------+---------
| 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
```

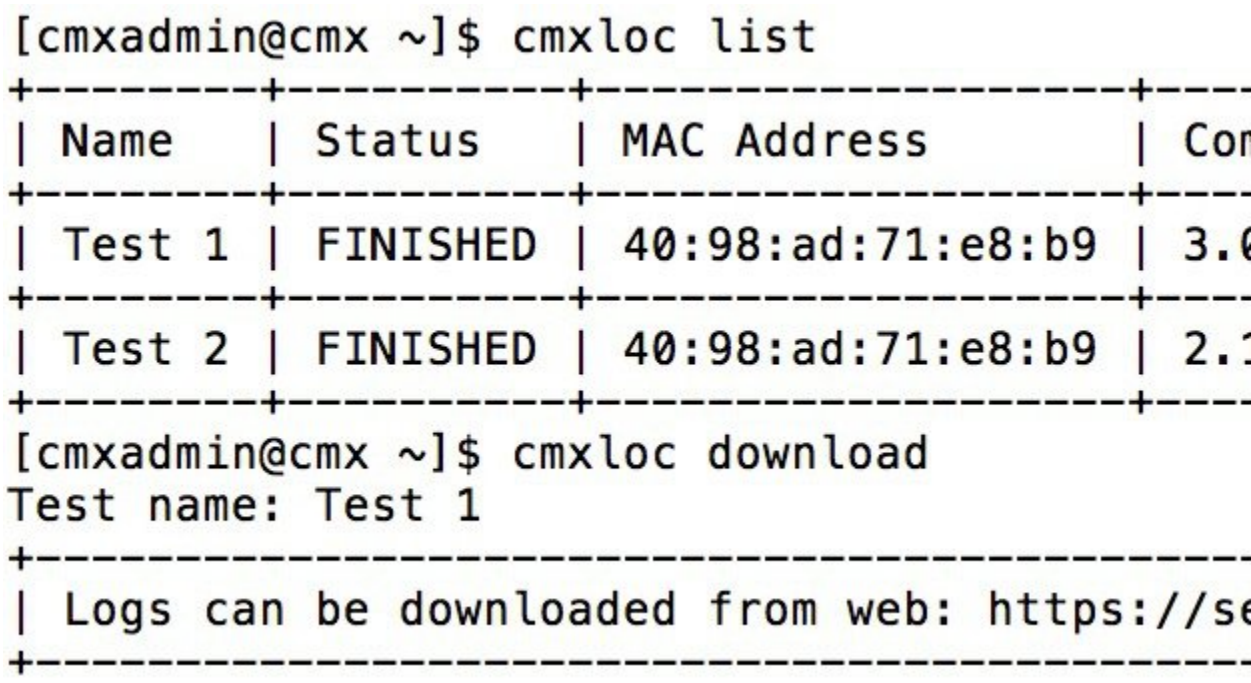
During the test you will see the computation method of each data point: RSSI, AoA or FUSION.

Figure 9: Output during accuracy test

