

Back Up and Restore Data on CMX 10.5 and Above

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Backup process](#)

[Creating the backup bundle](#)

[Backing up a High Availability setup](#)

[Moving the bundle from CMX to a different machine](#)

[Deleting the backup archive from CMX](#)

[Restoring the backup](#)

[Additional information](#)

[Restrictions of backup and restoration process](#)

[Difference between backup and virtual machine snapshot](#)

Introduction

This document describes how to back up and restore configuration and client data on a Cisco CMX 10.5 and later

Prerequisites

Requirements

General knowledge of CMX is required.

Components Used

All tests were performed on a CMX 10.6.0-177 running on MSE 3375 appliance, MacOS 10.4 and Windows 10 October 2018 update.

This includes CMX installed on a physical 3365/3375 appliance, as well as on a virtual machine. These components of CMX can be backed up:

- Database - Stores configuration data, such as, maps, controllers, location, and aggregated analytics data
- Cache - Stores analytics repeat visits
- Cassandra - Stores location history data and analytics raw visits
- Influxdb - Stores metrics data for systems (not included by default)
- Consul - Stores Consul configurations

- Floormaps - Stores floor images for UI display
- Licenses - Stores Cisco CMX license information
- Setup - Stores CMX setup data
- Connectimages - Stores Images on Connect Captive Portal
- Conf - Stores node configuration

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

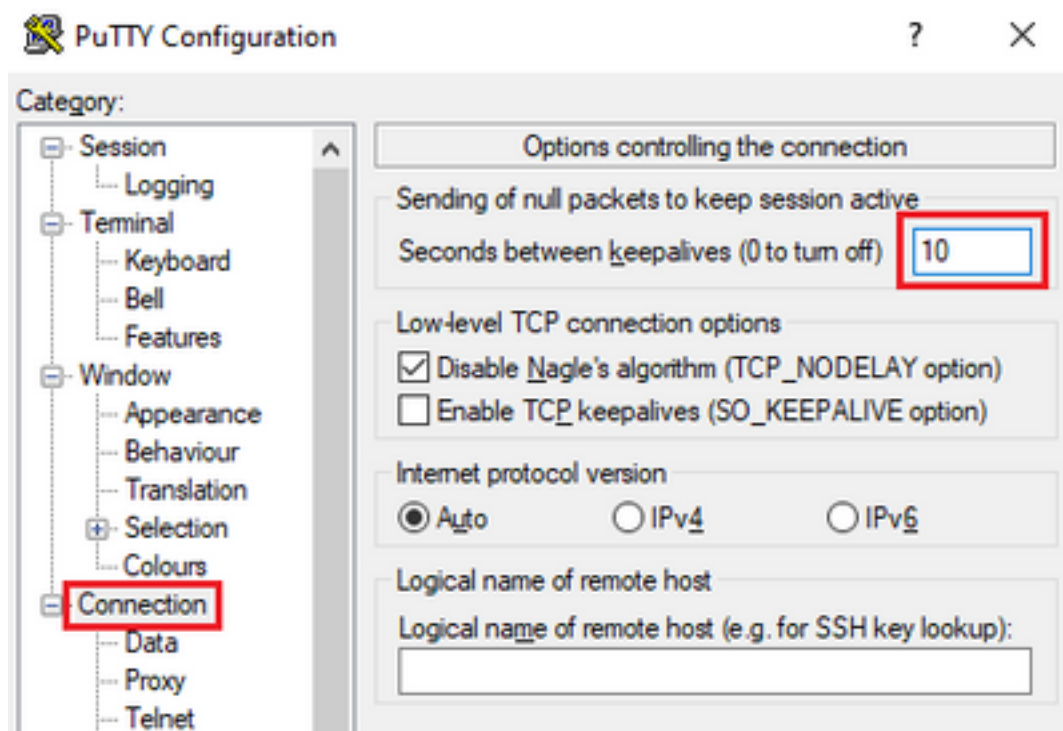
Backup process

Creating the backup bundle

CMX, no matter where installed, can be backed up using a `cmxos backup` command. By default, backup includes database, cache, cassandra, floormaps, licenses, setup, connectimages and configuration. Add the `--all` parameter to include the Influxdb data as well. By default, backup process stops CMX services while being performed. Add the parameter `--online` to perform the backup without stopping the CMX services. You are prompted to enter the directory where you want to save the backup tar.gz archive. Directory needs to have read, write and execute permissions. It is recommended to use the default /tmp directory.

