



Cisco CMX Commands

- [Using the Command-Line Interface, on page 4](#)
- [cassandraexport, on page 5](#)
- [cmxctl checkdb , on page 6](#)
- [cmxctl checklogs , on page 7](#)
- [cmxctl config analytics, on page 8](#)
- [cmxctl config aps delete, on page 11](#)
- [cmxctl config audit, on page 12](#)
- [cmxctl config auth, on page 17](#)
- [cmxctl config authinfo get, on page 22](#)
- [cmxctl config authserver, on page 23](#)
- [cmxctl config authserver sshmfa, on page 25](#)
- [cmxctl config banner, on page 27](#)
- [cmxctl config certs, on page 28](#)
- [cmxctl config controllers , on page 35](#)
- [cmxctl config data, on page 37](#)
- [cmxctl config devicelimitalert, on page 38](#)
- [cmxctl config featureflags, on page 39](#)
- [cmxctl config fips, on page 41](#)
- [cmxctl config fips ipsecauth, on page 43](#)
- [cmxctl config fips ucaplmode, on page 44](#)
- [cmxctl config fips ucaplmode autobackup, on page 46](#)
- [cmxctl config fips ucaplmode logFileAccess, on page 47](#)
- [cmxctl config fips ucaplmode logHTTPHeader, on page 48](#)
- [cmxctl config gateway, on page 49](#)
- [cmxctl config get, on page 50](#)
- [cmxctl config heatmaps summary, on page 52](#)
- [cmxctl config hyperlocation mixmode, on page 53](#)
- [cmxctl config import , on page 55](#)
- [cmxctl config ipsec, on page 56](#)
- [cmxctl config loginrate, on page 58](#)
- [cmxctl config manageacl, on page 59](#)
- [cmxctl config maps address, on page 60](#)
- [cmxctl config maps alist, on page 61](#)

- `cmxctl config maps buildings`, on page 63
- `cmxctl config maps campuses`, on page 64
- `cmxctl config maps delete`, on page 65
- `cmxctl config maps floors`, on page 66
- `cmxctl config maps import`, on page 67
- `cmxctl config maps reprocessimage`, on page 69
- `cmxctl config maps zones`, on page 70
- `cmxctl config qlesspyworker`, on page 71
- `cmxctl config reload`, on page 72
- `cmxctl config rfid timeout`, on page 73
- `cmxctl config set`, on page 74
- `cmxctl config smartlicense enable`, on page 76
- `cmxctl config smartlicense register`, on page 77
- `cmxctl config smartlicense status`, on page 78
- `cmxctl config smartlicense renewauthorization`, on page 79
- `cmxctl config smartlicense renewregistration`, on page 80
- `cmxctl config smartlicense reregister`, on page 81
- `cmxctl config smartlicense deregister`, on page 82
- `cmxctl config smartlicense secondaryudi`, on page 83
- `cmxctl config tls`, on page 84
- `cmxctl config uptimethreshold`, on page 85
- `cmxctl config verify`, on page 86
- `cmxctl debug`, on page 88
- `cmxctl disable`, on page 89
- `cmxctl dump`, on page 91
- `cmxctl enable`, on page 92
- `cmxctl heterarchy`, on page 94
- `cmxctl influxdb wipe`, on page 95
- `cmxctl jobs`, on page 96
- `cmxctl metrics notification`, on page 97
- `cmxctl restart`, on page 98
- `cmxctl stack`, on page 100
- `cmxctl start`, on page 101
- `cmxctl status`, on page 103
- `cmxctl stop`, on page 106
- `cmxctl trace mac`, on page 108
- `cmxctl trace status`, on page 109
- `cmxctl trace update`, on page 110
- `cmxctl users`, on page 111
- `cmxctl users unlock`, on page 112
- `cmxctl version`, on page 113
- `cmxloc delete`, on page 114
- `cmxloc download`, on page 115
- `cmxloc find`, on page 116
- `cmxloc list`, on page 117
- `cmxloc monitor`, on page 118

- `cmxloc start`, on page 119
- `cmxos addswap` , on page 120
- `cmxos adminui`, on page 121
- `cmxos apiserver disable`, on page 122
- `cmxos apiserver enable`, on page 123
- `cmxos apiserver reset`, on page 124
- `cmxos apiserver restart`, on page 125
- `cmxos apiserver start`, on page 126
- `cmxos apiserver status`, on page 127
- `cmxos apiserver stop`, on page 128
- `cmxos apiserver user`, on page 129
- `cmxos backup` , on page 130
- `cmxos backupsched`, on page 131
- `cmxos benchmark disk` , on page 132
- `cmxos changedate`, on page 133
- `cmxos checkpostgresdatasize` , on page 134
- `cmxos clean` , on page 135
- `cmxos configure` , on page 137
- `cmxos date`, on page 138
- `cmxos encryptdisk`, on page 139
- `cmxos etchosts`, on page 141
- `cmxos firstboot` , on page 142
- `cmxos fixhaproxy` , on page 143
- `cmxos health`, on page 144
- `cmxos inventory` , on page 145
- `cmxos kill`, on page 146
- `cmxos monit`, on page 147
- `cmxos ntp`, on page 148
- `cmxos openports` , on page 149
- `cmxos patch`, on page 150
- `cmxos reboot`, on page 151
- `cmxos reconfigure` , on page 152
- `cmxos rediscleanup`, on page 155
- `cmxos restore` , on page 156
- `cmxos shutdown`, on page 158
- `cmxos smartlicenseudi`, on page 159
- `cmxos sslcert` , on page 160
- `cmxos sysproxy`, on page 161
- `cmxos techsupport` , on page 163
- `cmxos techsupport dump` , on page 164
- `cmxos upgrade` , on page 165
- `cmxos vacuumdb`, on page 167
- `cmxos verify` , on page 168
- `cmxos wipeoutdisk`, on page 169

Using the Command-Line Interface

Starting from Cisco CMX 10.3.1, you can use the **Tab** key to auto complete any Cisco CMX command on the command line interface. If you enter **cmxos** and then click the **Tab** key, the CLI displays the available keywords. If you enter a partial string and then click the **Tab** key, the CLI then displays the complete string.

Cisco CMX CLI does not support **read-only** user accounts. It supports only **cmxadmin** and **root user** accounts.

cassandraexport

To export Cisco CMX history data from Cassandra to a CSV file, use the **cassandraexport** command.

```
cassandraexport [--date <yyyy/mm/dd>] [--table <tablename> | --file <filename> | --sql <sql statement> | --rowperfetch <rows per fetch>]
```

Syntax Description		
--date <yyyy/mm/dd>		Date on which the export is to be performed. This is required.
--table <table name>		(Optional) Name of the table to export.
--file <filename>		(Optional) Name of the CSV file. The default is /tmp/CassandraExport_sql.csv.
--sql <sql statement>		This option is not currently supported.
--rowperfetch <rows per fetch>		(Optional) The default is 1000 rows.

Command Default None.

Command Modes CMX root user

Command History	Release	Modification
	Cisco CMX Release 10.3.0	This command was introduced.

Usage Guidelines This command extracts a maximum of only one day of data, starting from midnight of the date given to the time when the command is issued.

You can use these methods to export Cisco CMX data from Cassandra:

- The method that we most recommend is through the Notifications feature (**Manage > Notifications > New Notification**). For more information, see the “Managing Notifications from Applications” section in the *Cisco Connected Mobile Experiences Configuration Guide* for this release at: <http://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/products-installation-and-configuration-guides-list.html>
- An alternative method is to use the **cassandraexport** command, and to export daily. We recommend that you schedule the export during a quiet period of the day, for example 2:00 A.M. If you use this method during a time when the system is continuously changing, a timeout can occur.
- Use the Cisco CMX History API only if your export does not exceed 2000 records, for example 100 floors.

Example

The following example shows how to export Cisco CMX data from Cassandra to a CSV file:

```
[cmxadmin@server]# /opt/cmx/bin/cassandraexport --date 2017/06/14
```

```
Data exported into the file /tmp/CassandraExport_201706150220-02.csv
```

cmxctl checkdb

To check the database for schema integrity, use the **cmxctl checkdb** command.

```
cmxctl checkdb { cassandra | postgres }
```

Syntax Description	cassandra Checks the cassandra schema.				
	postgres Checks the postgres schema.				
Command Default	None				
Command Modes	CMX admin user				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.3</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.3	This command was introduced.
Release	Modification				
Cisco CMX Release 10.3	This command was introduced.				

Example

The following example shows how to the schemen integrity for cassandra and postgres database:

```
[cmxadmin@server]# cmxctl checkdb cassandra

Schema passed analytics
Schema passed loc
Schema passed mse
Cassandra passed schema validation

[root@server]# cmxctl checkdb postgres
Schema passed analytics
Schema passed loc
Schema passed mse
Postgres passed schema validation
```

cmxctl checklogs

To check logs and generate a report, use the **cmxctl checklogs** command.

cmxctl checklogs

Command Default

None

Command Modes

CMX admin user

Usage Guidelines

After a report is generated, the specific log that shows the error can be viewed for additional details. For example, `/opt/cmx/var/log/cmxjobs.log.3` has 108 errors, use the command **more** `/opt/cmx/var/log/cmxjobs.log.3` to view the corresponding file.

The following example shows how to check logs and generate a report:

```
[cmxadmin@cmx]# cmxctl checklogs

*****
Checking /opt/cmx/var/log/cmxjobs.log.3 for errors..
/opt/cmx/var/log/cmxjobs.log.3 has 108 errors
*****
Checking /opt/cmx/var/log/system-cron.log for errors..
/opt/cmx/var/log/system-cron.log has 0 errors
*****
Checking /opt/cmx/var/log/cmxjobs.log for errors..
/opt/cmx/var/log/cmxjobs.log has 81 errors
*****
Checking /opt/cmx/var/log/collectd.log for errors..
/opt/cmx/var/log/collectd.log has 0 errors
*****
Checking /opt/cmx/var/log/consul.log for errors..
/opt/cmx/var/log/consul.log has 0 errors
*****
Checking /opt/cmx/var/log/qless-py-worker.log for errors..
/opt/cmx/var/log/qless-py-worker.log has 0 errors
*****
Checking /opt/cmx/var/log/influxdb.log for errors..
/opt/cmx/var/log/influxdb.log has 0 errors
*****
Checking /opt/cmx/var/log/cmxjobs.log.4 for errors..
/opt/cmx/var/log/cmxjobs.log.4 has 108 errors
*****
```

cmxctl config analytics

To configure general analytics settings, use the **cmxctl config analytics** command:

```
cmxctl config analytics {cleanRedis | enableMinDwellFilter {True | False} | setMinDwellFilter <value> | setNumMonthsRepeatHistory <value> | view}
```

Syntax Description		
cleanRedis		Removes old, invalid Redis bloom filters.
enableMinDwellFilter {True False}		<ul style="list-style-type: none"> • True—Enables the minimum dwell filter. • False—Disables the minimum dwell filter. This is the default.
setMinDwellFilter <value>		Sets the minimum dwell filter value [0-1440]. The default is 0.
setNumMonthsRepeatHistory <value>		Sets the number of months [0-6] to retain the repeat history. The default is 6.
view		Displays the general analytics settings.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.5	Additional subcommands were added.
	Cisco CMX Release 10.3.1	This command was introduced.

Usage Guidelines

You can set a minimum dwell filter to filter out visitors whose dwell at the root campus level is less than a specified amount. The root campus level encompasses all campuses; it represents the root of the hierarchy. This affects the aggregated data, so once the filter is enabled, it applies to all reports for that day moving forward (until it is disabled again). This filter does not affect the raw visits.

If you configure the minimum dwell filter setting, you must restart Cisco CMX for the change to take effect. Use the **cmxctl restart** command to restart Cisco CMX.



Note Use the minimum dwell filter only if you don't want to see devices that spend less than the minimum number of minutes at the root campus level.

Repeat history is kept for the current month and the set number of previous months. This set number of months must be in the range of 0 to 6 months. You do not need to restart Cisco CMX to put this setting into effect.



Note If you use the **setNumMonthsRepeatHistory** command, all current repeat history is deleted.

Examples

The following example shows how to display the current general analytics settings:

```
[cmxadmin@cmx]# cmxctl config analytics view
```

```
+-----+-----+
| enableMinimumDwellFilter | True |
+-----+-----+
| minimumDwellFilter       | 30  |
+-----+-----+
| numMonthsRepeatHistory   | 6   |
+-----+-----+
```

The following example shows how to set and enable the Analytics minimum dwell filter setting:

```
[cmxadmin@cmx]# cmxctl config analytics setMinDwellFilter 30
```

```
+-----+-----+
| enableMinimumDwellFilter | False |
+-----+-----+
| minimumDwellFilter       | 0    |
+-----+-----+
| numMonthsRepeatHistory   | 6    |
+-----+-----+
```

```
[root@server]# cmxctl config analytics enableMinDwellFilter True
```

```
+-----+-----+
| enableMinimumDwellFilter | True  |
+-----+-----+
| minimumDwellFilter       | 30   |
+-----+-----+
| numMonthsRepeatHistory   | 6    |
+-----+-----+
```

```
[root@server]# cmxctl analytics restart
```

```
.....
```

```
Service Analytics has successfully restarted.
```

The following example shows how to disable the minimum dwell filter setting:

```
[cmxadmin@cmx]# cmxctl config analytics cleanRedis
```

```
Cleaning up old bloom filters from redis on 2018-06-26
```

```
Month filter cutoff date = 2017-12-01
```

```
Current valid ids = [4, 3, 2, 1, 17, 18, 8, 9, 11, 12, 13, 14, 19]
```

```
cutoff = 2017-12-01
```

```
validids = [4, 3, 2, 1, 17, 18, 8, 9, 11, 12, 13, 14, 19]
```

```
cutoff = 2018-06-25
```

```
validids = [4, 3, 2, 1, 17, 18, 8, 9, 11, 12, 13, 14, 19]
```

```
Deleting key: Day_2018-06-23_2
```

```
Deleting key: Day_2018-06-24_4
```

```
Deleting key: Day_2018-06-21_2
```

```
Deleting key: Day_2018-06-21_12
```

```
Deleting key: Day_2018-06-24_12
```

```
Deleting key: Day_2018-06-22_12
```

```
Deleting key: Day_2018-06-23_4
```

```
Deleting key: Day_2018-06-21_8
```

```
Deleting key: Day_2018-06-23_12
```

```
Deleting key: Day_2018-06-22_2
```

```
Deleting key: Day_2018-06-24_8
```

```
Deleting key: Day_2018-06-22_8
```

```
Deleting key: Day_2018-06-21_14
```

```
Deleting key: Day_2018-06-22_4
```

```
Deleting key: Day_2018-06-23_14
```

```
Deleting key: Day_2018-06-24_2
```

The following example shows how to set the repeat history setting:

```
[cmxadmin@cmx]# cmxctl config analytics setNumMonthsRepeatHistory 5
```

Doing this will delete current history for ALL months. This will affect aggregated report data but will NOT affect raw visits data. Do you want to continue? [y/N]: y
Successfully change the number of months tracked for repeat history.

```
+-----+  
| enableMinimumDwellFilter | False |  
+-----+  
| minimumDwellFilter      | 0   |  
+-----+  
| numMonthsRepeatHistory  | 5   |  
+-----+  
[root@server]# #
```

cmxctl config aps delete

To delete an access point from Cisco CMX, use the **cmxctl config aps delete** command.

cmxctl config aps delete *MAC Address*

Syntax Description	<i>MAC Address</i> Displays the MAC address of the access point.				
Command Default	None.				
Command Modes	CMX admin user				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco CMX Release 10.4</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco CMX Release 10.4	This command was introduced.
Release	Modification				
Cisco CMX Release 10.4	This command was introduced.				
Usage Guidelines	This command should be run at the cmxadmin level.				

cmxctl config audit

To enable and manage the remote logging of system events (syslogs), use the **cmxctl config audit settings** command. To view logged files, use the **cmxctl config audit view** command.

cmxctl config audit { **restart** | **settings** | **status** | **view** }

Syntax Description		
restart		Restarts rsyslog service.
settings		Enables, disables and configures audit log settings. See Usage Guidelines for information.
status		Displays whether audit logging is running on CMX, or is disabled. For example, Remote Audit Logging = Disabled.
view		Displays all or specific log files. See Usage Guidelines for information.

Command Default By default, remote system logging is disabled.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 11.1.1	This command was modified to support multiple rsyslog servers, and the audit is enhanced with log level and module level.
	Cisco CMX Release 10.6.3	This command was modified to include restart and status keywords.
	Cisco CMX Release 10.5.0	This command was introduced.

Usage Guidelines

- The command **cmxctl config audit settings** prompts you to enter the following configuration questions. If you enter no value, CMX selects the default value, shown in [brackets].



Note To enable remote audit logging, enter a remote syslog IP address, port number and domain name. Otherwise, only local audit logging is enabled.

Examples

The following example shows how to enable remote system logging of selected events:

```
[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: 10.11.22.44
Please enter rsyslog port [514]:
Enter CA cert file for Remote syslog server: /home/cmxadmin/52.crt
Please enter rsyslog server's Common Name(CN) or Subject Alternate Name(SAN): ServerCrt

Do you want to add another rsyslog server? [y/N]: y

--- Configuring Rsyslog Server 2 ---
Please enter rsyslog IP: 10.11.22.45
Please enter rsyslog port [514]:
Enter CA cert file for Remote syslog server: /home/cmxadmin/54.crt
Please enter rsyslog server's Common Name(CN) or Subject Alternate Name(SAN): ServerCrt

Maximum limit of 2 syslog servers reached.
Please enter the email IDs (comma separated) for mail alerts: abc
Configured 2 rsyslog server(s) for TLS forwarding
Processing certificate 1/2: /home/cmxadmin/52.crt
Checking for CRL Distribution Points
Found CRL URI(s)
CRL successfully downloaded from http:// 10.11.22.47/rootca.crl
Creating new CRL collection with this CRL.
Import Rsyslog CA Certificate successful to rsyslogca1.crt
Certificate 1 imported successfully as rsyslogca1.crt
Processing certificate 2/2: /home/cmxadmin/54.crt
Checking for CRL Distribution Points
Found CRL URI(s)
CRL successfully downloaded from http:// 10.11.22.47/rootca.crl
Replacing existing CRL in the CRL collection.
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: rsyslogcal.crt, rsyslogca2.crt, ... rsyslogca2.crt (for IPSec)

Please select the events to be logged

All Events [yes/no] (yes, no) [yes]: no

Connection Events [yes/no] (yes, no) [yes]:

Management Events [yes/no] (yes, no) [yes]:

Auth Events [yes/no] (yes, no) [yes]:

Configuration Events [yes/no] (yes, no) [yes]:

Security Configuration Events [yes/no] (yes, no) [yes]:

Security Events [yes/no] (yes, no) [yes]:

Misc 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

[cmxadmin@cmx]#**cmxctl config audit settings**

Enable or Disable Remote Syslogging [Enable / Disable] [Enable]:

If logs size goes beyond lgb, drop or overwrite messages? [drop / overwrite] [overwrite]:

Please enter rsyslog IP:

Please enter rsyslog port [514]:

Please enter rsyslog DNS name: *yoursyslogserver.yourco.com*

Please enter the email IDs (comma separated) for mail alerts: *email@example.com*

Follow the prompts to select what events you would like logged:

Please select the events to be logged

All Events [yes/no] [yes]:

Settings saved

Starting rsyslog service

If you enter **yes**, all events are logged. If **no**, answer the following prompts:

```
Enter day [today(1)/yesterday(2)/last week(3)/last month(4)/all(5)] [5]:
Enter event type [MGMT_EVENT(1)/CONN_EVENT(2)/AUTH_EVENT(3)/CONF_EVENT(4)/ALL(5)] [5]:
Enter identity [root(1)/admin(2)/all(3)] [3]:
Enter status [success(1)/failure(2)/all(3)] [3]:
```

- The command **cmxctl config audit view** prompts you to enter which types of logs you want to view.

```
Show all logs [yes/no] [yes]:
```

If you enter **yes**, all logged events are displayed. If **no**, answer the following prompts, or **Enter** to accept the default value.

```
Enter day [today(1)/yesterday(2)/last week(3)/last month(4)/all(5)] [5]:
Enter event type [MGMT_EVENT(1)/CONN_EVENT(2)/AUTH_EVENT(3)/CONF_EVENT(4)/ALL(5)] [5]:
Enter identity [root(1)/admin(2)/all(3)] [3]:
Enter status [success(1)/failure(2)/all(3)] [3]:
```

Examples

The following example shows how to enable remote system logging of all events:

```
[cmxadmin@cmx]# cmxctl config audit settings
Enable or Disable Remote Syslogging [Enable / Disable] [Enable]:
If logs size goes beyond lgb, drop or overwrite messages? [drop / overwrite] [overwrite]:
Please enter rsyslog IP: 168.172.1.20
Please enter rsyslog port [514]: 514
Please enter rsyslog DNS name: s1s1296@wowco.com
Please enter the email IDs (comma separated) for mail alerts: email@example.com

Remote Audit Logging = Enabled

Please select the events to be logged
All Events [yes/no] [yes]: yes
Settings saved

Restarting rsyslog service
Shutting down system logger: [OK]
Starting system logger: [OK]
```

The following example shows how to display all admin-level success status logs for the current day.