```
Time                                X          Y
2018-07-13T20:12:32.191+0200        27.23      22.4
2018-07-13T20:12:34.328+0200        27.21      22.4
2018-07-13T20:12:36.483+0200        28.0       23.3
2018-07-13T20:12:38.586+0200        27.97      23.3
2018-07-13T20:12:40.593+0200        26.31      21.6
```

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



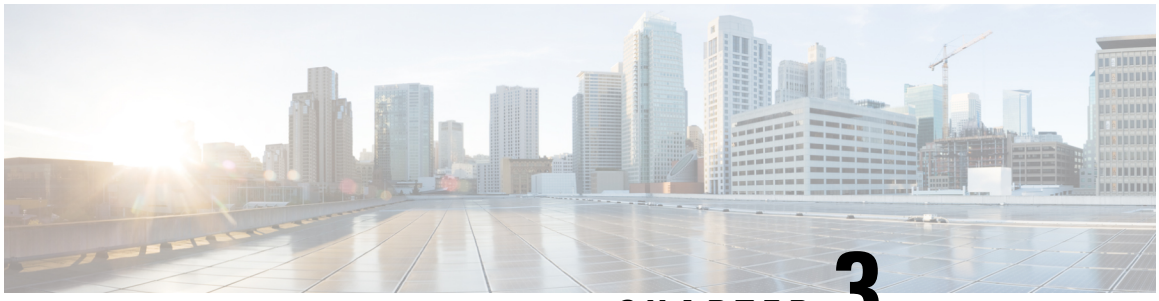
Understanding the test results

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, on page 85
- The Analytics Dashboard, on page 85
- Customized Widgets, on page 94
- Create a Realtime Report, on page 100
- Performing Heatmap Analysis, on page 100
- Set SSID Filter Parameters for Analytics Service, on page 101
- Disable Cisco CMX Analytics Service (CLI), on page 102

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

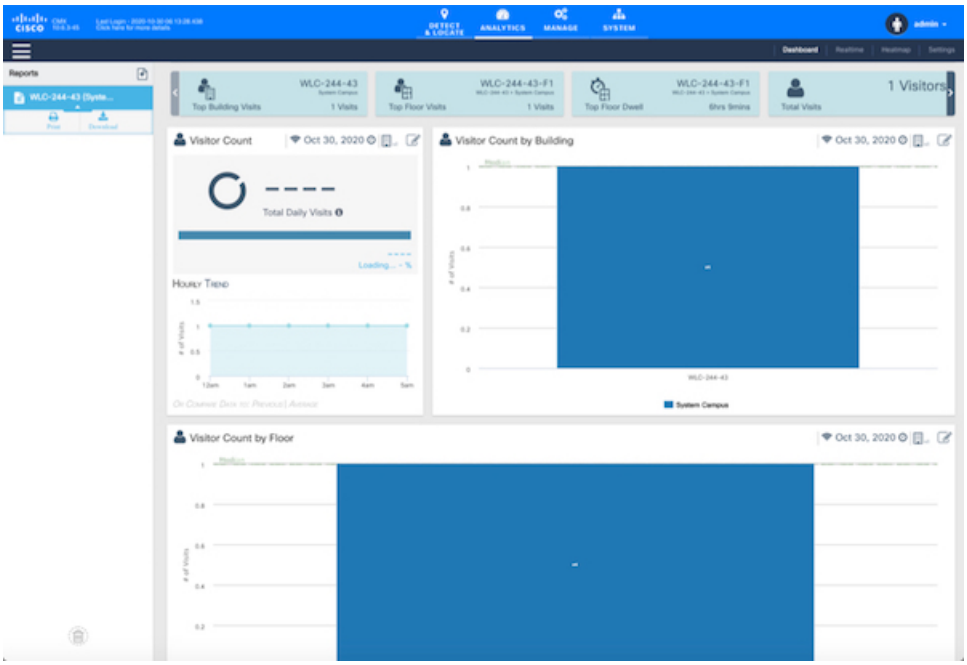
The Analytics service's Dashboard is designed to help you visualize and understand various parameters associated with visitors' movement within a given zone. You can use the Dashboard on a daily basis to examine current trends or events. You can also customize the Dashboard with different widgets, as 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 91.

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:

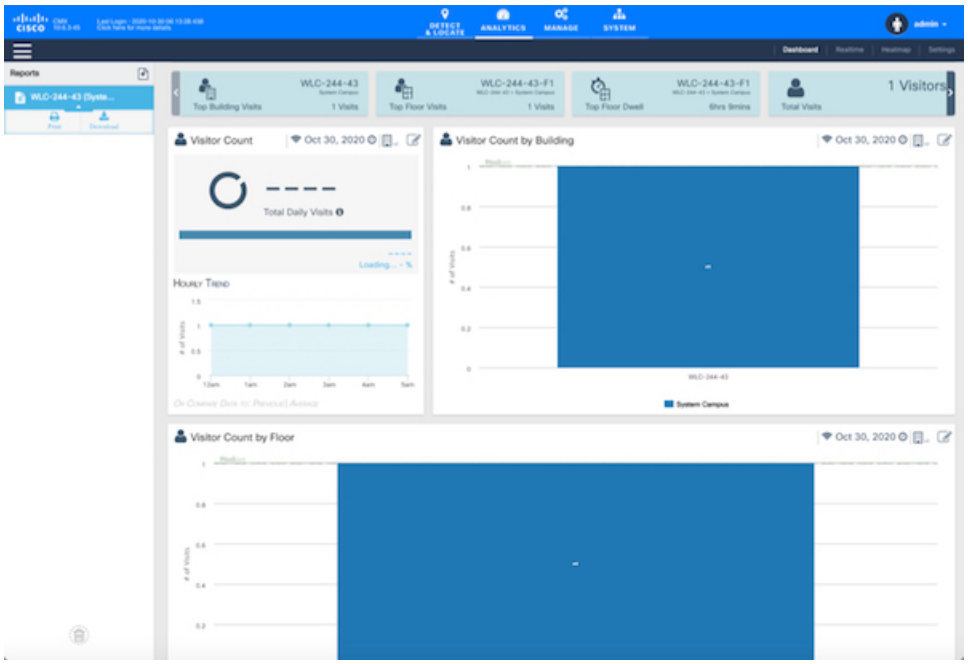
- the Unique Device widget is no longer available for analytics reports
- reports where multiple zones and floors are selected can result in duplicate device counts when a device visits more than one zone or floor. So if a device visits zone 1 and zone 2, the device count is displayed as 2. However, 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.
- **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**.

To print a custom report, follow the steps:

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**.

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.

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

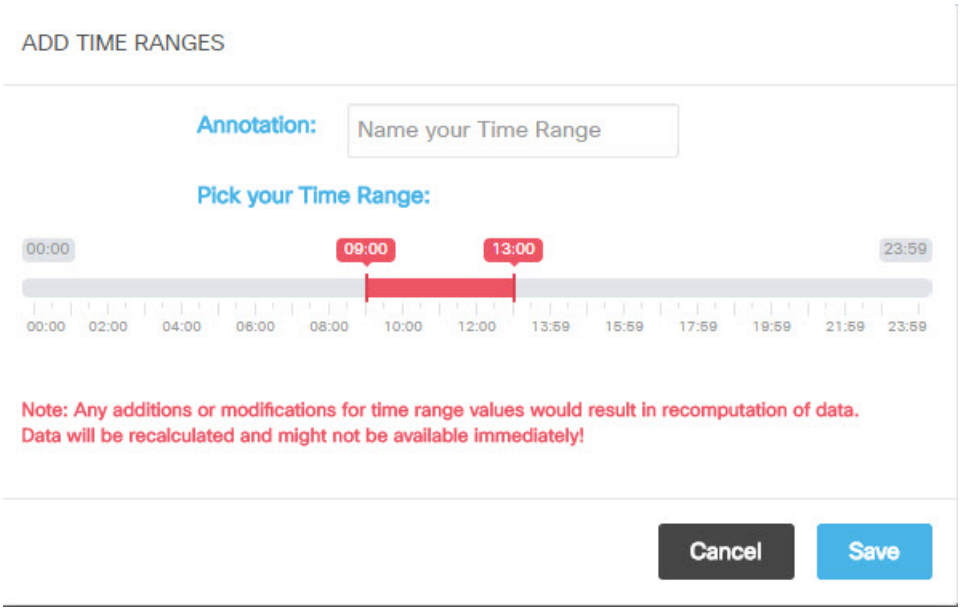
Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).

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.

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 174.

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:

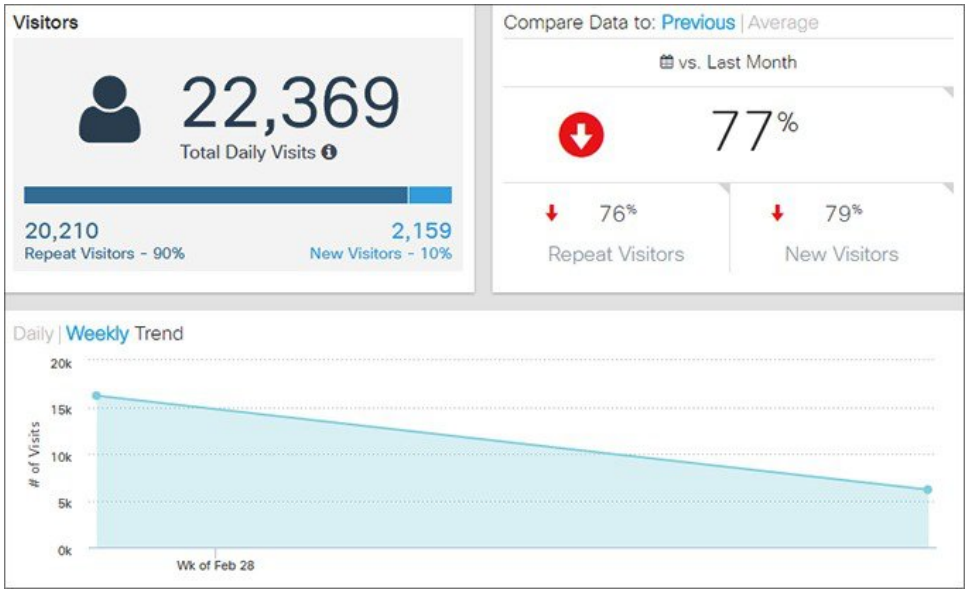
- **Summary**—This is the default view. This view consists of the **Visitors**, **Compare Data to**, and **Hourly Trend** charts. A breakup of new and repeat visitors is also provided. The **Compare Data to** chart presents comparative data for the current day and the previous day. You can also compare 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.

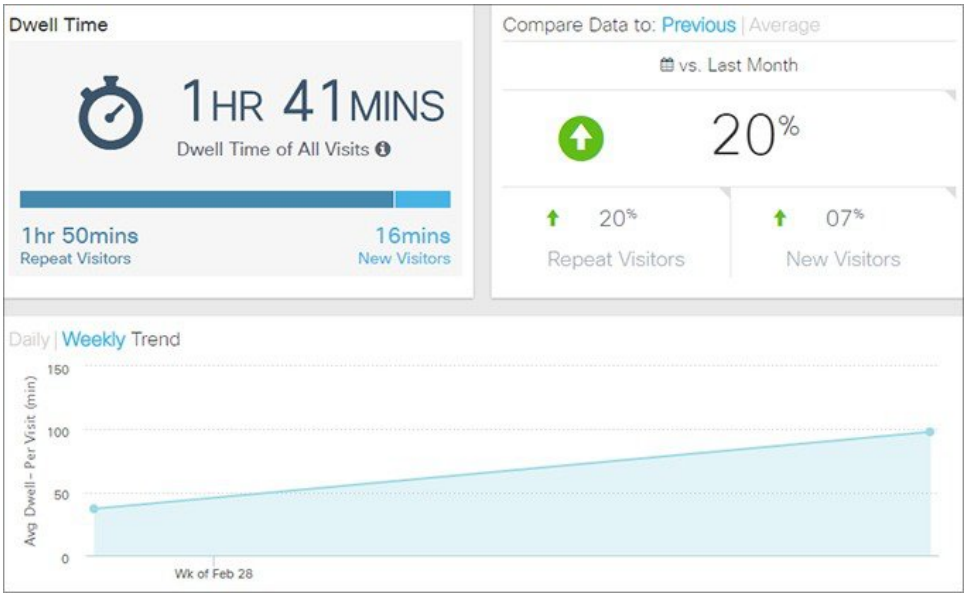
Average dwell time can be viewed in the following formats:

- **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 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:

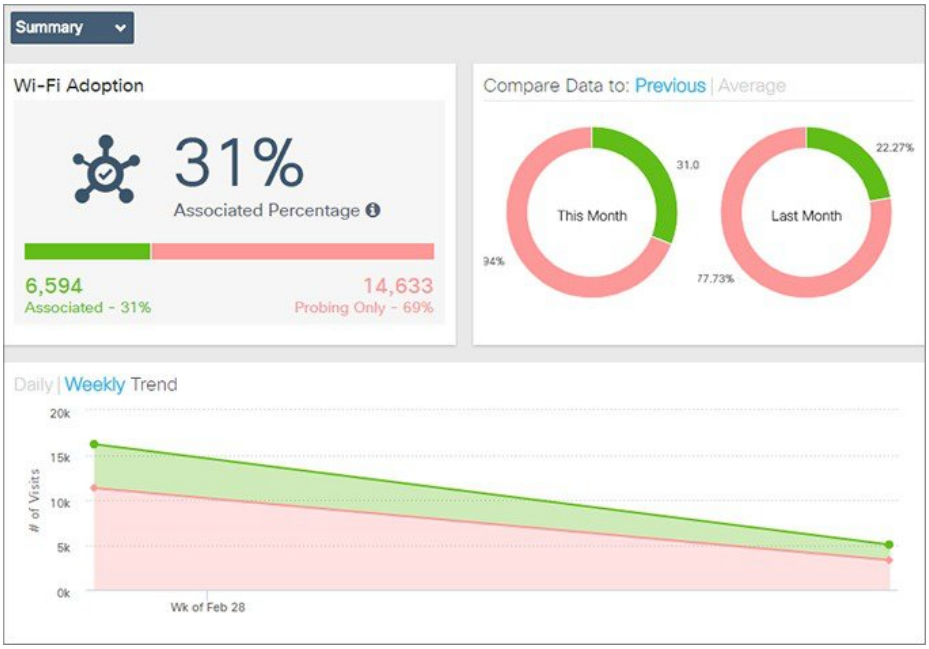
- **Summary**—This is the default view. The Summary view consists of the **Associated Status**, **Compare Data to**, and **Hourly Trend** charts.
- **Chart**-A line chart with a summary of associated and probing clients. The view can toggle to show associated clients in terms of percentage and total 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:

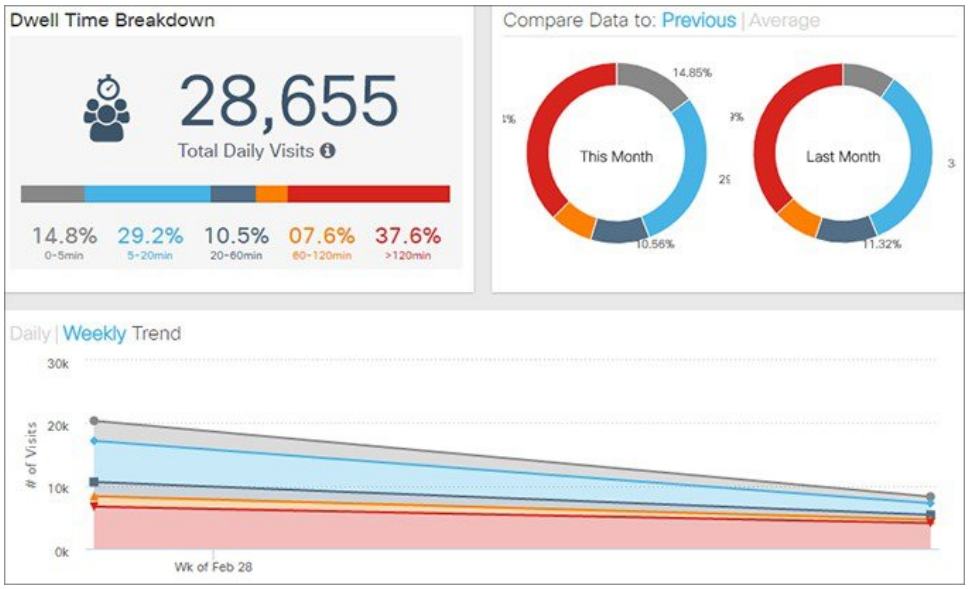
- **Summary**—This is the default view. The summary view consists of the **Dwell Time Breakdown**, **Compare Data to**, and **Daily Trend** charts. The dwell time breakdown is displayed in the following ranges:
  - **0-5 minutes**
  - **5-20 minutes**
  - **20-60 minutes**
  - **60-120 minutes**
  - **>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.

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.

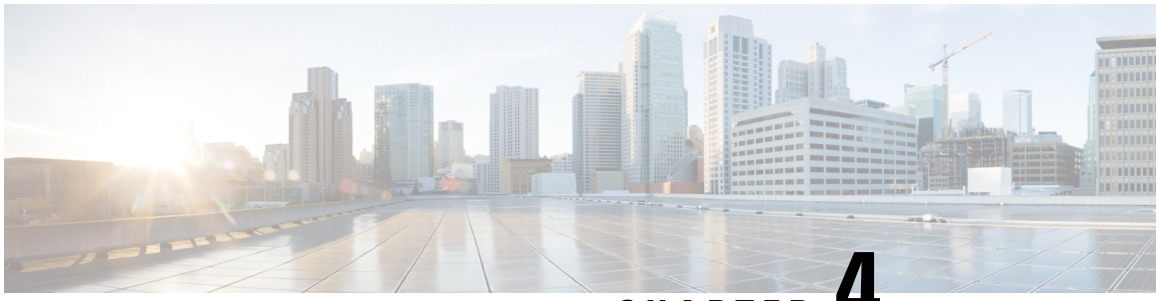
Step 2 To disable Cisco CMX Analytics Service, run the **cmxctl disable analytics** command.

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

Managing Cisco CMX Configuration

- Overview of the Manage Service, on page 105
- Managing Perimeters and Zones on Location Maps, on page 106
- Managing Licenses, on page 112
- Managing Users, on page 116
- Managing Notifications from Applications, on page 119
- Managing the Cisco CMX Cloud Apps, on page 129
- Setting Up Outbound Proxy, on page 136
- Setting Up Outbound Proxy in HA-Enabled Setup, on page 137
- Configuring Basic CMX Settings, on page 137
- Root User Changes, on page 138

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 106.
- **Licenses**—Enables you to manage and add licenses. For more information, see Managing Licenses, on page 112.
- **Users**—Enables you to manage and add users. For more information, see Managing Users, on page 116.
- **Notifications**—Enables you to manage and add email and HTTP notifications. For more information, see Managing Notifications from Applications, on page 119.
- **Cloud Apps**—Enables you to manage Cisco CMX Cloud service. For more information, see Managing the Cisco CMX Cloud Apps, on page 129.

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 116.

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.

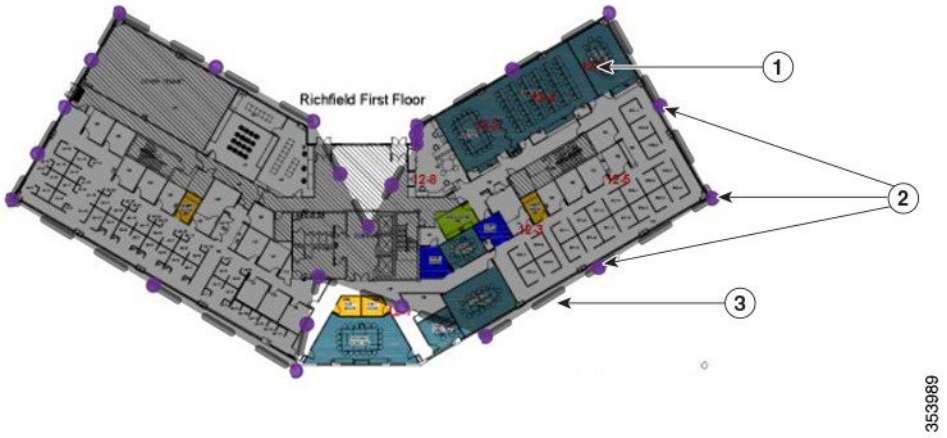
Step 4 Click the Subzone in the corresponding zone.

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 13: 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 14: 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.

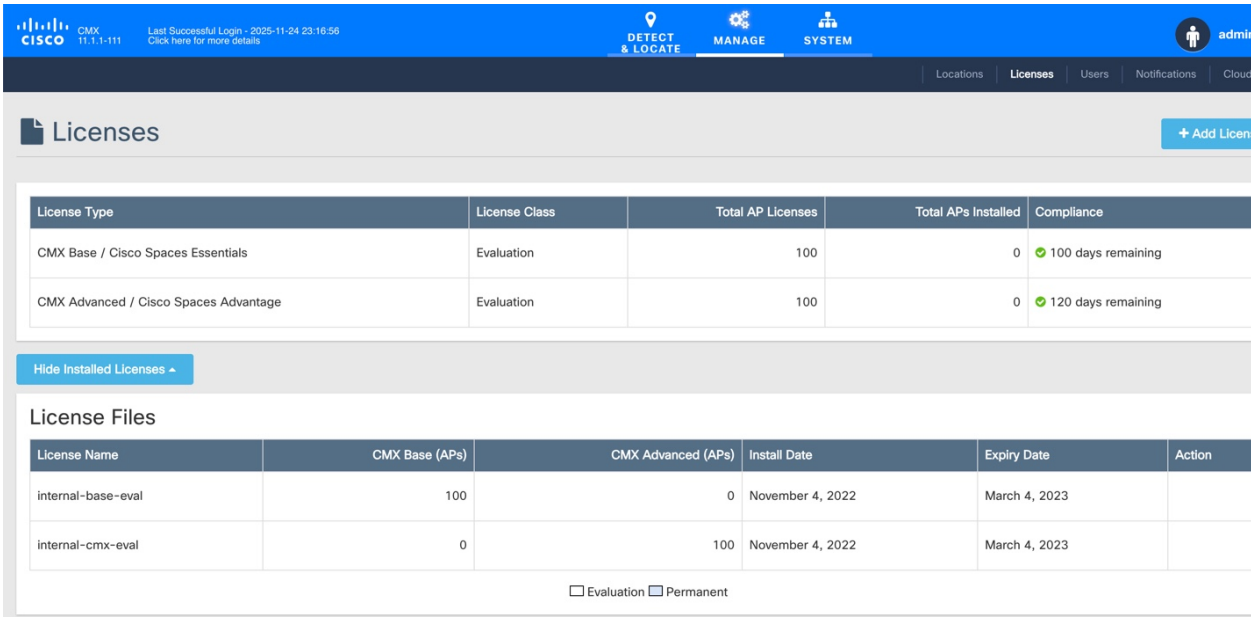
Step 8 Click outside the zone to save your changes.

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 15: Licenses



Note

- Cisco CMX Release 10.3 supports High Availability. For more information, see Enabling High Availability for Cisco CMX, on page 158.
- 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.

License Models

These are ther Cisco CMX license models:

- **Cisco CMX Essentials (formerly called Cisco CMX Base)**: Includes RSSI Location Calculation, GUI access to **DETECT**, **MANAGE**, and **SYSTEM** services. It supports Permanent and Term licenses.

Note The Cisco CMX Essentials (formerly called Cisco CMX Base) License does not provide access to Cisco CMX Hyperlocation or Partner Stream. The Cisco CMX Advantage (formerly called Cisco CMX Advanced) License is required to access these services. Cisco CMX Hyperlocation, Cisco CMX Advance Location services migrated from Cisco CMX Essentials (formerly called Cisco CMX Base) License to Cisco CMX Advantage (formerly called Cisco CMX Advanced) 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 Advantage (formerly called Cisco CMX Advanced) license.

- **Cisco CMX Advantage (formerly called Cisco CMX Advanced)**: Includes both base and advanced features, encompassing the full suite of Cisco CMX capabilities along with Partner Stream. This license grants access to Cisco's digitization toolkits and services within Cisco Spaces.

Note To utilize Cisco Spaces alongside Cisco CMX with CMX APIs, you are required to obtain the Cisco Spaces Advantage licenses.

Note

- DNA Advantage customers with a Cisco Spaces Extend license continue to have access to Cisco CMX Essentials (formerly known as Cisco CMX Base) along with CMX partner stream capability.
- To use this service, the IT team must have a Cisco CMX hardware appliance, and cloud tethering occurs via the Cisco CMX appliance.

Add a License

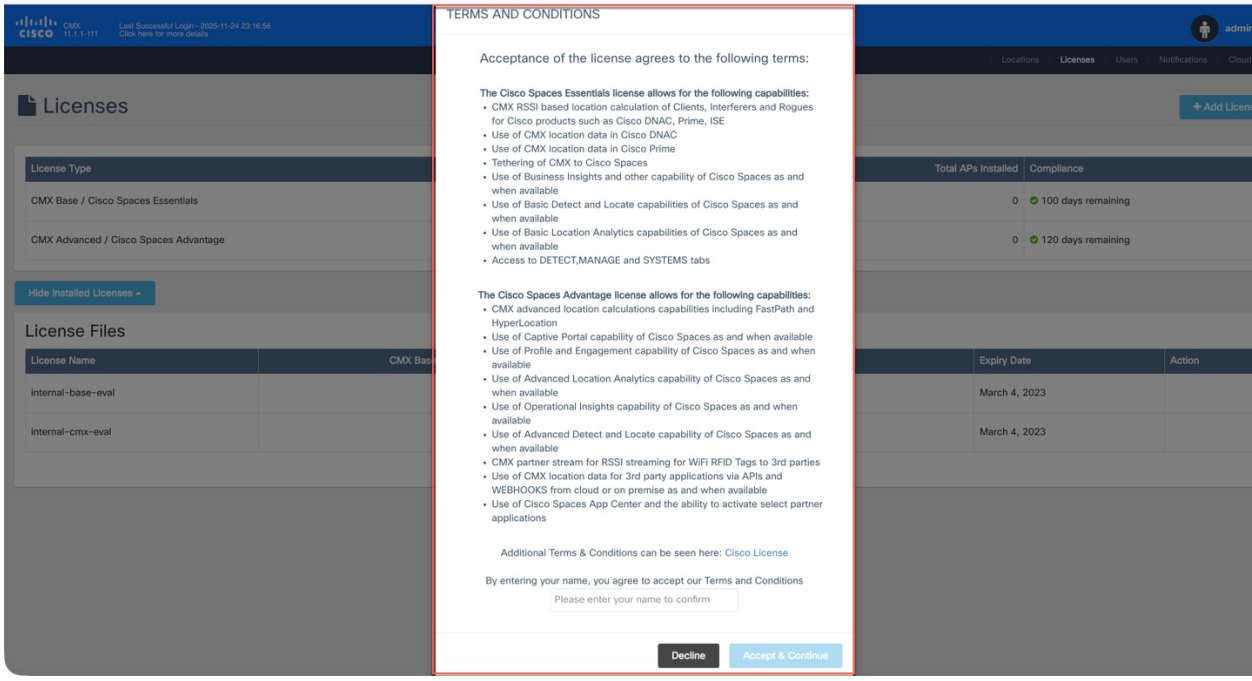
Procedure

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.

Figure 16: Terms and Conditions



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 installed 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 116.

Note
The password for the new user must be minimum 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 7: 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 116.

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.

View Active User Sessions

Check and manage current active sessions for users in Cisco Mobile Connected Experiences (CMX).

Use this task to monitor which users are currently logged in, see relevant session details, and perform session management actions (such as deleting sessions if needed).

Before you begin

Ensure that you have administrator or sufficient privileges to access the user management section in Cisco CMX.

Follow these steps to view active user sessions:

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 In the **Users** window, scroll down to the **Active Sessions** section.

The **Active Sessions** table displays information about all sessions that are in active status.

Step 4 View these session details:

- **Username**: Displays the username of the logged in account user.
- **Session Type**: Displays the session type as **SSH** or **GUI**.
- **IP Address**: Displays the system IP from which the user is logged in.
- **Session ID**: Displays the internal ID to uniquely identify the session. The format of this session ID is different for SSH and GUI sessions types.
- **Logged in time**: Displays the date and time when the session started.
- **Actions**: Displays the **Delete** option to remove the corresponding session. Use this option to delete individual sessions.
- **Select**: Displays the checkbox to select multiple the active session to proceed with delete. Use this option to perform bulk delete.

Step 5 (Optional) To delete an individual session, click the **Delete** action for that session.

Step 6 (Optional) To delete multiple sessions at once, select the checkboxes for the sessions you want to remove, then use the **Delete Selected (x)** option.

You view a list of all current active user sessions and, if needed, remove selected sessions from Cisco CMX.

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

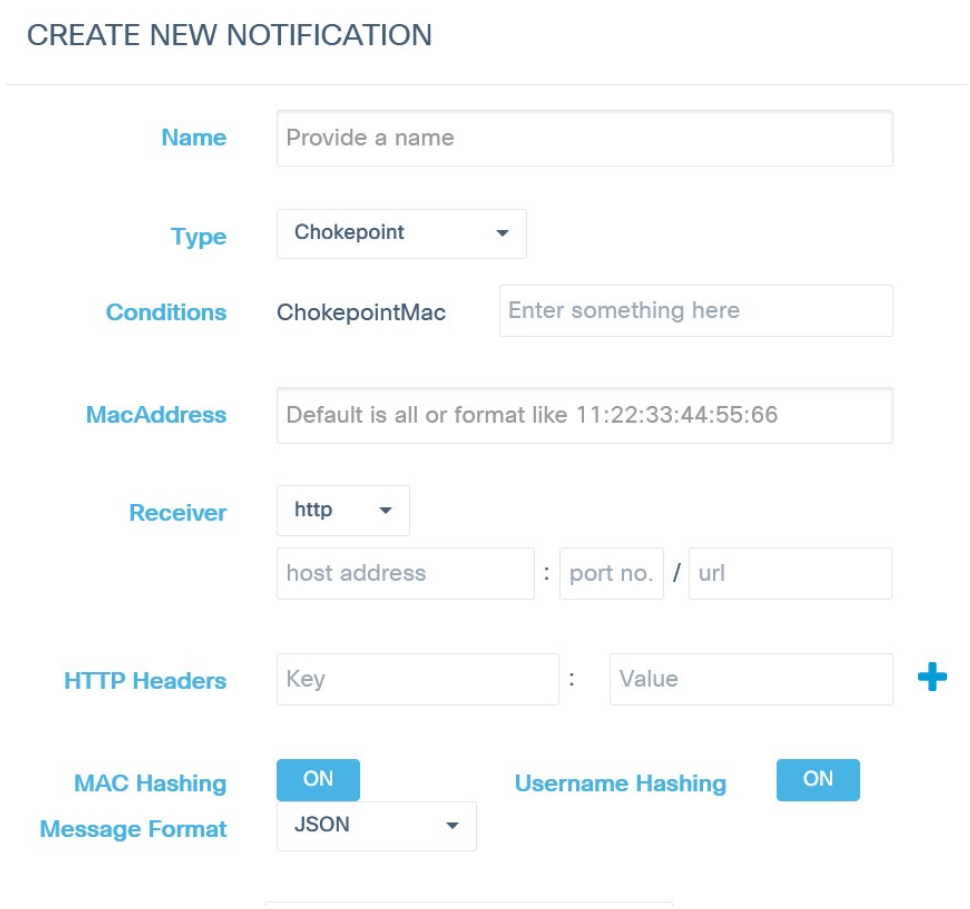
Procedure

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 17: 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 8: 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.
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.
- **Username Hashing**: Click to disable the username hashing. By default, username hashing is enabled.
- **Message Format**: From the **Message Format** drop-down list, choose the format as **JSON** or **XML**.
- **Salt**: Enter a secret hash key.

Step 5 Click **Create**. The new notification is created and displayed in the Notifications window.

We recommend that you maintain a maximum of five active northbound notifications for better performance. Currently, there is no enforcement for validating total active northbound notifications.

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 9: 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

Type	Description
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 **Note** Some client devices uses Extended Unique Identifier (EUI-64) to auto-generate the IPv6 address. In this scenario, MAC address of the device is displayed in the **IPv6 address** field too. When the controller sends the client data to Cisco CMX using NMSP, IPv6 address and MAC address of the device is displayed in the northbound notification. However, Cisco CMX hashes the IPv6 address to comply with privacy regulations as per General Data Protection Regulation (GDPR).
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
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.

Type	Description
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);

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 10: 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

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 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
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 136.

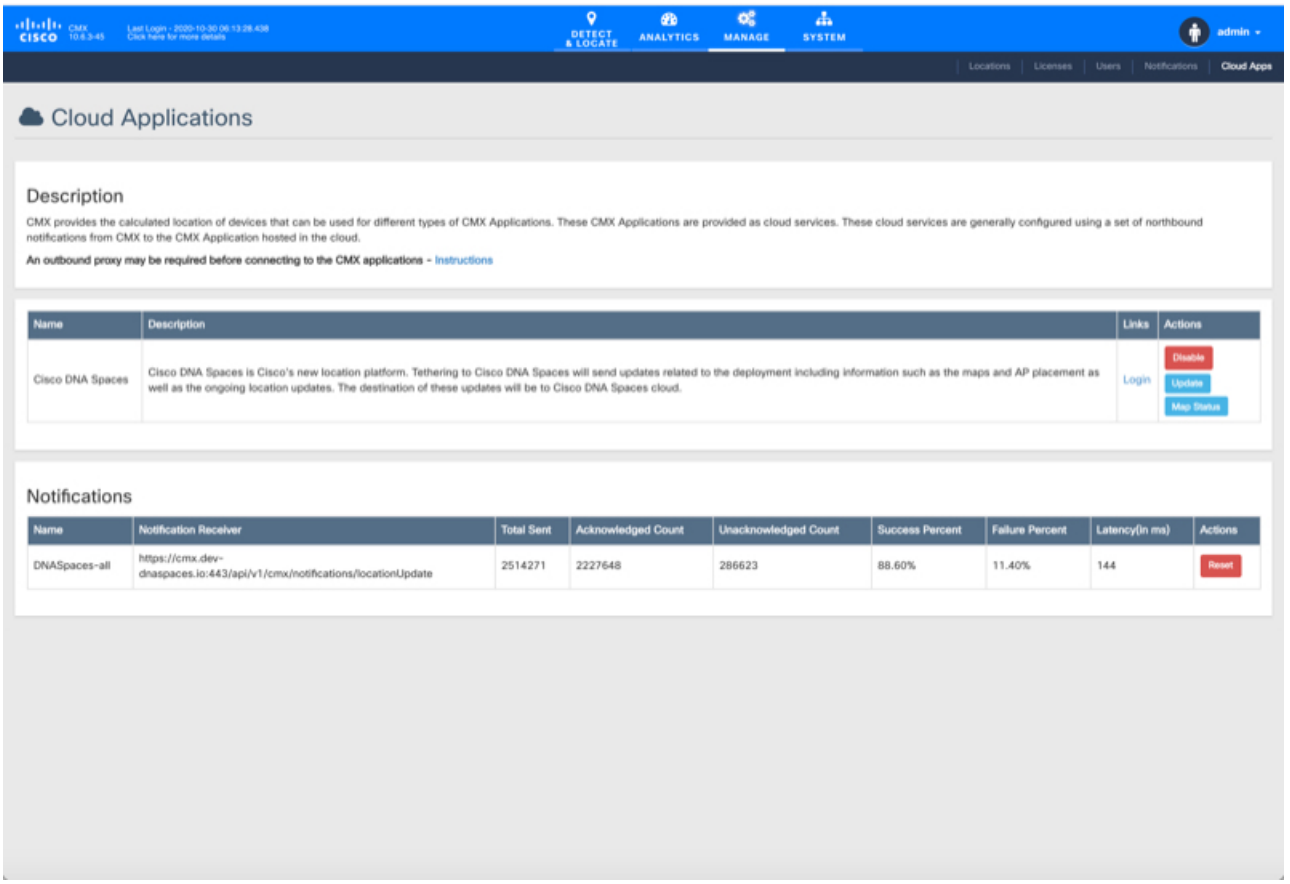
Procedure

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 18: 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.

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 132.

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**.

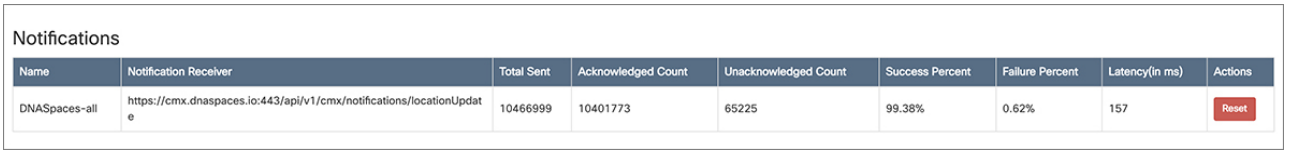
   The token to enable Cisco BLE Management can be obtained from the **Cisco BLE Management** service available in Cisco DNA Spaces. In the **Cisco BLE Management**, use the **Setup** tab to generate token.

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.

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 19: Cloud Apps Notification


Notifications

Name	Notification Receiver	Total Sent	Acknowledged Count	Unacknowledged Count	Success Percent	Failure Percent	Latency(in ms)	Actions
DNASpaces-all	https://cmx.dnaspaces.io:443/api/v1/cmx/notifications/locationUpdate	10466999	10401773	65225	99.38%	0.62%	157	Reset

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**.

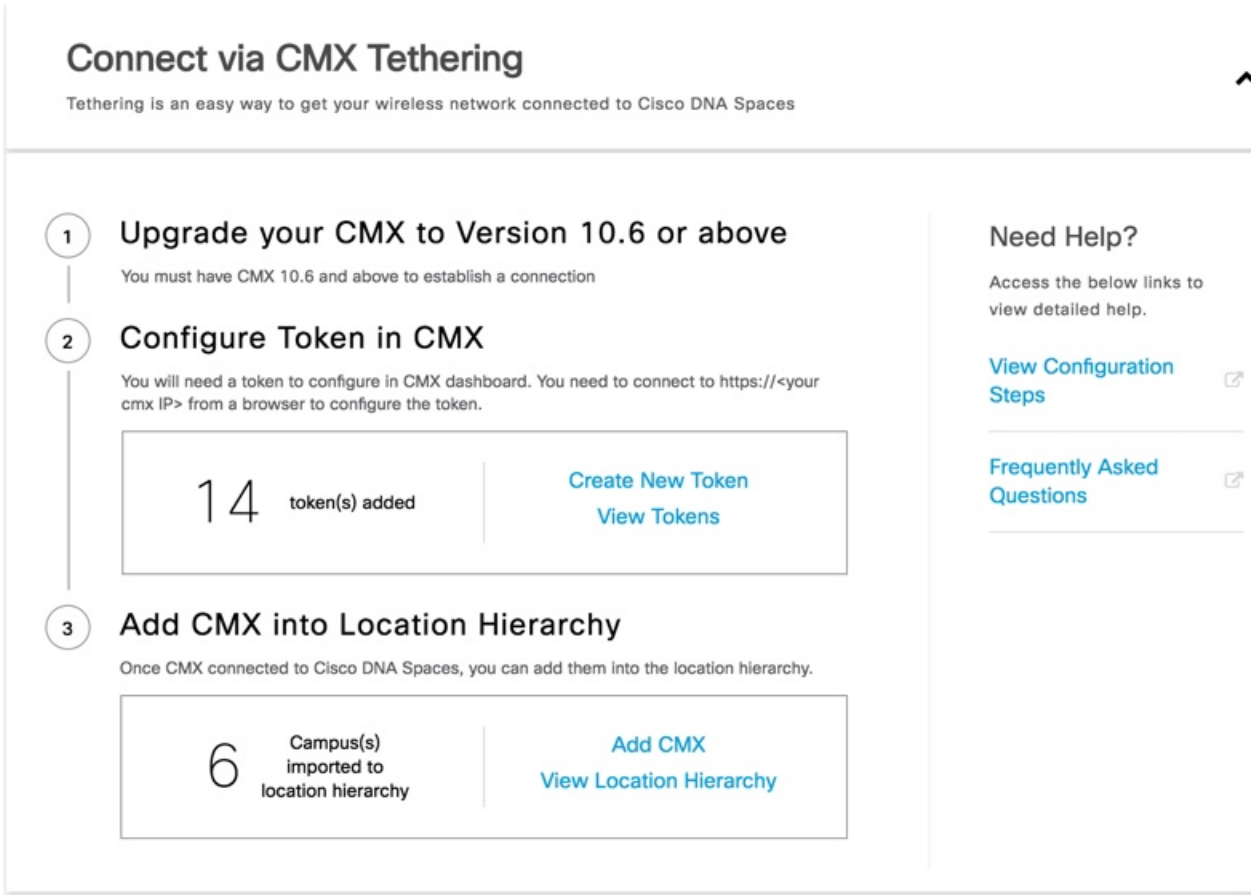
Step 6 Click **Select** for **10.6 or later**.

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.

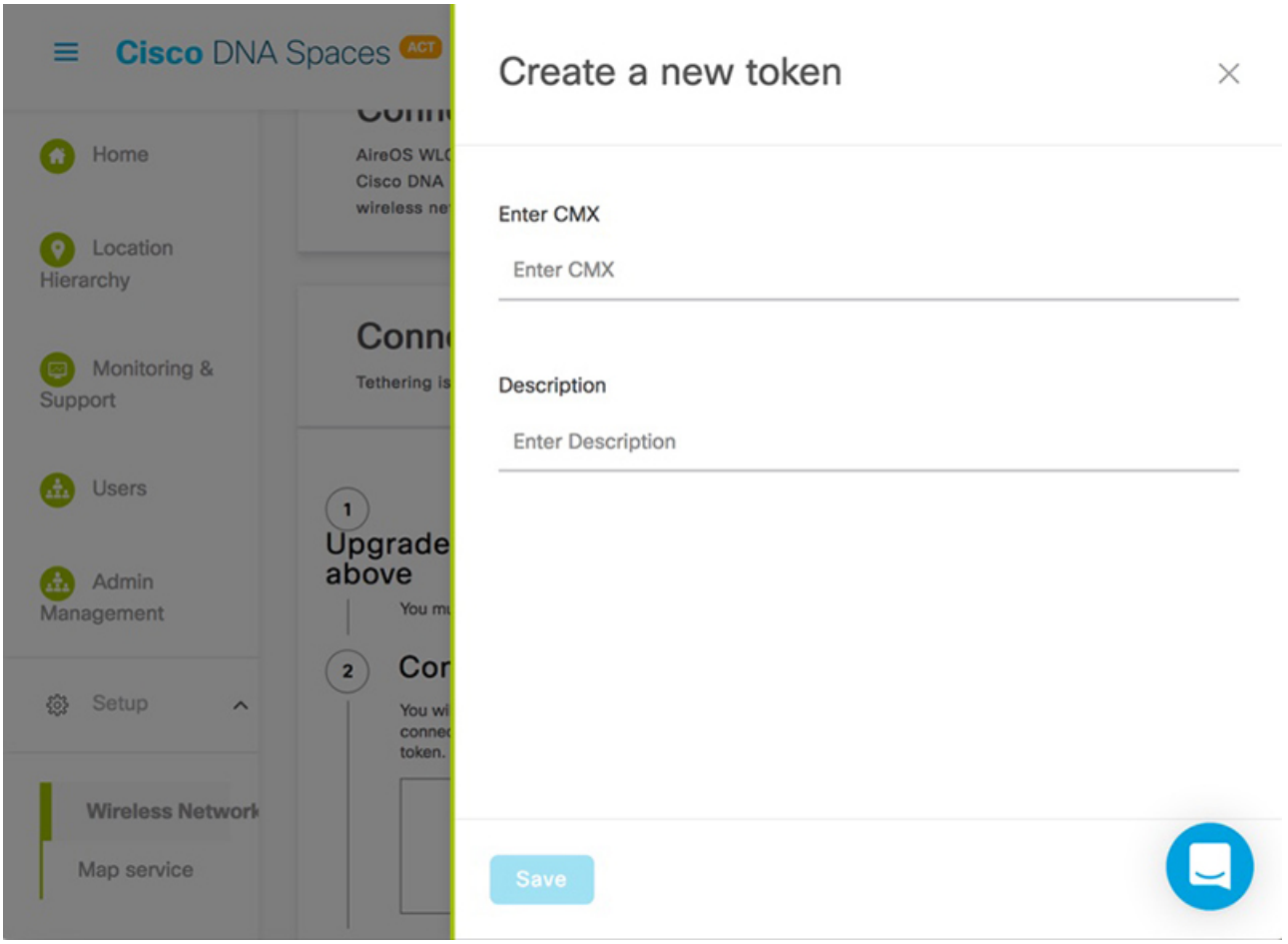
Figure 20: Connect via CMX Tethering Network Bar



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 21: 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.

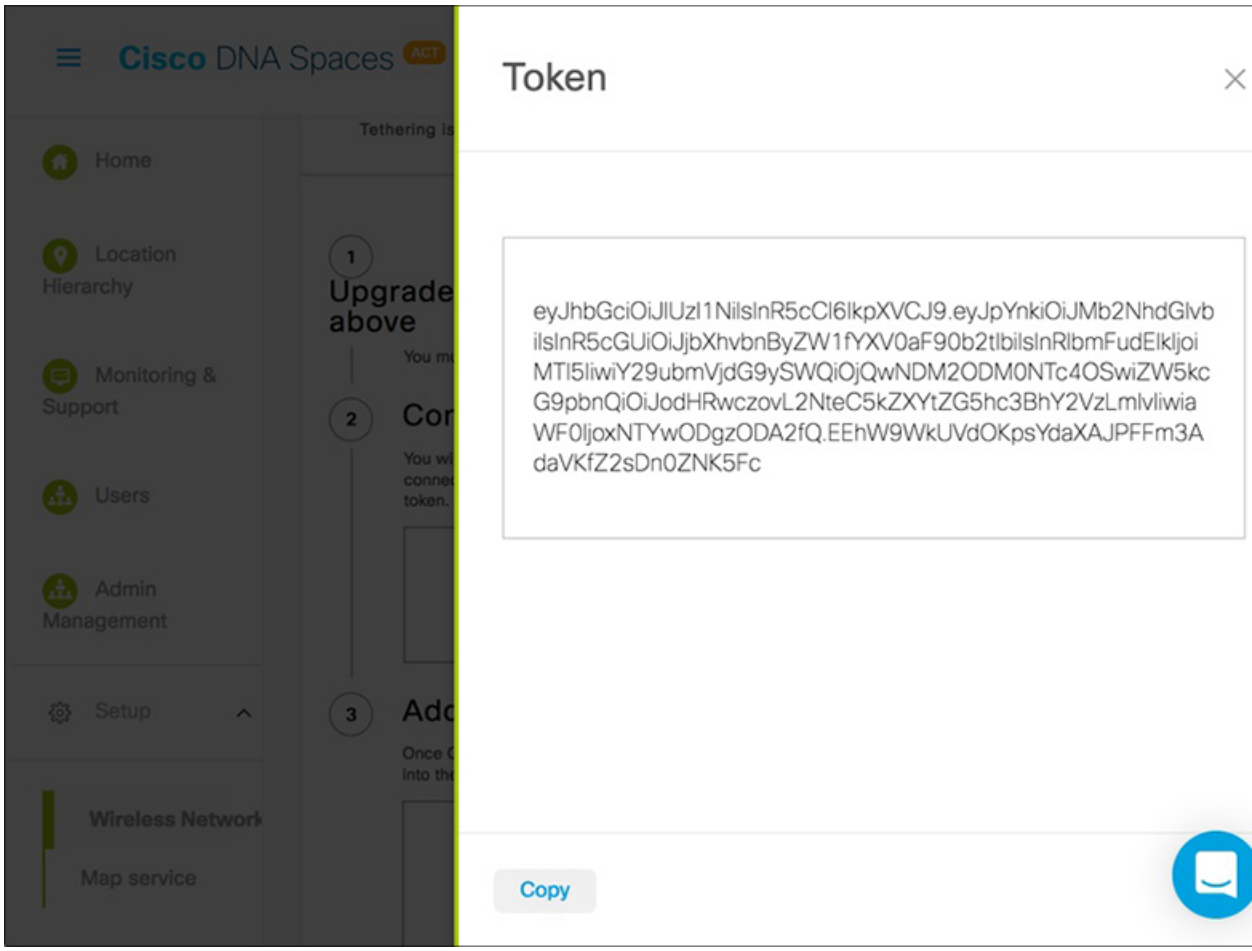
The newly added token is listed on the **Cisco Tethering Tokens** window. A Cisco CMX wireless network is shown as active after its establishes connection with Cisco DNA Spaces. You can also view the first heard and last heard timestamp details in this window.

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 22: 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**.

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.

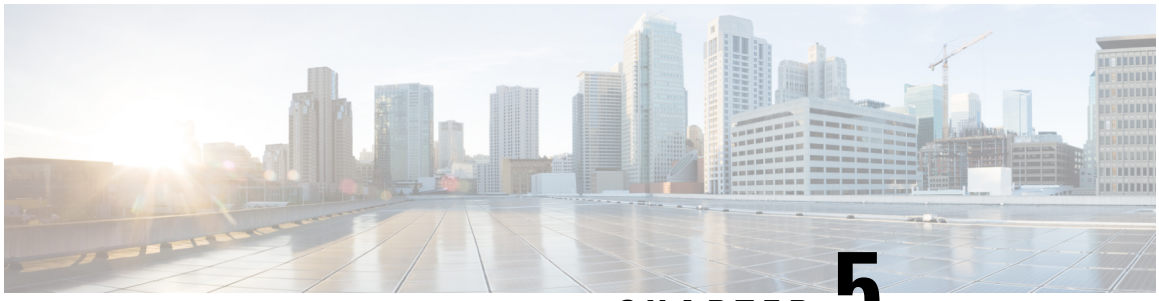
Root User Changes

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 5

Managing Cisco CMX System Settings

- Overview of the System Service, on page 139
- Viewing the Overall System Health, on page 139
- Understanding the Node Table, on page 141
- Understanding the System Update Table, on page 141
- Understanding the Coverage Details Table, on page 142
- Understanding Smart License, on page 143
- Understanding the Controllers Table, on page 143
- Managing Dashboard Settings, on page 144
- Viewing Live System Alerts, on page 174
- Viewing Patterns, on page 174
- Understanding the Metrics Tab, on page 175

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.

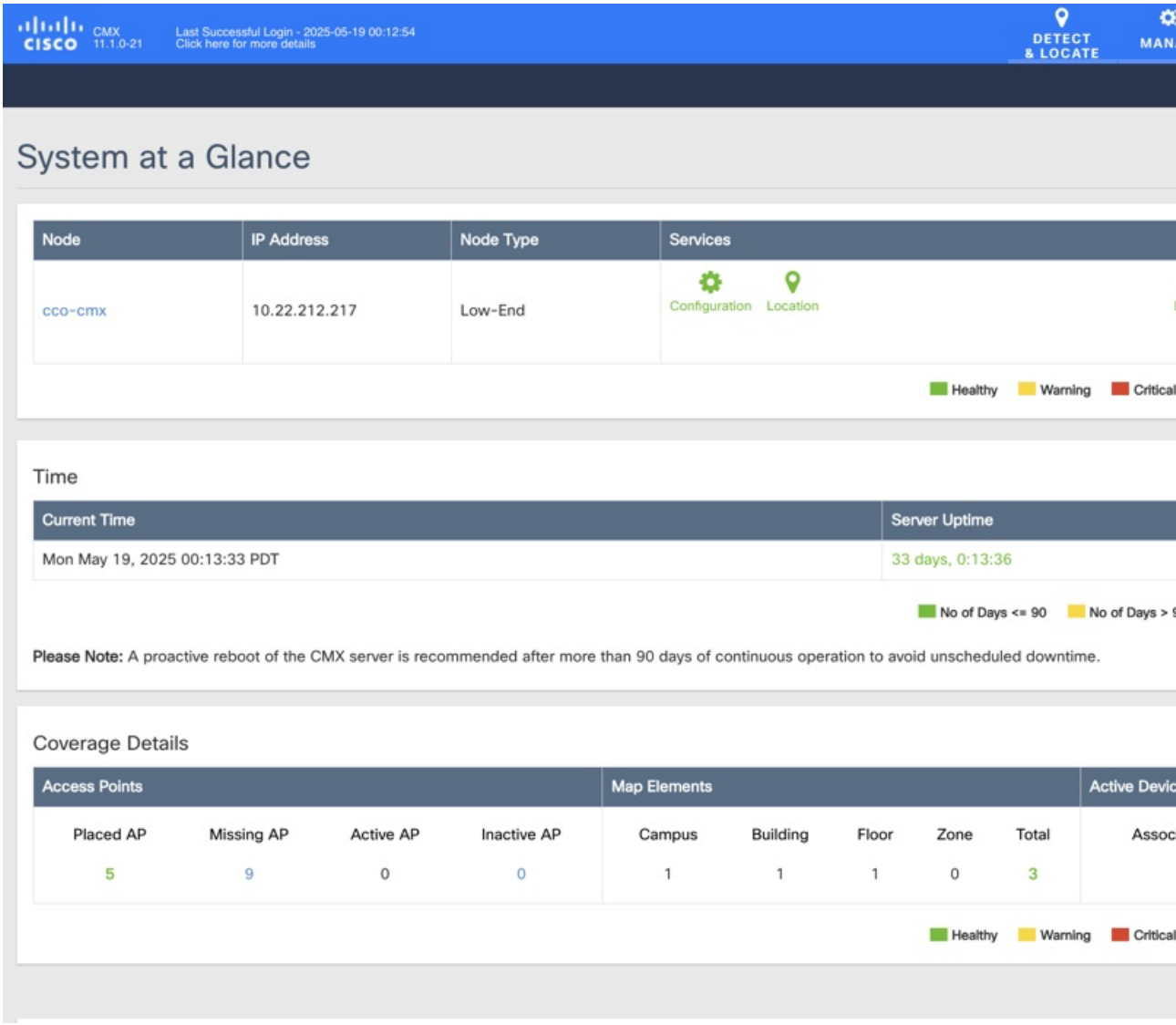
Viewing the Overall System Health

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 #unique_150.
- System Update Table. For details, see #unique_151.
- Coverage Details Table. For details, see Understanding the Coverage Details Table, on page 142.
- High Availability Table.
- Smart License Table. For more information, see #unique_153.
- Controllers Table. For details, see Understanding the Controllers Table, on page 143.

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 177.
- **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 174.
- **CPU**—Shows the load on the CPU, in percentage.
  - Click it to view the **Live Alerts** window. See Viewing Live System Alerts, on page 174.

Understanding the System Update Table

The **Time** table in the **System at a Glance** window displays information about the current running duration of Cisco CMX services and the overall server running duration.

The table displays the following details:

- **Current Time**: Displays the current system time.
- **Server Uptime**: Displays the VM or server duration in days since the last reboot.
- **Longest Running Service**: Displays the longest running process or service since the last restart.

Use the **cmxctl config uptimethreshold setthresholddays** command to configure the uptime threshold configuration settings. The default threshold is 90 days. An alert is generated when the system uptime crosses the configured threshold value. You can configure the threshold as the system performance may vary for different users, based on the load or capacity on the system, and the users must be alerted accordingly.

Note

- The system update time value is displayed in green if greater than 90 days.
- The system update time value is displayed in yellow if lesser than 90 days.

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.
  - **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 Smart License

The **Smart License** table in the **System at a Glance** window displays the Cisco CMX smart license and related AP information.

The table displays the following details:

- **License Type**: Displays the Cisco CMX smart license type.
- **Reported AP**: Displays the total number of installed APs reported by Cisco CMX to the CSSM smart account.
- **Last Reported On**: Displays the date when Cisco CMX last reported the installed APs to CSSM smart account. If there are no reporting failures, this is always the previous date.

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 153.
- 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.

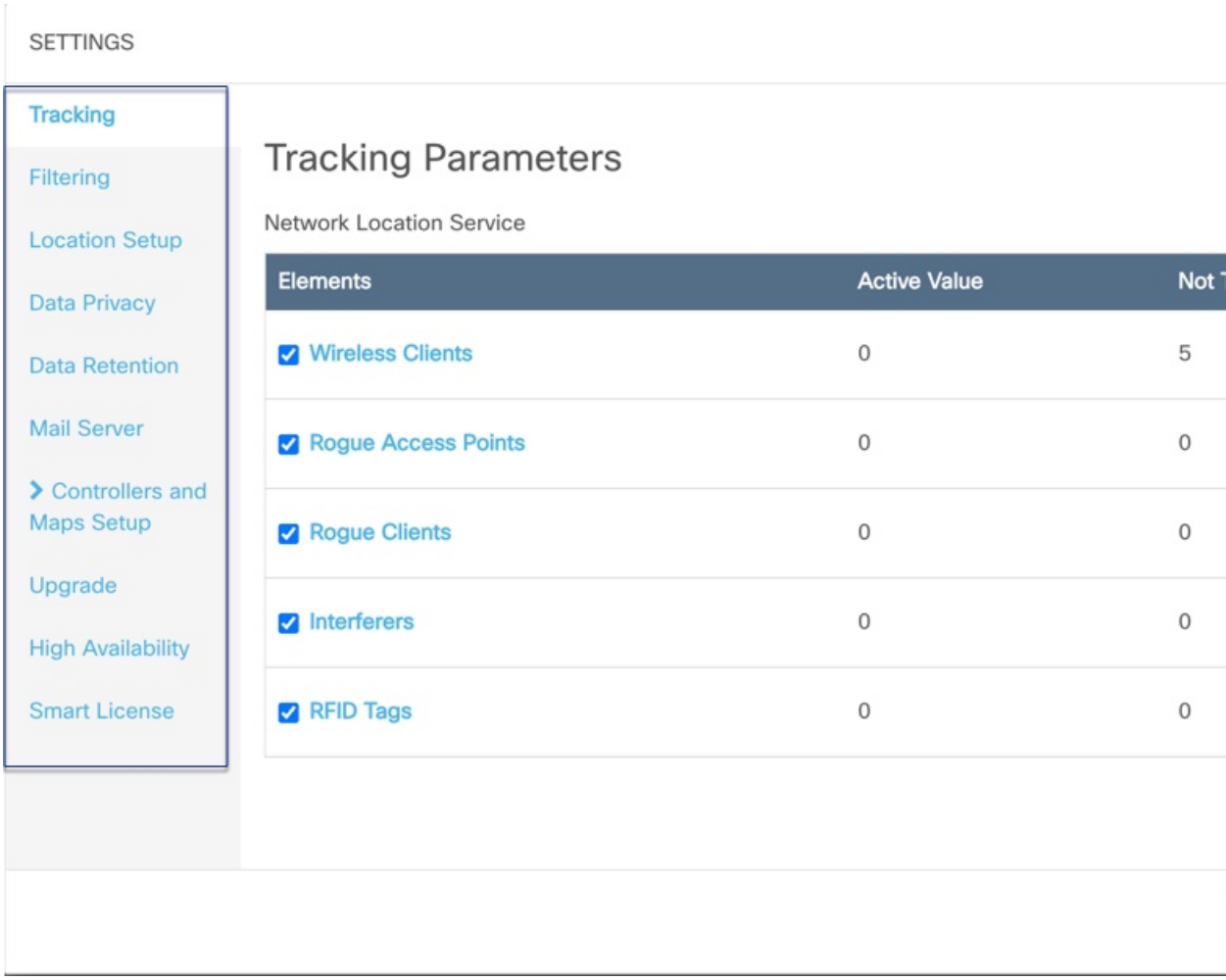
Step 3 Click **Settings** at the top-right corner of the window.

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 23: 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

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**—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.

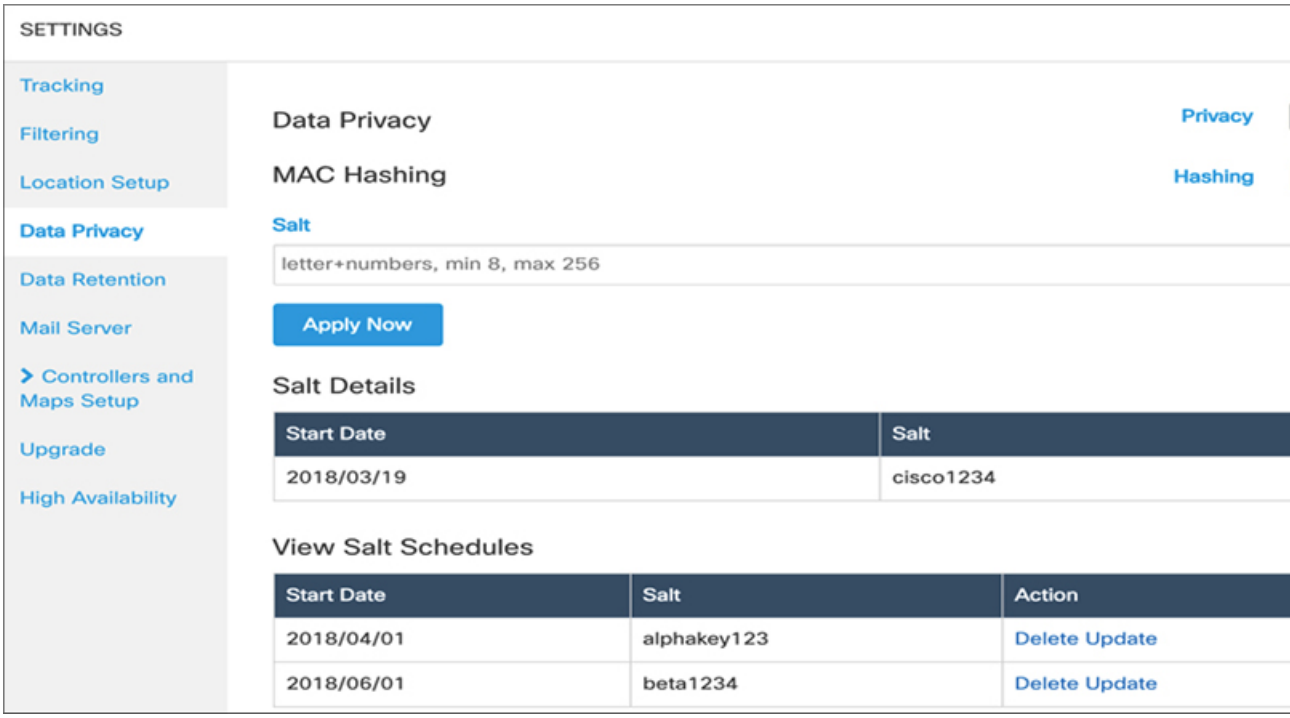
The **SETTINGS** window is displayed.

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 24: 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).

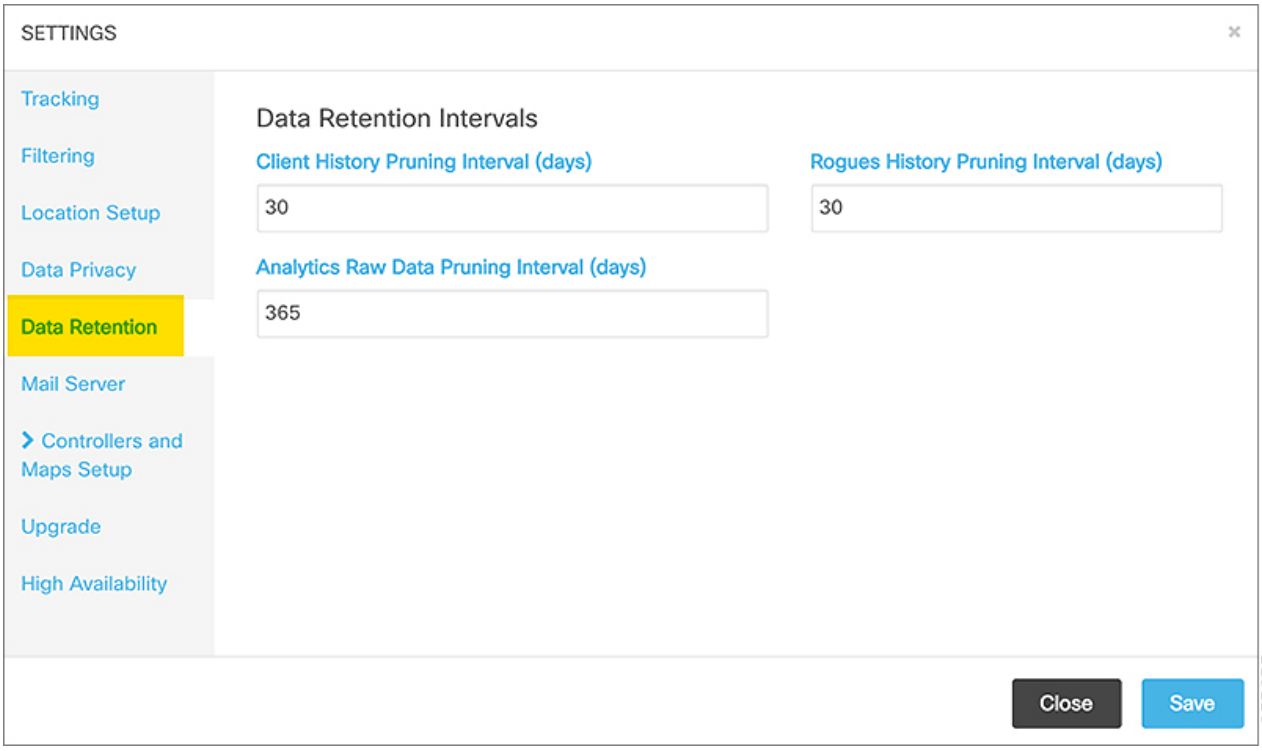
Step 2 Choose **System > Dashboard**.
The **System at a Glance** window is displayed.

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 25: 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 106.

To import maps and controllers directly from Cisco Prime Infrastructure, do the following:

Before you begin

Ensure that while exporting maps from Cisco Prime Infrastructue, 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.

Note (CSCwb72332) Cisco CMX does not support Exchangeable image file format (Exif) orientation data for floor map images. If a floor image with Exif orientation data is uploaded, Cisco CMX displays the floor image in its original orientation.

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

- Cisco CMX does not support Cisco Catalyst 9800 Series Wireless Controllers with special characters > or # in the message-of-the-day (MOTD) banner.

- After adding controllers, you must verfiy if the controller status is up and running. Using the CLI, you can run the command **cmxctl config controllers show** to display the list of controllers with the status. An **Active** status indicates an established connection.
- To validate the controller status using user interface, you need to navigate to the **System** tab. The controllers list is displayed in the tab and the new controller should appear in green. For more information, see Understanding the Controllers Table, on page 143.
- 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 Catalyst Center

Cisco CMX allows you to import maps from Catalyst Center. When you import a map from Catalyst 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.

After you add Cisco CMX in Catalyst Center and perform a map synchronization, Catalyst Center pushes the maps to Cisco CMX and overwrites the existing maps in Cisco CMX. For more information, see the About Cisco Connected Mobile Experiences section in the Cisco Catalyst Center User Guide.

Catalyst Center sends regular API queries to Cisco CMX to get client information and map files. To troubleshoot client and map synchronization issues, you can use Catalyst Center API calls. Refer to Devnet for details on the APIs.

In Catalyst 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 Catalyst 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 Catalyst 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 Catalyst 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 Catalyst Center **Network Hierarachy**:

- Cisco CMX does not import the address and latitude/longitude of the sites from the Catalyst Center.
- No limitation for the number of nested sites. Catalyst 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 Catalyst 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 High Availability 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 High Availability pair.
- **Secondary Server**—The CMX server that will be the backup or standby server in the High Availability pair.

Cisco CMX High Availability 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 High Availability 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 High Availability role. High Availability requires both primary and secondary servers, the role for one server needs to change. To change the High Availability role of a server from primary to secondary, use the **cmxha secondary convert** command in cmxadmin mode.

The Cisco CMX High Availability 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 High Availability Admin interface is different from the regular Cisco CMX interface that can be accessed at http://*cmx_ip_address*. Use the Cisco CMX High Availability Admin interface specifically monitoring and managing High Availability.

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 High Availability 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 High Availability by using either Cisco CMX web UI or CLI.

If your Cisco CMX setup with High Availability 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 137.

Note

- We recommend that you use the Cisco CMX web UI for High Availability configuration.
- The High Availability feature on Cisco CMX is part of the Cisco CMX Base license, which you would install on the primary High Availability server. The secondary High Availability server automatically receives a copy of the Cisco CMX license during sync up. There is no High Availability-specific license to install.
- Some processes running on the primary and secondary servers use Virtual Router Redundancy Protocol (VRRP). VRRP uses multicast address 224.0.0.18 and protocol number 112.

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 High Availability

- 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 High Availability is required.
- Both the primary and the secondary server should be IP connected with delay of less then 250ms if Layer 3 High Availability is used.
- From Cisco CMX release 10.6.2, NTP server settings must be configured on both Primary and Secondary server instance before High Availability 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.
- Cisco CMX uses VRRP to check keepalive from both Cisco CMX units in High Availability, ensuring no restrictions between the High Availability pair, as the Gateway must be reachable to establish Cisco CMX reachability.

Additional pre-requisites for High Availability Pairing for Cisco CMX Release 11.0.1 are as follows:

1. Run the **cmxha primary convert** command and convert the Secondary server to Primary before you upgrade to Cisco CMX Release 11.0.1 from the earlier release.
2. After the upgrade is complete, run the **cmxha secondary convert** command to convert to Secondary server.
3. Before performing High Availability pairing, run the **cmxha web status** command to verify the **Web service enabled** and **Web service running** status as `true`.
4. (Optional) If any of the status displayed is not `true`, run the **cmxha web enable** command to change the status as `true`.

5. To confirm that the dates on both Primary and Secondary server are the same, run the **cmxos date** command. This is applicable for the failover Secondary server also.

SSH Login Failure Issue

With bug CSCwb54539, SSH login fails to a Primary High Availabilty server when accessing from a Secondary High Availabilty server.

The secondary Cisco CMX server fails to setup the SSH key as it was altered and hence not able to establish a connection with the Primary server. The IP address of the Primary server is added to the Secondary server host list. However, the IP address of the Secondary server is not added to the Primary server.

To work around this issue, setup the SSH key in the Secondary server and also add the IP address of the Secondary server in the Primary server's known_host list.

We recommend that you follow these steps to work around this issue:

1. Log in to the Primary server and run the **cmxha config enable** command.
2. Enter the IP address of the Secondary server and virtual IP address (if used).

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 11: High Availability State Information

Configuration Description	Node State
CMX High Availability 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 High Availability 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.

Smart License

Smart License is a flexible approach that streamlines the process of managing your software licenses. Use Cisco Smart Software Manager (CSSM) to view and manage Cisco CMX Smart Licenses for your Cisco Smart account.

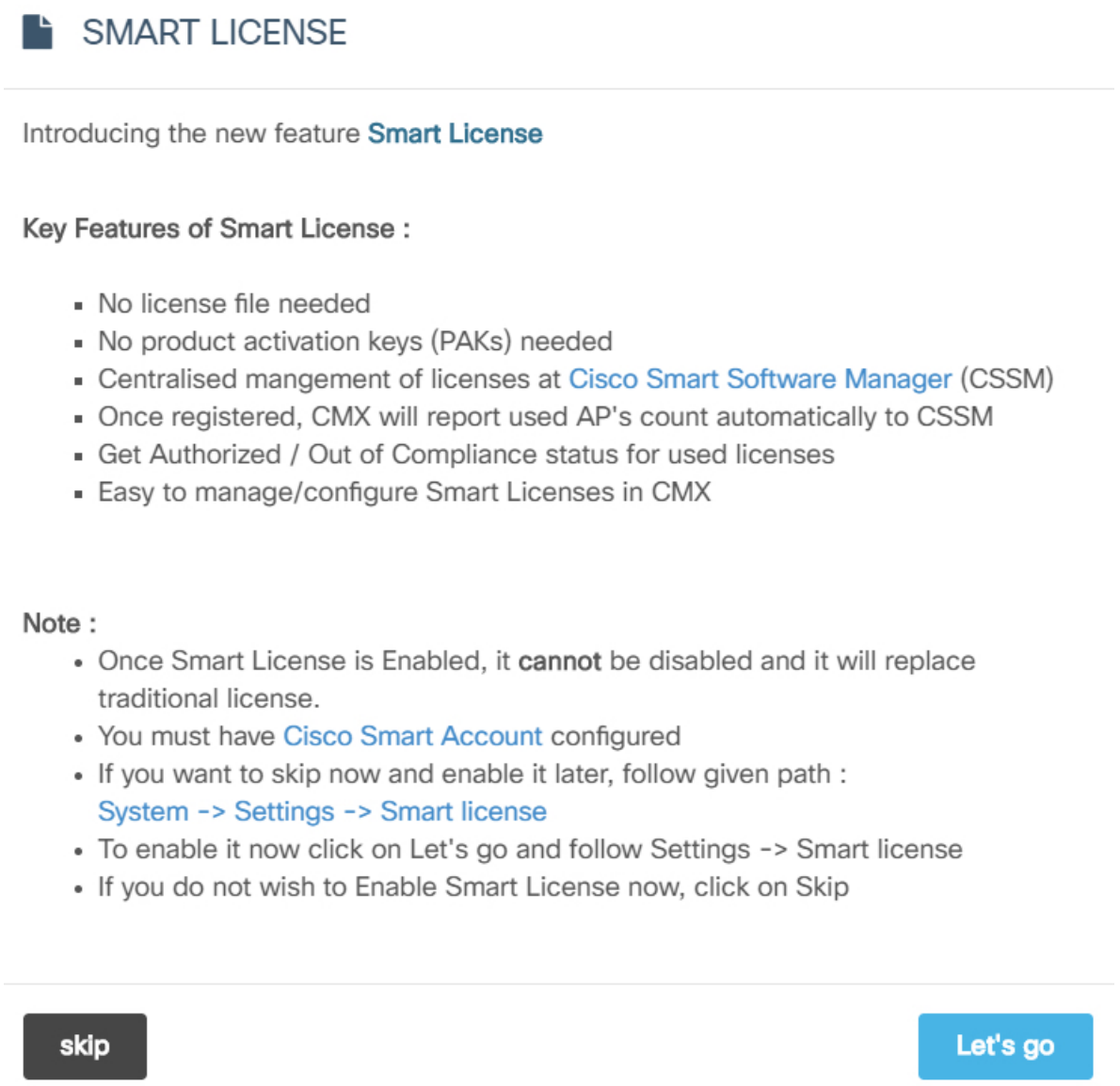
Smart License support in Cisco CMX helps you to maintain the licensing information with CSSM central repository and to manage software licenses easily. Smart License in Cisco CMX helps to eliminate storing of Product Activation Keys (PAK) and reduce the efforts in gathering information during license renewal.

Use Cisco CMX GUI or CLI to configure Smart License. Use CLI to configure Smart License setup for High Availability.

Use the **Settings** option under the **System** tab to configure Smart License. You can view AP count and status by choosing **System** > **Dashboard**.

When you login to Cisco CMX for the first time after upgrading to Cisco CMX Release 10.6.3, a pop-up message is displayed with Smart License information. You can choose to enable Smart License or skip. If you want to enable Smart License later, navigate to **System** > **Settings** > **Smart License** > **Enable**.

Figure 26: Smart License



Each Cisco CMX instance reports the installed or placed AP count to CSSM. An uninterrupted internet connectivity is required for Smart License to report the AP count to CSSM. Cisco CMX attempts AP count reporting every 24 hours and internet connectivity is required to establish this communication with CSSM.

If the AP count exceeds the purchased license count for a particular Smart Account, all registered Cisco CMX instances of that account becomes out of compliance.

The Report Count Timer Task job reports the installed AP count and is scheduled to run every 24 hours.

Note

- Smart License configuration is optional. If you set up Smart License, then traditional licensing is disabled permanently. A fresh Cisco CMX installation is required if you want to revert to traditional licensing setup.
- Smart License configuration is same for both Cisco CMX physical appliances (Cisco 3375 Appliance for Cisco Mobile Experiences and Cisco 3365 Mobility Services Engine (MSE)) and virtual machine.

Set Up Smart License on Cisco CMX with High Availability

You must provide the secondary Cisco CMX UDI in primary Cisco CMX before enabling Smart License. Use the CLI to setup Smart License on Cisco CMX with High Availability.

Before you begin

You must start with Smart License setup only after a successful High Availability setup. Before setting up Smart License, ensure that Smart Account (CSSM account) is setup for Cisco CMX and the Entitlement (license) types. We recommend that you also create a token ID for the registration process.

Procedure

Step 1 In the secondary Cisco CMX, run the **cmxos smartlicenseudi** command to get secondary Cisco CMX UDI.

Step 2 Copy the UDI and serial number of the secondary Cisco CMX.

Step 3 In the primary Cisco CMX, run the **cmxctl config smartlicense secondaryudi** command.

Step 4 Provide the copied UDI and serial number of the secondary Cisco CMX.

Note

- Note that the UDI of primary and secondary CMX is same. However, serial number is different.
- If you get an error message `Primary and Secondary udi does not match`, run the **cmxos smartlicenseudi** command on both primary and secondary Cisco CMX to verify the UDI.
- Re-registration and registration renewal are not allowed in secondary CMX when the failover state is active.
- In case of a restore action on another node or Cisco CMX or VM, the UDI and serial number differs and hence a re-registartion is required.
- If High Availability is disabled, re-register on the primary Cisco CMX to use it as a standalone Cisco CMX that is associated with the corresponding CSSM account.

What to do next

After sucessfully configuring secondary UDI, you can proceed to set up and register standalone Smart License. Verify the smart license details after the registration is complete.

Set Up Smart License on Cisco CMX (GUI)

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.

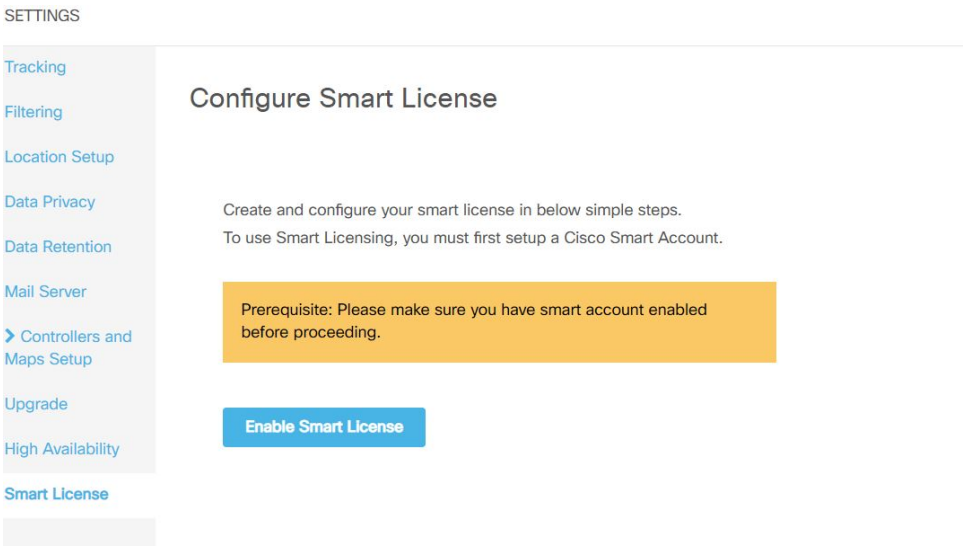
Step 3 Click **Settings** at the top-right corner of the window.

The **SETTINGS** window is displayed.

Step 4 In the left pane, click **Smart License**.

Step 5 Click **Enable Smart License**.

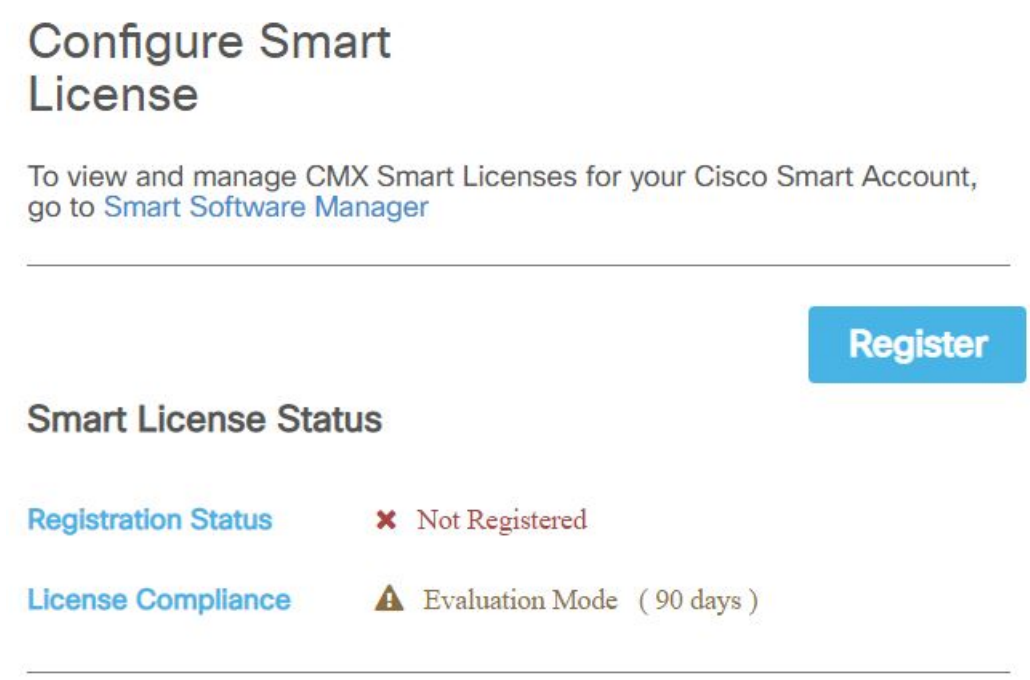
Figure 27: Configure Smart License > Enable Smart License



The Smart License Status window is displayed.

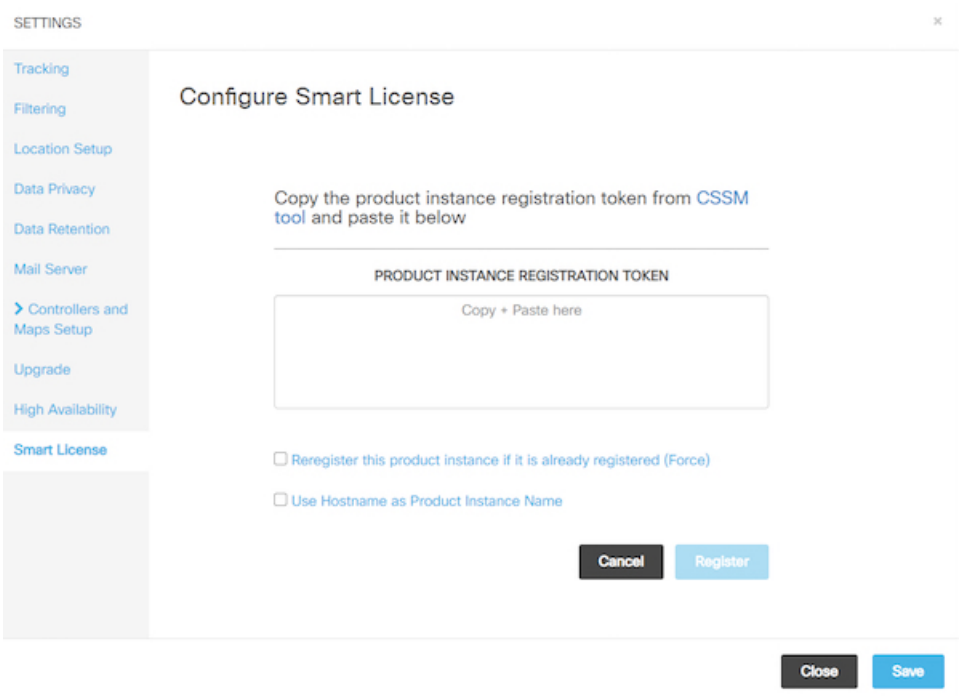
Step 6 Click **Register** to register the product instance.

Figure 28: Configure Smart License > Register



Step 7 In the Product Instance Registration Token field, enter the token ID from the CSSM smart account.

Figure 29: Product Instance Registration Token



Step 8 Click **Register**.

A success notification message is displayed in green color. All error messages are displayed in red color.

Step 9 (Optional) If an error is encountered, do either of the following:

- If token ID is invalid or expired, then verify token ID in Smart Account and try again with the correct token ID.
- If a communication error message is displayed, then check your network connectivity and try again.

After registering, the Smart License Status window is displayed.

Step 10 In the Smart License Status window, verify the Registration Status, License Compliance, Smart Account Name, Virtual Account, and Product Instance Name.

Note
If hostname sharing configuration is selected at the time of registration, then hostname is displayed as "Product Instance Name". Otherwise, by default a combination of UDI_PID and UDI_SN is displayed in Cisco CMX as well as in Smart Account.

After Smart License is enabled, various Cisco CMX services are available depending on the Cisco CMX license types SEE, EXTEND, and ACT. By default, Cisco CMX pulls ACT licenses.

The following table lists the services available for the corresponding license type:

Table 12: License Types and Services

License Type	Services Enabled	Services Disabled
ACT	**a.** Analytics **b.** Hyperlocation Configuration **c.** Partner Stream Notification	NA
EXTEND	**a.** Partner Stream Notification	**a.** Analytics **b.** Hyperlocation Configuration
SEE	NA	**a.** Analytics **b.** Hyperlocation Configuration **c.** Partner Stream Notification

Set Up Smart License on Cisco CMX (CLI)

Before you begin

Ensure that all Cisco CMX services such as location, database and configurations are successfully running.

Procedure

Step 1 Connect to Cisco CMX through the console.

Step 2 To enable Smart License, run the **cmxctl config smartlicense enable** command.

A message is displayed when Smart License is enabled successfully. We recommend that you try again if you get a failure message.

Step 3 To register Smart License, run the **cmxctl config smartlicense register** command.

Step 4 Enter the token ID from CSSM smart account to register the Cisco CMX product instance.

After Smart License is successfully registered, AP count along with license type in use reporting is initiated.

If the registration process is a failure, one of the following messages is displayed prompting you to take appropriate action:

Message	Action
`Invalid / Expired Token ID`	Verify token ID in Smart Account and try to register again with the correct token ID.
`Already registered`	Try to re-register using the **cmxctl config smartlicense reregister** command.
`Communication error`	Check the network connectivity and try to register again.

Note
We recommend that you try to register again if you see any other message than the ones mentioned above.

Step 5 (Optional) To verify the registration status, run the **cmxctl config smartlicense status** command.

Registration status is displayed as `Registered` and license compliance status as either `Authorized/Out of Compliance/Evaluation Mode` depending upon the reported AP count.

Configure Smart License

Before you begin

Use the Configure Smart License window to manage Cisco CMX smart licenses. You can renew authorization and registration, re-register and de-register Cisco CMX smart licenses.

Procedure

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

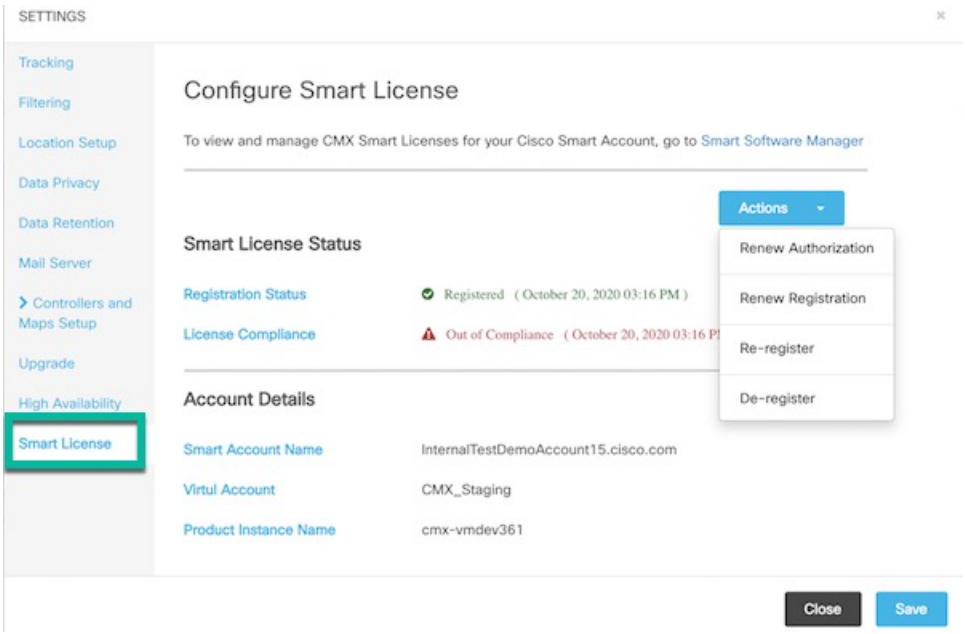
Step 2 Choose **System > Dashboard**.
The **System at a Glance** window is displayed.

Step 3 Click **Settings** at the top-right corner of the window.

The **SETTINGS** window is displayed.

Step 4 In the left pane, click **Smart License**.

Figure 30: Configure Smart License



Step 5 In the **Smart License Status** area, the following information is displayed:

- **Registration Status**: Displays the Cisco CMX smart license registered status.
- **License Compliance**: Displays the Cisco CMX smart license compliance details.

Step 6 In the **Account Details** area, the following information is displayed:

- **Smart Account Name**: Displays the Cisco CMX smart license account name.
- **Virtual Account**: Displays the Cisco CMX virtual account name.
- **Product Instance Name**: Displays the Cisco CMX product instance name.