```
[cmxadmin@cmx]# cmxctl config audit view
Show all logs [yes/no] [yes]: no
Enter day [today(1)/yesterday(2)/last week(3)/last month(4)/all(5)] [5]: 1
Enter event type [MGMT_EVENT(1)/CONN_EVENT(2)/AUTH_EVENT(3)/CONF_EVENT(4)/ALL(5)] [5]: 5
Enter identity [root(1)/admin(2)/all(3)] [3]: 2
Enter status [success(1)/failure(2)/all(3)] [3]: 1
```

CMX displays the selected logs.

The following example shows how to view the audit log status.

```
[cmxadmin@cmx]# cmxctl config audit status
Remote Audit Logging = Enabled
Remote Syslog Server IP = 10.20.1.10
Remote Syslog Server Port = 4514
Connection Protocol = TLS
```

The following example shows how to restart rsyslog service.

```
[cmxadmin@cmx]# cmxctl config audit restart  
rsyslog service restarted
```


cmxctl config auth

To set strong CMX authentication requirements for passwords, logging in, and session timeout, use the **cmxctl config auth settings** command. To view these authentication settings, use the **cmxctl config auth show** command.

```
cmxctl config auth {settings | show}
```

Syntax Description	settings	Configures CMX authentication settings.
	show	Displays CMX authentication settings.

Command Default By default, strong authentication is not enabled.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.2	This command was modified to set fail interval to 15 minutes when UCAPL mode is enabled. Added two new parameters: Maximum password lifetime and Password Expiry Warning Period .
	Cisco CMX Release 11.1.1	This command was modified and added three new parameters: <ul style="list-style-type: none"> • Max Concurrent Sessions per user • Max global Concurrent sessions • Absolute Session Timeout in minutes
	Cisco CMX Release 10.6.2	This command was modified to set fail interval to 15 minutes when UCAPL mode is enabled. Added two new parameters: Maximum password lifetime and Password Expiry Warning Period .
	Cisco CMX Release 10.6	This command was modified to add the default values for FIPS and UCAPL.
	Cisco CMX Release 10.5.0	This command was introduced.

Usage Guidelines The command **cmxctl config auth** prompts you to set the appropriate values, according to your system authentication settings.

If **Enable strong password** is set to **Yes**, you can extend the password upto 127 characters. However, we recommend you to ensure that password should have minimum one lower case, one upper case, one digit and a special character.



Note When you run the **cmxctl config auth settings** command, the changes will only be in effect for new sessions. When changing the session timeout, the current session must be logged out and then logged in again. Furthermore, it is important to note that these changes will not affect existing sessions.

```
Enable strong password [yes / no] (yes, no) [yes]:
Minimum password length [8-127] [8]:
Maximum password lifetime [1-9999] [9999]:
Password Expiry Warning Period [1-30] [14]:
Unsuccessful login attempts before account lock [3-5] (3, 4, 5) [3]:
Fail interval in minutes [1-120] [15]:
Account lockout interval in minutes [1-120] [30]:
Max Concurrent Sessions per user [5-25] [10]:
Max global Concurrent sessions [5-100] [50]:
Absolute Session Timeout in minutes [10-480] [480]:
Session idle timeout in minutes [1-720] [30]:
SSH session limits updated successfully:
Note:
Restart CMX services for the changes to take effect.
Logout and login again for session timeout changes to take effect.
```

CMX authentication defaults with FIPS/UCAPL disabled:

```
Enable strong password [yes / no] (yes, no) [yes]:
Minimum password length [8-127] [8]:
Maximum password lifetime [1-9999] [9999]:
Password Expiry Warning Period [1-30] [14]:
Unsuccessful login attempts before account lock [3-5] (3, 4, 5) [3]:
Fail interval in minutes [1-120] [15]:
Account lockout interval in minutes [1-120] [30]:
Max Concurrent Sessions per user [5-25] [10]:
Max global Concurrent sessions [5-100] [50]:
Absolute Session Timeout in minutes [10-480] [480]:
Session idle timeout in minutes [1-720] [30]:
```

CMX authentication defaults in FIPS mode enabled:

```
Strong password is enabled for FIPS/UCAPL mode.
Minimum password length [8-127] [8]:
Maximum password lifetime [1-9999] [9999]:
Password Expiry Warning Period [1-30] [14]:
Unsuccessful login attempts before account lock [3-5] (3, 4, 5) [3]:
Fail interval in minutes [1-120] [15]:
Account lockout interval in minutes [1-120] [30]:
Max Concurrent Sessions per user [5-25] [10]:
Max global Concurrent sessions [5-100] [50]:
Absolute Session Timeout in minutes [10-480] [480]:
Session idle timeout in minutes [1-720] [30]:
```

- CMX authentication defaults with FIPS/UCAPL off:

```
Enable strong password: yes/no
Minimum password length: 8-20 characters
Maximum password lifetime: [1-9999]
Password Expiry Warning Period [1-30]
Unsuccessful login attempts before account lock: 3-5 attempts
Fail interval in minutes: [1-120]
Set session timeout in minutes: 10-60 minutes
```

- CMX authentication defaults in FIPS mode:

```

Enable strong password [yes / no] [yes]:
Minimum password length [8-20] [8]:
Maximum password lifetime [1-9999] [9999]:
Password Expiry Warning Period [1-30] [14]:
Unsuccessful login attempts before account lock [3-5] [3]:
Account lockout interval in minutes [1-120] [30]:
Session idle timeout in minutes [1-120] [30]:
Restart services for the changes to take effect

```

- CMX authentication defaults in UCAPL mode:

```

Enable strong password [yes / no] [yes]:
Minimum password length [15-20] [15]:
Maximum password lifetime (in days): 60 days
Password Expiry Warning Period (in days): 7 days
Unsuccessful login attempts before account lock is set to 3 for UCAPL mode.
Fail interval in minutes [1-120] [15]:
Account lockout interval in minutes [1-120] [30]:
Session timeout is set to 15 minutes for UCAPL mode.
Enable Global session timeout (10 mins) for UCAPL mode [yes / no] [no]:
Global Session timeout set to: 15 minutes
Restart services for the changes to take effect

```



Note Fail interval is automatically set to 15 minutes when UCAPL mode is enabled. Cisco CMX account will be locked if consecutive failed login attempts occur within the set fail interval period.

- CMX authentication defaults in UCAPL over FIPS mode:

```

Enable strong password: yes
Minimum password length: 15-20 characters
Unsuccessful login attempts before account lock: 3
Enable Global session timeout (10 mins) for Web UI: yes

```

The following example shows how to display security parameters for a FIPS-enabled

```

[cmxadmin@cmx]# cmxctl config auth show
Enable strong password : yes
Minimum password length : 8
Maximum password lifetime in days : 9999
Password Expiry Warning Period in days : 14
Unsuccessful login attempts before account lock : 3
Fail interval in minutes : 15
Account Lockout interval in minutes : 30
Session idle timeout in minutes : 30
Absolute Session Timeout in minutes : 480
Max Concurrent Sessions per user : 10
Max global Concurrent sessions : 50

```

The following example shows how to view the auth settings:

```

[cmxadmin@cmx]# cmxctl config auth show
Enable strong password : yes
Minimum password length : 8
Maximum password lifetime in days : 9999
Password Expiry Warning Period in days : 14
Unsuccessful login attempts before account lock : 3

```

```

Fail interval in minutes : 15
Account Lockout interval in minutes : 30
Session idle timeout in minutes : 30
Absolute Session Timeout in minutes : 480
Max Concurrent Sessions per user : 10
Max global Concurrent sessions : 50

```

The following example shows how to configure auth settings in the Fips and non Fips mode:

```

[cmxadmin@cmx]# cmxctl config auth settings
Enable strong password [yes / no] (yes, no) [yes]:
Minimum password length [8-127] [8]:
Maximum password lifetime [1-9999] [9999]:
Password Expiry Warning Period [1-30] [14]:
Unsuccessful login attempts before account lock [3-5] (3, 4, 5) [3]:
Fail interval in minutes [1-120] [15]:
Account lockout interval in minutes [1-120] [30]:
Max Concurrent Sessions per user [5-25] [10]:
Max global Concurrent sessions [5-100] [50]:
Absolute Session Timeout in minutes [10-480] [480]:
Session idle timeout in minutes [1-720] [30]:
SSH session limits updated successfully:
Note:
Restart CMX services for the changes to take effect.
Logout and login again for session timeout changes to take effect.

```

Examples

The following example shows how to display security parameters for a FIPS-enabled CMX:

```

[cmxadmin@cmx]# cmxctl config auth show

Enable strong password : yes
Minimum password length : 8
Maximum password lifetime : 9999
Password Expiry Warning Period : 30
Unsuccessful login attempts before account lock : 3
Fail interval in minutes : 15
Account Lockout interval in minutes : 30
Session idle timeout in minutes : 30

```

Examples

The following example shows how to configure auth settings:

```

[cmxadmin@cmx]# cmxctl config auth settings
Enable strong password [yes / no] [yes]: yes
Minimum password length [8-127] [8]: 8
Maximum password lifetime [1-9999] [9999]:9999
Password Expiry Warning Period [1-30] [14]:30
Unsuccessful login attempts before account lock [3-5] [3]: 3
Fail interval in minutes [1-120] [15]: 15
Account lockout interval in minutes [1-120] [30]: 30
Session idle timeout in minutes [1-720] [30]:
Restart services for the changes to take effect

```

The following example shows how to view the auth settings:

```

[cmxadmin@cmx]# cmxctl config auth show
Enable strong password : yes

```

```
Minimum password length : 8
Maximum password lifetime :9999
Password Expiry Warning Period :30
Unsuccessful login attempts before account lock : 3
Fail interval in minutes : 15
Account Lockout interval in minutes : 30
Session idle timeout in minutes : 30
```

Related Commands

Command	Description
cmxctl config fips	Enables FIPS mode, which requires strong authentication.
cmxctl config fips ucaplmode	Enables UCAPL over FIPS mode, which requires strong authentication.

cmxctl config authinfo get

To view the the SHA1 (keyHash) and SHA2(sha2KeyHash) strings, use the **cmxctl config authinfo get** command.

cmxctl config authinfo get

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.4	This command was introduced.

Usage Guidelines

This command gets the authorization information for NMSP connections to the controllers.

Example

The following example shows how to get the authorization information:

```
[cmxadmin@cmx]# cmxctl config authinfo get
+-----+-----+-----+
| macAddress          | keyHashString          | sha2KeyHashString      |
+-----+-----+-----+
| 00:0c:29:07:36:84 | e743ac54029ce36282c582f04bfb45ec187c824d | 560d69882adb90dda10227651da0c6a2850999620b50f83ed0d157fb87d1a920 |
+-----+-----+-----+
```

cmxctl config authserver

To add and manage external RADIUS authentication servers, use the **cmxctl config authserver** command.

cmxctl config authserver { **delete** | **settings** | **show** | **sshmfa** }

Syntax Description	delete	Removes an external RADIUS authentication server.
	settings	Adds and configures an external RADIUS authentication server for CMX GUI and SSH access.
	show	Shows external server configuration.
	sshmfa	Adds and configures AAA/RADIUS access to CMX GUI and SSH.

Command Default External Remote Authentication Dial-In User Service (RADIUS) authentication server is not configured.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 11.1.1	This command was modified to include sshmfa keyword (option to configure SSH access (SSH Multi-Factor Authentication – SSH MFA)).
	Cisco CMX Release 10.6.3	This command was introduced.

Usage Guidelines Before running this command, create a RADIUS user with information similar to the following example:

Table 1: Example of RADIUS authentication user

Entry	Values
File name:	/usr/local/etc/raddb/users
#Create user with User-Name =	radiusUser
radiusUser Cleartext-Password :=	"Cisco123"
Reply-Message =	"Hello, %{User-Name}"

Usage Guidelines The **cmxctl config authserver settings** command prompts you to configure the authentication server:

```

Enter external RADIUS authentication server host :
Enter RADIUS server shared secret key :
Configure local account. This account can be used if RADIUS server is not reachable.
Enter username :
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

```

Examples

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



Note This example uses the values described in the Usage Guidelines.

```

[cmxadmin@cmx]# cmxctl config authserver settings

[cmxadmin@cmx]# cmxctl config authserver settings
Enter external RADIUS authentication server host : 192.0.2.1
Enter RADIUS server shared secret key :
Configure local account. This account can be used if RADIUS server is not reachable.
Enter username : radiusUser
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.

```


cmxctl config authserver sshmfa

To configure access to GUI, use the **cmxctl config authserver sshmfa** command.

```
cmxctl config authserver sshmfa { add <users.csv> | delete <users.txt> | list }
```

Syntax Description

add <users.csv> Adds and configures AAA users for SSH access.

delete <users.txt> Removes AAA users for SSH access.

list Shows the list of configured AAA users for SSH access.

Command Default

External Remote Authentication Dial-In User Service (RADIUS) authentication server is not configured.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 11.1.1	This command was introduced.

Usage Guidelines

When enabled, GUI access is granted to all AAA/RADIUS users; however, SSH access for AAA/RADIUS users is granted only to selected AAA/RADIUS users.

The prerequisites for enabling SSH access with SSH Multi-Factor Authentication (SSH MFA) on the CMX box for users authenticated by an External Authentication Server are as follows:

- Download the **CA chain certificate** of the authority that signs all user certificates to the CMX box.
- Download the **user certificates** for those users who will be granted SSH access. These certificate files must be in **PEM format**.
- Prepare a **CSV file** containing the username and the full path of the corresponding user certificate file on each line, formatted as:

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

These files must be in place before enabling SSH access for users authenticated via the external server. This setup ensures that SSH access with MFA is granted only to selected users with valid certificates.

Manage AAA users for SSH Access in Cisco CMX

After the feature is enabled, use these commands to manage AAA users for SSH access:

To add AAA users, use the **cmxctl config authserver sshmfa add** <users.csv> command.

The input file will be in CSV format identical to the one used while enabling External Authentication Server. It will contain each line with format <username>,<full_path_of_user_certificate_file>



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

```
[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
```

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

The input file should contain only the usernames 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
```

To list the currently configured users for SSH MFA, use the **cmxctl config authserver sshmfa list** command.



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

```
[cmxadmin@cmx ~]$ cmxctl config authserver sshmfa list
MFA enabled users : cmxuser1,cmxuser2
```

cmxctl config banner

To create and manage a banner that displays when users log into CMX, use the **cmxctl config banner** command.

cmxctl config banner {**disable** | **edit** | **show**}

Syntax Description	disable	Disable the login banner.
	edit	Edit the login banner text.
	show	Display the login banner.
Command Default	By default, CMX has no login banner.	
Command Modes	CMX admin user	
Command History	Release	Modification
	Cisco CMX Release 10.5.0	This command was introduced.
	Cisco CMX Release 10.6	This command was modified to include disable keyword.
Usage Guidelines	None	

Examples

The following example shows how to create the login banner “CentOS release 7.0.”

```
[cmxadmin@cmx]# cmxctl config banner edit
Current Login Banner = []
Enter text to be displayed as login banner. Enter a single period on a line to terminate.
CentOS release 7.0
.
```

When you log into the CLI, you would see something like this:

```
login as: cmxadmin
CentOS release 7.0
cmxadmin@168.172.1.20's password:
Last login: 6/5/2018 1:10 PM
```

When you log into CMX from a browser, the banner message appears in a pop-up window on the login page.

The following example shows how to disable the login banner.

```
[cmxadmin@cmx]# cmxctl config banner disable
Login banner disabled successfully
```

cmxctl config certs

To create, import, or manage security key certificates, use the **cmxctl config certs** command.

```
cmxctl config certs { clear | clientcertvalidation { enable | disable } | createcsr |
importcacert filename.pem | importcrl filename.pem | importcrlurl URL | importrsyslogca
filename.pem | importradiusca filename.pem | importservercert filename.pem | installnewcerts
| keytype { RSA | ECDSA } | show }
```

Syntax Description	Description
clear	Clears certificate files in the <code>/opt/cmx/srv/certs</code> directory.
clientcertvalidation	When FIPS or UCAPL is enabled, configures CMX to validate all client certificates. <ul style="list-style-type: none"> • Enable — requires every CMX user to have a client certificate. • disable — does not check for client certificates.
createcsr	Creates a new public and private keypair, and generates a corresponding Certificate Signing Request (CSR).
importcacert <i>filename.pem</i>	Imports a Certificate of Authority (CA) Privacy Enhanced Mail (pem) file.
importcrl <i>filename.pem</i>	Imports a Certificate Revocation List (CRL) pem file.
importcrlurl <i>URL</i>	Imports the URL of the CRL online, to keep the CRL current.
importrsyslogca <i>filename.pem</i>	Imports a CA pem file for the remote syslog server.
importradiusca <i>filename.pem</i>	Imports a CA pem file for the Radius/AAA server.
importservercert <i>filename.pem</i>	Imports the signed certificate and private key for the CMX server, concatenated into a single pem file. <p>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 (within 30 days), an alert is generated on System > Alerts tab in Cisco CMX. The alert will be generated once a day until certificate expires or new valid certificate is installed.</p>

installnewcerts	<p>Generates new self-signed certificates and adds the Subject Alternative Name (SAN) IP in the self-signed certificates.</p> <p>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 (within 30 days), an alert is generated on System > Alerts tab in Cisco CMX. The alert will be generated once a day until certificate expires or new valid certificate is installed.</p> <p>With Cisco CMX Release 11.1.0, a new parameter (optional) --add-ip-san is added that enables you to add the Subject Alternative Name (SAN) IP in the self-signed certificates.</p>
keytype	<p>Selects your encryption algorithm key type.</p> <ul style="list-style-type: none"> • RSA — Install the Rivest–Shamir–Adleman (RSA) encryption algorithm. • ECDSA — Install the Elliptic Curve Digital Signature Algorithm (ECDSA).
show	Displays certificate details.

Command Default By default, authentication certificates are not created, imported, or validated.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 11.1.1	The cmxctl config certs keytype command was modified to include the 2048 bit rsa key length.
	Cisco CMX Release 11.1.0	The command cmxctl config certs installnewcerts was modified to include --add-ip-san optional parameter to add the Subject Alternative Name (SAN) IP address in the self-signed certificates.
	Cisco CMX Release 10.6.2	This command was modified to include importradiusca filename.pem keyword.
	Cisco CMX Release 10.6	This command was modified to include clientcertvalidation , importcontrollerca , and importrsyslogca keywords.
	Cisco CMX Release 10.5.0	This command was introduced.

Usage Guidelines



Note Certificates and keys are stored in the `/opt/cmx/srv/certs` folder.

Cisco recommends following this deployment order for **cmxctl config certs** commands.

1. **cmxctl config certs clear** — Optional, but recommended. Clears any certificates from the `/opt/cmx/srv/certs` directory.
2. **cmxctl config certs keytype** — Selects your key type: RSA (the default) or ECDSA. If you select the RSA, then two RSA key size options available are **2048** and **4096**.
3. **cmxctl config certs installnewcerts** — Generates new self-signed certificates in the `/opt/cmx/srv/certs` directory.
4. **cmxctl config certs createcsr** — Creates a Certificate Signing Request (CSR).
 - Private key — `/opt/cmx/srv/certs/cmserverkey.pem`
 - CSR — `/opt/cmx/srv/certs/cmservercsr.pem`
5. Send the CSR to an external CA, to obtain a signed certificate for the CMX server.
6. **cmxctl config certs importca-cert** — Installs the CA certifications. At the prompt, provide an export and import password specific to this command.
7. **cmxctl config certs importservercert** — Installs the CA-signed server certificate and the private key as a concatenated pem file. At the prompt, provide an export and import password specific to this command.

The command **cmxctl config certs clientcertvalidation enable** prompts you to answer whether or not you want CMX to accept invalid client certificates.

Do you want to accept invalid client certificate? [yes/no] [no]:

- **no**—Enables client certificate validation, and will not accept invalid client certificates.
- **yes**—Enables client certificate validation, but will accept invalid client certificates.

Examples

The following example shows how to clear out old certificates from the `/opt/cmx/srv/certs` directory.

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

The following example shows how to select key type ECDSA:

```
[cmxadmin@cmx]# cmxctl config certs keytype
Please enter key type [RSA / ECDSA] [RSA]:ECDSA
Keytype is set to ECDSA.
```

The following example shows how to generate new self-signed certification files in the `/opt/cmx/srv/certs` directory using an RSA key:

```
[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
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.

The following example shows how to select the key type RSA and RSA key length:

```

[cmxadmin@cmx~]$cmxctl config certs keytype
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.

```

The following example shows how to create a new certificate signing request (CSR):

```

[cmxadmin@cmx]# cmxctl config certs createcsr

For SAN field of CSR, enter FQDN for CMXX 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]: Yourco, Inc.
Organizational Unit Name (eg, section) []: Gulag 10
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.

```

Sometimes two or more files need to be combined (or *concatenated*) before you can import the resulting file. For example, you may have intermediate CA certificates as well as root certs. This example shows how to concatenate the files root-ca-cert.pem and intermediate-ca-cert.pem, and import the resulting file to CMX.

1. Concatenate the files:

```
[cmxadmin@cmx]# cat root-ca-cert.pem intermediate-ca-cert.pem >
ca-chain.pem
```

2. Import the new file **ca-chain.pem**:

```
[cmxadmin@cmx]# cmxctl config certs importcacerts ca-chain.pem

Importing CA certificate.....
Enter Export Password: caexportpw
Verifying - Enter Export Password: caexportpw
Enter Import Password: caimportpw
Import CA Certificate successful
0
```

The **importservercert** command requires you to combine the server key and the server certificate into one pem file. The following example shows how to combine the files and import the resulting file.



Note Import CA chain certificates before importing the server certificate.

1. Concatenate the files:

```
[cmxadmin@cmx]# cat cmxserverkey.pem signed-cert.pem >
server-key-cert.pem
```

2. Import the new file **server-key-cert.pem**:

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

Importing Server certificate.....

Successfully transferred the file
```

At the prompts, provide an export and import password specific to this command.

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

The following example shows how to display the details of the server certificate and all CA chain certificates:

```
[cmxadmin@cmx]# cmxctl config certs show
```


Certificate details

```

***** Certificate Listing *****
=====
***** UMLC 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: Jan 19 05:17:33 2018 GMT
      Not After : Jan 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:

```

The following example shows how to add SAN IP address:

```
[cmxadmin@cmx]# cmxctl config certs installnewcerts --add-ip-san
```

```

Keytype is RSA, generating RSA key with length 4096
Generating RSA private key, 4096 bit long modulus (2 primes)

++++
++++
e is 65537 (0x010001)
Generating RSA private key, 4096 bit long modulus (2 primes)
++++++
e is 65537 (0x010001)
Signature ok
Subject=C = US, ST = CA, L = San Jose, O = MSE, CN = ServerCrt
Getting CA Private Key
FIPS mode is disabled. Skipping Check for subjectAltName(SAN).
OCSP URI not found, skipping OCSP check.
Validation of server certificate is successful
Certificates are valid.
This is IPV4 Address
OCSP URI not found, exiting.
New self-signed certificates installed successfully.
To apply these certificate changes, CMX Services will be restarted now.

```

Please press Enter to continue.

Related Commands

Command	Description
cmxctl config fips	Enables FIPS mode, which requires these certificates.
cmxctl config fips ucaplmode	Enables UCAPL over FIPS mode, which requires these certificates.

cmxctl config controllers

To manage Cisco Wireless Controllers (Cisco WLC), use the **cmxctl config controllers** command.

cmxctl config controllers {**activeaps** | **add** | **delete** | **floors** *wlc-ip-address* | **import** | **missingaps** | **show**}

Syntax Description		
activeaps		Displays active access points.
add		Adds a Cisco WLC. Note Cisco CMX does not support Cisco Catalyst 9800 Series Wireless Controllers with special characters > or # in the message-of-the-day (MOTD) banner.
delete		Deletes a Cisco WLC.
floors <i>wlc-ip-address</i>		Displays floors managed by Cisco WLCs.
import		Imports a Cisco WLC from Cisco Prime Infrastructure by providing the corresponding credentials, or by placing an exported Cisco Prime Infrastructure MAP file in the /opt directory of the Cisco CMX server and providing the path to the exported MAP file.
missingaps		Lists the access points from which Cisco CMX has received data, but the access points are not yet placed on a map.
show		Displays information pertaining to a Cisco WLC.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.3.1	The missingaps and floors keywords were added.
	Cisco CMX Release 10.3.0	This command was introduced.

Usage Guidelines The message "controller added successfully" after a Cisco WLC is added, refers only to the correct parsing of the command. You should issue a **cmxctl controllers show** command to ensure that the Cisco WLC is not active.

The **missingaps** keyword uses SNMP to retrieve the AP's MAC addresses from the access point's configuration cache every six hours. If the AP MAC address is not present, it will be displayed as NA on the CLI.

In addition, the AP MAC address will be displayed only if you have enabled the **configuration.apimport feature** flag by using the **cmxctl config featureflags configuration.apimport: true** command. For example:

```
[cmxadmin@server]# cmxctl config featureflags configuration.apimport true

+-----+-----+
| location.compactlocationhistory | false |
+-----+-----+
| configuration.apimport           | true  |
+-----+-----+
```

The AP MAC address import occurs every 6 hours, so for new APs added to the controller, the AP MAC value for missingap will be available only after the next job run.

Examples

Starting from Cisco CMX Release 10.3.1, you can specify SNMP settings when you use the **cmxctl config controllers add** command. For example:

```
[cmxadmin@cmx]# cmxctl config controllers add
Please enter controller type [WLC / NGWC] [WLC]: WLC
Please enter controller ip: 0.0.0.0
Please enter the controller version [Optional]:
Please enter controller SNMP version [v1 / v2c / v3] [v2c]: v2c
Please enter controller SNMP write community [private]:
.....
Controller Added 0.0.0.0
```

The following example shows how to display the Cisco WLC information:

```
[cmxadmin@cmx]# cmxctl config controllers show

+-----+-----+-----+-----+-----+-----+
| IP Address | Type | Version | Device Version | SHA2 | Status |
+-----+-----+-----+-----+-----+-----+
| 30.30.30.65 | WLC | 8.0.72.141 | - | No | ACTIVE |
+-----+-----+-----+-----+-----+-----+
| 30.30.30.44 | WLC | 8.0.72.141 | - | No | ACTIVE |
+-----+-----+-----+-----+-----+-----+
| 30.30.30.46 | WLC | 8.0.72.141 | - | No | ACTIVE |
+-----+-----+-----+-----+-----+-----+
| 30.30.30.70 | WLC | 8.0.72.141 | - | No | ACTIVE |
+-----+-----+-----+-----+-----+-----+
| 30.30.30.93 | WLC | 8.0.72.141 | - | No | ACTIVE |
+-----+-----+-----+-----+-----+-----+
| 30.30.30.97 | WLC | 8.0.72.141 | - | No | ACTIVE |
+-----+-----+-----+-----+-----+-----+
| 30.30.30.35 | WLC | 8.0.72.141 | - | No | ACTIVE |
+-----+-----+-----+-----+-----+-----+
| 30.30.30.58 | WLC | 8.0.72.141 | - | No | ACTIVE |
+-----+-----+-----+-----+-----+-----+
| 30.30.30.82 | WLC | 8.0.72.141 | - | No | ACTIVE |
+-----+-----+-----+-----+-----+-----+
| 30.30.30.84 | WLC | 8.0.72.141 | - | No | ACTIVE |
+-----+-----+-----+-----+-----+-----+
| 30.30.30.53 | WLC | 8.0.72.141 | - | No | ACTIVE |
+-----+-----+-----+-----+-----+-----+
```

cmxctl config data

To manage history data, use the **cmxctl config data** command.

cmxctl config data deleteAll

Syntax Description	deleteALL Deletes all client history and analytics raw data.				
Command Default	None.				
Command Modes	CMX admin user				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.5</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.5	This command was introduced.
Release	Modification				
Cisco CMX Release 10.5	This command was introduced.				

Example

This example shows how to delete client history and raw analytics data.

```
[cmxadmin@cmx]# cmxctl config data deleteAll
Do you wish to continue? All client history data, analytics data will be deleted and CMX
services will be restarted. [y/N]: y
Stopping all the services
All the Application services are stopped
Data Deletion Began
Deleting All Analytics Raw Visits Data
Deleting All Clients History Data
Starting all the services
All the Application services are restarted
```

cmxctl config devicelimitalert

To manage percent setting at which warning alert is generated for unique device count on Cisco CMX, use the **cmxctl config devicelimitalert** command.

cmxctl config devicelimitalert {**getalertpercent** | **setalertpercent** *percent*}

Syntax Description	getalertpercent Displays the current percent setting after which warning alert is generated for Unique Device Count on Cisco CMX.				
	setalertpercent Sets a percentage limit for Unique Device Count warning alert on Cisco CMX.				
	<i>percent</i> Enter the percent settings after which a warning alert is generated for Unique Device Count on Cisco CMX. Percent value can be between 1-99. The default value is 90%.				
Command Default	None.				
Command Modes	CMX admin user				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.6.2</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.6.2	This command was introduced.
Release	Modification				
Cisco CMX Release 10.6.2	This command was introduced.				
Usage Guidelines	This command should be run at the cmxadmin level.				

Example

The following example shows how to set percent setting after which a warning alert is generated for **Unique Device Count** on Cisco CMX:

```
[cmxadmin@cmx]# cmxctl config devicelimitalert setalertpercent
Percent after which Unique Device Alert gets generated [1-99] [90]: 50
Changed the Warning Alert Percent Setting for Device Count Successfully
```

Example

The following example shows how to display the percent setting for **Unique Device Count** warning alert on Cisco CMX:

```
[cmxadmin@cmx]# cmxctl config devicelimitalert getalertpercent
90
```

cmxctl config featureflags

To list and toggle feature flags, use the **cmxctl config featureflags** command.

```
cmxctl config featureflags {feature name} {true | false}
```

Syntax Description

service.featurename Name of the Cisco CMX service and feature.

- location.compactlocationhistory
- configuration.oi.host
- configuration.apimport
- location.ssidfilterpersistblockedmacs
- location.rogueapclienthistory
- location.filteredssidscleanupatmidnight
- nm脾b.cmxgrouping
- monit
- container.influxdbreporter
- nm脾b.autolearnssids
- configuration.highendbypass
- apiserver.enabled
- location.computelocthroughassociatedap
- analytics.queueuetime

true Enables the feature of the service.

false Disables the feature of the service

Command Default

None

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.6.2	This command was modified to add more location feature names.
Cisco CMX Release 10.2.2	This command was changed. The display default for analytics.sma was changed to false.
Cisco CMX Release 10.2.0	This command was introduced.

Example

The following example shows how to list the feature flags:

```
[cmxadmin@cmx]# cmxctl config featureflags
+-----+
| location.compactlocationhistory      | false |
+-----+
| configuration.oi.host                 | true  |
+-----+
| configuration.apimport                | false |
+-----+
| location.ssidfilterpersistblockedmacs | false |
+-----+
| location.rogueapclienthistory        | false |
+-----+
| location.filteredssidscleanupatmidnight | true  |
+-----+
| nmsplb.cmxgrouping                   | false |
+-----+
| monit                                 | true  |
+-----+
| container.influxdbreporter           | true  |
+-----+
| nmsplb.autolearnssids                 | true  |
+-----+
| configuration.highendbypass           | false |
+-----+
| apiserver.enabled                     | true  |
+-----+
| location.computelocthroughassociatedap | false |
+-----+
| analytics.queueuetime                 | false |
+-----+
```


cmxctl config fips

To enable, verify, and manage Federal Information Processing Standards (FIPS) mode, use the **cmxctl config fips** command.

cmxctl config fips {enable | status | verify}

Syntax Description	enable	Enables FIPS mode.
	status	Displays FIPS mode status.
	verify	Verifies that your CMX system is correctly configured to support FIPS mode.

Command Default By default, FIPS mode is disabled.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6	This command was introduced.

Usage Guidelines Cisco CMX supports the Federal Information Processing Standard 140-2 (FIPS 140-2). FIPS 140-2 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 140-2 compliant, you can enable FIPS. Once you do so, the system uses the cryptographic algorithms defined by the NIST for FIPS 140-2 for all encrypted communication between its internal and external components.



Note FIPS is a prerequisite to UCAPL mode. Enable and configure FIPS before running the **cmxctl config fips ucapl** command. See [cmxctl config fips ucaplmode](#), on page 44.

Cisco recommends that you run these commands before enabling FIPS mode:

- **cmxctl config certs...**—Removes old certificates and installs or imports new ones.
- **cmxctl config audit settings**—Configures CMX authentication settings.
- **cmxctl config certs importsyslogca <cert.pem>**—Imports a CA pem file for the remote syslog server.
- **cmxctl config fips verify**—Checks to see if your system is correctly configured for FIPS.



Note Note that the command **cmxctl config fips enable** is irreversible. You cannot disable FIPS mode after you enable the FIPS mode.

The following example shows how to check that your CMX system is correctly configured to support FIPS mode. In this example, the system lacks the strong password required for FIPS compliance.

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

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

Related Commands

Command	Description
cmxctl config auth	Sets strong CMX authentication requirements, which are required for FIPS and UCAPL modes.
cmxctl config certs	Creates, imports, and manages security key certificates, which are necessary for FIPS and UCAPL modes.

cmxctl config fips ipsecauth

To enable and manage pre-shared key (PSK) authentication in Federal Information Processing Standards (FIPS) mode, use the **cmxctl config fips ipsecauth** command.

cmxctl config fips ipsecauth { **disablepsk** | **enablepsk** | **status**}

Syntax Description	ipsecauth	Manages IPsec authentication.
	disablepsk	Disables pre-shared key (PSK) authentication.
	enablepsk	Enables PSK authentication.
	status	Displays the current IPsec authorization type. The default is pubkey .
Command Default	By default, pre-shared key (PSK) authentication is disabled.	
Command Modes	CMX admin user	
Command History	Release	Modification
	Cisco CMX Release 10.6	This command was introduced.

The following example shows how to enable pre-shared key (PSK) authentication.

```
[cmxadmin@cmx]# cmxctl config fips ipsecauth enablepsk
IPsec auth type changed to PSK.
IPsec is configured with PSK : U9u3Pr8agBoUQoP2bKtXtk555J1JxfNr
Configuring ipsec ....
In primary
Stopping strongSwan IPsec...
Starting strongSwan 5.6.2 IPsec [starter]...
```

cmxctl config fips ucaplmode

To enable, view status, or disable compliance with the U.S. Department of Defense Unified Capabilities Approved Products List (UCAPL) certification, use the **cmxctl config fips ucaplmode** command.

cmxctl config fips ucaplmode {enable | disable | status}

Syntax Description	enable	enable
	enable	Enables UCAPL over FIPS mode.
	disable	Disables UCAPL over FIPS mode.
	status	Displays UCAPL mode status.

Command Default By default, UCAPL mode is disabled.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6	This command was introduced.

Usage Guidelines 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, 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 disk encryption, among other restrictions.

Once UCAPL mode is enabled, the following authentication changes are made, if they are not already specified:

- Enable strong password : yes
- Minimum password length : 15
- Unsuccessful login attempts before account lock : 3
- Session timeout in minutes : 10

The following example shows how to enable UCAPL over FIPS mode:

```
[cmxadmin@cmx]# cmxctl config fips ucaplmode enable
UCAPL mode enabled.
```

The CMX processes restart.

Related Commands	Command	Description
	cmxctl config audit	Enables and manages audit logging, which is necessary for UCAPL mode.
	cmxctl config auth	Sets strong CMX authentication requirements, which are required for FIPS and UCAPL modes.

Command	Description
cmxctl config certs	Creates, imports, and manages security key certificates, which are necessary for FIPS and UCAPL modes.
cmxctl config fips	Enables FIPS mode, which is a prerequisite to enable UCAPL mode.
cmxos encryptdisk	Enables post-installation disk encryption of the CMX /opt partition, which is a prerequisite to enable UCAPL mode.

cmxctl config fips ucaplmode autobackup

To enable or disable an automatic backup that will run when UCAPL mode is enabled, use the **cmxctl config fips ucaplmode autobackup** command.

cmxctl config fips ucaplmode autobackup

Command Default By default, the CMX automatic backup is disabled. The backup duration is weekly.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6	This command was introduced.

Usage Guidelines All auto-backups are run weekly, on the day and hour you select.



Note You can configure the auto-backup without being in UCAPL mode, but it will not run until UCAPL mode is enabled.

The following example shows how to enable and configure an automatic backup for every Saturday night, while in UCAPL mode.

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

Do you want to enable it ? (yes/no) [yes]: yes
CMX Auto Backup frequency is weekly.
Please select day and hour of the week to run the auto-backup.

Day of the week: [0=Sunday, 1=Monday ... 6=Saturday] [0]: 6
Hour of the day: [0-23] [2]: 10
CMX auto-backup is now enabled.
Redirecting to /bin/systemctl restart crond.service
auto-backup will execute every Saturday at 10:10 AM
```

cmxctl config fips ucaplmode logFileAccess

To enable read/write access to configuration file, use the **cmxctl config fips ucaplmode logFileAccess** command.

cmxctl config fips ucaplmode logFileAccess

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.6	This command was introduced.

The **cmxctl config fips ucaplmode logFileAccess** command prompts you to enable file access logging:

```
[cmxadmin@cmx]# cmxctl config fips ucaplmode logFileAccess
Enable File Access Logging [yes / no] [no]: yes
Restarting Audit Service
...
```

cmxctl config fips ucaplmode logHTTPHeaders

To enable HTTP headers logging, use the **cmxctl config fips ucaplmode logHTTPHeaders** command.

cmxctl config fips ucaplmode logHTTPHeaders

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6	This command was introduced.

Usage Guidelines We recommend that you enable this command only if needed. Note that this command can degrade the performance of the system due to the excessive logging. Disable this command when not needed.

The **cmxctl config fips ucaplmode logHTTPHeaders** command prompts you to enable file access logging:

```
[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: 4061
Attempting to restart Haproxy
....Service Haproxy has successfully restarted
logHTTPHeaders is enabled.
```


cmxctl config gateway

To change the gateway configuration for cloud beacon management, use the **cmxctl config gateway** command.

```
cmxctl config gateway { cmx_cloud_url URL | show }
```

Syntax Description	cmx_cloud_url	Configure the cloud URL for Beacon Management.
	URL	Enter the cloud URL for Beacon Management.
	show	Displays the cloud URL configured for Beacon Management.
Command Default	None	
Command Modes	CMX admin user	
Command History	Release	Modification
	Cisco CMX Release 10.5	This command was introduced.

Examples

The following example shows how to display the gateway configuration for cloud beacon management:

```
[cmxadmin@cmx]# cmxctl config gateway show
CMX_CLOUD_SERVER: demo.com
```

cmxctl config get

To display configuration information for Cisco CMX services, use the **cmxctl config get** command.

```
cmxctl config get [analytics | cache_6378 | cache_6379 | cache_6380 | cache_6381 | cache_6382
| cache_6383 | cache_6385 | cache_6378 | cassandra | configuration | connect | database | haproxy
| hyperlocation | location | matlabengine | metrics | nmsplb]
```

Syntax Description

analytics	Performs analytics on calculated location data.
agent	Manages Cisco CMX system lifecycle. Starts, stops, and monitors all the services running in Cisco CMX.
cache_6378	Caches the service used by location service.
cache_6379	Caches the service used by location service.
cache_6380	Caches the service used by analytics service.
cache_6381	Caches the service used by analytics service.
cache_6382	Caches the service used by analytics service.
cache_6383	Caches the service used by analytics service.
cache_6385	Caches the service used by analytics service.
cassandra	Displays the cassandra database service used by the location service for historical data.
configuration	Configures nodes and clusters.
connect	Displays the connect services.
database	Displays the database service used by analytics and configuration service.
haproxy	Displays the TCP or HTTP load balancer gateway to all service APIs.
hyperlocation	Displays hyperlocation configuration.
location	Displays location service to compute location.
matlabengine	Provides access point heatmap for location service.
metrics	Collects system metrics.
nmsplb	Displays the load balancer service used for distributing Network Mobility Services Protocol (NMSP) messages to location services.

Command Default

The default command **cmxctl config get** displays configuration information for all supported services when executed without options.

Command Modes

CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.5	Additional services were documented.
	Cisco CMX Release 10.3.0	This command was introduced.

Examples

The following example shows how to display configuration information for the CMX analytics service.