Step 7 Click **Actions** drop-down list to view the following options:

- **Renew Authorization**: Click to renew Cisco CMX smart license authorization.

  Note
  - This action is optional as renew authorization is performed automatically when Cisco CMX communiccates with CSSM. Alternatively, Smart License agent performs renew authorization automatically after every 30 days from backend. As Cisco CMX reports installed AP count to CSSM daily, renew authorization is initiated automatically from backend.
  - We recommend that you perfrom this action if you want to troubleshoot or renew authorization manually if status is `Out of Compliance`. You also can renew authorization manually to reflect any recent Smart Account updates to reflect in Cisco CMX.

- **Renew Registration**: Click to renew Cisco CMX smart license registration.

  Note
  - This action is optional as renew registration is performed by Cisco CMX automatically in backend at the time of registration.
  - This action renews the Registration ID and Certificate with CSSM. Cisco CMX performs this action automatically every 6 months from backend.

- **Re-register**: Click to re-register Cisco CMX smart license in the CSSM.

  Note
  - This action forcefully re-registers Smart License and overrides any existing registered instance. This action results in reported data lose of that particular instance in Smart Account.
  - We recommend that you perfom this action to troubleshoot Smart License or when High Availability pair updates are complete.

- **De-register**: Click to de-register Cisco CMX smart license in the CSSM.

  Note
  We recommend that you perform this action if Cisco CMX is not in use and you want to deregister the instance from CSSM.

Troubleshoot Smart License

Possible Cause

All Cisco CMX instances are out of compliance because it exceeds the number of purchased licenses in Smart Account.

Solution

Manage the installed APs within the same instances in a way to adhere with the requirements of your purchased license count or purchase additional licenses from Smart Account. After this is done, status off all Cisco CMX instances becomes **Authorized** automatically when Cisco CMX reports the installed AP count to CSSM next time. If you want to change the status manually, do either of the following:

- Cisco CMX GUI: Navigate to **System** > **Settings** > **Smart License** and choose **Renew Authorization** from **Actions** drop-down list
- Cisco CMX CLI: Run the **cmxctl config smartlicense renewauthorization** command.

Possible Cause

If Cisco CMX with High Availability is in split-brain state, what is the expected behaviour and recovery process of Smart Licensing?

Solution

Both primary and secondary CMX reports the installed AP count to CSSM simultaneously and create duplicate AP count report. This changes the status of product instance as `Out of Compliance`.

To resolve this issue, deregister Smart License from secondary CMX using CLI or Cisco CMX GUI or remove secondary CMX from Smart Account itself. In primary CMX, perform **Renew Authorization** action. This changes primary CMX status as `Authorized` and acts as a standalone CMX Smart Licensing.

After High Availability pair is recovered successfully, set up Smart License for High Avaliability again.

Possible Cause

Cisco CMX shows Smart License status as `Not registered` and displays unknown instances in Smart Account.

Solution

To resolve this issue, remove the unknown instances from Smart Account under **Actions** menu in the Product Instance page. Then, proceed to register or re-register from Cisco CMX.

Possible Cause

Smart License reporting fails.

Solution

Smart License reporting is scheduled to run every 24 hours. If it fails one time due to unexpected network issue, it automatically tries to report again after 24 hours. As long as Smart License is registered successfully and authorization is in place, Smart License reporting works as expected.

Possible Cause

Getting `Communication error` message for Smart License actions performed.

Solution

Verify Cisco CMX network status to ensure that internet access is available and retry again. If the issue persists, check the proxy settings.

Possible Cause

High Availability setup was not working and a new setup is configured.

Solution

Set up Smart License for High Availability again.

Possible Cause

When you perform Smart License deregistration action for the very first time or retry deregistration action and still the `Product Instance is not valid` message displays.

Solution

The product instance you are trying to deregister is already removed from CSSM. Expect a delay in CSSM to process the action but the product instance is already de-registered successfully. We recommend that you proceed with registering or re-registering action.

Possible Cause

Following messages displays:

- `Authorization Failed` message on GUI or CLI
- `Product Already Registered` message displays when you try to register eventhough you deregistered the product instance using GUI or CLI
- `Authorization Failed` or `Id certificate does not match` or `Renew Registration failed` message displays on GUI or CLI after a successful High Availability failback.
- If backup restore was done on another node or CMX or VM and the UDI is diffferent

Solution

Perform **Re-register** using CLI or use **Actions** in Smart License Status page.

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**

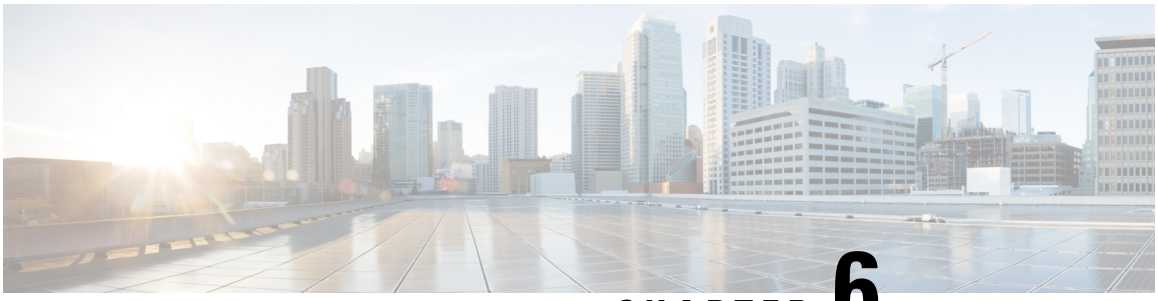
To view the Presence metrics:

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 6

FIPS, CC, and UCAPL Support in Cisco CMX

Cisco CMX supports the Federal Information Processing Standard 140-2 (FIPS). FIPS is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components. The US Federal government requires that all IT products dealing with Sensitive, but Unclassified (SBU) information meet these standards. If your system needs to be FIPS compliant, you can enable FIPS. Once you do so, the system uses the cryptographic algorithms defined by the NIST for FIPS for all encrypted communication between its internal and external components.

The Common Criteria for Information Technology Security Evaluation (referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. Main focus of CC is to establish secure connection with external entities. Another main focus is providing extensive audit logging functionality to capture all the important configuration activities and system events within the product.

Cisco CMX supports FIPS and Common Criteria through a single mode called FIPS mode. Going forwards FIPS mode in Cisco CMX is referred to both FIPS and CC features and functionalities. If you need to enable FIPS and CC on Cisco CMX, you need to enable FIPS mode on Cisco CMX. Once you do so, the system uses the cryptographic algorithms defined by the NIST for FIPS for all encrypted communication between its internal and external components. Additionally all the connection in and out of CMX (e.g. Web connection, controller connection, rsyslog server connection) are encrypted using TLS, HTTPS or IPSec.

The U.S. Department of Defense Unified Capabilities Approved Products List (UCAPL) mode is a higher level of security than FIPS alone. Its purpose is to maintain a single consolidated list of products that have completed interoperability and cybersecurity certification. Less secure protocols, such as HTTP, SHA1, TLS ver. 1, and RSA 1024 are no longer supported.

Once you have enabled FIPS mode, you have the option to enable UCAPL mode. UCAPL requires a 15-20 character password, and a fixed timeout period of ten minutes, among other restrictions.

Note

- FIPS and UCAPL mode commands are available only to users with CMX admin user credentials through the Cisco CMX command line. Refer to Cisco CMX Command Reference, release 10.6 for more information.
- When FIPS or UCAPL authentication mode is enabled, you cannot enable or disable IPSec service. It is enabled by default when FIPS or UCAPL mode is enabled.
- When FIPS or UCAPL authentication mode is enabled, you can use the IPSec commands to restart, stop, or start IPSec services, and change or check authentication type.
- All IPSec commands are available when FIPS mode is disabled.

  For more information about IPSec 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
- (CSCvo95518) Cisco CMX Release 10.6.2 and later with FIPS mode enabled can establish a Network Mobility Services Protocol (NMSP) connection with Cisco Catalyst 9800 wireless controllers running Release 16.12, with FIPS and CC mode enabled.

  In contrast, Cisco CMX Release 10.6.2 and later with FIPS mode enabled cannot establish an NMSP connection with Cisco WLCs running Release 8.x.

  Note Before enabling FIPS mode on Cisco CMX, remove all the non-FIPS compliant controllers from Cisco CMX. Otherwise, establishing NMSP connectivity after restarting Cisco CMX services will require an extensive amount of time.

- FIPS Mode Requirements, on page 185
- UCAPL Mode Requirements, on page 185
- Setting up FIPS or UCAPL Mode Correctly, on page 187
- Choosing an Encryption Key Type, on page 188
- Creating a Certificate Signing Request, on page 188
- Viewing Stored Certificates, on page 190
- Validating Mutual Certificate During NMSP Connection in FIPS Mode, on page 191
- Verifying FIPS Readiness, on page 192
- Enabling and Managing FIPS Mode, on page 193
- Configuring Notification Listener in FIPS Mode, on page 194
- Enabling and Managing UCAPL Mode, on page 195
- Enabling Logging in UCAPL mode, on page 195
- Validating Client Certificates, on page 196
- Setting Up a UCAPL Automatic Backup, on page 197
- Working with the Certificate Revocation List, on page 198
- Disk Wipeout, on page 199

FIPS Mode Requirements

FIPS mode initiates a set of interoperability and cybersecurity configuration changes designed to bring your CMX systems into compliance with the the Federal Information Processing Standard 140-2 (FIPS).

Authentication Requirements

- CMX sessions time out after no more than 30 minutes.
- Imported controllers in FIPS mode must be updated to Secure Socket Shell (SSH) authentication, to enable their Network Mobility Services Protocol (NMSP) connection.

Log in Requirements

There are no additional log in requirements for FIPS.

Password Requirements

- Password length: The password must be 8 to 20 characters long.
- Minimum: Password must include one uppercase letter (A to Z), one lowercase letter (a to z), one digit (0 to 9), and one symbol from the allowed set: !"#$%&'()*+,-./:;<=>?@[]_^`{|}~ (space also allowed).

Protocol Requirements

- Transport Layer Security (TLS) 1.1 or higher.
- Internet protocol security (IPsec) for User Datagram Protocol (UDP) connection.
- Advanced Encryption Standard (AES) 256.
- Secure Hash Algorithm (SHA) 1 or higher.
- One of the following:
  - Rivest, Shamir, and Adelman (RSA) 2048 or higher.
  - Elliptic Curve Digital Signature Algorithm (ECDSA) with a National Institute of Standards and Technology (NIST) curve of P-256 or higher.

UCAPL Mode Requirements

UCAPL mode initiates a set of interoperability and cybersecurity configuration changes designed to bring your CMX systems into compliance with the the U.S. Department of Defense Unified Capabilities Approved Products List (UCAPL). UCAPL mode requires encryption of the `/opt` disk partition, as well as the following authentication, login, password, and protocols.

Note FIPS mode is a required prerequisite for UCAPL mode. Once FIPS has been enabled, the UCAPL mode option becomes available through the CMX **cmxctl config fips ucaplmode** command.

Authentication Requirements

- Two-factor authentication—Every user needs a signed client certificate. If your certificate is for user Tom, you can't log in as user Harry.
- Cisco Prime authentication is required when importing controllers and maps.

Log in Requirements

- User accounts are disabled for 30 minutes after three consecutive unsuccessful logins in one hour. The user sees a message when his account has been temporarily disabled. An admin can re-enable the user.
- There is a four-second delay between login prompts following a failed login.

Password Requirements

- Password length: 15-20 characters.
- Minimum: Password must include one uppercase letter (A to Z), one lowercase letter (a to z), one digit (0 to 9), and one symbol from the allowed set: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] _ ^ ` { | } ~ (space also allowed).
- No more than three consecutive repeating characters.
- Password cannot match any of the last five passwords.
- A password change is required every 60 days.
- Password changes are limited to one password change per user per day.
- A user must log in again after a password change.

Protocol Requirements

- Transport Layer Security (TLS) 1.1 or higher.
- Internet protocol security (IPsec) for User Datagram Protocol (UDP) connection.
- Advanced Encryption Standard (AES) 256.
- Secure Hash Algorithm (SHA) 1 or higher.
- One of the following:
  - Rivest, Shamir, and Adelman (RSA) 2048 or higher.

- Elliptic Curve Digital Signature Algorithm (ECDSA) with a National Institute of Standards and Technology (NIST) curve of P-256 or higher.

Setting up FIPS or UCAPL Mode Correctly

Cisco recommends that you follow this general command deployment order when deploying FIPS or UCAPL mode. Your requirements may vary. For a full description and usage guidelines for each of 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

Before you begin

You must run the following commands before enabling FIPS or UCAPL mode.

- To enable remote audit logging, run the **cmxctl config audit settings** command.
- To install remote syslog server certificate, run the **cmxctl config certs importrsyslogca** command.

Procedure

Step 1 Connect to CMX via SSH.

Step 2 Enter the **cmxctl config auth settings** command to enable strong password authentication, set minimum password length, set the number of unsuccessful login attempts, and set session timeout time.

Step 3 Enter the **cmxctl config certs keytype** command to select a keytype: RSA (the default) or ECDSA.

Step 4 Enter the **cmxctl config certs clear** command to clear out old or existing certificates.

Step 5 Enter the **cmxctl config certs createcsr** command to generate a new private and public keypair for the CMX server, and create a Certificate Signing Request (CSR). See Creating a Certificate Signing Request, on page 188 for more information.

Step 6 Have your certificates signed by authenticating third parties. See Installing Certificates in Cisco CMX, on page 20 for more information.

Step 7 Enter the **cmxctl config certs importcacert** command to install the concatenated CA certificates.

Step 8 Enter the **cmxctl config certs importservercert** command to install the concatenated server certificates.

Note
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), an alert is generated on **System > Alerts** tab. The alert will be generated once a day until certificate expires or new valid certificate is installed.

Step 9 Enter the **cmxctl config fips verify** command to verify that your CMX system is correctly configured to support FIPS mode. See Verifying FIPS Readiness, on page 192 for more information.

Step 10 Enter the **cmxctl config audit settings** command to enable and manage the remote logging of system events (syslogs).

Step 11 Enter the **cmxctl config certs importrsyslogca** command to create, import, or manage security key certificates.

Step 12 Enter the **cmxctl config fips enable** command to enable FIPS mode.
The command restarts the CMX services.

Note
When FIPS or UCAPL authentication mode is enabled, access to the command line through PuTTY or other standard SSH clients is restricted. In these cases, we recommend that you connect directly from a console, or use the VMWare vSphere console.

Step 13 Optionally, enter the **cmxctl config fips ucaplmode enable** command to enable UCAPL mode.

The CMX `/opt` partition must be encrypted before you can enable UCAPL. 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.

The command restarts the CMX services. You must enter the encryption passphrase each time the device restarts, before logging in.

Choosing an Encryption Key Type

You can select a supported encryption algorithm for FIPS and UCAPL mode using the **cmxctl config certs keytype** command. Options are Rivest–Shamir–Adleman (RSA), or Elliptic Curve Digital Signature Algorithm (ECDSA).

Procedure

Step 1 Connect to Cisco CMX via SSH or through the console.

Step 2 Enter the **cmxctl config certs keytype** command.

Step 3 Select the encryption algorithm you prefer. For RSA keytype, select key length 2048 or 4096.

Step 4 See the following example:

```
Please enter key type [RSA / ECDSA] (RSA, ECDSA) [RSA]:
Please enter RSA key size [2048 / 4096] (2048, 4096): 4096
Keytype is set to RSA with 4096-bit key size.

NOTE: Please re-generate the certificate for this change to take effect.
```

Creating a Certificate Signing Request

You can create a certificate signing request (CSR) with a corresponding public and private keypair using the **cmxctl config certs createcsr** command. When generating a CSR, you can now configure the Subject Alternative Name (SAN) as an extension in the certificate. You can set SAN to Public FQDN entry of the Cisco CMX server. The same SAN value is used as the default value for the **Common Name** field. You can override this default value by entering another value for common name.

Note If FIPS mode is enabled in Cisco CMX, certification validation is performed every time when CMX services are restarted. If certificate validation fails, Cisco CMX will not restart.

Procedure

Step 1 Connect to Cisco CMX via SSH or through the console.

Step 2 Enter the **cmxctl config certs clear** command to remove certificate files in the /opt/cmx/srv/certs directory.

Step 3 Enter the **cmxctl config certs createcsr** command.

The output and certificate information will vary, depending upon whether you chose the RSA or ECDSA encryption algorithm. Follow the prompts for your system. See the following example.

```
For SAN field of CSR, enter FQDN for CMX server []: servername.domain.com
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]: CA
Locality Name (eg, city) []: San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Cisco Systems, Inc.
Organizational Unit Name (eg, section) []: Enterprise
Common Name (e.g. server FQDN or YOUR name) [servername.domain.com]:
wirelesstestserver.domain.com
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 in: /opt/cmx/srv/certs
The Private key is in: /opt/cmx/srv/certs

CSR created successfully.
```

The new CSR and the Private key are both stored in the `/opt/cmx/srv/certs` directory.

Viewing Stored Certificates

You can see the certificates stored in the CMX /opt/cmx/srv/certs directory using the **cmxctl config certs show** command.

Procedure

Step 1 Connect to Cisco CMX via SSH or through the console.

Step 2 Enter the **cmxctl config certs show** command.

Your certifications display, similar to this example:

```
Certificate details

************************  Certificate Listing  ********************
======================================================================
**********************  CA Certificate(s)  ************************
======================================================================
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            b6:c0:fc:05:f6:27:45:1a
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=CA, L=San Jose, O=MSE, CN=RootCA
        Validity
            Not Before: Jul 19 05:17:33 2018 GMT
            Not After : Jul 18 05:17:33 2021 GMT
        Subject: C=US, ST=CA, L=San Jose, O=MSE, CN=RootCA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:ba:f2:2b:cd:87:90:23:f0:64:f5:83:d5:f2:90:
                    43:1a:16:36:c9:67:1a:82:f1:8f:6b:eb:1c:47:f1:
                    c4:fd:bf:55:98:ab:06:c0:90:dc:d7:13:1f:d3:2f:
                    12:e8:f2:74:66:65:7c:49:12:72:0c:27:9c:2e:84:
                    7e:29:a8:b6:18:62:5f:c2:97:a4:1c:e7:45:a2:cb:
                    f3:35:f3:64:15:e5:f0:27:6f:f1:07:61:41:9b:4c:
                    96:b3:56:d4:28:a4:85:90:86:52:4c:04:bc:da:38:
                    cc:f8:05:5b:3e:5c:03:b4:59:ec:8b:c9:5d:eb:61:
                    76:ba:20:3f:64:6c:25:5d:50:1e:85:37:ad:09:b2:
                    4a:fa:58:15:89:91:d9:5f:b8:9d:dd:64:31:8b:a4:
                    df:99:ff:ae:72:19:f8:a3:93:81:b9:4e:07:74:74:
                    95:b6:42:7b:5a:7d:38:92:4a:f4:86:5a:54:66:f0:
                    c1:fe:38:31:df:24:1c:40:94:36:67:8b:b3:56:93:
                    62:26:29:c2:cd:7f:7d:66:9d:f1:78:54:88:4f:6c:
                    b3:b7:80:54:05:03:09:c9:f9:14:65:8a:21:00:b5:
```

Validating Mutual Certificate During NMSP Connection in FIPS Mode

Cisco CMX establishes TLS/HTTPS connection with external systems. Cisco CMX uses NMSP and Northbound notification receivers (HTTP type) for establishing connection with Cisco Catalyst 9800 Series Wireless Controller. Certificate exchange is initiated during the SSL/TLS handshake when connections are successfully established between Cisco CMX and controller. However, certificates were not mutually validated by both connections.

To validate certificates on both sides, you must configure the following:

- For Cisco CMX: Configure or import controller CA certificate and Northbound Receiver's certificate for validating the certificate.
- For Cisco Wireless LAN Controller: Import Cisco CMX CA certificate.

Note

- Certificate validation happens only if FIPS is enabled on both Cisco CMX and controller. For example, if Cisco CMX is in FIPS mode, you can only synchronization and validate certificates if FIPS is enabled in controller.
- Cisco CMX Release 10.6.2 and later with FIPS mode enbaled can establish a NMSP connection with Catalyst 9800 Wireless LAN Controllers running Release 16.12 with FIPS/CC mode enabled. However, Cisco CMX Release 10.6.2 and later with FIPS mode enabled cannot establish a NMSP connection with controller running Release 8.x.
- We recommend that before enabling FIPS mode in Cisco CMX, remove all non-FIPS compliant controllers from Cisco CMX. Otherwise, establishing NMSP connectivity after restarting Cisco CMX services will require an extensive anount of time.

To validate certificates, perform the following steps:

Procedure

Step 1 To export CA certificates from Cisco CMX, enter this command and copy the certificate text that needs to be added into the unified controller. **cmxctl config certs exportnmspca**

Step 2 To import Cisco CMX CA certificates into unified controller, enter this command. **crypto pki trustpool import terminal**

Information similar to the following appears:

```
CMX-eWLC-1(config)# crypto pki trustpool import terminal
% Enter PEM-formatted CA certificate.
% ENd with a blank line or "quit" on a line by itself.
<<Copy the Cisco CMX certificate text here>>
% PEM files import succeeded.
```

Step 3 To export controller CA certificate, enter the following commands:

a) To find the trustpoint label, enter the **show wireless management trustpoint** and note down the trustpoint, for example ewlc-tp1.
b) To export CA certificate, enter the **crypto pki export <trustpoint> pem terminal** command and copy and paster the CA certificate contents (BEGIN-END block) into a file.

Note
In this command, replace <*trustpoint*> with the trustpoint name from Step 3a. You can ignore "General Purpose Certificate' output.

Step 4 To import controller CA certificate into Cisco CMX, enter this command: **cmxctl config certs importcontrollerca <filename>** command.

Ensure that the file is in PEM format. You can also merge multiple CA certificates into a single file.

Step 5 Restart Cisco CMX services for the changes to take effect.

Step 6 (Optional) To view the installed certificates, run the **cmxctl config certs show** command.

Verifying FIPS Readiness

The **cmxctl config fips verify** command displays a simple grid, which identifies whether or not your CMX system is correctly configured to support FIPS mode. Cisco recommends that you run this command before trying to enable FIPS.

Procedure

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

Step 2 Enter the **cmxctl config fips verify** command.
In this example, the command output indicates that the certificate authority (CA), server, and client certificates are not ready to support FIPS.

```
[cmxadmin@cmx]# cmxctl config fips verify

Certificates Required

+--------------------------------------+
| CA Certificate               | True |
+--------------------------------------+
| Server Certificate           | True |
+--------------------------------------+
| Server Key                   | True |
+--------------------------------------+
| Rsyslog CA Certificate       | False|
+--------------------------------------+

Certificate Validation

+--------------------------------------+
| CA Cert Validation           | True |
+--------------------------------------+
| Server Cert Validation       | True |
```

```
+--------------------------------------+
| Client Cert Validation        | True |
+--------------------------------------+

Security Configuration

+--------------------------------------+
| Strong Password               | True |
+--------------------------------------+
| Security Parameters           | True |
+--------------------------------------+

Audit Logging

+--------------------------------------+
| Audit Logging Status          | False|
+--------------------------------------+
```

What to do next

If the system shows any out-of-compliance areas (False), check Setting up FIPS or UCAPL Mode Correctly, on page 187 to address the discrepancies.

Enabling and Managing FIPS Mode

Use the **cmxctl config fips** commands to verify your CMX system is ready for Federal Information Processing Standards (FIPS) mode, to enable or disable FIPS mode, and to show its running status.

You should take precautions while performing **cmxctl config fips disable**. Ensure that you do not perform any delete action by running the **cmxctl config certs clear** on certificates such as ca.crt, server.crt and so on while FIPS is enabled. The FIPS mode will then go into a deadlock situation and can never be disabled. This is because even for disabling the FIPS mode, system checks for certificates and if not found, it will fail to disable FIPS stating the error - "Problem in disbaling FIPS mode". And if you try to add self-signed certificates, they will not get added because FIPS is enabled. We recommend that you do not attempt to clear certificates while FIPS is enabled. Ensure that you adhere to the necessary precationary measures when Cisco CMX is in FIPS mode.

Procedure

Step 1 Connect to CMX via SSH.

Step 2 Enter the **cmxctl config fips verify** command, to confirm that all the necessary security and certificate requirements are in place.

```
[cmxadmin@cmx]# cmxctl config fips verify

Certificates Required

+--------------------------------------+
| CA Certificate                | True |
+--------------------------------------+
| Server Certificate            | True |
+--------------------------------------+
```

```
| Server Key                     | True |
+--------------------------------------+
| Rsyslog CA Certificate         | False|
+--------------------------------------+

Certificate Validation

+--------------------------------------+
| CA Cert Validation             | True |
+--------------------------------------+
| Server Cert Validation         | True |
+--------------------------------------+
| Client Cert Validation         | True |
+--------------------------------------+

Security Configuration

+--------------------------------------+
| Strong Password                | True |
+--------------------------------------+
| Security Parameters            | True |
+--------------------------------------+

Audit Logging

+--------------------------------------+
| Audit Logging Status           | False|
+--------------------------------------+
```

Step 3 Enter the **cmxctl config fips enable** command to start FIPS mode.
The CMX processes restart.

What to do next

Using a console, enter the **cmxctl config fips status** command, to verify that FIPS is running on your Cisco CMX device.

Configuring Notification Listener in FIPS Mode

In FIPS mode, notifications are sent to only those notification listeners with the **Receiver Type** set as "HTTPS". If Receiver type is set to HTTP, that notification listener will not receive any notification in FIPS mode.

For more information about how to create a notification, see Create a New Notification, on page 120.

After FIPS mode is enabled (and Cisco CMX services restarted), you will need to change the **Receiver type** of every listener to **HTTPS** in order to receive notifications.

When the Receiver Type is HTTPS, you must import CA certificate corresponding to the Notification listener (CA that signed the Server Certificate of the notification listener). The certificate file needs to be in PEM format. This is mandatory field.

After all the listeners are modified to set Receiver Type as **HTTPS** and corresponding CA certificate is imported, you must restart the Cisco CMX services for the certificate changes to take effect.

When notifications are generated, Cisco CMX establishes HTTPS connection with notification listener and use the CA certificate to validate the listener's certificate before sending the notification. If the certificate validation fails, the notification is not sent to the listener.

Enabling and Managing UCAPL Mode

Use the **cmxctl config fips ucapl** commands to enable or disable the U.S. Department of Defense Unified Capabilities Approved Products List (UCAPL) mode, and to show its running status.

Before you begin

The CMX `/opt` partition must be encrypted before you can enable UCAPL.

Procedure

Step 1 Connect to CMX command line either from a console, or from a VMWare vSphere console.

Step 2 Enter the **cmxctl config fips ucaplmode enable** command to start UCAPL mode.
The CMX processes restart.

What to do next

Using a console, enter the **cmxctl config fips ucaplmode status** command, to verify that UCAPL mode is running on your Cisco CMX device.

Enabling Logging in UCAPL mode

Cisco CMX release 10.6 supports logging HTTP headers and access to important files and folders when UCAPL mode is enabled.

Logging HTTP Headers

You can log all the HTTP headers received in every incoming HTTPS request to local syslog i.e. /var/log/messages. This feature can be turned on or off using command given below.



Note This operation of logging all the headers is CPU intensive and can cause performance degradation. So use it cautiously and turn it off when not required.

Procedure

Step 1 To enable this feature, run the **cmxctl config fips ucaplmode logHTTPHeaders** command.

```
[cmxadmin@cmx]# cmxctl config fips ucaplmode logHTTPHeaders
Enable HTTP Headers Logging [yes / no] [no]: yes
Restarting haproxy service
True
```

```
Done
The nodeagent service is currently running with PID: 1470
Attempting to restart Haproxy
.....
Service Haproxy has successfully restarted
logHTTPHeaders is enabled.
```

Step 2 To view these logs, run the **cmxctl config audit view** command.

Step 3 (Optional) To disable this feature, run the **cmxctl config fips ucaplmode logHTTPHeaders** command.

```
[cmxadmin@cmx]# cmxctl config fips ucaplmode logHTTPHeaders
Enable HTTP Headers Logging [yes / no] [no]:
Restarting haproxy service
True
Done
The nodeagent service is currently running with PID: 1470
Attempting to restart Haproxy
.....
Service Haproxy has successfully restarted
logHTTPHeaders is disabled.
```

Logging File Access

You can log access to important files and folders, whenever those files/folders are added/deleted/modified, while in UCAPL mode. This feature can be turned on or off using command given below.

Procedure

Step 1 To enable this feature, run the **cmxctl config fips ucaplmode logFileAccess** command.

```
[cmxadmin@cmx]# cmxctl config fips ucaplmode logFileAccess
Enable File Access Logging [yes / no] [no]: yes
Restarting Audit Service
Stopping logging:                                          [  OK  ]
Redirecting start to /bin/systemctl start auditd.service
```

Step 2 (Optional) To disable the feature, run the **cmxctl config fips ucaplmode logFileAccess** command.

```
[cmxadmin@cmx]# cmxctl config fips ucaplmode logFileAccess
Enable File Access Logging [yes / no] [no]:
Restarting Audit Service
Stopping logging:                                          [  OK  ]
Redirecting start to /bin/systemctl start auditd.service
```

Validating Client Certificates

Use the **cmxctl config certs clientcertvalidation** command when CMX is in FIPS or UCAPL mode to obtain a valid, signed client certificate for every CMX user ID.

Procedure

Step 1 Connect to CMX through SSH or the console.

Step 2 (Optional) Use the **cmxctl config {FIPS | ucaplmode} status** command to verify whether FIPS or UCAPL is currently enabled.or not.

Step 3 Use the **cmxctl config certs clientcertvalidation** command to enforce CMX validation of client certificates.

Setting Up a UCAPL Automatic Backup

Cisco CMX supports automatic weekly backups in the U.S. Department of Defense Unified Capabilities Approved Products List (UCAPL) mode. You can enable the backups before or after entering UCAPL mode, but the backups will not begin until UCAPL is enabled.

Procedure

Step 1 Connect to the CMX CLI either from a console or SSH.

Step 2 Enter the **cmxctl config fips ucaplmode autobackup** command to configure the automatic backup:

```
[cmxadmin@cmx]#cmxctl config fips ucaplmode autobackup
CMX Auto Backup is currently disabled.
```

Step 3 Respond to the following prompt: **Do you want to enable it? (yes/no) [yes]:**

Click **Yes** or press **Enter** to enable auto backup if CMX is already in UCAPL mode. If CMX is not in this mode, auto backups begin, when UCAPL mode is enabled. The default option is **yes**.

```
CMX Auto Backup frequency is weekly.
Please select day and hour of the week to run the auto-backup.
```

Step 4 Respond to the following prompt: **Day of the week: [0=Sunday, 1=Monday ... 6=Saturday] [0]:**

Enter a number from **0** (Sunday) to **6** (Saturday) to specify the day of the week the backup should be performed. The default is **Sunday**.

Step 5 Respond to the following prompt: **Hour of the day: [0-23] [2]:**

Enter a number from **0** (midnight) to **23** (11 p.m.) to specify the hour of the backup. The default is **2** a.m.

If UCAPL mode is already enabled, your confirmation will resemble this:

```
CMX auto-backup is now enabled.
Redirecting to /bin/systemctl restart crond.service
auto-backup will execute every Saturday at 10:10 AM
```

If UCAPL mode is not yet enabled, your confirmation will resemble this:

```
CMX auto-backup is configured. But, it will be enabled only when UCAPL mode is enabled.
Redirecting to /bin/systemctl restart crond.service
auto-backup will execute every Monday at 9:10 AM
```

Step 6 (Optional) To disable autobackup, run the **cmxctl config fips ucaplmode autobackup** command again, and enter **yes** or press **Enter** when prompted.

```
[cmxadmin@cmx]#cmxctl config fips ucaplmode autobackup
CMX Auto Backup is currently enabled.

Do you want to disable it ? (yes/no) [yes]:yes
CMX Auto Backup is now disabled.
Redirecting to /bin/systemctl restart crond.service
```

Working with the Certificate Revocation List

Cisco CMX supports certificate validation of the Certificate Revocation List (CRL) as per FIPS/CC requirement. There are three options for supporting the CRLs in Cisco CMX. Once CRL is installed properly, then Cisco CMX server certificate is validated against CA certificate and against CRL as well. If the Cisco CMX server certificate is revoked and reflected in the CRL then the Cisco CMX server certificate validation will fail and Cisco CMX services will fail to start in FIPS mode.

The available options are:

- **Automatic download of CRL if CA certificate support CDP extension**—If the CA certificate that has signed the CMX server certificate is being imported contains a CRL Distribution Point (CDP) extension in the CA certificate, then the CDP extension contains the URL where CRL can be downloaded from. CMX attempts to download this URL from the internet (if access is available).
- **Manual import of CRL (in PEM format)**—If the internet access is not available on CMX server (directly or through HTTP proxy), then you can download the CRL from its location and import the downloaded file into CMX.
- **Configuring URL for the CRL for periodic automatic download**—In this option, the URL of the CRL file can be configured directly into CMX. CMX will then download the CRL periodically – once a day and update it. This will keep the CRL file up-to-date as the CRLs as periodically updated.

Manual Import of CRL

To import the CRL file, follow the below steps:

Before you begin

Download the CRL from its location. This CRL file will be mostly in DER format. Before you import into Cisco CMX, you will need to covert it from DER to PEM format. On a separate server, you can convert the CRL file from DER to PEM format. To convert the CRL file, run the **openssl x509 -inform der -in crlfile -out crl.pem** command.

Procedure

Step 1 SCP the CRL file in PEM format to Cisco CMX.

Step 2 Run the **cmxctl config certs importcrl** command to import the CRL file.

```
[cmxadmin@cmx]# cmxctl config certs importcrl
Enter the full path of the CRL file /home/cmxadmin/server.crl.pem
Successfully transferred the file
CRL file imported successfully
CMX Certificate validation against CRL is successful.
0
```

Step 3 To configure the the CRL URL, run the **cmxctl config certs importcrlurl** command.

```
[cmxadmin@cmx]# cmxctl config certs importcrlurl
Please enter URL to downlaod CRL: http://example.com/testca.crl
Redirecting to /bin/systemctl restart crond.service
```

Note
If internet access is available directly (or via proxy), configuring URL of the CRL into Cisco CMX will be the best option for supporting CRL, as it will automatically download the CRL once a day and keep the local copy up-to-date.

Disk Wipeout

This feature allows a Cisco CMX user to wipe out the entire disk including data and executables. This feature can be used when you no longer need to use the system and want to de-commission it and/or use for some other purpose.

After performing this operation, system will not boot as usual and will not provide the normal login prompt. The system becomes unusable and all the data on the disk is deleted and not accessible anymore.

Note This disk wipeout feature is currently available only in FIPS mode. System needs to be in FIPS mode in order to use this command. Additionally, this command is available only from console window and it is not allowed from SSH session.

To wipeout the disk, run the **cmxos wipeoutdisk** command from console window.

```
[root@server]# cmxos wipeoutdisk
WARNING: This command will wipe out the entire disk.
It will remove entire CMX installation along with all the existing data.
Once completed, this box will not be useable.
Do you want to continue? [y/N]: y
lave you closed all SSH sessions to this CMX? [y/Nl: y
WARNING: This is your last chance.
If you want to take backup, please exit now.
Vou can take backup and transfer it to some other machine.
I*hen execute this command again.
Do you want to continue with disk wipeout? [y/N]: y_
Stopping the CMX services

nonit.service is not a native service, redirecting to /sbin/chkconfig.
cuting /sbin/chkconfig min it off
Stopping nodeagent Process...

cuting shutdown
```

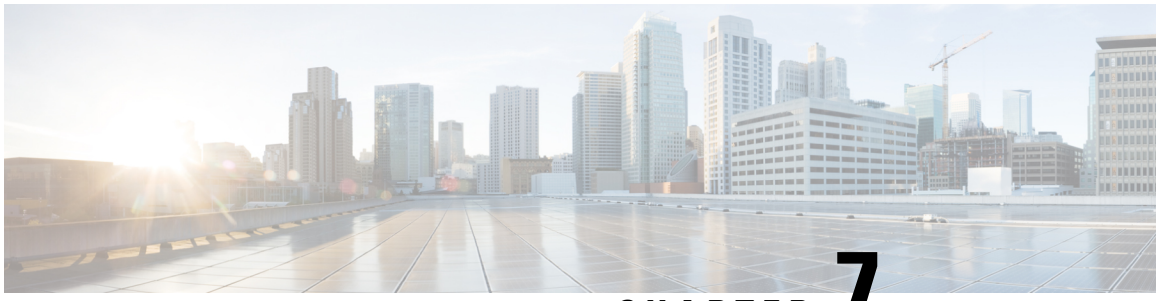
If the disk was encrypted previously, it will prompt for the disk encryption password in order to clean the disk. This password will not be asked if the disk was not encrypted earlier. The operation will take half an hour or more based on the total disk space.

```
Welcome to emergency mode! After logging in, type "journalctl -xb" to view
system logs, "systemctl reboot"
to reboot, "systemctl default" or ÄD to
boot into default mode.
Error getting authority: Error initializing authority: Error sending credentials:
Error sending mess
age: Broken pipe (g-io-error-quark, 44)

Entered Rescue mode on Sun Jan 27 14:27:48 UTC 2019.
Proceeding with disk wipeout...
Wiping out OUA disk
Jnmounting /opt partition ...
/opt disk is encrypted. Removing encryption ...
Enter passphrase to be deleted:
WARNING!