```
[cmxadmin@cmx]# cmxctl config get analytics
{
  "services": {
    "analytics": {
      "maxdirectmemory": "1536M",
      "maxnewsizem": "400M",
      "mem": "1536M"
    }
  }
}
```

Optionally, you can filter the results by using one of the listed configuration keywords. For example:

```
[cmxadmin@cmx]# cmxctl config get cassandra
{
  "services": {
    "cassandra": {
      "keycachesize": "100",
      "maxnewsizem": "800M",
      "mem": "4096M"
    }
  }
}
[root@server]$ cmxctl config get cassandra maxnewsizem
{"maxnewsizem": "800M"}
```

cmxctl config heatmaps summary

To show the details of the heapmap from the location service, use the **cmxctl config heatmaps summary** command.

cmxctl config heatmaps summary

Command Default	None.	
Command Modes	CMX admin user	
Command History	Release	Modification
	Cisco CMX Release 10.4	This command was introduced.
Usage Guidelines	This command should be run at the cmxadmin level.	

cmxctl config hyperlocation mixmode

To manage mixed mode for hyperlocation for a specified floor, use the **cmxctl config hyperlocation mixmode** command.

cmxctl config hyperlocation mixmode *Floor ID* {**enable** | **disable**}

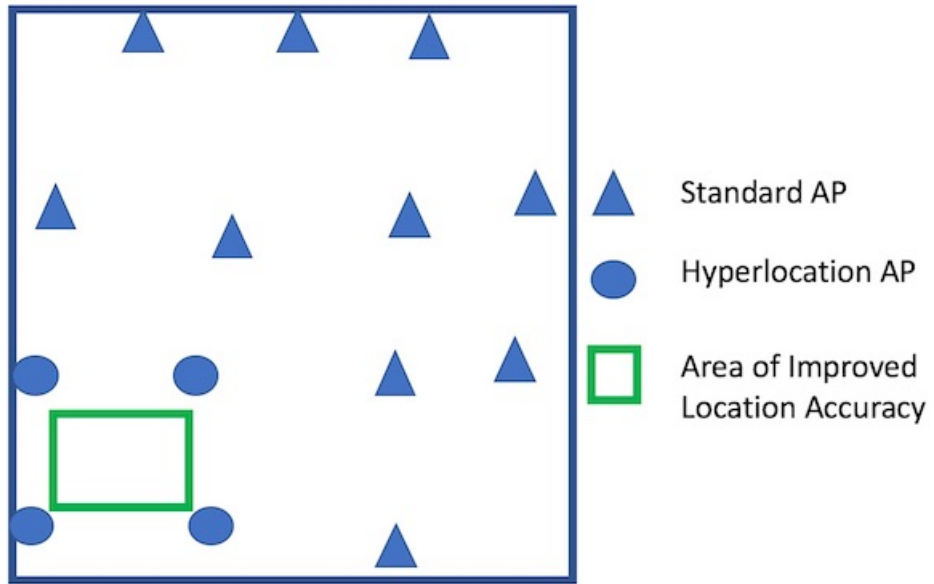
Syntax Description	<i>Floor ID</i> Provides the specific floor ID.				
	enable Enables mixed mode support for hyperlocation for the specified floor.				
	disable Disables mixed mode support for hyperlocation for the specified floor.				
Command Default	None				
Command Modes	CMX admin user				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.4</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.4	This command was introduced.
Release	Modification				
Cisco CMX Release 10.4	This command was introduced.				

Usage Guidelines We recommend that you use this command in a scenario where on a single floor there are both Hyperlocation enabled AP and non Hyperlocation APs. 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, when clients are at least 10M inside of the convex hull.

This command does not support the interspersation 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.

The following is an example of a supported deployment:

Figure 1: Supported Hyperlocation Mixed Mode Deployment



cmxctl config import

To import a map and Cisco Catalyst 9800 Wireless Controller from Cisco Prime Infrastructure, use the **cmxctl config import** command.

```
cmxctl config import {prime | status}
```

Syntax Description	prime Imports maps from Cisco Prime Infrastructure.
	status Shows import status.
Command Default	None.
Command Modes	CMX admin user

Examples

The following example shows how to import a map and controller from Cisco Prime Infrastructure:

```
[cmxadmin@cmx]# cmxctl config import prime

Please enter PI ip address: x.x.x.x
Please enter PI username [root]: root
Please enter PI password [Public123]:
Import successfully started from PI x.x.x.x. Check import status using cmxctl config
import status.
```

cmxctl config ipsec

To manage IP security (IPSec) protocol, use the **cmxctl config ipsec** command.

cmxctl config ipsec {**authtype** | **disable** | **enable** | **restart** | **start** | **status** | **stop**}

Syntax Description	
authtype	Changes IPSec authentication type.
disable	Disables IPSec protocol.
enable	Enables IPSec protocol.
restart	Restarts IPSec tunnel.
start	Starts IPSec tunnel.
status	Shows IPSec status.
stop	Stops IPSec status.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.1	This command was introduced.

Usage Guidelines The default authentication type for IPSec is “PUBKEY”/Public Key. It is set when you run the **cmxctl config ipsec enable** command.

Example

The following example shows how to enable IPSec:

```
[cmxadmin@cmx]# cmxctl config ipsec enable
Do you want to enable IPSec? (y/n) [n]: y
IPSec is enabled and Authtype set to PUBKEY
Configuring ipsec ...
In primary
Stopping strongSwan IPsec failed: starter is not running
Starting strongSwan 5.6.2 IPsec [starter]...
IPSEC tunnel established successfully with 192.0.2.1
```

The following example shows how to display the status of the IPSec service:

```
[cmxadmin@cmx]# cmxctl config ipsec status
IPSec is enabled
IPSec Authentication Type = Public Key (Certificate)

Security Associations (1 up, 0 connecting):
    rsyslog[2]: ESTABLISHED 18 seconds ago,
    192.0.2.1[cisco-cmx-ova-30]...192.0.2.3[cisco-cmx-ova-32]
```



```
rsyslog{2}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c549935a_i c02aee35_o
rsyslog{2}: 192.0.2.1/32 === 192.0.2.3/32
```

The following example shows how to change the authentication type:

```
[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]...
Failed to establish IPSEC tunnel with 192.0.2.3 (cisco-cmx-ova-32)
```

The following example shows how to restart the IPsec service:

```
[cmxadmin@cmx]# cmxctl config ipsec restart
Starting IPsec tunnel ...
Stopping strongSwan IPsec...
Starting strongSwan 5.6.2 IPsec [starter]...
establishing CHILD_SA rsyslog{2}
generating CREATE_CHILD_SA request 2 [ N(USE_TRANSP) SA No TSi TSr ]
sending packet: from 192.0.2.1[500] to 192.0.2.3[500] (272 bytes)
received packet: from 192.0.2.3[500] to 192.0.2.1[500] (208 bytes)
parsed CREATE_CHILD_SA response 2 [ N(USE_TRANSP) SA No TSi TSr ]
CHILD_SA rsyslog{2} established with SPIs c8553144_i c727bbd3_o and TS 10.30.114.175/32 ===
10.30.114.177/32
connection 'rsyslog' established successfully
IPsec tunnel established successfully
```

cmxctl config loginrate

To configure login rate limit, use the **cmxctl config loginrate** command.

cmxctl config loginrate {**disable** | **enable** | **resetall** | **resetuser***username* | **status**}

Syntax Description	Parameter	Description
	disable	Disables login rate limit.
	enable	Enables login rate limit.
	resetall	Resets login rate details for all the users.
	resetuser <i>username</i>	Resets login rate details for a specific user.
	status	Displays the login rate status as enabled or disabled.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.1	This command was introduced.

Example

The following example shows how to enable login rate limit:

```
[cmxadmin@cmx]# cmxctl config loginrate enable
Enter the allowed number of login failure for a user per source ip [3]: 3
Enter the number of source IPs for which login failure is to be maintained [3]: 3
Enter the total allowed number of login failure for a user [10]: 10
Login rate limit enabled
```

The following example shows how to disable login rate limit:

```
[cmxadmin@cmx]# cmxctl config loginrate disable
Login rate limit is disabled
```

The following example shows how to reset login rate limit for a specific user:

```
[cmxadmin@cmx]# cmxctl config loginrate reset admin
The user details have been reset.
```

cmxctl config manageacl

To manage CMX access control lists (ACLs), use the **cmxctl config manageacl** command.

cmxctl config manageacl {**add** | **disable** | **enable** | **status**}

Syntax Description	add	Adds an access control list.
	disable	Disables ACL authentication.
	enable	Enables ACL authentication.
	status	Displays access control list status information.

Command Default By default, access control lists are disabled.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6	This command was introduced.

Usage Guidelines When ACLs are enabled, only the servers added in the ACL will be allowed to access CMX through SSH or HTTPS.

The following example shows how to enable access control lists, and add servers to the ACL.

```
[cmxadmin@cmx]# cmxctl config manageacl enable

[cmxadmin@cmx]# cmxctl config manageacl add
inside aclAdd.
Enter the ip address to be added in the ACL: 168.172.12.18
Do you want to add more ip address in the ACL [Y/n]: Y
Enter the ip address to be added in the ACL: 172.19.35.122
Do you want to add more ip address in the ACL [Y/n]: n
```

The following example shows how to display access control list status information.

```
[cmxadmin@cmx]# cmxctl config manageacl status

ACL is enabled
The following ip addresses are allowed to access the CMX box.
Use add command to add the ipaddresses if the list is empty.
168.172.10.10
168.172.10.57
168.172.12.18
168.172.35.122
```

cmxctl config maps address

To set a directory path to an optional map address file, use the **cmxctl config maps address** command.

```
cmxctl config maps address --path filepath
```

Syntax Description	--path Sets the directory path to an optional map address file. See Usage Guidelines for more information. <i>filepath</i>
Command Default	None.
Command Modes	CMX admin user
Usage Guidelines	Use the cmxctl config maps address command to access an optional map address file that you can associate with a map. This is not a necessary step for maps you create in CMX and PI, but you may have a map from another source that requires a valid address.



Note The first entry in each line of the map address file should be the fully-qualified name and address in Campus>Building format. For example: My Campus>My Building, 123 Road St, San Jose CA 95137.

Command History	Release	Modification
	Cisco CMX Release 10.5	Additional keywords were documented.
	Cisco CMX Release 10.3.0	This command was introduced.

Examples

The following example shows how to set the path to a map address file, which you can then associate with a map.

```
[cmxadmin@cmx]# cmxctl config maps address --path /home/cmxadmin/campusPath.csv
cmxctl config maps address --path /home/cmxadmin/campusPath.csv
Now importing address for: North Campus>Building 9

Done importing addresses
```

cmxctl config maps aplist

To display a list of access points (APs) and their status for a specified floor, use the **cmxctl config maps aplist** command.

cmxctl config maps aplist [--active | --inactive] *floorID*

Syntax Description	<p>--active Optional. Display only the active access points (APs) on the specified floor.</p> <p>--inactive Optional. Display only the inactive access points (APs) on the specified floor.</p> <p><i>floorID</i> The identifying number for the floor. Use the cmxctl config maps floors command to see the Floor ID.</p>						
Command Default	All access points display for the designated floor.						
Command Modes	CMX admin user						
Usage Guidelines	<p>To see all the APs on a floor, use the cmxctl config maps aplist command without additional arguments.</p> <p>To get the Floor ID for a CMX floor map, use the cmxctl config maps floors command.</p>						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.5</td> <td>Additional keywords were documented.</td> </tr> <tr> <td>Cisco CMX Release 10.3.0</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.5	Additional keywords were documented.	Cisco CMX Release 10.3.0	This command was introduced.
Release	Modification						
Cisco CMX Release 10.5	Additional keywords were documented.						
Cisco CMX Release 10.3.0	This command was introduced.						

Examples

The following example shows how to list all the APs on the Registration Floor of Bld-4.

First, use the **cmxctl config maps floors** command to get the Location Floor ID for the floor you want to view:

```
[cmxadmin@cmx]# cmxctl config maps floors
```

Floor Name	Location Floor ID	Analytics Floor ID
North Campus>Bld-4>Registration	727035700041482593	35

Now run the **cmxctl config maps aplist** command, and paste in the Floor ID:

```
[cmxadmin@cmx]# cmxctl config maps aplist 72703570082593
```

Name	EthMacAddress	RadioMacAddress	FloorId	Status
CMX-AP05-7069	None	70:69:5a:51:48:40	72703570082593	INACTIVE
CMX-AP01-7070	40:01:7a:b2:c7:a2	70:70:8b:06:19:60	72703570082593	ACTIVE
CMX-AP02-7071	40:01:7a:b2:c8:86	70:70:8b:06:1d:e0	72703570082593	ACTIVE

```
+-----+-----+-----+-----+-----+
| CMX-AP06-7072 | 4c:77:6d:9e:61:9e | 70:69:5a:51:52:80 | 72703570082593 | ACTIVE |
+-----+-----+-----+-----+-----+
| CMX-AP03-7073 | 40:01:7a:b2:c7:92 | 70:70:8b:06:19:20 | 72703570082593 | ACTIVE |
+-----+-----+-----+-----+-----+
| CMX-AP04-7074 | 4c:77:6d:9e:61:04 | 70:69:5a:51:48:e0 | 72703570082593 | ACTIVE |
+-----+-----+-----+-----+-----+
```

cmxctl config maps buildings

To see a list of buildings for a CMX Campus or for all buildings, use the **cmxctl config maps buildings** command.

```
cmxctl config maps buildings [--campus campusname | --csv]
```

Syntax Description	
--campus	Optional. Restricts the list of buildings to a particular campus.
<i>campusname</i>	The name of the campus you would like to include.
--csv	Optional. Displays the results in comma-separated values (CSV) format, which can be cut and pasted into a spreadsheet.

Command Default Running the command without arguments will display all buildings on all campuses.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.5	Additional keywords were documented.
	Cisco CMX Release 10.3.0	This command was introduced.

Usage Guidelines Command *options* must follow the last command *keyword* with a space and two dashes. For example:

```
[root@server]# command keyword --option1 --option2.
```

 When you select the option `--csv`, the map information you specify is displayed in comma-separated values (CSV) format, which can be cut and pasted into a spreadsheet.

Examples

The following example shows how to display a list of all buildings, in CSV format. The output format is *Campus Name > Building Name, Location Building ID, Analytics Building ID*.

```
[cmxadmin@cmx]# cmxctl config maps buildings --csv
System Campus>TMT,749980497668473090,18
System Campus>LCN,727001546461545854,16
System Campus>PCH,769481534004431937,15
North Campus>Newtech Building,732849996352089441,13
```

The following example shows how to display a list of building maps for North Campus:

```
[cmxadmin@cmx]# cmxctl config maps buildings --campus North Campus
+-----+-----+-----+
| Building Name          | Location Building ID | Analytics Building ID |
+-----+-----+-----+
| North Campus>Newtech 1 | 727001546461544629  | 48                    |
+-----+-----+-----+
| North Campus>Newtech 2 | 725930212039482938  | 49                    |
+-----+-----+-----+
```

cmxctl config maps campuses

To see a list of your CMX Campuses, use the **cmxctl config maps campuses** command.

cmxctl config maps campuses [--csv]

Syntax Description	--csv Optional. Displays the results in comma-separated values (CSV) format, which can be cut and pasted into a spreadsheet.
---------------------------	-------------------------------------------------------------------------------------------------------------------------------------

Command Default	Running the command without arguments will display all campuses in table format.
------------------------	----------------------------------------------------------------------------------

Command Modes	CMX admin user
----------------------	----------------

Command History	Release	Modification
	Cisco CMX Release 10.5	Additional keywords were documented.
	Cisco CMX Release 10.3.0	This command was introduced.

Usage Guidelines	Command <i>options</i> must follow the last command <i>keyword</i> with a space and two dashes. For example: [root@server]# command keyword --option1 --option2.
-------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------

When you select the option --csv, the map information you specify is displayed in comma-separated values (CSV) format, which can be cut and pasted into a spreadsheet.

Examples

The following example shows how to display a list of campus maps:

```
[cmxadmin@cmx]# cmxctl config maps campuses

+-----+-----+-----+
| Campus Name | Location Campus ID | Analytics Campus ID |
+-----+-----+-----+
| North Campus | 727001546461544473 | 14 |
+-----+-----+-----+
| South Campus | 384920494820170003 | 15 |
+-----+-----+-----+
```

If you want the campus map to be displayed in CSV format, add the --csv flag:

```
[cmxadmin@cmx]# cmxctl config maps campuses --csv

North Campus,727001546461545275,14
South Campus,384920494820170003,15
```


cmxctl config maps delete

To delete a map, or all maps in your CMX network, use the **cmxctl config maps delete** command.

```
cmxctl config maps delete [--name mapname | --all]
```

Syntax Description

--name	Optional. Deletes a specific map.
<i>mapname</i>	The name of the map you want to delete.
--all	Optional. Deletes all CMX maps.

Command Default

The default for all delete options are not to confirm the delete.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.5	Additional keywords were documented.
Cisco CMX Release 10.3.0	This command was introduced.

Usage Guidelines

For all **cmxctl config maps delete** command options, you are asked to confirm the deletion.

If you enter the **cmxctl config maps delete** command without optional flags, you are asked to provide the map heirarchy in *campus-name>building-name>floor-name* format.

```
Please enter the hierarchy to be deleted (campus-name>building-name>floor-name):
```

Example

This example shows how to delete the Newtech 1 Security floor in North Campus:

```
[cmxadmin@cmx]# cmxctl config maps delete
Please enter the hierarchy to be deleted (campus-name>building-name>floor-name):
North Campus>Newtech 1>Security
map deleted.
```

This example shows how to delete the map named NorthCampus.

```
[cmxadmin@cmx]# cmxctl config maps delete --name NorthCampus
Confirm delete hierarchy: NorthCampus ? [y/N]: y
Map deleted.
```

cmxctl config maps floors

To list the floor maps in a selected campus, building, or all floors, use the **cmxctl config maps floors** command.

cmxctl config maps floors [--campus *mapname* --building *mapname* --csv]

Syntax Description

--campus Optional. Restricts the list of floors to a particular campus.

mapname The name of the campus you would like to include.

--building Optional. Restricts the list of floors to a particular building.

mapname The name of the building you would like to include.

--csv Optional. Displays the results in comma-separated values (CSV) format, which can be cut and pasted into a spreadsheet.

Command Default

None.

Command Modes

CMX admin user

Usage Guidelines

Command *options* must follow the last command *keyword* with a space and two dashes. For example:

```
[cmxadmin@server]# command keywords --option1 --option2.
```

When you select the option **--csv**, the map information you specify is displayed in comma-separated values (CSV) format, which can be cut and pasted into a spreadsheet.

Command History

Release	Modification
Cisco CMX Release 10.5	Additional keywords were documented.
Cisco CMX Release 10.3.0	This command was introduced.

Examples

The following example shows how to display a list of floor maps for North Campus, building A9:

```
[cmxadmin@cmx]# cmxctl config maps floors --campus North Campus --building A9
```

```
+-----+-----+-----+
| Floor Name           | Location Floor ID | Analytics Floor ID |
+-----+-----+-----+
| North Campus>A9>Main Floor | 615446507270015464 | 16                 |
+-----+-----+-----+
| North Campus>A9>Lab Floor  | 727001546461544650 | 17                 |
+-----+-----+-----+
| North Campus>A9>Offices Floor | 615447265700154640 | 18                 |
+-----+-----+-----+
```

cmxctl config maps import

To import CMX location maps, use the **cmxctl config maps import** command.

```
cmxctl config maps import --type {PI | FILE} --path importpath --override {yes | no} --importzones {yes | no}
```

Syntax Description	
--type {PI FILE}	Identifies the source of the map you want to import. <ul style="list-style-type: none"> • PI—Imports a Cisco Prime Infrastructure map. • FILE—Imports a maps archive file.
--path <i>importpath</i>	Designates the path to the map you want to import.
--override {yes no}	Resolves how the import should handle duplicate map names: <ul style="list-style-type: none"> • yes—Overwrites any duplicate map names. • no—Does not overwrite duplicate map names. See Usage Guidelines for more information.
--importzones {yes no}	This option resolves how the import should handle duplicate zone names: <ul style="list-style-type: none"> • yes—Overwrites any duplicate zone names. • no—Does not overwrite duplicate zone names. See Usage Guidelines for more information.

Command Default None.

Command Modes CMX admin user

Usage Guidelines

- When CMX accepts your request to import a map from Cisco Prime Infrastructure, you are prompted to answer the following questions. The defaults are in [brackets].

```
Please enter PI ip address:
Please enter PI username [root]:
Please enter PI password [Public123]:
```

- When the **--override** or **--importzones** options are set to yes, existing maps or zones with the same names will be overwritten by the import. If you select no, the import will fail if there are conflicting map or zone names. You will need to resolve the conflict by changing the name and importing it again.
- Starting from Cisco CMX Release 10.3.1, you must provide the full (absolute) path to the tar file when using the **cmxctl config maps import** command. For example:


```
/opt/cmx/srv/floormaps/Importfile.tar.gz .
```
- Command *options* must follow the last command *keyword* with a space and two dashes. For example:


```
[cmxadmin@server]# command keyword --option1 --option2.
```

Command History	Release	Modification
	Cisco CMX Release 10.5	Additional keywords were documented.
	Cisco CMX Release 10.3.1	The import keyword was modified.
	Cisco CMX Release 10.3.0	This command was introduced.

Examples

The following example shows how to import a map, overwriting any existing maps or zones with the same name:

```
[cmxadmin@cmx]# cmxctl config maps import --type PI --path  
/opt/Import_fdff5788ad650.tar.gz --override yes --importzones yes  
  
Please enter PI ip address: 168.172.206.3  
Please enter PI username [root]: root  
Please enter PI password [Public123]: *****  
Import successfully started from PI 168.172.206.3.
```

cmxctl config maps reprocessimage

When CMX floor map images occasionally become misaligned, use the **cmxctl config maps reprocessimage** command to realign them.

```
cmxctl config maps reprocessimage --imagename imagename
```

Syntax Description	--imagename Identify the image needing reprocessing.						
	<i>imagename</i> The name of the image you would like to reprocess.						
Command Default	None.						
Command Modes	CMX admin user						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.5</td> <td>Additional keywords were documented.</td> </tr> <tr> <td>Cisco CMX Release 10.3.0</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.5	Additional keywords were documented.	Cisco CMX Release 10.3.0	This command was introduced.
Release	Modification						
Cisco CMX Release 10.5	Additional keywords were documented.						
Cisco CMX Release 10.3.0	This command was introduced.						

Usage Guidelines Sometimes maps can become misaligned. When this happens, the **cmxctl config maps reprocess image** command reprocesses the image and realigns the map.

The default folder path for CMX maps is `/opt/cmx/srv/floormaps`.

Example

The following example shows how to reprocess floor tile images when they become misaligned:

```
[cmxadmin@cmx]# cmxctl config maps reprocessimage --imagename domain_2_147753.png
File domain_2_147753.png exists in /opt/cmx/srv/floormaps. Proceeding...
Image processing job submitted for domain_2_147753.png.
```

cmxctl config maps zones

To list the floor maps in a selected campus, building, or all floors, use the **cmxctl config maps floors** command.

cmxctl config maps zones [--campus *mapname* --building *mapname* --csv]

Syntax Description

--campus Optional. Restricts the list of floors to a particular campus.

mapname The name of the campus you would like to include.

--building Optional. Restricts the list of floors to a particular building.

mapname The name of the building you would like to include.

--csv Optional. Displays the results in comma-separated values (CSV) format, which can be cut and pasted into a spreadsheet.

Command Default

All zones display when the command is run without options.

Command Modes

CMX admin user

Usage Guidelines

Command *options* must follow the last command *keyword* with a space and two dashes. For example:

```
[root@server]# command keywords --option1 --option2.
```

When you select the option **--csv**, the map information you specify is displayed in comma-separated values (CSV) format, which can be cut and pasted into a spreadsheet.

Command History

Release	Modification
Cisco CMX Release 10.5	Additional keywords were documented.
Cisco CMX Release 10.3.0	This command was introduced.

Examples

The following example shows how to display a list of zones for North Campus Bld-4:

```
[cmxadmin@cmx]# cmxctl config maps floors --campus North Campus building Bld-4

[cmxadmin@cmx]# cmxctl config maps zones
+-----+-----+-----+
| Floor Name                | Zone Name | Analytics Zone ID |
+-----+-----+-----+
| North Campus>Bld-4>1st Floor | NOC      | 376                |
+-----+-----+-----+
| North Campus>Bld-4>1st Floor | School   | 375                |
+-----+-----+-----+
```

cmxctl config qlesspyworker

To manage qlesspyworker, use the **cmxctl config qlesspyworker** command.

cmxctl config qlesspyworker cleanRedis

Syntax Description	cleanRedis Removes stale and invalid qlesspyworker history data.				
Command Default	None.				
Command Modes	CMX admin user				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.5</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.5	This command was introduced.
Release	Modification				
Cisco CMX Release 10.5	This command was introduced.				

Example

```
[cmxadmin@cmx]# cmxctl config qlesspyworker cleanRedis
QlessHistoryCleanupTask started
Deleted 0 qless-job-history records that were idle for 1209600 seconds.
Found 0 SMA-job records, deleted all.
QlessHistoryCleanupTask completed
```

cmxctl config reload

To forcefully generate a configuration file, use the **cmxctl config reload** command.

cmxctl config reload

Command Default

None

Examples

The following example shows how to forcefully generate a configuration file:

```
[cmxadmin@cmx]# cmxctl config reload

2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: WARNING Skipping confd config file.
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/analytics.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/cassandra/cassandra-env.sh in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/cassandra/cassandra.yaml in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/collectd.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/configuration.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/connect.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/halo.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/haproxy.cfg in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/influxdb.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/location.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/matlabengine.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/nmsplb.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/nmspproxy.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/postgresql.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/redis_6379.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/redis_6380.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: INFO Target config
/opt/cmx/etc/redis_6381.conf in sync
2015-03-10T17:45:50Z cmx-vmdev117 -verbose[17174]: ERROR template:
redis.template.conf:15:20: executing "redis.template.conf" at <getv ($tag | printf ...>:
error calling getv: key does not exist
```


cmxctl config rfid timeout

To set the timeout for maintaining RFID tags in Cisco CMX, use the **cmxctl config rfid timeout** command.

```
cmxctl config rfid timeout {get |set value}
```

Syntax Description

get	Displays the timeout value.
set value	Sets the timeout value that Cisco CMX maintains RFID tags before expiring them. The time range is 60 to 10800 seconds. The default value is 300 seconds.

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.3.1	This command was introduced.

Usage Guidelines

We recommend that you set the RFID tag timeout value below 600 seconds. An ideal RFID tag timeout value is 300 seconds. The RFID timeout must be set to a range between 60 - 600 seconds irrespective of your longest RFID tag's chirp interval.

Example

The following example shows how to set the timeout for RFID tags, and then verify the setting:

```
[cmxadmin@cmx]# cmxctl config rfid timeout set
Need to include a timeout within 60 to 10800 seconds

[cmxadmin@server]# cmxctl config rfid timeout set 300

[cmxadmin@server]# cmxctl config rfid timeout get
300 seconds
```

cmxctl config set

To set a config key for a Cisco CMX service, use the **cmxctl config set** command.

```
cmxctl config set {analytics | cache_6378 | cache_6379 | cache_6380 | cache_6381 | cache_6382
| cache_6383 | cache_6385 | cache_6378 | cassandra | configuration | connect | database | haproxy
| hyperlocation | location | matlabengine | metrics | nmsplb}
```

Syntax Description

analytics	Performs analytics on calculated location data.
agent	Manages Cisco CMX system lifecycle. Starts, stops, and monitors all the services running in Cisco CMX.
cache_6378	Caches the service used by location service.
cache_6379	Caches the service used by location service.
cache_6380	Caches the service used by analytics service.
cache_6381	Caches the service used by analytics service.
cache_6382	Caches the service used by analytics service.
cache_6383	Caches the service used by analytics service.
cache_6385	Caches the service used by analytics service.
cassandra	Enables cassandra database service used by the location service for historical data.
configuration	Configures nodes and clusters.
connect	Enables connect services.
database	Enables the database service used by analytics and configuration service.
haproxy	Enables the TCP or HTTP load balancer gateway to all service APIs.
hyperlocation	Enables hyperlocation.
location	Enables location service to compute location.
matlabengine	Provides access point heatmap for location service.
metrics	Collects system metrics.
nmsplb	Enables the load balancer service used for distributing Network Mobility Services Protocol (NMSP) messages to location services.

Command Default	None.	
Command Modes	CMX admin user	
Command History	Release	Modification
	Cisco CMX Release 10.5	Additional options were documented.
	Cisco CMX Release 10.4	This command was introduced.

Example

This example shows how to generate a key for the service **location**.

```
[cmxadmin@cmx]# cmxctl config set location key 2512
{"key": "2512"}
Change will take effect on service restart.
```

Restart the service.

```
[cmxadmin@cmx]# cmxctl restart location
Done
The nodeagent service is currently running with PID: 3299
Attempting to restart Location
.....
Service Location has successfully restarted
```

To verify the key, use the **cmxctl config get location** command:

```
[cmxadmin@cmx]# cmxctl config get location
{
  "services": {
    "location": {
      "key": "2512",
      "maxdirectmemory": "1536M",
      "maxnewsize": "800M",
      "mem": "6144M"
    }
  }
}
```

cmxctl config smartlicense enable

To enable Smart License in Cisco CMX, use the **cmxctl config smartlicense enable** command.

cmxctl config smartlicense enable

Syntax Description This command has no arguments or keywords.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.3	This command was introduced.

Usage Guidelines A Cisco Smart account is mandatory to enable smart license. Once enabled, you cannot disable smart license.

Examples

The following example shows how to enable smart license:

```
[cmxadmin@server]# cmxctl config smartlicense enable
```

```
Once Smart License is Enabled, It cannot be disabled !!!
To use Smart License, you must first setup a Cisco Smart Account
Prerequisite: Please make sure you have smart account enabled before proceeding.
Do you want to Enable Smart License [yes/no] ? [yes] :
```

cmxctl config smartlicense register

To register Cisco CMX product instance with smart account, use the **cmxctl config smartlicense register** command.

cmxctl config smartlicense register

Syntax Description This command has no arguments or keywords.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.3	This command was introduced.

Usage Guidelines Use the product instance registration token ID from CSSM tool to register product instance.

Examples

The following example shows how to register product instance:

```
[cmxadmin@server]# cmxctl config smartlicense register
```

Copy the product instance registration Token Id from CSSM tool and paste it below

Please Enter Token Id : **XYZ**

```
Do you want to use your Hostname as Product instance Name [yes/no] ? [no]: yes
Registration started with Token Id : XYZ
Registration is in progress ...
```

```
Product Instance Registered Successfully
```

cmxctl config smartlicense status

To check the smart license status of Cisco CMX, use the **cmxctl config smartlicense status** command.

cmxctl config smartlicense status

Syntax Description This command has no arguments or keywords.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.3	This command was introduced.

Usage Guidelines Use this command to check the license compliance status and smart account details.

Examples

The following example shows how to check smart license status:

```
[cmxadmin@server]# cmxctl config smartlicense status
Registration Status : Registered
Registration Date : Thu Oct 22 00:15:58 PDT 2020

License Compliance : Out of Compliance

Out of Compliance Start Date : Thu Oct 22 00:16:01 PDT 2020
Smart Account Name : InternalTestDemoAccount.cisco.com
Virtual Account : CMX_Test

Product Instance Name : CMX Virtual Platform

Is Authorization Failed : False
```

cmxctl config smartlicense renewauthorization

To renew authorization manually, use the **cmxctl config smartlicense renewauthorization** command.

Syntax Description This command has no arguments or keywords.

```
cmxctl config smartlicense renewauthorization
```

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.3	This command was introduced.

Usage Guidelines Use this command to manually renew the authorization of Smart License in Cisco CMX by communicating with CSSM.

Examples

The following example shows how to renew authorization manually:

```
[cmxadmin@server]# cmxctl config smartlicense renewauthorization  
  
Do you want to Renew Authorization Manually [yes/no] ? [no]: yes  
Authorization Renewal is in progress ..-  
  
Product Authorization Renewed Successfully
```

cmxctl config smartlicense renewregistration

To renew Cisco CMX product registration manually, use the **cmxctl config smartlicense renewregistration** command.

cmxctl config smartlicense renewregistration

Syntax Description This command has no arguments or keywords.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.3	This command was introduced.

Usage Guidelines Use this command to manually renew the registration ID and certificate with CSSM. This is optional as Cisco CMX automatically does this from backend.

Examples

The following example shows how to renew product registration manually:

```
[cmxadmin@server]# cmxctl config smartlicense renewregistration

Do you want to Renew Registration Manually [yes/no] ? [no] : yes
Registration Renewal is in progress ...

Product Registration Renewed Successfully
```


cmxctl config smartlicense reregister

To re-register Cisco CMX product instance manually, use the **cmxctl config smartlicense reregister** command.

cmxctl config smartlicense reregister

Syntax Description This command has no arguments or keywords.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.3	This command was introduced.

Usage Guidelines Use this command to perform a forceful re-registration to override any existing registered instances. This deletes previously reported data in the Smart Account related to that particular instance.

Examples

The following example shows how to re-register product instance:

```
[cmxadmin@server]# cmxctl config smartlicense reregister
```

```
Re-register will override existing registered instance if any
```

```
Existing data like Reported license,Count etc. if any will be lost from Smart Account
Do you want to Re-register product instance Manually [yes/no] ? [no]: yes
```

```
Copy the product instance registration Token Id from CSSM tool and paste it below
```

```
Please Enter Token Id : XYZ
```

```
Do you want to use your Hostname as Product Instance Name [yes/no] ? [no]: yes
```

```
Re-registration started with Token Id : XYZ
```

```
Re-registration is in progress ...
```

```
Product Instance Re-registered Successfully
```

cmxctl config smartlicense deregister

To deregister product instance manually, use the **cmxctl config smartlicense deregister** command.

cmxctl config smartlicense deregister

Syntax Description This command has no arguments or keywords.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.3	This command was introduced.

Usage Guidelines Use this command to deregister Cisco CMX product instance from CSSM.

Examples

The following example shows how to deregister product instance:

```
[cmxadmin@server]# cmxctl config smartlicense deregister
Do you want to de-register this product instance [yes/no] ? [no] : yes
fee-registration is in progress ...

Product Instance De-registered Successfully
```

cmxctl config smartlicense secondaryudi

To configure secondary UDI on Cisco CMX primary for a High Availability setup, use the **cmxctl config smartlicense secondaryudi** command.

cmxctl config smartlicense secondaryudi

Syntax Description This command has no arguments or keywords.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.3	This command was introduced.

Usage Guidelines Use the secondary UDI and serial number to configure secondary UDI in Cisco CMX primary setup.

Examples

The following example shows how to configure secondary UDI:

```
[cmxadmin@server]# cmxctl config smartlicense secondaryudi  
Please enter secondary's UDI : VMware Virtual Platform  
  
Please enter secondary's serial number : 123ABC-XXX-YYY
```

cmxctl config tls

To update the supported Transport Layer Security (TLS) version in haproxy, use the **cmxctl config tls** command.

```
cmxctl config tls { show | settings }
```

Syntax Description	show	Displays the configured TLS versions.
	settings	Configures minimum and maximum versions of TLS protocol.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 11.1.0	This command was introduced.

Usage Guidelines We recommend that you use the TLSV1.3. Use his command to change the TLS setting for haproxy. For example, to use TLS v1.2, run the command to update or override the default setting. This configuration is applicable only for haproxy and port 443.

Example

The following example shows how to display and update the TLS protocol version.

```
[cmxadmin@server]# cmxctl config tls show
Configured TLS versions:
TLS Min Version = TLSv1.3
TLS Max Version = TLSv1.3
```

```
[cmxadmin@server]# cmxctl config tls settings
TLS Min version [TLSv1.2 (2)/ TLSv1.3 (3) ]: [3]: 2
TLS Max version [TLSv1.2 (2)/ TLSv1.3 (3) ]: [3]: 3
```

```
Following TLS protocol values will be changed.
  TLS Min Version = TLSv1.2
  TLS Max Version = TLSv1.3
```

```
Cisco recommends using TLSv1.3 only.
Do you still want to enable TLSv1.2? This action will require a Haproxy service restart.
[y/N]:
```

cmxctl config uptimethreshold

To configure system uptime threshold, use the **cmxctl config uptimethreshold** command.

```
cmxctl config uptimethreshold { getthresholddays | setthresholddays value }
```

Syntax Description

getthresholddays	Displays uptime threshold in days to generate an alert.
setthresholddays value	Sets uptime threshold, in days, to generate an alert. The default setting for system uptime threshold is 90 days. The valid range is 1 to 365 days.

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.6.3	This command was introduced.

Usage Guidelines

Use this command to configure a threshold for system uptime. An alert is generated when the system uptime crosses the configured threshold value.

Examples

The following example shows how to set the system uptime threshold:

```
[cmxadmin@cmx]# cmxctl config uptimethreshold setthresholddays
Days after which alerts gets generated [1-365] [90]: 100
Changed the Threshold Days Setting for System Uptime Successfully.
```

cmxctl config verify

To verify the Cisco Connected Mobile Experiences (Cisco CMX) installation and configuration, use the **cmxctl config verify** command.

cmxctl config verify

Command Default

None.

Command Modes

CMX admin user

Examples

The following example shows how to verify the Cisco CMX installation and configuration:

```
[cmxadmin@cmx]# cmxctl config verify
Verifying node configuration...
NetworkManager: unrecognized service
Consul v0.4.1
Consul Protocol: 2 (Understands back to: 1)
confd 0.6.0
+-----+-----+-----+-----+
| module | check | passed | msg
|
+=====+=====+=====+=====+
| netman_stopped | NetworkManager service is not | Success |
|
| | running | |
|
+-----+-----+-----+-----+
--+
| matlabengine | http://matlabengine.service.co | Failed | check the log files
under |
| | nsul:5577/api/services/matlabengine/status | | /opt/cmx/var/log
|
+-----+-----+-----+-----+
| database | connect to database port:5432 | Success |
|
+-----+-----+-----+-----+
| consul_dns | 127.0.0.1 (consul) is present | Success |
|
| | as dns server in | |
|
| | /etc/resolv.conf | |
|
+-----+-----+-----+-----+
--+
| etchost_hacks | consul service hostnames not | Success |
|
| | static in /etc/hosts | |
|
+-----+-----+-----+-----+
| analytics | http://analytics.service.consul | Failed | check the log files
under |
| | 1:5556/api/services/analytics/ | | /opt/cmx/var/log
|
```

```

| | status | |
|
+-----+-----+-----+-----+
| hostname_ping | ping to hostname:cmx-master-1 | Success |
|
+-----+-----+-----+-----+
--+
| location | http://location.service.consul | Failed | check the log files
under |
| | :5555/api/services/location/st | | /opt/cmx/var/log
|
| | atus | |
|
+-----+-----+-----+-----+
--+
| confd_installed | Confd is installed | Success |
|
+-----+-----+-----+-----+
| consul_installe | Consul is installed | Success |
|
| d | | |
|
+-----+-----+-----+-----+
--+
| nmsplb | http://nmsplb.service.consul:6 | Failed | check the log files
under |
| | 001/api/services/nmsplb/status | | /opt/cmx/var/log
|
+-----+-----+-----+-----+
| configuration | http://configuration.service.c | Failed | check the log files
under |
| | onsul:6000/api/services/config | | /opt/cmx/var/log
|
| | uration/status | |
|
+-----+-----+-----+-----+
| cassandra | connect to cassandra port:9042 | Success |
|
+-----+-----+-----+-----+

```

cmxctl debug

To create a debug tarball in the current directory, use the **cmxctl debug** command.

cmxctl debug

Command Default	None.	
Command Modes	CMX admin user	
Command History	Release	Modification
	Cisco CMX Release 10.4	This command is depreciated.

Usage Guidelines The debug tarball that is created will be approximately 300 MB in size, and takes at 90 seconds to complete. This command should to be run using the cmxadmin (non-root) account. This commnd is depreciated in Cisco CMX release 10.4 and we recommend that you use **cmxos techsupport** command.

Examples

The following example shows how to create a debug tarball in the current directory:

```
[cmxadmin@cmx]# cmxctl debug
running locally
Dumping debug information...
[localhost] Executing task 'dump_config'
cp: cannot stat `/opt/cmx/share/upgrade.answers': No such file or directory
[localhost] Executing task 'dump_state'
running 'ps aux'
running 'ifconfig -a'
running 'cmxctl status'
running 'ulimit -a'
running 'ps -u root,postgres -o %cpu,%mem,cmd'
running 'netstat -o -n -a'
running 'df -h'
running 'ntpdate -d 172.19.28.250'
running 'consul members'
[localhost] Executing task 'dump_apis'
getting /api/config/v1/clusters
getting /api/config/v1/nodes
[localhost] Executing task 'dump_hosts'
pinging configuration.service.consul
pinging location.service.consul
pinging 6379.cache.service.consul
pinging 6380.cache.service.consul
pinging 6381.cache.service.consul
pinging database.service.consul
pinging analytics.service.consul
pinging halo.service.consul
Done.
```


cmxctl disable

To disable a service, use the **cmxctl disable** command.

```
cmxctl disable {consul | qllesspyworker | cassandra | iodocs | cache_6382 | cache_6383 | cache_6380
| cache_6381 | cache_6384 | cache_6385 | influxdb | metrics | confd | cache_6379 | cache_6378 |
haproxy | database | analytics | connect | gateway | location | configuration | matlabengine |
hyperlocation | nmsplb | agent }
```

Syntax	Description
analytics	Performs analytics on calculated location data.
agent	Manages Cisco CMX system lifecycle. starts, stops, and monitors all the services running in Cisco CMX.
cache_6378	Caches the service used by location service.
cache_6379	Caches the service used by location service.
cache_6380	Caches the service used by analytics service.
cache_6381	Caches the service used by analytics service.
cache_6382	Caches the service used by analytics service.
cache_6383	Caches the service used by analytics service.
cache_6385	Caches the service used by analytics service.
cassandra	Enables cassandra database service used by the location service for historical data.
confd	Internal service.
configuration	Configures nodes and clusters.
connect	Enables connect services.
consul	Internal service.
database	Enables the database service used by analytics and configuration service.
haproxy	Enables the TCP or HTTP load balancer gateway to all service APIs.
hyperlocation	Enables hyperlocation.
location	Enables location service to compute location.
matlabengine	Provides access point heatmap for location service.
metrics	Collects system metrics.

nmsplb	Enables the load balancer service used for distributing Network Mobility Services Protocol (NMSP) messages to location services.
influxdb	Enables database services used for storing statistics from various services.
iodocs	Enables online document service for REST API offered by various services.
qlesspyworker	Internal service.
gateway	Enables gateway services that establishes secure bidirectional communication with Cisco CMX Cloud applications.

Command Default None

Command Modes CMX admin user

Examples

The following example shows how to disable the cassandra database service:

```
[cmxadmin@cmx]# cmxctl disable cassandra
Done
The nodeagent service is currently running with PID: 31776
Stopping cassandra process...
Done
Successfully shutdown cassandra Process.
```

cmxctl dump

To create a configuration tarball in the current directory, use the **cmxctl dump** command.

cmxctl dump

Command Default

None

Command Modes

CMX admin user

Examples

The following example shows how to create a configuration tarball in the current directory:

```
[cmxadmin@cmx]# cmxctl dump
running locally
Dumping configuration information...
[localhost] Executing task 'dump_config'
Done.
```

cmxctl enable

To enable a service, use the **cmxctl enable** command.