Hiis is the last keyslot. Device will become unusable after purging this key.
Are you sure? (Type uppercase yes): YES
Logical volume vg_cmx/lv_opt is used by another device.
Wiping out the disk now. This operation will take long time.
shred: /dev/sda3: pass 1/2 (random)...
shred: /dev/sda3: pass 1/2 (random)...502MiB/121GiB 0/
shred: /dev/sda3: pass 1/2 (random)...
1.0GiB/121GiB 0/
shred: /dev/sda3: pass 1/2 (random)... 1.5GiB/121GiB lx
```

Once the operation is complete, press **Enter** to continue. After rebooting, system will not boot as usual and you cannot login to the Linux system or Cisco CMX.



CHAPTER 7

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, on page 201
- Unlocking Users, on page 202
- Setting Strong Password Authentication, on page 203
- Password Recovery, on page 205
- Resetting Cisco CMX GUI Administrator Password, on page 208
- Setting Up External Server Authentication, on page 209
- Manage AAA users for SSH Access, on page 214
- Log in to SSH as AAA User, on page 215
- Setting Up Audit Logging, on page 215
- Performing Scheduled Backup for Cisco CMX, on page 218
- Performing Manual Backup for Cisco CMX, on page 218
- Restoring Data, on page 221
- Encrypting the CMX /opt Directory, on page 223
- Display a Login Banner, on page 225
- Managing NTP Servers, on page 226
- Troubleshooting Cisco CMX Server Shutdown Problems, on page 230

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 209.

- 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. Use the **cmxos apiserver user** command to create/modify the Cisco CMX API users for this account.

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, or through the console if FIPS or UCAPL is enabled.

Step 2 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 minimum values 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, or through the console if FIPS or UCAPL is enabled.

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. CMX default: Not required. FIPS: Yes. UCAPL: Yes. **Note** If **Enable strong password** is set to **Yes**, you can extend the password up to 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. The range is 8 to 20 characters. The default is 8 characters. CMX default: 8 characters. FIPS: 8-20 characters. UCAPL: 15-20 characters.

Prompt	Action
Maximum password lifetime [1-9999] [9999]:	This is the duration after which the password will expire. You must change the password before it expires. The range is 1 to 9999 days. The default for CMX is 9999 days. CMX default: 9999 days. characters. UCAPL: 60 days.
Password Expiry Warning Period [1-30] [14]:	Password expiry warning period duration. Range is 1-30 days. CMX default: 14 days. characters. UCAPL: 7 days. **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. FIPS: 3-5. UCAPL: 3.
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 lockout interval time in minutes. Range is 1-120. Default is 30.

Prompt	Action
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. FIPS: 30 minutes or less. UCAPL: 10 minute timeout required.
Max Concurrent Sessions per user [5-25] [10]:	Set the maximum number of concurrent sessions allowed per user to log in to the SSH and GUI. The range is five to 25, and the default is 10 logins per user.
Max global Concurrent sessions [5-100] [50]:	Set the maximum number of global concurrent sessions allowed to log in including SSH and GUI. The range is between five to 100, and the default is 50 login.
Absolute Session Timeout in minutes [10-480] [480]:	Set the limit for the absolute session timeout in minutes. The range is between 10 and 480 minutes, and the default is 480 minute.

Cisco CMX then restarts its authorization services.

Password Recovery

If you are using Cisco CMX Release 11.0.1, follow the process below to recover the password in console access.

Note To recover the cmxadmin 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.

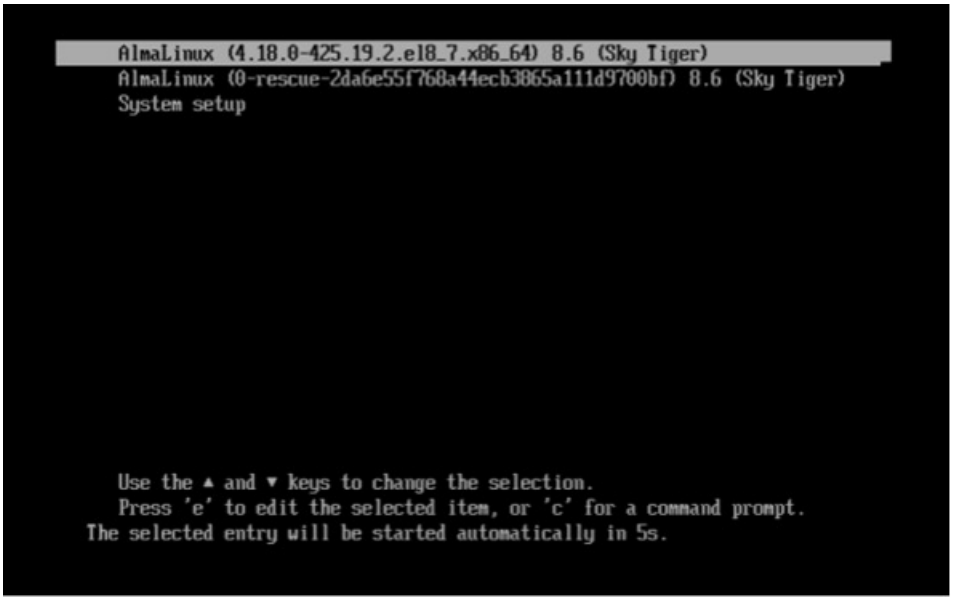
Procedure

Step 1 Power on the Cisco CMX VM.

Step 2 Establish console access.

The **System Setup** window is displayed and stays for a span of five seconds.

Figure 31: Console Access

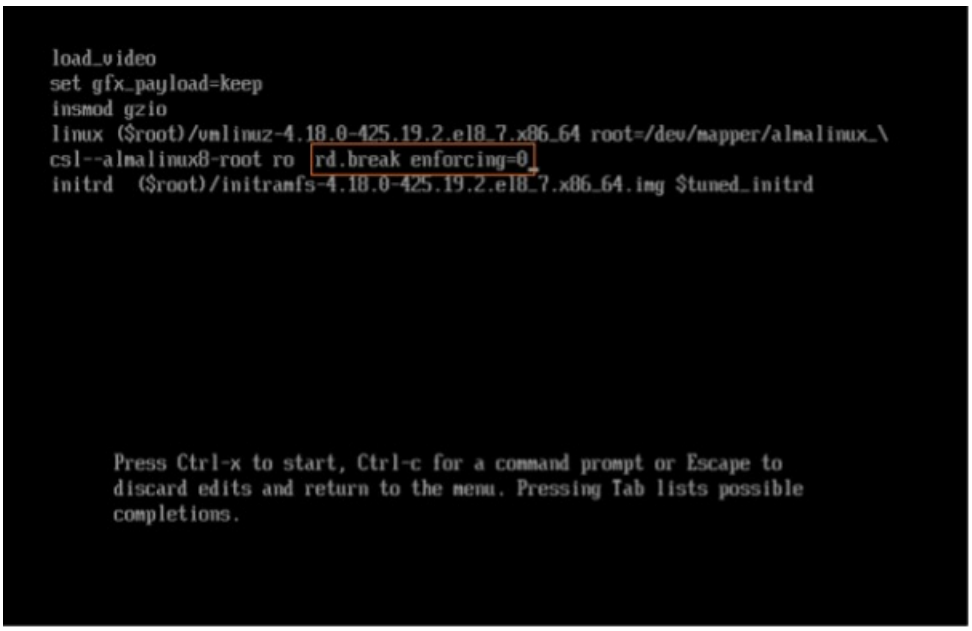


Step 3 Press **e** to edit the configuration.

Step 4 Use the arrow keys to navigate to the line starting with `linux`.

Step 5 At the end of the line, add the following text: **rd.break enforcing=0**.

Figure 32: System Setup Window



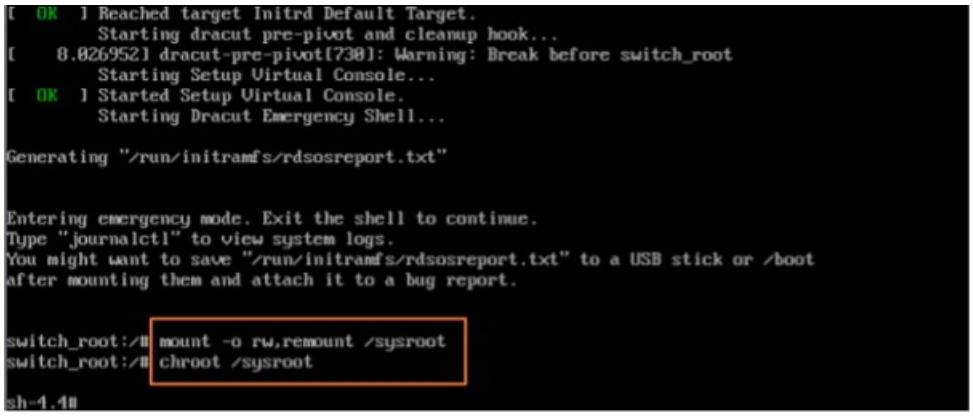
Step 6 Press **Ctrl+x** to exit the configuration and return to shell.

Step 7 Run the following commands:

a. mount -o rw,remount /sysroot

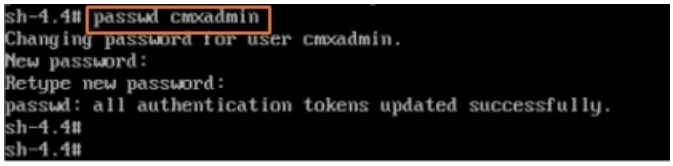
b. chroot /sysroot

Figure 33: Shell Access



Step 8 To change the password for cmxadmin, run the **passwd cmxadmin** command.

Figure 34: Password Change

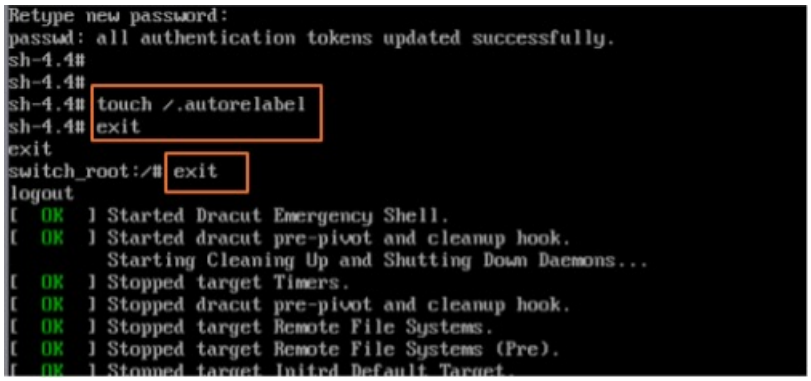


Step 9 To complete the password recovery process, run the **touch /.autorelabel** command.

Step 10 To exit from the shell, run the **exit** command.

Step 11 To reboot, run the **exit** command.

Figure 35: Reboot



The system is rebooted and the Cisco CMX login prompt is displayed.

Step 12 On the Cisco CMX login prompt, log in with cmxadmin user and the new password.

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 208 and Resetting Password - Cisco CMX Release 10.6 and Later with CentOS 7.0, on page 209.

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 External Server Authentication

Cisco CMX supports external AAA server authentication for both GUI and SSH access. Use external AAA authentication servers, such as Radius Server, and AD and allow Cisco CMX to delegate CMX's authentication functionality to the external AAA server. With this, Cisco CMX users can be directly managed, added, and deleted directly in the AAA server.

When the feature is enabled, the local user management for Cisco CMX GUI users is suspended and local GUI users are deleted. When a Cisco CMX user tries to log in to the Cisco CMX GUI, Cisco CMX authenticates the user against the credentials stored in this external AAA server. After the user is authenticated, Cisco CMX provides access to the GUI based on the user's role in Cisco CMX. From end-user perspective, this authentication by the AAA server is transparent and there is no change in the GUI behavior.

When you enable External AAA server authentication for SSH access, Cisco CMX allows only the preconfigured list of AAA server users to log in to the SSH terminal. The local **cmxadmin** user remains active but cannot log in via SSH. The **cmxadmin** user can log in to the console window.

SSH access to Cisco CMX for AAA server users uses 2-factor authentication – user certificate and AAA authentication. The AAA user must provide their own user certificate as a parameter in the SSH command. After Cisco CMX verifies the certificate, it collects and sends the AAA password credentials to the AAA server. Once the AAA server authenticates the credentials, Cisco CMX allows the user to log in to SSH and provides the **cmxadmin** role to the user.

The logged-in user has the same privileges as the **cmxadmin** user on SSH. The logged-in user can perform all activities that the **cmxadmin** user performs.



Note

- You must ensure that the password in the RADIUS credentials does not include any of the following characters: !, @, #, $, %, ^, &, *, () and -. If you include these characters, Cisco CMX will fail authentication, and you will be unable to log in to the Cisco CMX GUI.
- Cisco CMX does not support Terminal Access Controller Access-Control System (TACACS) protocol.

Before you begin

Prerequisites for SSH access (SSH Multi-Factor Authentication – SSH MFA)

You must download these files to the Cisco CMX before you enable SSH access for External Authentication Server users:

1. **CA chain certificate**: Download the certificate of the Authority that signs all user certificates.
2. **User certificates**: Download certificates for users who will receive SSH access. (You must save certificate files in PEM format)
3. **CSV format file**: Create a file that contains the username and certificate filename on each line in the format shown below:

```
<username>,<full_path_of_user_certificate_file>
```

Procedure

Step 1 To configure external RADIUS authentication, run the **cmxctl config authserver** command.

You configure access to the GUI with this command.

Cisco CMX also provides an option to configure SSH access (SSH Multi-Factor Authentication – SSH MFA). If you select this option, Cisco CMX grants SSH access to selected AAA/RADIUS users.

Step 2 Use these subcommads as required:

a) **cmxctl config authserver delete**: Removes the external RADIUS authentication server.
b) **cmxctl config authserver settings**: Sets the external RADIUS authentication server.
c) **cmxctl config authserver show**: Shows the external server configuration.

Configuring Cisco CMX Users in the External Authentication Server

Before enabling this feature, the passwords and roles of the Cisco CMX GUI users should be configured in the external authentication server. A Cisco CMX user's ID and the role should be configured exactly as expected by Cisco CMX in this external authentication server.

Apart from this, a secret shared key should also be configured on the external authentication server. Later,the same shared key should be configured on Cisco CMX.

Configuring an External Authentication Server in Cisco CMX

You can configure an external authentication server using the **cmxctl config authserver settings** command. Provide the server IP address, shared secret key (which is already configured in the external authentication server, as described earlier), the local user name as a **`Last Resort`** user and the password.

If the connection to the external AAA server is lost due to some reason, a user can log in using this **Last Resort** user credentials, in which case, authentication is done by the Cisco CMX server itself. Thus, the system can function properly even if connectivity to the external AAA server is lost.

Next, Cisco CMX provides an option to enable SSH Multi-Factor Authentication (SSH MFA). You provide the required details according to the prerequisites mentioned in Setting Up External Server Authentication. Cisco CMX creates local logins for the given list of users and grants SSH access only to these users. You can add or delete users for SSH access later using additional commands.

The following example shows how to configure an external RADIUS authentication server.

```
[cmxadmin@cmx]# cmxctl config authserver settings
Enter external RADIUS authentication server host : 1.2.3.4
Enter RADIUS server shared secret key : password
Configure local account. This account can be used if RADIUS server is not reachable.
Enter username : cmxadmin
Enter password :
Repeat for confirmation:
Do you want to configure RADIUS Multi-Factor Authentication for SSH? [yes/no] (yes, no):
yes
Enter CA chain certificate file path: user-ca.pem
Enter file with list of MFA user IDs: mfa_users.csv
Checking for CRL Distribution Points
Import Radius CA Certificate successful
0
External RADIUS authentication server configured successfully
RADIUS authentication enabled successfully
User 'cmxuser1' created successfully
User 'cmxuser2' created successfully

=== User Management Summary ===
operation: add
Total users processed: 2
Successful operations: 2
Failed operations: 0

SSH Multi-Factor Authentication users configured successfully
SSH MFA configured successfully
Stopping strongSwan IPsec failed: starter is not running
Starting strongSwan 5.6.2 IPsec [starter]...
Starting connection radius...
Connection radius established successfully External RADIUS authentication server configured
 successfully
```

Configuring an External AAA Server with Cisco CMX

You can authenticate Cisco CMX users to connect with an external AAA server. For every authentication request, the server must sent Access-Accept or Access-Reject response packet depending upon the outcome of the authentication.

An external AAA server must be configured with the following details for AAA server and Cisco CMX to work together to perform external authentication. There are two types of AAA servers: Cisco ISE and freeradius.



Note In Cisco CMX Release 10.6.3, the External Authentication (AAA) feature is enabled without the Federal Information Processing Standard 140-2 (FIPS) or the U.S. Department of Defense Unified Capabilities Approved Products List (UCAPL) mode. Prior to Cisco CMX Release 10.6.3, the External Authentication (AAA) feature was only available with UCAPL mode enabled.

Procedure

Step 1 Access-Accept response must include the following Vendor Specific Attribute (VSA) information with value as appropriate role corresponding to the authenticated user.

a) Provide the **Attribute** value as **`Cisco-AVpair`**. For this VSA, provide **Type** as **`1`**.

b) Enter "shell:cmx-user-role=<ROLE>", wherein values for <ROLE> can be "Admin", "System", "Manage", "Location" and "Read Only".

Note
Value string is case-sensitive.

Step 2 For **freeradius AAA server**, the sample string for role **Admin** in "users" is **`Cisco-AVPair = "shell:cmx-user-role=Admin"`**.

Step 3 For **Cisco ISE**, follow the steps:

a) In section **Policy> Policy Elements> Dictionaries > System> Radius> Radius Vendors** (if not configured already), add Vendor or Vendor specific attribute (VSA).

- **Vendor ID**: Enter the value as **`9 (Cisco Systems)`**.
- **VSA Type/ID**: Enter the value as **`1`**.

b) Add a Network Device Profile and associate correct vendor dictionary that contains VSA.

c) Add Cisco CMX as a Network Device and associate correct Network Device Profile.

d) Create authorization policies that sends Access-Accept packets in response to authentication requests.

- In the response, add Vendor Specific Attribute (Vendor ID=9 for Cisco Systems) named "cisco-avpair" (Type = 1) with a value of "shell:cmx-user-role=<ROLE>". <ROLE> can have the values "Admin", "System", "Manage", "Location" and "Read Only".

Note
Value string is case-sensitive.

e) Create one authorization policy for every role that needs to be supported.

f) Create Policy Set with required authorization policies.

For more information on ISE configuration, see https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215525-use-radius-for-device-administration-wit.html.

Note
Along with UDP port 1812, UDP port 500 must be accessible from Cisco CMX to AAA/ISE when using IPSec.

Displaying External Authentication Server Settings

To display the settings of the currently configured external authentication server, run the **cmxctl config authserver show** command.

```
[cmxadmin@cmx]# cmxctl config authserver show
External RADIUS authentication server host : 1.2.3.4
RADIUS server shared secret key : password
Local user : cmxadmin
```

Deleting External Authentication Server Settings

To delete the currently configured external authentication server settings, run the **cmxctl config authserver delete** command.

When these settings are deleted, CMX reverts to local user management. Standard CMX UI users are re-created locally and their passwords are set to default. If new users were added to External Authentication Server, prior to disabling feature, you will need to configure those users in CMX UI as well.

SSH MFA Access Disablement and AAA User Impact

- When this feature is disabled, SSH MFA access is removed for all configured AAA users.
- All locally created SSH accounts for these AAA users are deleted.
- The user **cmxadmin** retains SSH access.

Note Only the cmxadmin user can disable this feature, and it must be done via the console window.

Since the AAA user accounts need to be deleted, those users are forcefully logged out of SSH, and then the logins are deleted. Therefore, it is necessary to disable this feature from the console window only.

Note If you have this feature enabled and later disable FIPS mode, this feature is also disabled and External Authentication Server details are deleted. Then CMX reverts to local user management as described above.

The following example shows how to delete the configured external authentication server settings.

```
[cmxadmin@cmx]~]#$ cmxctl config authserver delete
External RADIUS authentication server is removed.
```

Manage AAA users for SSH Access

After enabling the feature, you can manage AAA (authentication, authorization, and accounting) users for SSH access using the following commands.

Add AAA users

Use this command to add AAA users:**cmxctl config authserver sshmfa add <users.csv>**

The input file must be in CSV format, identical to the format used when enabling the External Authentication Server.

Each line in the CSV file should follow this format: `<username>,<full_path_of_user_certificate_file>`

Ensure that the corresponding user certificate files in PEM format are present on the Cisco CMX system.



Note

- The user certificate files must be in PEM format and located on the CMX system before adding users.
- This process allows secure SSH access management through AAA user configuration.

```
[cmxadmin@cmx ~]$ cmxctl config authserver sshmfa add mfa_add_users.list

User 'cmxuser2' created successfully

=== User Management Summary ===

operation: add
Total users processed: 1
Successful operations: 1
Failed operations: 0
SSH MFA users added successfully
```

Delete AAA users

To delete AAA users, use this command: **cmxctl config authserver sshmfa delete <users.txt>**

The input file should contain only the usenames in the file in text format, one username per line.

```
[cmxadmin@cmx-160-1111 ~]$ cmxctl config authserver sshmfa delete mfa_delete_users.list
User 'cmxuser2' and home directory deleted successfully
=== User Management Summary ===
operation: delete
Total users processed: 1
Successful operations: 1
Failed operations: 0
SSH MFA users deleted successfully
```

List AAA users

To list the currently configured users for SSH MFA access, run the command.

```
[cmxadmin@cmx ~]$ cmxctl config authserver sshmfa list

MFA enabled users : cmxuser1,cmxuser2
```

Log in to SSH as AAA User

Follow these steps to log in to Cisco CMX SSH terminal as AAA/RADIUS user.

Procedure

Step 1 To combine user certificate and private key, concatenate the user private key file and the signed user certificate file into a single PEM file.

Step 2 Log in to Cisco CMX SSH terminal from a remote linux server.

ssh -i <user-key-certfile_fullpath> <aaa_user>@<cmx_ip_address>

```
[user@remote-server]# ssh -i aaauser1.key-cert.pem aaauser1@10.10.10.1

(aaauser1@cmx) Password:

[aaauser1@cmx ~]$
```

Setting Up Audit Logging

You can enable remote logging of system events, and specify which syslog events you want to log, send to a remote server and view locally on Cisco CMX.

With Cisco CMX Release 11.1.1, support is available for configuring a maximum of two servers using either TLS or IPSEC.

Procedure

Step 1 Connect to CMX via SSH, or through the console if FIPS or UCAPL is enabled.

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
*** CMX Audit Log Settings (Maximum 2 syslog servers supported) ***	View text message as configuring Maximum 2 Syslog Servers.
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.

Prompt	Action
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 Cisco CMX to log. Yes logs all events. No prompts you to select the event types you want to log, and confirms the update.

```
Please select the events to be logged All Events [yes/no] (yes, no) [yes]:
Please select the modules to be logged All Modules [yes/no] (yes, no) [yes]: Audit Log Level
 (1, 2, 3) [1]:
Remote Audit Logging = Enabled Found 1 rsyslog servers Deleting connection: rsyslog_server1

Starting rsyslog service
Settings saved
```

Note
In Cisco CMX, audit logging is not enabled for user-related activities such as modifying a user and monitoring the user modification activities. Audit logging is not available for the **Settings** option and associated actions such as filtering probing clients or tracking parameters.

CMX then restarts the affected loggers.

Example

This example shows how to log all events using 2 syslog servers.

```
[cmxadmin@cmx]#  $ cmxctl config audit settings
 *** CMX Audit Log Settings (Maximum 2 syslog servers supported) ***
Enable or Disable Remote Syslogging [Enable / Disable] (Enable, Disable) [Enable]:
If logs size goes beyond 1gb, drop or overwrite messages? [drop / overwrite] (drop, overwrite)
 [overwrite]:
Protocol for rsyslog connection [TLS / IPSEC] (TLS, IPSEC) [TLS]:
--- Configuring Rsyslog Server 1 ---
Please enter rsyslog IP: 10.20.2.3
Please enter rsyslog port [514]: 4514
Enter CA cert file for Remote syslog server: rsyslog1.crt
Please enter rsyslog server's Common Name(CN) or Subject Alternate Name(SAN): rsyslog1
Do you want to add another rsyslog server? [y/N]: y
--- Configuring Rsyslog Server 2 ---
Please enter rsyslog IP: 10.30.4.5
Please enter rsyslog port [514]: 4514
Enter CA cert file for Remote syslog server: rsyslog2.crt
Please enter rsyslog server's Common Name(CN) or Subject Alternate Name(SAN): rsyslog2
```

```
Maximum limit of 2 syslog servers reached.
Please enter the email IDs (comma separated) for mail alerts: user@domain.com
Configured 2 rsyslog server(s) for TLS forwarding
Processing certificate 1/2: /home/cmxadmin/rsys;pog1.crt
Checking for CRL Distribution Points
Import Rsyslog CA Certificate successful to rsyslogca1.crt
Certificate 1 imported successfully as rsyslogca1.crt
Processing certificate 2/2: /home/cmxadmin/rsyslog1.crt
Checking for CRL Distribution Points

Import Rsyslog CA Certificate successful to rsyslogca2.crt
Certificate 2 imported successfully as rsyslogca2.crt
Successfully imported 2 certificates:
• Combined file: rsyslogca.crt (for TLS)
• Individual files: rsyslogca1.crt, rsyslogca2.crt, ... rsyslogca2.crt (for IPSec)
Please select the events to be logged All Events [yes/no] (yes, no) [yes]:
Please select the modules to be logged All Modules [yes/no] (yes, no) [yes]: Audit Log Level
 (1, 2, 3) [1]:
Remote Audit Logging = Enabled Found 2 rsyslog servers Deleting connection: rsyslog_server1
 Deleting connection: rsyslog_server2
Starting rsyslog service
```

What to do next

Viewing Audit Logs

You can now filter audit logs not only by event types but also by specific modules. This enhancement allows more precise log viewing based on modules.

To view audit logs, use the following command:

```
[cmxadmin@cmx-1110-193 ~]$ cmxctl config audit view
Show all logs [yes/no] (yes, no) [yes]: no
Enter day [today(1)/yesterday(2)/last week(3)/last month(4)/all(5)] (1, 2, 3, 4, 5) [5]: 1
Enter event type [MGMT_EVENT(1)/CONN_EVENT(2)/AUTH_EVENT(3)/CONF_EVENT(4)/ALL(5)] (1, 2,
3, 4, 5) [5]: 1
Enter identity [root(1)/admin(2)/all(3)] (1, 2, 3) [3]:
Enter status [SUCCESS(1)/FAILURE(2)/ALL(3)] (1, 2, 3) [3]:
Enter module
[CMXAGENT(1)/CMXOS(2)/Analytics(3)/Config(4)/Hyperlocation(5)/Location(6)/NMSPLB(7)/MALTAB(8)
/HA(9)/Certs(10)/Common(11)/ALL(12)] (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12) [12]:
```

Viewing Audit Status

To check the current audit logging status and configured remote syslog servers, use the following command:

```
[cmxadmin@cmx-1110-193 ~]$ cmxctl config audit status

Remote Audit Logging = Enabled
Configured Servers (2):
Remote Syslog Server 1:
  Server IP: 10.20.2.3
  Server Port: 4514
Remote Syslog Server 2:
  Server IP: 10.30.4.5
  Server Port: 4514
```

This output confirms that remote audit logging is enabled and lists the configured remote syslog servers.

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 218.

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

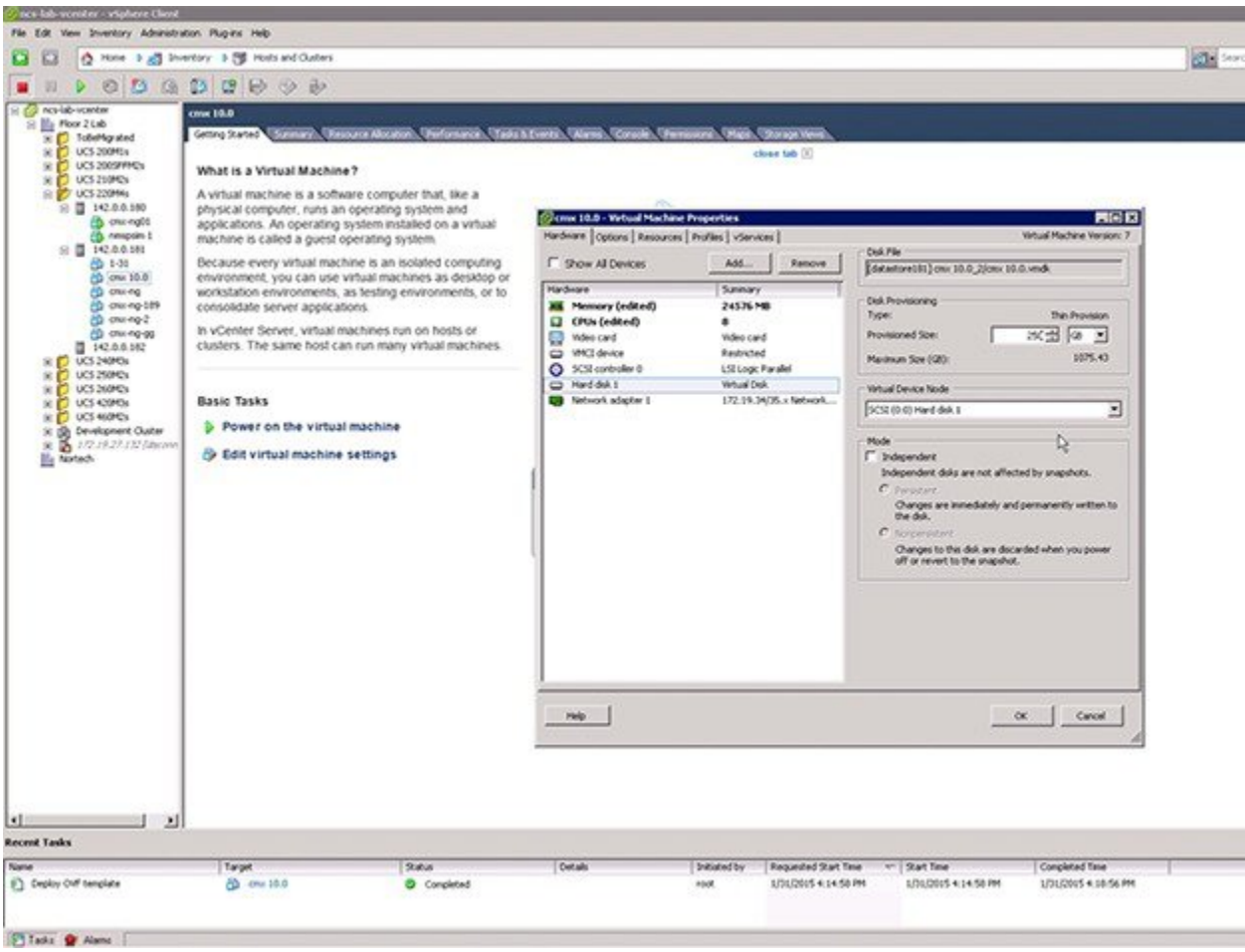
Step 2 Shutdown the virtual machine by entering the following command:

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 36: 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 10.6* 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 10.6* 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.

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, 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.
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, or through the console if FIPS or UCAPL is enabled.

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."

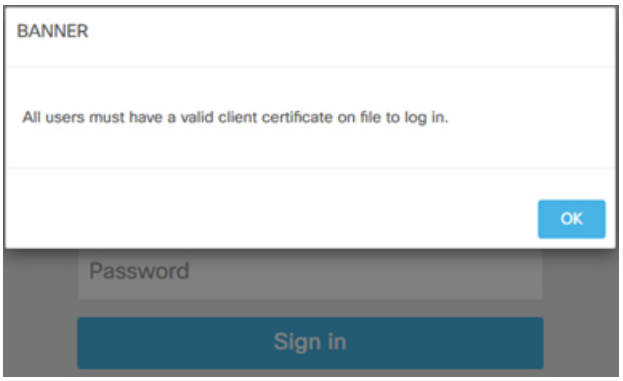
```
Current Login Banner = []
```

```
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 37: 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 with Chronyd Service, verify if the settings are configured at `/etc/chrony.conf`.

```
[cmxadmin@cmx]#  cat /etc/chrony.conf
#servers to synchronize from
server ntp.server.example.com iburst
allow 192.0.1.1/24
```

```
makestep 1.0 3
keyfile /etc/chrony.keys
leapsectz right/UTC
logdir /var/log/chrony
```

Step 2 To find unused **key ID** from `/etc/chrony.keys`, run the **grep -v '#' |grep -v "$"**

```
[cmxadmin@cmx]# cat /etc/chrony.keys | grep -v '#' |grep -v "$"
1 SHA256 HEX: C4ECA8710F9E93C54EE6388BBC05D8D9FD71CAC111688C1260CB64C60C708882
5 SHA256 HEX: DAE5F1D3C746988ABABCBF0A9FB53D0A6D004DF827814884F4CD2049156494A6
```

In the above example, 1 and 5 are already in use.

Step 3 Select any unused **key ID**. For example, 21.

Step 4 Generate the key using the selected number (for example, 21) and hash algorithm of SHA256 or SHA384 or SHA512.

Step 5 Save the same in the location `/etc/chrony.keys` file.

```
[cmxadmin@cmx]# chronyc keygen 21 SHA256 256 | tee -a /etc/chrony.keys
21 SHA256 HEX: 0E50E2818864DA450CEC234A332B9169A24EA7CF3B8D179E542805F1E1AC8EFB
```

Step 6 From the command output, copy or export the the ENCRYPTED PRIVATE KEY block, for example **21 SHA256 HEX: 0E50E2818864DA450CEC234A332B9169A24EA7CF3B8D179E542805F1E1AC8EFB**.

Step 7 To restart the chronyd services, run the **systemctl restart chronyd** command.

Step 8 SCP the file to Cisco CMX server.

Step 9 Connect to CMX command line either from a console, or from a VMWare vSphere console.

Step 10 To delete all the NTP configurations, run the **cmxos ntp clear** command.

Step 11 To configure authenticated NTP server:

a. Run the **cmxos ntp type** command.

b. Enter the hostname or IP addresses of the NTP server.

c. Enter the server key.

```
[cmxadmin@cmx]# cmxos ntp type
Current NTP Type = <Not Set>
Select NTP Type [1] Unauthenticated, [2] Authenticated or [3] Skip (1, 2, 3) [3]:2

Changing the NTP Type Authenticated

Enter hostname / IP for NTP Server #1 (blank to skip) (): 192.0.2.1
Please ensure Server Key has Hashing algo either SHA256, SHA384 or SHA512 only
Please enter the Server Key (Correct Key Format sample -> 1 SHA256
HEX:E78EE456FF9AD89279411E51071AE86CE1DE4016): 21 SHA
256 HEX: 0E50E2818864DA450CEC234A33289169A24EA7CF3B8D179E542865F1E1AC8EFB
Checking 1+ server 192.0.2.1 15 reachable
OK
Key file successfully replaced and permissions set.
NTP Server added successfully

Chrony Service restarted successfully
```

Step 12 Repeat step 11 to add the second NTP server.

Note that you need to wait for a few minutes for the NTP servers to sysnchronize.

Step 13 (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
Server  = 192.0.1.2
Status  = Synchronized
Key  = 1 SHA256 HEX:E78EE456FF9AD89279411E51071AE86CE1DE4D16
```

```
[cmxadmin@cmx]# cmxos ntp status --verbose
NTP Type = Authenticated
Server  = 192.0.1.2
Status  = Synchronized
Key  = 1 SHA256 HEX:E78EE456FF9AD89279411E51071AE86CE1DE4D16

  .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
 / .- Source state '*' = current best, '+' = combined, '-' = not combined,
| /             'x' = may be in error, '~' = too variable, '?' = unusable.
||                                                 .- xxxx [ yyyy ] +/- zzzz
||      Reachability register (octal) -.           |  xxxx = adjusted offset,
||      Log2(Polling interval) --.      |          |  yyyy = measured offset,
||                                \     |          |  zzzz = estimated error.
||                                 |    |           \
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* 10.22.244.168                 2   6   377    63    -24us[  -32us] +/-  722us

Remote address  : 192.0.1.2 (0A16F4A8)
Remote port     : 123
Local address   : 192.0.1.3 (0A16F4A4)
Leap status     : Normal
Version         : 3
Mode            : Server
Stratum         : 2
Poll interval   : 6 (64 seconds)
Precision       : -24 (0.000000060 seconds)
Root delay      : 0.000763 seconds
Root dispersion : 0.000183 seconds
Reference ID    : AB442642 ()
Reference time  : Fri Oct 18 07:43:39 2024
Offset          : +0.000032190 seconds
Peer delay      : 0.000315516 seconds
Peer dispersion : 0.000000089 seconds
Response time   : 0.000204549 seconds
Jitter asymmetry: +0.00
NTP tests       : 111 111 1111
Interleaved     : No
Authenticated   : Yes
TX timestamping : Kernel
RX timestamping : Kernel
Total TX        : 14
Total RX        : 14
Total valid RX  : 14
Total good RX   : 14
Name/IP address             Mode KeyID Type KLen Last Atmp  NAK Cook CLen
==============================================================================
192.0.1.2                SK     1    3  160    -    0    0    0    0
```

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

Cisco CMX supports up to two unauthenticated NTP Servers.

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 address of the first NTP server.

Step 4 To configure another NTP server, select 'y' and provide IP address of the second NTP server.

Step 5 (Optional) To verify the status of the NTP server configuration, run the **cmxos ntp status** command.

```
cmxadmin@cmx ~]$ cmxos ntp type
Current NTP Type = <Not Set>
Select NTP Type [1] Unauthenticated, [2] Authenticated or [3] Skip (1, 2, 3) [3]: 1
Changing the NTP Type = Unauthenticated
Please enter the NTP server name (blank for no NTP server) []: ntp1.domain.com
Setting ntp server ntp1.domain.com
Do you want to add another NTP server? [y/n] (y, n): y
Please enter NTP server 2 (blank to stop adding servers) []: ntp2.domain.com
Setting ntp server ntp2.domain.com

Status of Unauthenticated NTP Servers can be checked by running following command.

[cmxadmin@cmx ~]$ cmxos ntp status
NTP Type = Unauthenticated
Server 1 = 10.10.11.12, Status  = Synchronized
Server 2 = 10.10.20.20, Status  = Synchronized
```

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
```