```
cmxctl enable {consul | qllesspyworker | cassandra | iodocs | cache_6382 | cache_6383 | cache_6380
| cache_6381 | cache_6384 | cache_6385 | influxdb | metrics | confd | cache_6379 | cache_6378 |
haproxy | database | analytics | connect | gateway | location | configuration | matlabengine |
hyperlocation | nmsplb | agent }
```

Syntax	Description
analytics	Performs analytics on calculated location data.
agent	Manages Cisco CMX system lifecycle. starts, stops, and monitors all the services running in Cisco CMX.
cache_6378	Caches the service used by location service.
cache_6379	Caches the service used by location service.
cache_6380	Caches the service used by analytics service.
cache_6381	Caches the service used by analytics service.
cache_6382	Caches the service used by analytics service.
cache_6383	Caches the service used by analytics service.
cache_6384	Caches the service used by analytics service.
cache_6385	Caches the service used by analytics service.
cassandra	Enables cassandra database service used by the location service for historical data.
confd	Internal service.
configuration	Configures nodes and clusters.
connect	Enables connect services.
consul	Internal service.
database	Enables the database service used by analytics and configuration service.
haproxy	Enables the TCP or HTTP load balancer gateway to all service APIs.
hyperlocation	Enables hyperlocation.
location	Enables location service to compute location.
matlabengine	Provides access point heatmap for location service.

metrics	Collects system metrics.
nmsplb	Enables the load balancer service used for distributing Network Mobility Services Protocol (NMSP) messages to location services.
influxdb	Enables database services used for storing statistics from various services.
iodocs	Enables online document service for REST API offered by various services.
qlesspyworker	Internal service.
gateway	Enables gateway services that establishes secure bidirectional communication with Cisco CMX Cloud applications.

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.6	This command was introduced in a release prior to Cisco CMX Release 10.6.

Examples

The following example shows how to enable analytics service:

```
[cmxadmin@cmx]# cmxctl enable analytics
The nodeagent service is not running.
Agent is not running, starting it now.
Starting nodeagent Process...
Retrying..
Done
Started nodeagent service with PID: 31027
```

cmxctl heterarchy

To manage the deployment hierarchy, use the **cmxctl heterarchy** command.

cmxctl heterarchy {**backup** | **rebuild** | **repair** | **restore** | **retire** | **verify**}

Syntax Description	
backup	Backs up the deployment hierarchy.
rebuild	Rebuilds the deployment hierarchy.
repair	Repairs the deployment hierarchy.
restore	Restores the deployment hierarchy.
retire	Retires the deployment hierarchy.
verify	Verifies the deployment hierarchy.

Command Default None

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.2	This command was introduced.

Example

The following example shows how to verify the heterarchy:

```
[cmxadmin@cmx]# cmxctl heterarchy verify
Verifying heterarchy...
Checking user levels
Heterarchy is healthy.
```

cmxctl influxdb wipe

To wipe the influx database, use the **cmxctl influxdb wipe --silent** command.

cmxctl influxdb wipe --silent

Syntax Description	silent Silently wipe the influx database				
Command Default	None.				
Command Modes	CMX admin user				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.3</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.3	This command was introduced.
Release	Modification				
Cisco CMX Release 10.3	This command was introduced.				

The following example shows how to wipe the influx database:

```
[cmxadmin@cmx]# cmxctl influxdb wipe
This command will wipe the Influx database. All system metric data will be erased.
Do you want to continue?: y
Stopping influxdb Process...
executing shutdown
Retrying..
Retrying...
Retrying....
Done
Successfully shutdown influxdb Process.
Cleaning Influx database directories
Configuring InfluxDB
```

cmxctl jobs

To configure recurring background jobs, use the **cmxctl jobs** command.

```
cmxctl jobs { cancel jobname | list | run jobname | runnow jobname}
```

Syntax Description	
cancel <i>jobname</i>	Cancels a scheduled job.
list	Lists all the scheduled jobs.
run <i>jobname</i>	Runs a job at a specified time.
runnow <i>jobname</i>	Triggers a one-time run of the job.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.2	This command was introduced.

Usage Guidelines The Apache Cassandra database stores location history data. Pruning should be performed to maintain disk usage. Cisco CMX 10.2 introduces the option to prune database size. The default disk-pruning task runs at an interval of 90 days. You can also use the `cmxctl jobs runnow cleanupcassandra` command to run an on-demand job of cleaning up the Cassandra database, which is a normal scheduled task that runs once every two days.

Examples

The following example shows how to run a background job:

```
[cmxadmin@cmx]# cmxctl jobs run LocationIndexCleanup  
submitted the job, verify using cmxctl jobs list.
```


cmxctl metrics notification

To generate notification metrics for a Cisco Connected Mobile Experiences (Cisco CMX) file, use the **cmxctl metrics notification** command.

cmxctl metrics notification

Command Default

None

Command Modes

CMX admin user

Usage Guidelines

The **notification** keyword provides metrics for notification.

Examples

The following example shows how to generate metrics for a Cisco CMX file:

```
[cmxadmin@cmx]# cmxctl metrics notification
+-----+-----+-----+-----+-----+
| EndPoint | Success | Failure | SuccessRate |
FailureRate |
+=====+=====+=====+=====+=====+
+-----+-----+-----+-----+-----+
```

cmxctl restart

To restart a Cisco Connected Mobile Experiences (Cisco CMX) service, use the **cmxctl restart** command.

```
cmxctl restart {consul | qllesspyworker | cassandra | iodocs | cache_6382 | cache_6383 | cache_6380
| cache_6381 | cache_6384 | cache_6385 | influxdb | metrics | confd | cache_6379 | cache_6378 |
haproxy | database | analytics | connect | gateway | location | configuration | matlabengine |
hyperlocation | nmsplb | agent }
```

Syntax Description		
	analytics	Performs analytics on calculated location data.
	agent	Manages Cisco CMX system lifecycle. Starts, stops, and monitors all the services running in Cisco CMX.
	cache_6378	Caches the service used by location service.
	cache_6379	Caches the service used by location service.
	cache_6380	Caches the service used by analytics service.
	cache_6381	Caches the service used by analytics service.
	cache_6382	Caches the service used by analytics service.
	cache_6383	Caches the service used by analytics service.
	cache_6385	Caches the service used by analytics service.
	cassandra	Enables cassandra database service used by the location service for historical data.
	confd	Internal service.
	configuration	Configures nodes and clusters.
	connect	Enables connect services.
	consul	Internal service.
	database	Enables the database service used by analytics and configuration service.
	haproxy	Enables the TCP or HTTP load balancer gateway to all service APIs.
	hyperlocation	Enables hyperlocation.
	location	Enables location service to compute location.
	matlabengine	Provides access point heatmap for location service.
	metrics	Collects system metrics.

nmsplb	Enables the load balancer service used for distributing Network Mobility Services Protocol (NMSP) messages to location services.
influxdb	Enables database services used for storing statistics from various services.
iodocs	Enables online document service for REST API offered by various services.
qlesspyworker	Internal service.
gateway	Enables gateway services that establishes secure bidirectional communication with Cisco CMX Cloud applications.

Command Default None

Command Modes CMX admin user

Examples

The following example shows how to restart a Cisco CMX service:

```
[cmxadmin@cmx]# cmxctl restart database
Done
The nodeagent service is currently running with PID: 16718
Stopping postgres Process...
Successfully shutdown postgres Process.
Starting postgres Process...
Done
Started postgres service with PID: 25702
Exception while notifying CE
```

cmxctl stack

To generate the jstack for a java service, use the **cmxctl stack** command.

```
cmxctl stack {cmx_service}
```

Syntax Description	cmx_service Lists all Cisco CMX services. The services include: location, analytics, configuration, matlabengine, and nmsplb.
---------------------------	--------------------------------------------------------------------------------------------------------------------------------------

Command Default	None
------------------------	------

Command Modes	CMX admin user
----------------------	----------------

Command History	Release	Modification
	Cisco CMX Release 10.2	This command was introduced.

cmxctl start

To start a Cisco Connected Mobile Experiences (Cisco CMX) service, use the **cmxctl start** command.

```
cmxctl start {consul | qllesspyworker | cassandra | iodocs | cache_6382 | cache_6383 | cache_6380
| cache_6381 | cache_6384 | cache_6385 | influxdb | metrics | confd | cache_6379 | cache_6378 |
haproxy | database | analytics | connect | gateway | location | configuration | matlabengine |
hyperlocation | nmsplb | agent }
```

Syntax	Description
analytics	Performs analytics on calculated location data.
agent	Manages Cisco CMX system lifecycle. starts, stops, and monitors all the services running in Cisco CMX.
cache_6378	Caches the service used by location service.
cache_6379	Caches the service used by location service.
cache_6380	Caches the service used by analytics service.
cache_6381	Caches the service used by analytics service.
cache_6382	Caches the service used by analytics service.
cache_6383	Caches the service used by analytics service.
cache_6385	Caches the service used by analytics service.
cassandra	Enables cassandra database service used by the location service for historical data.
confd	Internal service.
configuration	Configures nodes and clusters.
connect	Enables connect services.
consul	Internal service.
database	Enables the database service used by analytics and configuration service.
haproxy	Enables the TCP or HTTP load balancer gateway to all service APIs.
hyperlocation	Enables hyperlocation.
location	Enables location service to compute location.
matlabengine	Provides access point heatmap for location service.
metrics	Collects system metrics.

nmsplb	Enables the load balancer service used for distributing Network Mobility Services Protocol (NMSP) messages to location services.
influxdb	Enables database services used for storing statistics from various services.
iodocs	Enables online document service for REST API offered by various services.
qlesspyworker	Internal service.
gateway	Enables gateway services that establishes secure bidirectional communication with Cisco CMX Cloud applications.

Command Default None

Command Modes CMX admin user

Examples

The following example shows how to display the status for the consul service:

```
[cmxadmin@cmx]# cmxctl start consul
Done
The nodeagent service is currently running with PID: 16718
Done
The analytics service is already running with pid: 1099
Done
Exception while notifying CE
Done
The location service is already running with pid: 16005
Done
Exception while notifying CE
Done
The configuration service is already running with pid: 16165
Done
Exception while notifying CE
Done
The matlabengine service is already running with pid: 1251
Done
Exception while notifying CE
Done
The nmsplb service is already running with pid: 1377
Done
Exception while notifying CE
```

cmxctl status

To view the status of one or all Cisco Connected Mobile Experiences (Cisco CMX) services, use the **cmxctl status** command.

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

Syntax	Description
analytics	Performs analytics on calculated location data.
agent	Manages Cisco CMX system lifecycle. starts, stops, and monitors all the services running in Cisco CMX.
cache_6378	Caches the service used by location service.
cache_6379	Caches the service used by location service.
cache_6380	Caches the service used by analytics service.
cache_6381	Caches the service used by analytics service.
cache_6382	Caches the service used by analytics service.
cache_6383	Caches the service used by analytics service.
cache_6385	Caches the service used by analytics service.
cassandra	Enables cassandra database service used by the location service for historical data.
confd	Internal service.
configuration	Configures nodes and clusters.
connect	Enables connect services.
consul	Internal service.
database	Enables the database service used by analytics and configuration service.
haproxy	Enables the TCP or HTTP load balancer gateway to all service APIs.
hyperlocation	Enables hyperlocation.
location	Enables location service to compute location.
matlabengine	Provides access point heatmap for location service.
metrics	Collects system metrics.

nmsplb	Enables the load balancer service used for distributing Network Mobility Services Protocol (NMSP) messages to location services.
influxdb	Enables database services used for storing statistics from various services.
iodocs	Enables online document service for REST API offered by various services.
qlesspyworker	Internal service.
gateway	Enables gateway services that establishes secure bidirectional communication with Cisco CMX Cloud applications.

Command Default None.

Command Modes CMX admin user

Usage Guidelines After installing the ISO file on the Cisco MSE 3355 or 3365, use the **cmxctl status** command to check if the CMX services are running. If they are not running, use the **cmxctl start** command.

Examples

The following example shows how to display the status for the consul service:

```
[cmxadmin@cmx]# cmxctl status consul
Done
The nodeagent service is currently running with PID: 6190
+-----+-----+-----+-----+
| Host          | Service      | Status  | Uptime (HH:mm) |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Analytics    | Running | 5 days, 05:49  |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Cache_6378   | Running | 5 days, 05:52  |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Cache_6379   | Running | 5 days, 05:49  |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Cache_6380   | Running | 5 days, 05:49  |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Cache_6381   | Running | 5 days, 05:49  |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Cache_6382   | Running | 5 days, 05:49  |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Cache_6383   | Running | 5 days, 05:49  |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Cache_6385   | Running | 5 days, 05:49  |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Cassandra    | Running | 5 days, 05:51  |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Confd        | Running | 5 days, 05:49  |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Configuration | Running | 5 days, 05:49  |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Connect      | Running | 5 days, 05:49  |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Consul       | Running | 5 days, 05:52  |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Database     | Running | 5 days, 05:52  |
```



```
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Haproxy      | Running | 5 days, 05:49 |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Hyperlocation | Running | 5 days, 05:47 |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Influxdb     | Running | 5 days, 05:49 |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Iodocs       | Running | 5 days, 05:50 |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Location     | Running | 5 days, 05:49 |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Matlabengine | Running | 5 days, 05:48 |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Metrics      | Running | 5 days, 05:49 |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Nmsplb      | Running | 5 days, 05:47 |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | Qlesspyworker | Running | 5 days, 05:50 |
+-----+-----+-----+-----+
| CMX-LowEnd-200 | gateway     | Running | 5 days, 05:50 |
+-----+-----+-----+-----+
```

cmxctl stop

To shut down a Cisco Connected Mobile Experiences (Cisco CMX) service, use the **cmxctl stop** command.

```
cmxctl stop { analytics | agent | cache_6378 | cache_6379 | cache_6380 | cache_6381 | cache_6382
| cache_6383 | cache_6385 | cassandra | configuration | confd | consul | database | haproxy |
location | matlabengine | metrics | nmsplb | influxdb | iodocs | qllesspyworker }
```

Syntax Description

analytics	Performs analytics on calculated location data.
agent	Manages Cisco CMX system lifecycle. starts, stops, and monitors all the services running in Cisco CMX.
cache_6378	Caches the service used by location service.
cache_6379	Caches the service used by location service.
cache_6380	Caches the service used by analytics service.
cache_6381	Caches the service used by analytics service.
cache_6382	Caches the service used by analytics service.
cache_6383	Caches the service used by analytics service.
cache_6385	Caches the service used by analytics service.
cassandra	Enables cassandra database service used by the location service for historical data.
confd	Internal service.
configuration	Configures nodes and clusters.
connect	Enables connect services.
consul	Internal service.
database	Enables the database service used by analytics and configuration service.
haproxy	Enables the TCP or HTTP load balancer gateway to all service APIs.
hyperlocation	Enables hyperlocation.
location	Enables location service to compute location.
matlabengine	Provides access point heatmap for location service.
metrics	Collects system metrics.

nmsplb	Enables the load balancer service used for distributing Network Mobility Services Protocol (NMSP) messages to location services.
influxdb	Enables database services used for storing statistics from various services.
iodocs	Enables online document service for REST API offered by various services.
qlesspyworker	Internal service.

Command Default

The services are running.

Command Modes

CMX admin user

Examples

The following example shows how to stop the analytics service:

```
[cmxadmin@cmx]# cmxctl stop analytics
Done
The nodeagent service is currently running with PID: 16987
Stopping analytics Process...
Service analytics with pid: 19095
Retrying..
Done
Successfully shutdown analytics Process.
```

cmxctl trace mac

To enable MAC address tracing, use the **cmxctl trace mac** command.

```
cmxctl trace mac { add | delete | status }
```

Syntax Description	add Add MAC address for tracing				
	delete Delete MAC address for tracing				
	status Display MAC address tracing settings				
Command Default	None.				
Command Modes	CMX admin user				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.3</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.3	This command was introduced.
Release	Modification				
Cisco CMX Release 10.3	This command was introduced.				

Examples

The following example shows how to enable MAC address tracing:

```
[cmxadmin@cmx]# cmxctl trace mac status
+-----+
| MAC Address |
+-----+
| 3c:a9:f4:6c:ee:44 |
+-----+
| ac:37:43:4b:cc:2f |
+-----+
| 3c:a9:f4:6c:5a:ac |
```

cmxctl trace status

To display current trace levels of each CMX service, use the **cmxctl trace status** command.

cmxctl trace status

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.3	This command was introduced.

Examples

The following example shows how to display current tarce levels:

```
[cmxadmin@cmx]# cmxctl trace mac status
+-----+
| MAC Address      |
+-----+
| 00:01:02:03:04:05 |
+-----+
```

cmxctl trace update

To update the trace level of a Cisco CMX service, use the **cmxctl trace update** command.

```
cmxctl trace update {service service-to-update | level tracelevel | [INFO | DEBUG]}
```

Syntax Description	service <i>service-to-update</i>	Configure service to update.
	level <i>tracelevel</i>	Configure trace level [INFO DEBUG]
Command Default	None.	
Command Modes	CMX admin user	
Command History	Release	Modification
	Cisco CMX Release 10.x	This command was introduced.

cmxctl users

To list or to configure Cisco Connected Mobile Experiences (Cisco CMX) users using the CLI, use the **cmxctl users** command.

```
cmxctl users { list | passwd username | logout userid}
```

Syntax Description	list	Lists all the current users.
	passwd	Sets the password for a user.
	<i>username</i>	Username of a user in Cisco CMX.
	logout <i>userid</i>	Account of a user in Cisco CMX.
Command Default	None.	
Command Modes	CMX admin user	

Examples

The following example shows how to list Cisco CMX users using the CLI:

```
[cmxadmin@cmx]# cmxctl users list
+-----+-----+-----+
| Username | Full Name | Roles |
+-----+-----+-----+
| monitor | Monitor User | Read Only |
+-----+-----+-----+
| admin | Admin User | Admin |
+-----+-----+-----+
```

cmxctl users unlock

To unlock CMX access for a CLI or GUI user after they have been locked out, use the **cmxctl users unlock** command.

```
cmxctl users unlock {cli username | gui username}
```

Syntax Description

cli *username* Unlocks the command line interface (CLI) user.

gui *username* Unlocks the graphical user interface (GUI) user.

Command Default

By default, active accounts will automatically unlock in **30 minutes**. Dormant accounts—accounts inactive for 35 days or more—do not automatically unlock.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.5	This command was introduced.

Usage Guidelines

The CMX admin can unlock accounts before the 30-minute expiry time.

The following example shows how to unlock the CMX user interface user *someguy*:

```
[cmxadmin@cmx]# cmxctl users unlock gui someguy
Account unlocked successfully
```


cmxctl version

To know the Cisco Connected Mobile Experiences (Cisco CMX) version, use the **cmxctl version** command.

cmxctl version

Command Default

None.

Command Modes

CMX admin user

Examples

The following example shows how to display version information for Cisco CMX:

```
[cmxadmin@cmx]# cmxctl version
Build Version : 10.1.0-27
Build Time : 2015-05-05 03:06:45.437430
-----
Name : cmx-ng-container
Commit Count : 17
Short Hash : bf20ec1
-----
Name : cmx-ng-location
Commit Count : 5
Short Hash : efc84fa
-----
Name : cmx-ng-ui
Commit Count : 5
Short Hash : d793df7
-----
Name : cmx-ova
Build Time : Fri Feb 20 06:34:38 UTC 2015
-----
```

cmxloc delete

To delete a location accuracy test in Cisco CMX, use the **cmxloc delete** command.

cmxloc delete

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.4	This command was introduced.

Usage Guidelines

This command should be run at the cmxadmin level.

cmxloc download

To view the link to download the log files, use the **cmxloc download** command.

cmxloc download *test name*

Command Default

None

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.4	This command was introduced.

Usage Guidelines

This command will move the log files into a location and can be downloaded using a browser.

cmxloc find

To search for the MAC address provided and return all the current attributes for the device, use the **cmxloc find** command.

cmxloc find *MAC address*

Syntax Description	<i>MAC Address</i> MAC address of the device.				
Command Default	None.				
Command Modes	CMX admin user				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.4</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.4	This command was introduced.
Release	Modification				
Cisco CMX Release 10.4	This command was introduced.				
Usage Guidelines	This command should be run at the cmxadmin level.				

cmxloc list

To list the accuracy tests in Cisco CMX, use the **cmxloc list** command.

cmxloc list

Command Default

None

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.4	This command was introduced.

Usage Guidelines

This command should be run at the cmxadmin level.

Example

The following example shows how to list all Cisco CMX accuracy tests:

```
[cmxadmin@cmx]# cmxloc list
```

Name	Status	MAC Address	Comp Freq (s)	Avg Error (m)	90% (m)	50% (m)
FB1	PAUSED	98:07:2d:2a:11:fa	0.0	0.0	0.0	0.0
Test1	FINISHED	98:07:2d:2a:11:fa	61.0	2.45	3.23	1.93
Test2	FINISHED	98:07:2d:2a:11:fa	33.25	4.36	6.27	3.44

cmxloc monitor

To monitor the location accuracy test, use the **cmxloc monitor** command.

cmxloc monitor *MAC Address*

Syntax Description

MAC Address MAC address of the device.

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.4	This command was introduced.

Usage Guidelines

This command searches for a client and returns the attributes. The command monitors for any location changes and will update the screen for the new location attributes. Press the enter key to terminate the command execution.

cmxloc start

To start a location accuracy test, use the **cmxloc start** command.

cmxloc start *MAC Address Test Name X, Y Locations Time*

Syntax Description	<i>MAC Address</i> MAC address of the device to run the location accuracy test.				
	<i>Test Name</i> Name of the new location accuracy test.				
	<i>X, Y Locations</i> X and Y location information.				
	<i>Time</i> Estimated time to run the test.				
Command Default	None				
Command Modes	CMX admin user				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.4</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.4	This command was introduced.
Release	Modification				
Cisco CMX Release 10.4	This command was introduced.				
Usage Guidelines	This command triggers the location accuracy test.				

cmxos addswap

To add a 10 GB space to the operating system, use the **cmxos addswap** command.

cmxos addswap

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes CMX admin user

Usage Guidelines This command should be run at the root user level.

Examples

The following example shows how to increase disk space in the operating system:

```
[cmxadmin@cmx]# cmxos addswap
10485760+0 records in
10485760+0 records out
10737418240 bytes (11 GB) copied, 29.6845 s, 362 MB/s
Setting up swapspace version 1, size = 10485756 KiB
no label, UUID=2734f069-e687-4635-b2d6-9381241bc7ee
swap added, run system info to verify
[root@cmx-vmdev146 ~]#
```


cmxos adminui

To start, stop, and restart the administrator UI, use the **cmxos adminui** command.

```
cmxos adminui {start | stop | restart}
```

Syntax Description

start Starts the administrator UI.

stop Stops the administrator UI.

restart Restarts the administrator UI.

Command Default

None

Command Modes

CMX admin user

Command History

Release

Modification

Cisco CMX Release 10.2 This command was introduced.

Example

The following example shows how to stop the administrator UI:

```
[cmxadmin@cmx]# cmxos adminui stop  
Stopping adminui...
```

cmxos apiserver disable

To disable Cisco CMX API server, use the **cmxos apiserver disable** command.

cmxos apiserver disable

Syntax Description	disable Disables the Cisco CMX API server.				
Command Default	None.				
Command Modes	CMX admin user				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.4</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.4	This command was introduced.
Release	Modification				
Cisco CMX Release 10.4	This command was introduced.				

Example

The following example shows how to disable the Cisco CMX API server:

```
[cmxadmin@cmx]# cmxos apiserver disable
```

```
Disabling CMX API Server...
```

```
Stopping CMX API Server...
```

cmxos apiserver enable

To enable Cisco CMX API server, use the **cmxos apiserver enable** command.

cmxos apiserver enable

Syntax Description	enable Enables the Cisco CMX API server.				
Command Default	None.				
Command Modes	CMX admin user				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco CMX Release 10.4</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco CMX Release 10.4	This command was introduced.
Release	Modification				
Cisco CMX Release 10.4	This command was introduced.				

Example

The following example shows how to enable the Cisco CMX API server:

```
[cmxadmin@cmx]# cmxos apiserver enable  
Enabling CMX API Server...  
Starting CMX API Server...
```

cmxos apiserver reset

To reset the configuration of the Cisco CMX API server, use the **cmxos apiserver reset** command.

cmxos apiserver reset

Syntax Description	reset Resets CMX API Server configuration.				
Command Default	None				
Command Modes	CMX admin user				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.4</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.4	This command was introduced.
Release	Modification				
Cisco CMX Release 10.4	This command was introduced.				

Example

The following example shows how to reset the Cisco CMX API server:

```
[cmxadmin@cmx]# cmxos apiserver reset
Resetting CMX API Server...
```

cmxos apiserver restart

To restart Cisco CMX API server, use the **cmxos apiserver restart** command.

cmxos apiserver restart

Syntax Description	restart Restarts the Cisco CMX API server.				
Command Default	None				
Command Modes	CMX admin user				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco CMX Release 10.4</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco CMX Release 10.4	This command was introduced.
Release	Modification				
Cisco CMX Release 10.4	This command was introduced.				

Example

The following example shows how to start the Cisco CMX API server:

```
[cmxadmin@cmx]# cmxos apiserver restart  
Restarting CMX API Server...
```

cmxos apiserver start

To start Cisco CMX API server, use the **cmxos apiserver** command.

cmxos apiserver { **start** | **stop** | **restart** | **enable** | **disable** | **status** | **user**}

Syntax Description	
start	Starts the Cisco CMX API server.
stop	Stops the Cisco CMX API server.
restart	Restarts the Cisco CMX API server.
enable	Enables the Cisco CMX API server.
disable	Disables the Cisco CMX API server.
status	Displays the current status of the Cisco CMX API server.
user	Sets the userid and password for the CMX API Server.

Command Default None

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.4	This command was introduced.

Example

The following example shows how to start the Cisco CMX API server:

```
[cmxadmin@cmx]# cmxos apiserver start
Starting CMX API Server...
```

cmxos apiserver status

To view the status of Cisco CMX API server, use the **cmxos apiserver status** command.

cmxos apiserver status

Syntax Description	status Displays the current status of the Cisco CMX API server.				
Command Default	None.				
Command Modes	CMX admin user				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.4</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.4	This command was introduced.
Release	Modification				
Cisco CMX Release 10.4	This command was introduced.				

Example

The following example shows how to view the status of Cisco CMX API server:

```
[cmxadmin@cmx]# cmxos apiserver status
+-----+
| CMX API Server Status |
+-----+-----+
| Configuration | Enabled |
+-----+-----+
| Status | Running |
+-----+-----+
| Uptime | 0 days 00:01:17 |
+-----+-----+
```

cmxos apiserver stop

To stop the CMX API Server, use the **cmxos apiserver stop** command.

cmxos apiserver stop

Syntax Description	stop Stops the Cisco CMX API server.				
Command Default	None				
Command Modes	CMX admin user				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.4</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.4	This command was introduced.
Release	Modification				
Cisco CMX Release 10.4	This command was introduced.				

Example

The following example shows how to start the Cisco CMX API server:

```
[cmxadmin@cmx]# cmxos apiserver stop
Stopping CMX API Server...
```


cmxos apiserver user

To manage user IDs and passwords for the Cisco CMX API server, use the **cmxos apiserver user** command.

cmxosapiserveruser {**add** *userid password* | **delete** *userid* | **list**}

Syntax Description

add	Adds a new CMX API server user.
<i>userid</i>	Enter a user ID (username) for the new CMX API server user.
<i>password</i>	Enter a temporary password for the new user.
delete <i>userid</i>	Deletes the specified user ID.
list	Displays CMX API server user IDs.

Command Default

None

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.5	This command was modified.
Cisco CMX Release 10.4	This command was introduced.

Example

The following example shows how to add a new user for the Cisco CMX API server:

```
[cmxadmin@cmx]# cmxos apiserver user add
Please enter the userid for the CMX API Server: user1
Please enter the password for the CMX API Server: password
Please re-enter the password for the CMX API Server: password
Restarting CMX API Server...
Stopping CMX API Server...
Starting CMX API Server...
Successfully updated userid/password and restarted the CMX API Server
```

The following example shows how to list Cisco CMX API server users:

```
[cmxadmin@cmx]# cmxos apiserver user list
+-----+
| User ID |
+-----+
| admin   |
+-----+
| user1   |
+-----+
```

cmxos backup

To back up a node, use the **cmxos backup** command.

cmxos backup {path | i | all | help}

Syntax Description	
--path DIRECTORY	Path where the backup file will be created.
-i, --include_only TEXT	Backups selected parts only. Options are database, cache, cassandra, influxdb, consul, floormaps, licenses, setup, and connect images.
--all	Includes InfluxDB data in backup bundle. If specific options are not selected, only the following services are included in the backup bundle: confd, database, cache, cassandra, floormaps, licenses, setup, and connect images.
--HELP	Shows the help content.

Command Default None.

Command Modes CMX admin user

Usage Guidelines This command should to be run using the cmxadmin (non-root) account. 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.

Examples

The following example shows how to back up a node:

```
[cmxadmin@cmx]# cmxos backup
Please enter the path for backup file [/tmp]:
[17:43:50] Preparing for backup...
[17:43:50] Backup Database...
[17:43:51] Backup Cache...
[17:43:51] Backup Cassandra...
[17:43:53] Backup InfluxDb...
[17:43:53] Backup Consul...
[17:43:53] Backup Floormaps...
[17:43:53] Backup node configuration...
[17:43:59] Creating tar file..
[17:43:59] Done Backup. Created backup file
/tmp/cmx_backup_cmx-vmdev117_2015_03_10_17_43.tar.gz
```

cmxos backupsched

To schedule a Cisco CMX backup capability, use the **cmxos backupsched** command.

cmxos backupsched {**schedule** | **unschedule** | **show**}

Syntax Description		
schedule	Schedules a backup.	
unschedule	Unscheduled a backup.	
show	Displays the current backup schedule.	

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.2	This command was introduced.

Usage Guidelines You can use this command to schedule a daily or weekly backup. For the daily backup schedule, you must select an hour based on the UTC time of the system. For the weekly backup schedule, enter a day of the week to schedule the backup. After the scheduled backup is completed, the CMX backup is available at /home/cmxadmin/cmxbakups.

You can create custom scripts to run specific commands during the scheduled backup. The pre-script /home/cmxadmin/bin/preScheduleBackup.sh helps you to run commands before the scheduled backup. The post-script /home/cmxadmin/bin/postScheduleBackup.sh helps to run the commands after the backup is completed.

cmxos benchmark disk

To benchmark disk performance, use the **cmxos benchmark disk** command.

```
cmxos benchmark disk [ --verbose ]
```

Syntax Description

--verbose Prints full output.

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.2	This command was introduced.

Usage Guidelines

You must manually stop all Cisco CMX services before executing this command.

Examples

The following example shows how to verify the disk performance:

```
[cmxadmin@cmx]# cmxos benchmark disk
This process will check disk performance on /opt/cmx/srv/
You must stop all CMX services manually before running this command
Do you want to continue?: yes
Running disk performance...this may take a while...please wait...
READ IOPS: 6085, WRITE IOPS: 2024
```

cmxos changedate

To update system date and time, use the **cmxos changedate** command.

cmxos changedate

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.6	This command was introduced.

Usage Guidelines

Enter the new date and time in YYYY-mm-dd hh:mm:ss format.

Example

The following example shows how to update system date and time:

```
[cmxadmin@cmx]# cmxos changedate  
Enter Date and Time(YYYY-mm-dd hh:mm:ss) : 2018-11-26 03:51:00  
2018-11-26 03:51:00  
System date and time changed successfully
```

cmxos checkpostgresdatasize

To display postgres data size, use the **cmxos checkpostgresdatasize** command.

cmxos checkpostgresdatasize

Command Default	None.
------------------------	-------

Command Modes	CMX admin user
----------------------	----------------

Command History	Release	Modification
	Cisco CMX Release 10.3	This command was introduced.

Examples

The following example shows how to display postgres data size:

```
[cmxadmin@cmx]# cmxos checkpostgresdatasize
651488 /opt/cmx/srv/postgres
```

cmxos clean

To clean up files on CMX, use the **cmxos clean** command.

```
cmxos clean {find | normal | {delete}}
```

Syntax Description

find Find files over 1 Gigabyte in size.

normal List files which can be cleaned.

delete Remove the files listed.

Command Default

None.

Command History

Release	Modification
Cisco CMX Release 10.3	This command was introduced.

Examples

The following example shows how to search for large files:

```
[cmxadmin@cmx]# cmxos clean find
Starting search for large files
Size: 1.96G File: /tmp/cmx_backup_CMX-LowEnd-200_2017_01_18_17_56.tar.gz
Size: 2.36G File: /tmp/cmx_backup_CMX-LowEnd-200_2017_03_14_11_16.tar.gz
Size: 2.43G File: /tmp/cmx_backup_CMX-LowEnd-200_2017_03_20_14_36.tar.gz
Size: 2.32G File: /tmp/cmx_backup_CMX-LowEnd-200_2017_01_18_18_00.tar.gz
Size: 1.45G File: /var/log/maillog-20170212.gz
Size: 2.63G File: /var/log/maillog-20170205.gz
Size: 6.84G File: /home/cmxadmin/cmx_backup_CMX-LAC-210_2017_03_23_22_09.tar.gz
Size: 1.17G File: /home/cmxadmin/CISCO_CMX-10.3.0-58.cmx
Completed search for large files

[cmxadmin@cmx]# cmxos clean normal
Files which can be removed in: /opt/cmx/var/log
/opt/cmx/var/log/adminui/adminui.pid
/opt/cmx/var/log/adminui/webui.ans
/opt/cmx/var/log/agent/server.log.3
/opt/cmx/var/log/agent/server.log.1
/opt/cmx/var/log/agent/server.log.5
/opt/cmx/var/log/agent/server.log.2
/opt/cmx/var/log/agent/server.log.4
/opt/cmx/var/log/backup.log.2
/opt/cmx/var/log/backup.log.3
/opt/cmx/var/log/setup.log.8
/opt/cmx/var/log/setup.log.7
/opt/cmx/var/log/cmxjobs.log.1
/opt/cmx/var/log/cmxjobs.log.5

[cmxadmin@cmx]# cmxos clean normal --delete
Are you sure you wish to remove files? [y/N]: y
Removing files in: /opt/cmx/var/log
Remove: /opt/cmx/var/log/agent/server.log.2
Remove: /opt/cmx/var/log/agent/server.log.1
Remove: /opt/cmx/var/log/cmxjobs.log.5
Remove: /opt/cmx/var/log/cmxjobs.log.2
```

```
Remove: /opt/cmx/var/log/cmxjobs.log.4  
Remove: /opt/cmx/var/log/cmxjobs.log.1  
Remove: /opt/cmx/var/log/cmxjobs.log.3
```


cmxos configure

To configure the network and operating system parameter, use the **cmxos configure** command.

cmxos configure

Command Default

None

Command Modes

CMX admin user

Usage Guidelines

This command should to be run at the root user level. You can use the --force option to force a fresh configuration if the device is already configured.

Examples

The following example shows how to configure the network and operating system parameters:

```
[cmxadmin@cmx]# cmxos configure --force
*** The system is already configured
*****
Checking if the machine meets required specification...
*****
+-----+-----+
| Check | expected | actual | Result |
+-----+-----+-----+-----+
| memory | 8GB | 25GB | ? |
+-----+-----+-----+-----+
| cpu | 4 | 8 | ? |
+-----+-----+-----+-----+
| disk | 50GB | 51GB | ? |
+-----+-----+-----+-----+
| hostname | rfc compliant hostname | cmx-vmdev146 | ? |
+-----+-----+-----+-----+
```

cmxos date

To show current date information for the system, use the **cmxos date** command.

cmxos date

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.6.1	This command was introduced.

Usage Guidelines

Run this command to see the current time and status of the system.

Example

The following example shows how to display current date information for the system:

```
[cmxadmin@cmx]# cmxos date
Current Date = Mon Mar 25 12:15:48 PDT 2019
Current UTC Date = Mon Mar 25 19:15:48 UTC 2019
NTP Server = *10.22.243.5
Offset: Time difference between server and client = -0.969
Delay: Round trip between server and client = 0.924
Jitter: Difference between two samples = 1.070
```

cmxos encryptdisk

To encrypt CMX data on the /opt partition, use the **cmxos encryptdisk** command.

cmxos encryptdisk

Command Default Encryption is not enabled.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.5	This command was introduced.

Usage Guidelines Use this command when your security protocol requires encryption of CMX data. For more information about this task, refer to Cisco CMX Configuration Guide, release 10.6.

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.



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.

Example

The following example show how to enable encryption after CMX installation:

```
[cmxadmin@cmx]# cmxos encryptdisk
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.

Press Enter.

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.

WARNING!

=====

This will overwrite data on /opt irrevocably.
Are you sure? (Type uppercase yes): **YES**

Enter a passphrase.

Enter passphrase:

Verify passphrase:

Command successful.

Opening /opt ...

Enter passphrase for /opt:

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

Press Enter.

Please enter passphrase for disk opt on /opt!:

cmxos etchosts

To configure etc hosts, use the **cmxos etchosts** command.

cmxos etchosts

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.2	This command was introduced.

Usage Guidelines This command will run and returns no status.

Examples

```
[cmxadmin@cmx]# cmxos etchosts
[cmxadmin@server]# cmxos etchosts --help
Usage: __main__.py etchosts [OPTIONS]
    Configure /etc/hosts properly
Options:
    --help  Show this message and exit.
```

cmxos firstboot

To set up the Cisco Connected Mobile Experiences (Cisco CMX) again, use the **cmxos firstboot** command.

cmxos firstboot

Command Default

None.

Command Modes

CMX admin user

Usage Guidelines

This command should be run at the root user level. You can use the `--force` option to force a fresh configuration if the device is already configured.

Examples

The following example shows how to set up Cisco CMX again:

```
[cmxadmin@cmx]# cmxos firstboot  
Not first boot...Exiting...
```

cmxos fixhaproxy

To verify the HA proxy permissions on Cisco Connected Mobile Experiences (Cisco CMX), use the **cmxos fixhaproxy** command.

cmxos fixhaproxy

Command Default

None.

Command Modes

CMX admin user

Usage Guidelines

This command should be run at the root user level.

Examples

The following example shows how to verify HA proxy permissions:

```
[cmxadmin@cmx]# cmxos fixhaproxy  
Raising haproxy setcap...
```

cmxos health

To check the health of a Cisco CMX system, use the **cmxos health** command.

```
cmxos health {filedescriptors | ntp}
```

Syntax Description	
filedescriptors	Checks the CMX file descriptors for issues.
ntp	Checks the CMX NTP systems for issues.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.5	This command was modified.
	Cisco CMX Release 10.2	This command was introduced.

Usage Guidelines The **cmxos health filedescriptors** command returns the total number of open file descriptors. The **cmxos health ntp** command returns the status of the CMX Network Time Protocol (NTP) systems.

Examples

The following example shows how to check the health of a Cisco CMX system:

```
[cmxadmin@cmx]# cmxos health filedescriptors
2195 total file descriptors open
```

```
[cmxadmin@server]# cmxos health ntp
NTP Synchronization error:
unsynchronised
  time server re-starting
  polling server every 8 s
```


cmxos inventory

To show full inventory of a node, use the **cmxos inventory** command.

cmxos inventory

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.2	This command was introduced.

Examples

The following example shows how to view the inventory details:

```
[cmxadmin@cmx]# cmxos inventory
UDI: AIR-MSE-3365-K9 Serial Number - FCH1904V055

State of the RAID array: Healthy and working normally
Capacity of the RAID array: 1.088 TB
Type of disks in RAID array: Spinning Disk Drive
All chassis fans operating normally
One of the power supplies in the chassis has failed or it has not been installed/connected
Disk Capacity: 1.0T
Disk space used: 33.2G
Memory installed: 63.00G
CPUs installed: 20
CPU Type: Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz
Server uptime: 6 Hours, 59 Minutes, 44 Seconds
Server boot time: Mon, 27 Mar 2017 16-44-36
Number of server reboots: 1
```

cmxos kill

To kill services, use the **cmxos kill** command.

cmxos kill silent

Syntax Description	--silent Silently kills services without confirmation.
---------------------------	---------------------------------------------------------------

Command Default	None.
------------------------	-------

Command Modes	CMX admin user
----------------------	----------------

Command History	Release	Modification
	Cisco CMX Release 10.2	This command was introduced.