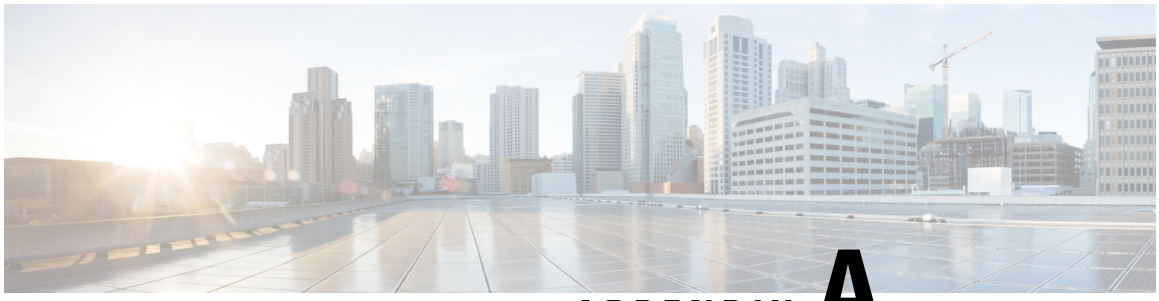
Note
If you need to restart NTP service, run the **cmxos ntp restart** command. It will restart NTP daemon. Run **cmxos ntp status** command to check the NTP status. You can add **--verbose** option to the command if you want detailed output.

```
[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.



APPENDIX A

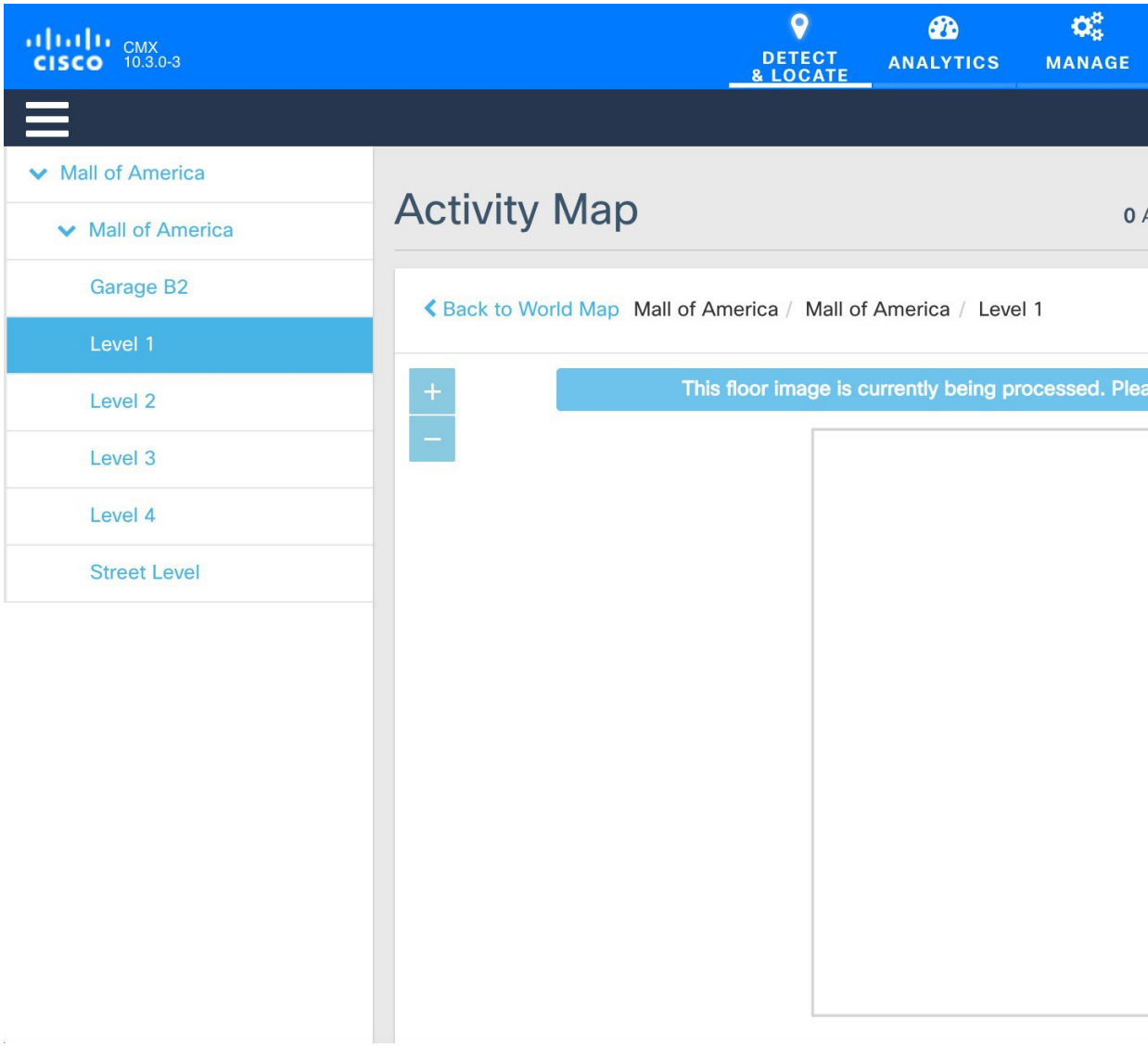
Guidelines for Managing Maps in Cisco CMX

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 Catalyst Center. For more information, see Importing Maps from Catalyst 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 to view the image'.

Guidelines for Managing Maps in Cisco CMX

Figure 38: Activity Map

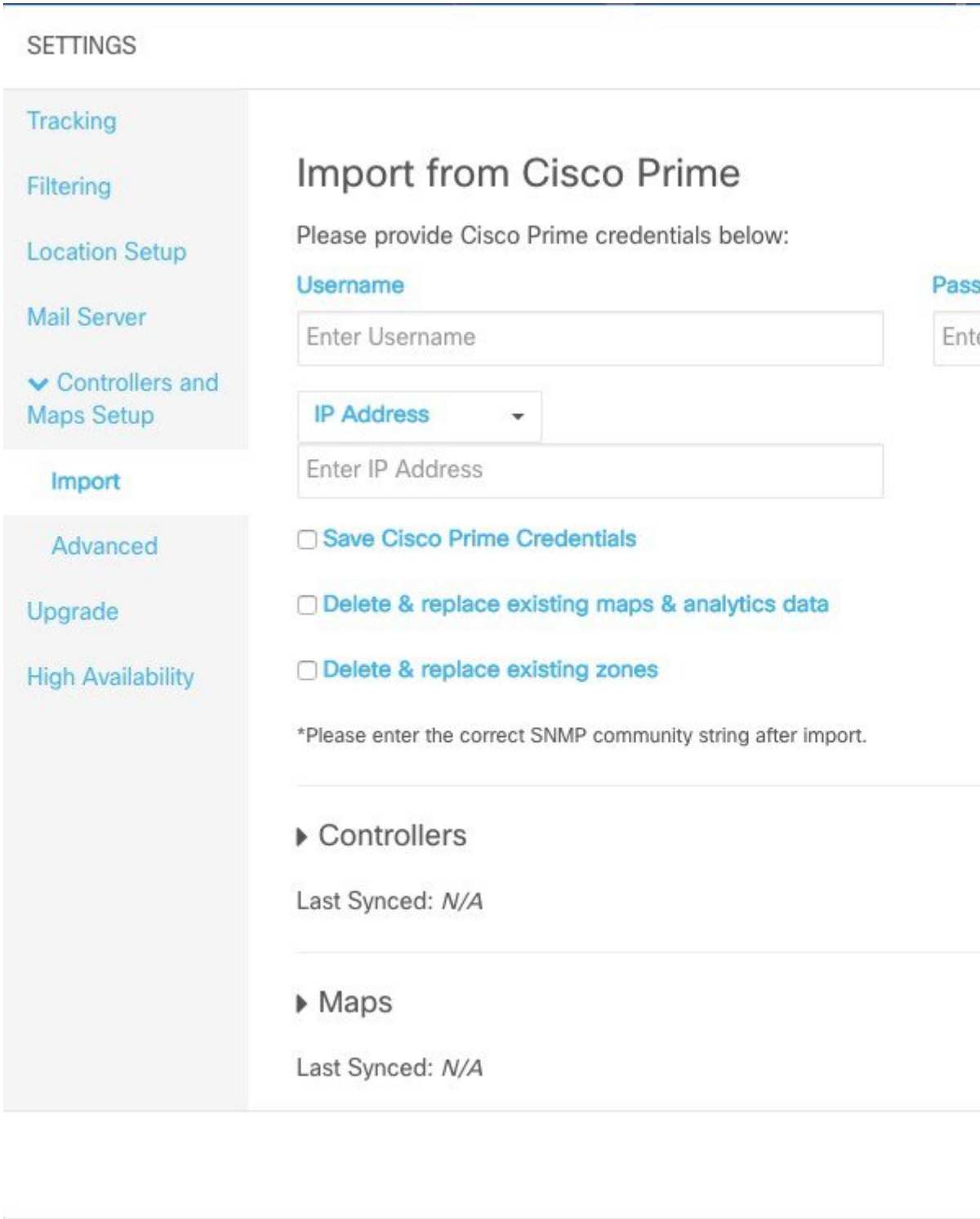


- Create and update the zones using Cisco CMX GUI map editor. All other map edit operations are to be performed using Prime Infrastructure.
- An AP can only be associated with a single floor map in Prime. If you are planning to move APs from one floor to another, you want to disassociate them from existing 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'

Guidelines for Managing Maps in Cisco CMX

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.

Figure 39: Impor from Cisco Prime



• Create a Map Using Cisco Prime Infrastructure, on page 234
• Delete a Map Using Cisco Prime Infrastructure, on page 234
• Move an Access Point Between Maps Using Cisco Prime Infrastructure, on page 235
• Export a Map Using Cisco Prime Infrastructure, on page 239
• Import New and Modified Maps to Cisco CMX, on page 240

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

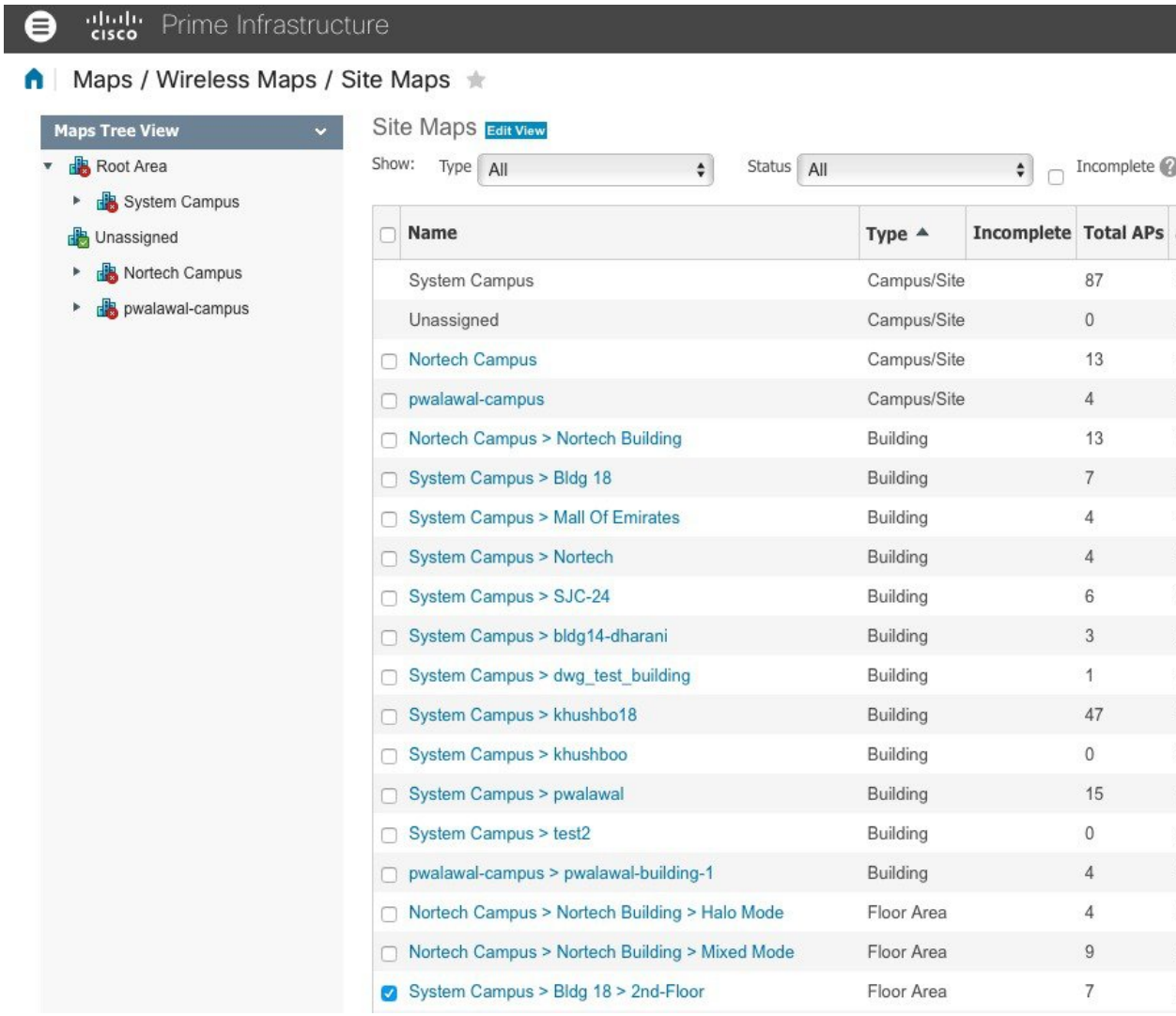
Step 1 Log in to Cisco Prime Infrastructure.

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**.

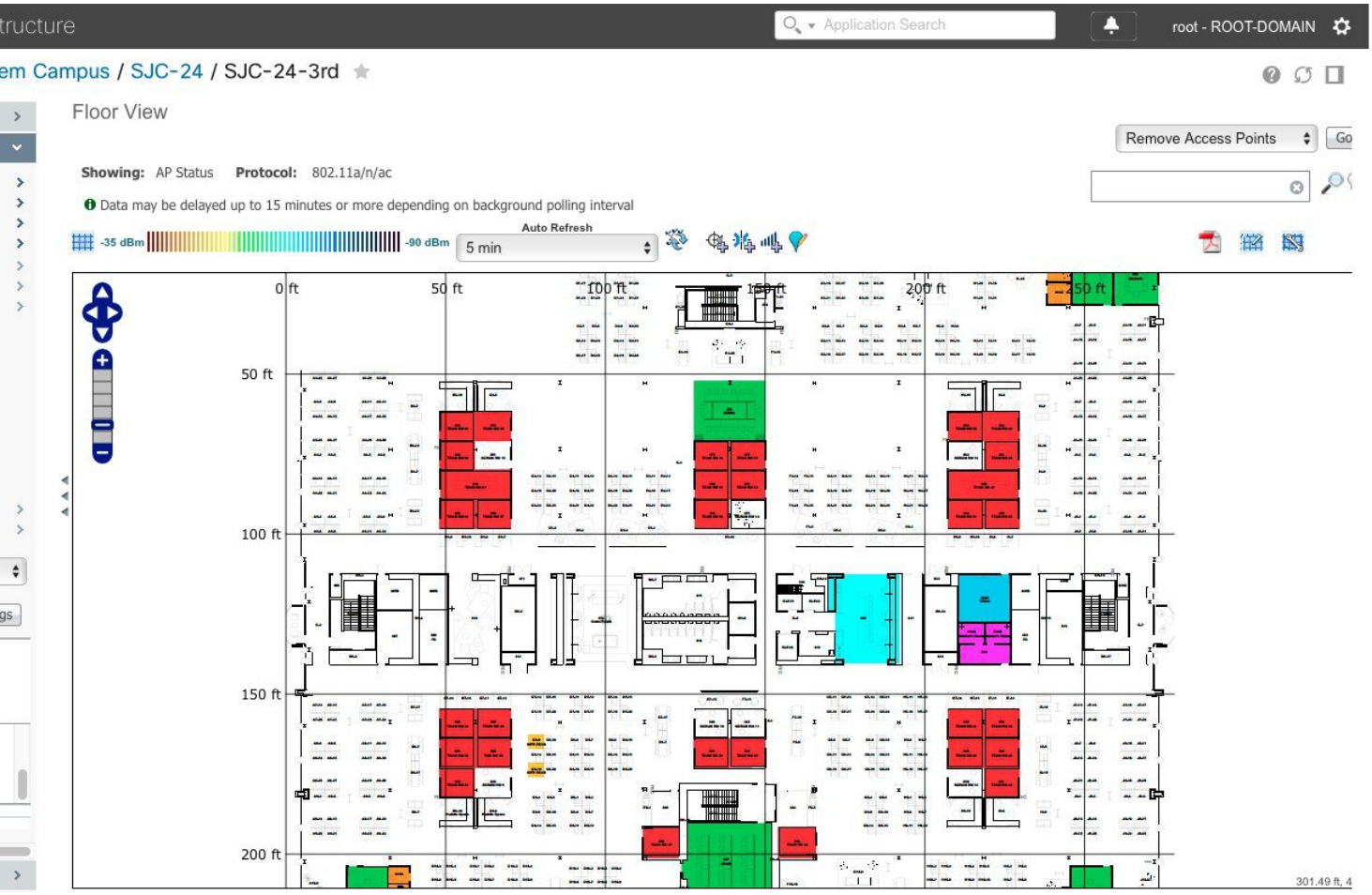
Step 4 From the **Select a command** drop-down list, choose **Floor Area**.

Guidelines for Managing Maps in Cisco CMX

Step 5 Click **Go**.

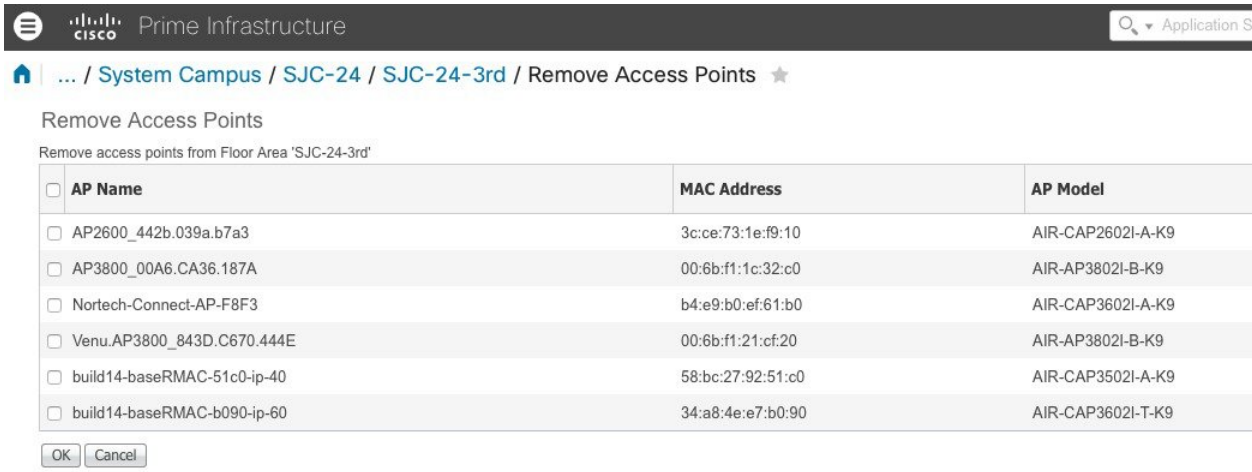
Step 6 Click on the floor Area from which you want to release the AP. The **Floor View** window is displayed.

Step 7 From the **Select a command** drop-down list, choose **Remove Access**



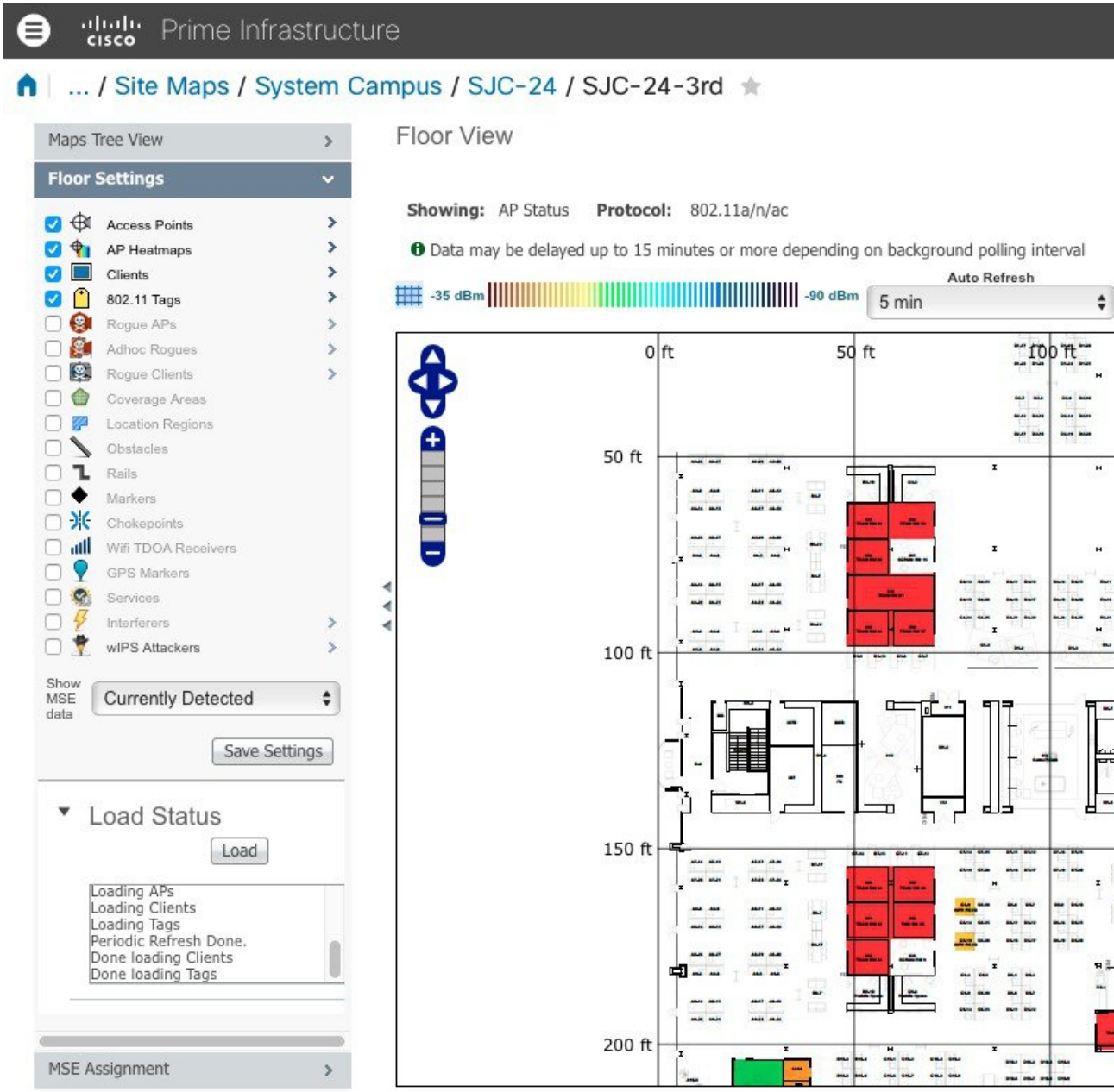
385468

Step 8 Select the AP to be deleted and click **OK**.

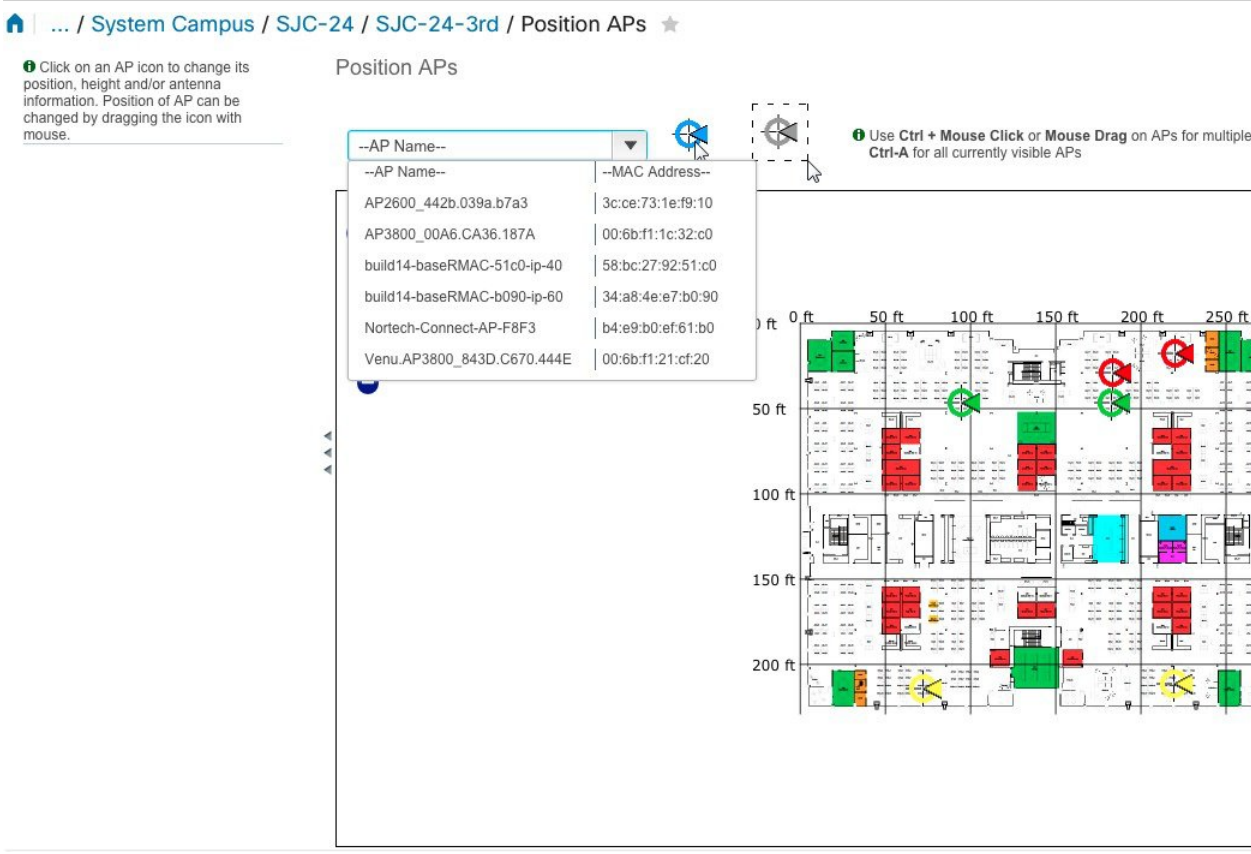


Guidelines for Managing Maps in Cisco CMX

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

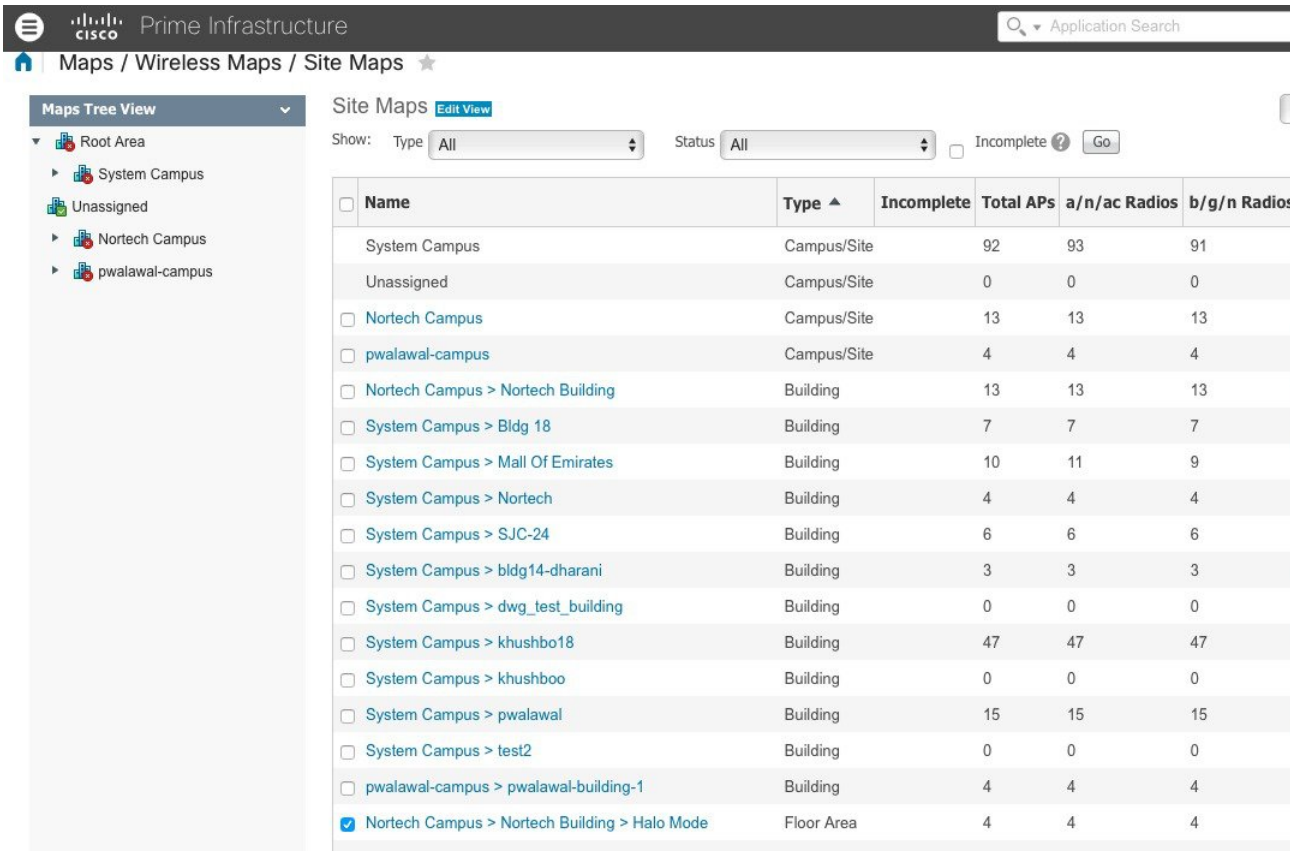
Step 1 Log in to Cisco Prime Infrastructure.

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 .

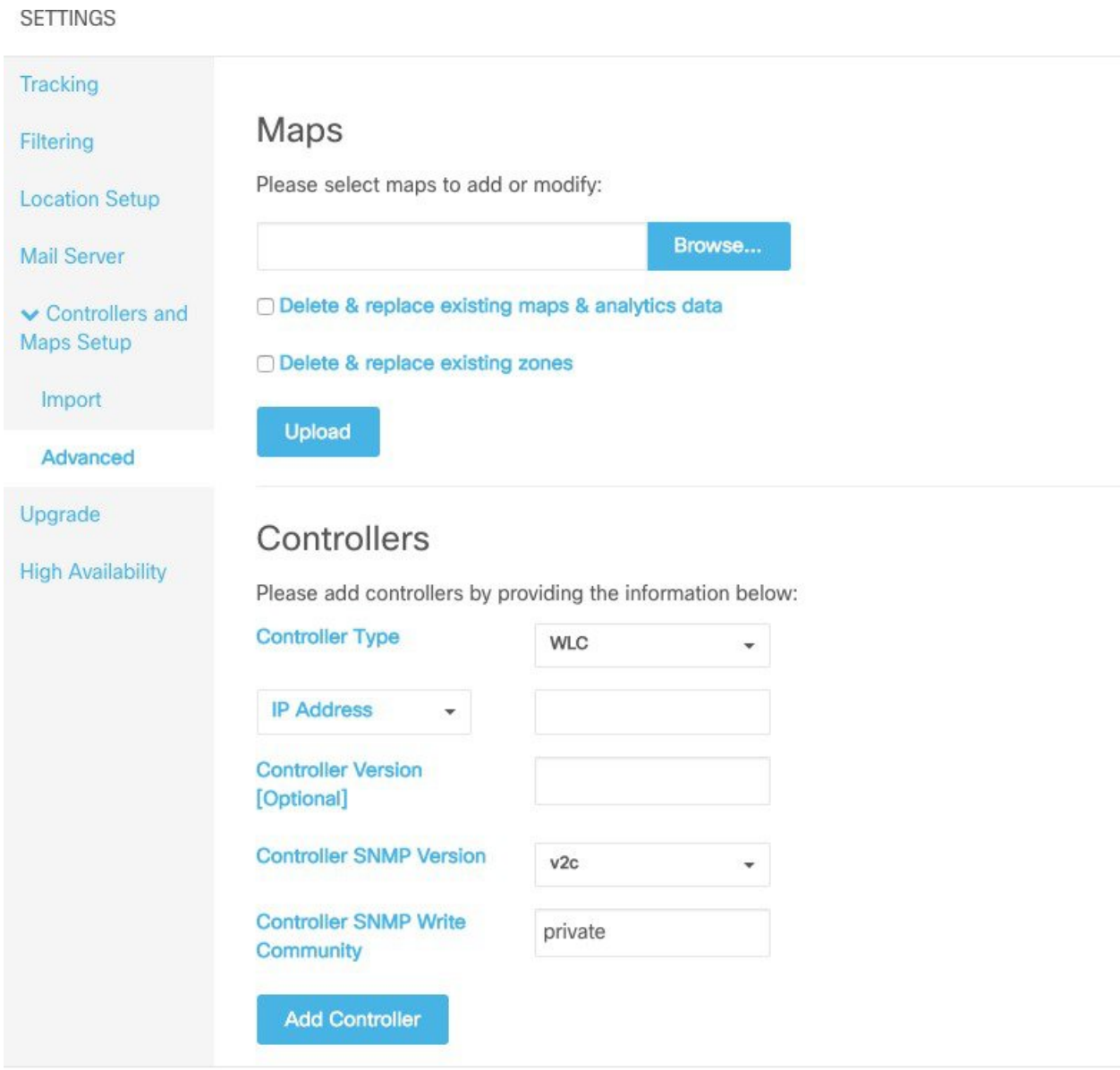


Step 6 Click **Go**.

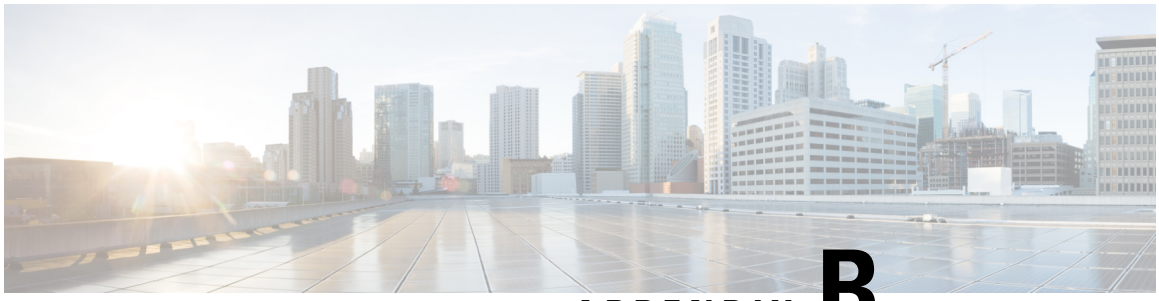
Import New and Modified Maps to Cisco CMX

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



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 106.

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?

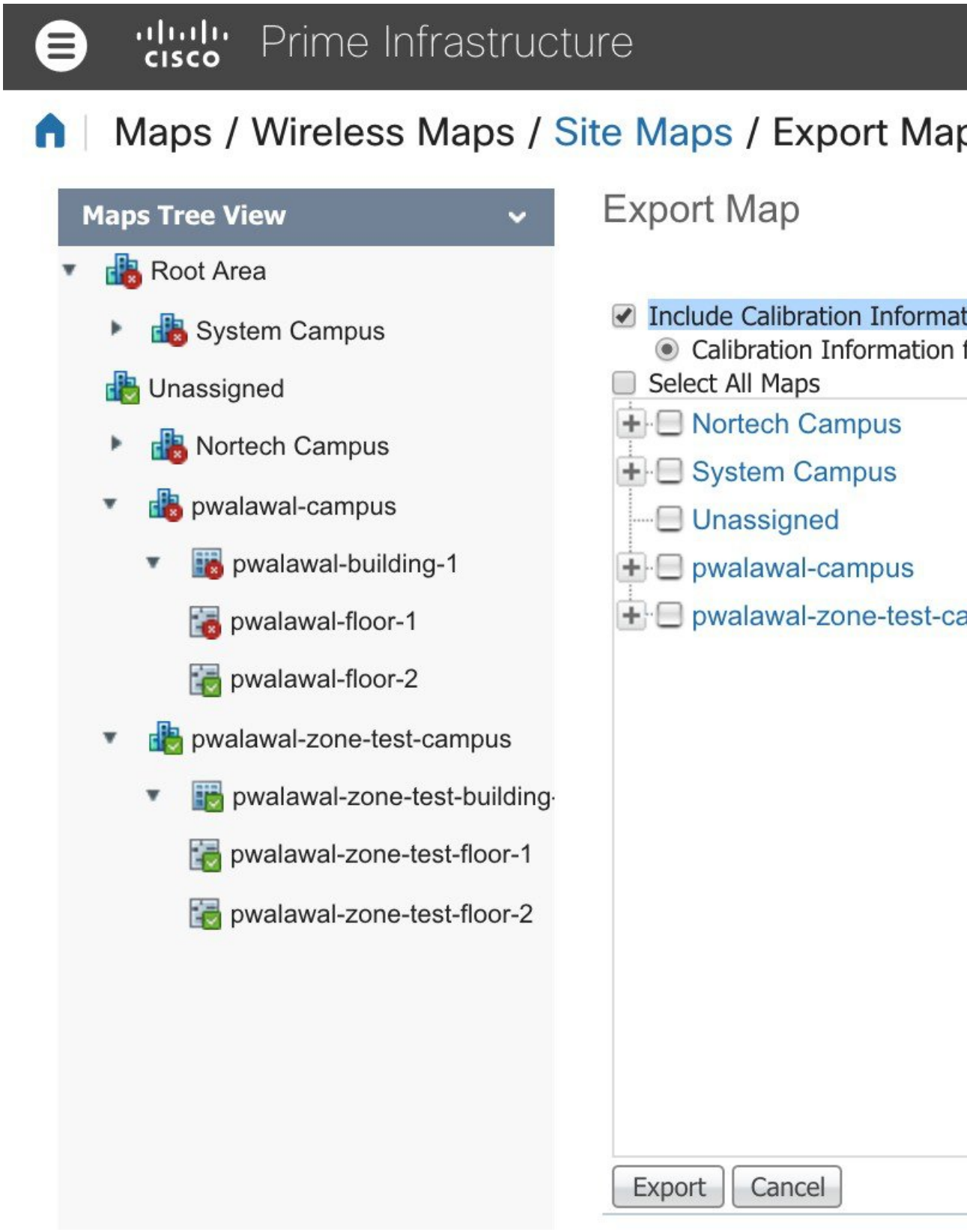
While exporting maps from Prime Infrastructure, Calibration model information was not included in the exported map file.

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 | -604xxxxxxxxxxxxxx | 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.

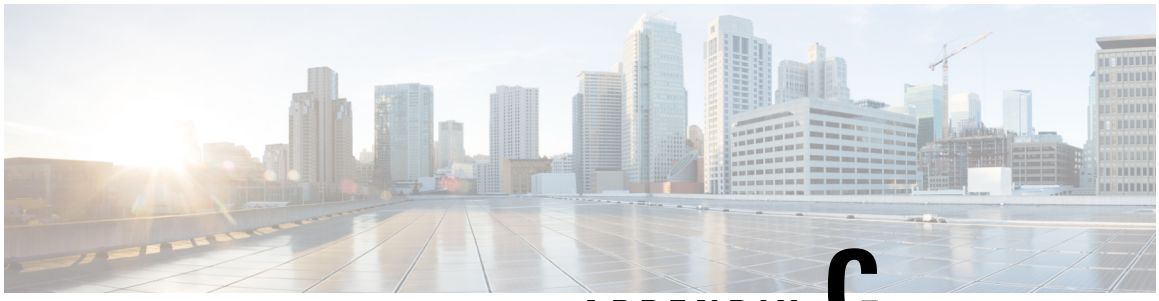
```
[cmxadmin@cmx-prod opt]# cmxctl config maps floors
+-------------------------------------------+---------------------+--------------------+

| 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.

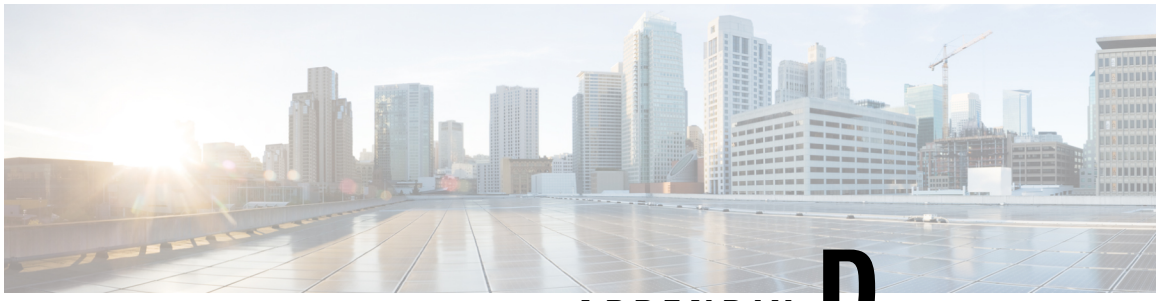
Monit Email	Customer Action
Socket 5432 is not responding	Run the **cmxctl database stop** and **cmxctl database start** command.
Socket 5432 is responding	No action required.
Swap usage is above 80%	Increase swap space or reduce memory usage.
Swap usage recovered	No action required.
SYS CPU usage is 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 13: 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 14: 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 15: Cassandra Database

Cassandra Database	Protocol
7000	TCP
7001	TCP
9042	SSL Communication

Table 16: 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 Spaces	In/Out	HTTPS	443
Cisco CMX	Catalyst Center	In/Out	SSH/HTTPS	22/443
Cisco CMX	Cisco Prime Infrastructure	In	HTTPS	443

Table 17: Cisco CMX Gateway Reachability Port Requirement

Ports	Description
6378, 6379, 6380, 6381, 6382, 6383, 6385, 16378, 16379, 16380, 16381, 16382, 16383, 16385	Redis
7000, 7001, 9042	Cassandra database
5432	Postgres database

Ports	Description
4242	High Availability REST and Web Service
22	SSH port and to synchronize files between servers

Note Additionally, ensure that the Virtual Router Redundancy Protocol (VRRP) and Internet Control Message Protocol (ICMP) are allowed between the two Cisco CMX servers and the gateway is reachable to establish Cisco CMX reachability using ICMP.

Cisco CMX Network Protocols and Port Matrix



INDEX

B

backup, automatic UCAPL 197

C

certificates, validate client 196
certificates, viewing 190
CSR, creating; certificate signing request 188

E

encryption 223
Encryption key, options 188

F

FIPS or UCAPL mode, suggested deployment 187
FIPS, enable and manage 193

U

UCAPL, enable and manage 195