Examples

The following example shows how to kill CMX services:

```
[cmxadmin@cmx]# cmxos kill
This command will force kill all CMX processes, for dev use only
Do you want to continue?:
```

cmxos monit

To manage the monitoring of Cisco CMX services, use the **cmxos monit** command.

cmxos monit {**configure** | **start** | **stop** | **wipe**}

Syntax Description	
configure	Configures the default monitor settings.
start	Enables monitored services.
stop	Enables monitored services.
wipe	Deletes the default monitoring settings.
	Note To reset to the default monitoring settings, use the cmxos monit configure command

Command Default Disabled.

Command Modes CMX admin user

Command History	Release	Modification
	Release 10.2.0	This command was introduced.

Example

The following example shows how to display the monitoring settings:

```
[cmxadmin@cmx]# cmxos monit configure
Deleting all monit configurations....
Configuring monit mail settings...
Configuring monit OS settings...
Configuring monit CMX services settings...
```

The following example shows how to enable monitoring of Cisco CMX services:

```
[cmxadmin@cmx]# cmxos monit start
Starting monit:
```

cmxos ntp

To configure authenticated and un-authenticated Network Time Protocol (NTP) servers on CMX, use the **cmxos ntp** command.

```
cmxos ntp {auth | {password | servers} | clear | restart | type}
```

Syntax Description

auth password	Configures local authentication password.
auth servers	Configures Authenticate NTP Servers.
clear	Clears the NTP server configuration.
restart	Restarts the NTP services.
status	Displays the NTP server status.
type	Configure NTP authentication type.

Command Default

By default, no NTP servers are configured.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.6	This command was introduced.

The following example shows how to set authenticate NTP server(s) using **cmxos ntp type** command.

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

Changing the NTP Type = Authenticated
Enter local password:
Repeat for confirmation:
Password changed and host key/cert file generated successfully.

Enter hostname / IP for NTP Server #1 (blank to skip) []: 1.2.3.4
Please enter complete path of exported IFF (encrypted) key file: /tmp/iffkey
Checking if server 1.2.3.4 is reachable ...
OK
Key file successfully saved as ntpkey_iffkey_ntpserver.3747444855
NTP Server added successfully

Enter hostname / IP for NTP Server #2 (blank to skip) []:
NTP Service restarted successfully
```

cmxos openports

To open ports, based on a node rule, use the **cmxos openports** command.

```
cmxos openports { analytics | location | database }
```

Syntax Description

analytics Adds a 10-GB swap space to a node.

location Configures the network and operating system parameters.

database Sets up the Cisco Connected Mobile Experiences (Cisco CMX) database again.

Command Default

None.

Command Modes

CMX admin user

Usage Guidelines

This command should be run at the root user level.

Examples

The following example shows how to open ports based on a node:

```
[cmxadmin@cmx]# cmxos openports analytics  
Opened port 6541  
Opened port 6542  
Successfully opened all ports. Saving iptables info...
```

cmxos patch

To install, remove or view patch for CMX system, use the **cmxos patch** command.

cmxos patch **install** *filename***list****remove** *filename* **removeall**

Syntax Description	
install <i>filename</i>	Installs a new patch for CMX system.
list	Displays the list of currently installed patches
remove <i>filename</i>	Removes the specified patch.
removeall	Removes all installed patches from the CMX system.

Command Default None

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6	This command was introduced.

Usage Guidelines Cisco CMX has a restricted shell to prevent a user from updating the Cisco CMX image. A patch upgrade is now required to modify and update Cisco CMX. Patch files are RPM files specifically signed for installation on Cisco CMX. The patch file name has a .cmxp extension.

Example

The following example shows how to install a patch:

```
[cmxadmin@cmx]# cmxos patch install
Please enter the patch file name: patch-10.0.x.cmxp

** Checking patch file integrity

Patch file integrity passed.

** Extract patch file contents.
Verifying patch signature.
Verification signature output: Verified OK

Patch file verification successful for /home/cmxadmin/cmx-test-patch-10.6.0.cmxp.

** Installing patch RPM: /opt/image/patches/cmx-test-patch-10.6.0-1.x86_64.rpm extracted
from patch file: /home/cmxadmin/cmx-test-patch-10.6.0.cmxp

** Patch installed successfully

** Patch completed successfully.
```

cmxos reboot

To reboot the system, use the **cmxos reboot** command.

cmxos reboot {**force** | **silent** | **failover**}

Syntax Description	force	Option to force an immediate reboot.
	silent	Option to silently reboot without prompting.
	failover	Failover to the secondary before reboot and only if high availability enabled.
Command Default	None.	
Command Modes	CMX admin user	
Command History	Release	Modification
	Cisco CMX Release 10.6.1	This command was introduced.
Usage Guidelines	Run this command if you need to reboot the system. The limited shell prevents the reboot otherwise.	

Example

The following example shows how to reboot the system:

```
[cmxadmin@cmx]# cmxos reboot
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!! CONFIRM REBOOT !!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Are you sure you want to reboot?:y
```

cmxos reconfigure

To change network configuration information after deployment, use the **cmxos reconfigure** command.

cmxos reconfigure

Command Default

None

Command Modes

CMX admin user

Usage Guidelines

This command, which should be run at the root user level, also allows you to change the IP address, netmask, default gateway, and DNS server information. Changing the hostname through command line is not supported. Use the **cmxos reconfigure** command to change a hostname, IP address, or any of the network parameters.

NTP server and timezone/date configurations are also executed by running this command.



Note

- Do not execute the **cmxos reconfigure** command when Cisco CMX services are not installed. This will prevent execution failures.
- After you run the **cmxos reconfigure** command to update DNS server information, the output displays the updated DNS server entries on the top along with the previous entries. This is an expected behaviour.

Examples

The following example shows how to reconfigure the network after Cisco CMX installation:

```
[cmxadmin@cmx]# cmxos reconfigure
This command will wipe all system metrics data when the configuration is changed
Do you want to continue?: yes
Please enter hostname [cisco-cmx-centos7-test0]:
Please enter IP address [192.0.2.1]:
Please enter netmask [255.255.255.0]:
Please enter gateway [192.0.2.2]:
Please enter DNS server [192.0.2.3]:
Please enter search domain name [example.com]:
Are the network settings correct?: yes
Stopping keepalived service
Verify keepalived service has been stopped
Successfully stopped the keepalived service.
Starting keepalived service
ERROR: Failed to start keepalived service.
*****
Configuring NTP Server...
*****
Please enter the NTP server name (blank for no NTP server) [ntp.esl.cisco.com]:
Setting ntp server ntp.esl.cisco.com
*****
Configuring Timezone and date...
*****
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa
2) Americas
```



```

3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#? 10

```

Please select a country.

```

1) Chile
2) Cook Islands
3) Ecuador
4) Fiji
5) French Polynesia
6) Guam
7) Kiribati
8) Marshall Islands
9) Micronesia
10) Nauru
11) New Caledonia
12) New Zealand
13) Niue
14) Norfolk Island
15) Northern Mariana Islands
16) Palau
17) Papua New Guinea
18) Pitcairn
19) Samoa (American)
20) Samoa (western)
21) Solomon Islands
22) Tokelau
23) Tonga
24) Tuvalu
25) United States
26) US minor outlying islands
27) Vanuatu
28) Wallis & Futuna
#? 25

```

Please select one of the following time zone regions.

```

1) Eastern (most areas)
2) Eastern - MI (most areas)
3) Eastern - KY (Louisville area)
4) Eastern - KY (Wayne)
5) Eastern - IN (most areas)
6) Eastern - IN (Da, Du, K, Mn)
7) Eastern - IN (Pulaski)
8) Eastern - IN (Crawford)
9) Eastern - IN (Pike)
10) Eastern - IN (Switzerland)
11) Central (most areas)
12) Central - IN (Perry)
13) Central - IN (Starke)
14) Central - MI (Wisconsin border)
15) Central - ND (Oliver)
16) Central - ND (Morton rural)
17) Central - ND (Mercer)
18) Mountain (most areas)
19) Mountain - ID (south); OR (east)
20) MST - Arizona (except Navajo)
21) Pacific
22) Alaska (most areas)
23) Alaska - Juneau area
24) Alaska - Sitka area
25) Alaska - Annette Island
26) Alaska - Yakutat
27) Alaska (west)
28) Aleutian Islands
29) Hawaii
#? 21

```

The following information has been given:

```

United States
Pacific

```

```

Therefore TZ='America/Los_Angeles' will be used.
Local time is now:      Mon May 21 08:25:39 PDT 2018.
Universal Time is now: Mon May 21 15:25:39 UTC 2018.
Is the above information OK?

```

```

1) Yes
2) No
#? 1

```

The Timezone selected is America/Los_Angeles

The current time is Mon May 21 08:25:40 PDT 2018

```

Enter Date (YYYY-mm-dd hh:mm:ss) (blank to sync with ntp): []:
*** No changes were detected

```



Note This command opens the Device Configuration window, where you can take the appropriate action, that is reconfigure the device or the DNS.

cmxos rediscleanup

To remove data from all the redis ports, use the **cmxos rediscleanup** command.

cmxos rediscleanup

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.6.1	This command was introduced.

Usage Guidelines

When you run this command, data entires from all redis cache ports will be removed. This may result in permanent loss of data for CMX services such as Connect.

We recommend that you use this command when the memory usage of redis instances are high. For example, qlesspy service uses redis instance 6378 and when the 6378 instance reaches memory full, qlesspy service will not start. To recover from this situation, run the **cmxos rediscleanup** command. You need not restart any services after running this command.

Example

The following example shows how to remove data from all redis ports:

```
[cmxadmin@cmx]# cmxos rediscleanup
Output of redis cleanup for port 6378 - OK

Output of redis cleanup for port 6379 - OK

Output of redis cleanup for port 6380 - OK

Output of redis cleanup for port 6381 - OK

Output of redis cleanup for port 6382 - OK

Output of redis cleanup for port 6383 - OK

Output of redis cleanup for port 6384 - OK

Output of redis cleanup for port 6385 - OK
```

cmxos restore

To restore a node, use the **cmxos restore** command.

```
cmxos restore {file | path | i | ignore_version | ignore_licenses | help}
```

Syntax Description

--file PATH	Path where the restore file is located.
--path DIRECTORY	Path where the restore file will be created.
-i, --include_only TEXT	Restore selected parts only. Options are database, cache, cassandra, influxdb, consul, floormaps, licenses, setup, connectimages.
--ignore_version	Skip version check during restore.
--ignore_licenses	Skip restoring Cisco CMX licenses contained in the backup bundle and retain local licenses.
--HELP	Shows the help content.

Command Default

None.

Command Modes

CMX admin user

Usage Guidelines

By default, this command performs restoration of all services excluding the InfluxDB data service. If you want to restore InfluxDB data, explicitly enter the InfluxDB service name along with other services by using *--include_only* while running the command.

Examples

The following example shows how to restore a node:

```
[cmxadmin@cmx]# cmxos restore
Please enter the backup file path: /tmp/cmx_backup_cmx-vmdev117_2015_03_10_17_43.tar.gz
[17:44:12] Preparing for restore...
[17:44:12] Untarring backup file...
[17:44:13] Stopping all services...
[17:44:16] Restoring Database...
Restarting database...
[17:44:26] Restoring Cache...
Stopping cache_6379...
Restarting cache_6379...
Stopping cache_6381...
Restarting cache_6381...
Stopping cache_6380...
Restarting cache_6380...
[17:44:55] Restoring Cassandra...
Stopping Cassandra...
Restarting Cassandra...
.....
[17:45:19] Restoring Influxdb...
[17:45:19] Restoring consul...
[17:45:19] Restoring floormaps...
[17:45:19] Running Post Restore Tasks...
[17:45:19] Migrating Schemas...
```

```
[17:45:19] Migrating Cassandra schemas...  
[17:45:20] Restarting all services...  
[17:45:23] Done
```

cmxos shutdown

To halt the system, use the **cmxos shutdown** command.

cmxos shutdown {**force** | **silent** | **failover**}

Syntax Description	force	Option to force an immediate halt.
	silent	Option to silently halt without prompting.
	failover	Failover to the secondary before halt and only if high availability enabled.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.1	This command was introduced.

Usage Guidelines Run this command for a graceful shutdown of the system. Because of the limited shell command restriction you cannot run this command otherwise.

Example

The following example shows how to shutdown the system:

```
[cmxadmin@cmx]# cmxos shutdown
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!! CONFIRM HALT !!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Are you sure you want to shutdown?:
```

cmxos smartlicenseudi

To get secondary UDI from Cisco CMX secondary server, use the **cmxos smartlicenseudi** command.

cmxos smartlicenseudi

Syntax Description This command has no arguments or keywords.

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.6.3	This command was introduced.

Usage Guidelines Run this command on secondary CMX server to print **UDI** and **Serial Number** of the secondary CMX on the terminal. Copy the values of **UDI** and **Serial Number** and manually enter them as inputs to run the command **cmxctl config smartlicense secondaryudi**.

Examples

The following example shows how to get secondary CMX UDI and serial number:

```
[cmxadmin@server]# cmxos smartlicenseudi  
  
UDI: VMware Virtual Platform  
  
Serial Number: 123456-EABCDEA71
```

cmxos sslcert

To replace default haproxy certificate, use the **cmxos sslcert** command.

cmxos sslcert

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.2	This command was introduced.

cmxos sysproxy

To enable an outbound proxy on your Cisco CMX server, use the **cmxos sysproxy** command.

cmxos sysproxy {**clear** | **disable** | **enable** | **no_proxy** | **proxy** | **show** | **ftp_proxy** | **http_proxy** | **https_proxy**}

Syntax Description

clear	Removes the proxy settings.
disable	Disables the use of the proxy settings.
enable	Enables the use of the proxy settings.
no_proxy	Sets the no_proxy environment variable.
proxy	Sets the proxy environment variables for http_proxy, https_proxy, ftp_or proxy.
show	Displays the proxy settings.
ftp_proxy	Sets the ftp proxy.
http_proxy	Sets the http proxy.
https_proxy	Sets the https proxy.

Command Default

Proxy is disabled.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.3.1	This command was introduced.

Usage Guidelines

This command supersedes the information from this post: <https://communities.cisco.com/docs/DOC-70904>.

Use this command for environments where an outbound proxy is required on the Cisco CMX server. For example, if you happen to be in a secure internal network where even outbound traffic via HTTPS requires that it move through a proxy server.

If you set the **proxy** setting on the Cisco CMX server, make sure to use the **no_proxy** setting on the attached controllers to avoid interference with the NMSP Network Mobility Services Protocol (NMSP).

If you change the Cisco CMX proxy settings, you must restart Cisco CMX for the change to take effect. Use the **cmxctl restart** command to restart Cisco CMX.

Example

The following example shows how to set a proxy on the Cisco CMX server, and then verify the change and restart Cisco CMX:

```
[cmxadmin@cmx]# cmxos sysproxy proxy https://proxy-wsa.esl.cisco.com:80

[cmxadmin@cmx]# cmxos sysproxy show
USE_PROXY=1
```

```
PROXY_URL=http://proxy-wsa.esl.cisco.com:80
NO_PROXY_LIST=""
[cmxadmin@cmx]# cmxctl restart
```

The following example shows how to enable a proxy on the Cisco CMX server, and then verify the change and restart Cisco CMX:

```
[cmxadmin@cmx]# cmxos sysproxy enable

[cmxadmin@cmx]# cmxos sysproxy show
USE_PROXY=1
PROXY_URL=http://proxy-wsa.esl.cisco.com:80
NO_PROXY_LIST=""
[cmxadmin@cmx]# cmxctl restart
```

The following example shows how to disable a proxy on the Cisco CMX server, and then verify the change and restart Cisco CMX:

```
[cmxadmin@cmx]# cmxos sysproxy disable

[cmxadmin@cmx]# cmxos sysproxy show
USE_PROXY=0
PROXY_URL=http://proxy-wsa.esl.cisco.com:80
NO_PROXY_LIST=""
[cmxadmin@cmx]# cmxctl restart
```

The following example shows how to clear proxy settings, and then verify the change and restart Cisco CMX:

```
[cmxadmin@cmx]# cmxos sysproxy clear
[cmxadmin@cmx]# cmxos sysproxy show
USE_PROXY=0
PROXY_URL=""
NO_PROXY_LIST=""
[cmxadmin@cmx]# cmxctl restart
```

cmxos techsupport

To collect technical support information, use the **cmxos techsupport** command.

cmxos techsupport { **all** | **cmx** | **location** | **map** | **network** | **services** | **system** }

Syntax Description	all Collect all technical support information				
	cmx Collect CMX information				
	location Collect location support information				
	map Collect map support information				
	network Collect network information				
	services Collect CMX services information.				
	system Collect system information				
	silent Silently run with prompting				
Command Default	None.				
Command Modes	CMX admin user				
Usage Guidelines	This command will return all CLI command outputs helpful for debugging.				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco CMX Release 10.3</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco CMX Release 10.3	This command was introduced.
Release	Modification				
Cisco CMX Release 10.3	This command was introduced.				

cmxos techsupport dump

To dump all technical support information, use the **cmxos techsupport dump** command.

cmxos techsupport dump

Command Default None.

Command Modes CMX admin user

Command History	Release	Modification
	Cisco CMX Release 10.3	This command was introduced.

cmxos upgrade

To upgrade Cisco Connected Mobile Experiences (Cisco CMX) with a new Red Hat Package Manager (RPM) or package, use the **cmxos upgrade** command.

cmxos upgrade

Command Default

None.

Command Modes

CMX admin user

Usage Guidelines

This command should be run at the root user level. The CLI accepts either a local file or an HTTP URL. This command works only when you have a later version than the existing one to upgrade.

Examples

The following example shows how to upgrade the Cisco CMX using RPM or package:

```
[cmxadmin@cmx]# cmxos upgrade
The nodeagent service is not running.
Agent is not running, starting it now.
Starting nodeagent Process...
Stopping nodeagent Process...
Done
Successfully shutdown nodeagent Process.
Stopping consul Process...
Successfully shutdown consul Process.
Stopping qlesspyworker Process...
Successfully shutdown qlesspyworker Process.
Stopping cassandra Process...
Successfully shutdown cassandra Process.
Stopping iodocs Process...
The iodocs service is not running.
Stopping redis6383 Process...
Successfully shutdown redis6383 Process.
Stopping redis6380 Process...
Successfully shutdown redis6380 Process.
Stopping redis6381 Process...
Successfully shutdown redis6381 Process.
Stopping influxdb Process...
The influxdb service is not running.
Stopping collectd Process...
The collectd service is not running.
Stopping confd Process...
The confd service is not running.
Stopping redis6379 Process...
Successfully shutdown redis6379 Process.
Stopping redis6378 Process...
Successfully shutdown redis6378 Process.
Stopping haproxy Process...
Stopping postgres Process...
Successfully shutdown postgres Process.
Stopping analytics Process...
The analytics service is not running.
Stopping location Process...
The location service is not running.
Stopping configuration Process...
The configuration service is not running.
```

```
Stopping halo Process...  
The halo service is not running.  
Stopping matlabengine Process...  
The matlabengine service is not running.  
Stopping nmsplb Process...  
The nmsplb service is not running.  
Shutting down
```

cmxos vacuumdb

To run the full vacuum command on the postgres database running within Cisco CMX, use the **cmxos vacuumdb** command.

cmxos vacuumdb

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.4	This command was introduced.

Usage Guidelines

This command internally runs the 'vacuumdb -vfa' on the postgres DB. This command is an advanced command and should not be regularly used by the customer. In case of the postgres DB taking up too much disk space, this command may be run to compact the DB.

cmxos verify

To verify the virtual machine configuration, use the **cmxos verify** command.

cmxos verify

Command Default None.

Command Modes CMX admin user

Examples

The following example shows how to verify the virtual machine configuration:

```
[cmxadmin@cmx]# cmxos verify
+-----+-----+-----+-----+
| Check | expected | actual | Result |
+=====+=====+=====+=====+
| memory | 8GB | 25GB | ? |
+-----+-----+-----+-----+
| cpu | 4 | 8 | ? |
+-----+-----+-----+-----+
| disk | 50GB | 51GB | ? |
+-----+-----+-----+-----+
| hostname | rfc compliant hostname | cmx-vmdev146 | ? |
+-----+-----+-----+-----+
```


cmxos wipeoutdisk

To wipeout CMX data, use the **cmxos wipeoutdisk** command.

cmxos wipeoutdisk

Command Default

None.

Command Modes

CMX admin user

Command History

Release	Modification
Cisco CMX Release 10.6	This command was introduced.

Usage Guidelines

This command is available only when the FIPS/UCAPL mode is enabled. After the command execution is complete, it will delete everything on the disk and make system unusable and it will not even boot normally.

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.

Example

The following example shows how to wipeout CMX data:

```
[cmxadmin@cmx]# 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
Have you closed all SSH sessions to this CMX? [y/N]: y
WARNING: This is your last chance.
If you want to take backup, please exit now.
You can take backup and transfer it to some other machine.
When 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
```