On a freshly installed CMX, backup process takes ~30 seconds. On a fully loaded and utilized CMX, creation of backup bundle can take up to an hour.

Make sure to enable keepalive messages in your SSH client so that the session does not time out while backup is being created. In PuTTY, this can be done under "Connection" Tab:



```
[cmxadmin@mse33752 ~]$ cmxos backup --online --all
Please enter the path for backup file [/tmp]:
backup name: cmx_backup_mse33752_2019_04_28_22_39
backup dir: /tmp/cmx_backup_mse33752_2019_04_28_22_39
```

```
tar file: /tmp/cmxc_backup_mse33752_2019_04_28_22_39.tar.gz
running: sudo -u cmx /opt/cmxc/bin/cmxcctl version
```

```
-----
Build Version   : 10.6.0-331
Build Time      : 2019-01-24 13:27:35.937025
-----
Image Version   : 10.6.0-177
-----
```

```
Preparing backup of following services: ['database', 'cache', 'cassandra', 'influxdb',
'floormaps', 'licenses', 'setup', 'connectimages', 'conf']
```

```
[22:39:56] Preparing for backup...
```

```
Preparing for backup...
```

```
Database size 51226723
```

```
Cache size 7794
```

```
Cassandra size 67462961
```

```
Floormaps size 1014394
```

```
Licenses size 6
```

```
Setup size 1912
```

```
Connectimages size 6
```

```
running: sudo -u cmx /opt/cmxc/bin/cmxcctl dump
```

```
running locally
```

```
Dumping configuration information...
```

```
[localhost] Executing task 'dump_config_only'
```

```
Done.
```

```
.
.
.
.
.
.
.
```

```
copy snapshot took 0.804718971252 seconds Backup Cassandra DB took: 8.50579595566 seconds
```

```
[22:40:07] Backup InfluxDb... Backup InfluxDb... Backup Influx DB took: 0.0411479473114 seconds
```

```
[22:40:07] Backup Floormaps... Backup Floormaps... Backup floor maps took: 0.055881023407
```

```
seconds [22:40:07] Backup licenses... Backup licenses... Backup licenses took: 0.000136137008667
```

```
seconds [22:40:07] Backup setup... Backup setup... Backup setup took: 0.00061297416687 seconds
```

```
[22:40:07] Backup connect images... Backup connect images... Backup connect images took:
```

```
0.000127077102661 seconds [22:40:07] Backup node configuration... Backup node configuration...
```

```
running: sudo -u cmx /opt/cmxc/bin/cmxcctl dump running locally Dumping configuration
```

```
information... [localhost] Executing task 'dump_config_only' Done. Backup configuration took:
```

```
0.383893013 seconds [22:40:07] Creating tar file.. Creating tar file.. running: tar -chf
```

```
/tmp/cmxc_backup_mse33752_2019_04_28_22_39.tar.gz --use-compress-program=pigz -C /tmp
```

```
cmxc_backup_mse33752_2019_04_28_22_39 running: chmod a+rw
```

```
/tmp/cmxc_backup_mse33752_2019_04_28_22_39.tar.gz running: chown cmxcadmin:cmxcadmin
```

```
/tmp/cmxc_backup_mse33752_2019_04_28_22_39.tar.gz Post backup took: 0.17880988121 seconds Done
```

```
Backup. Created backup file /tmp/cmxc_backup_mse33752_2019_04_28_22_39.tar.gz [22:40:07] Done
```

```
Backup. Created backup file /tmp/cmxc_backup_mse33752_2019_04_28_22_39.tar.gz running:
```

```
/opt/apache-cassandra-3.9/bin/nodetool --ssl -h cassandra.service.consul -p 7199 clearsnapshot
```

```
Requested clearing snapshot(s) for [all keyspaces]
```

At the end of the output, name of the backup archive is specified:

```
[22:40:07] Done Backup. Created backup file /tmp/cmxc_backup_mse33752_2019_04_28_22_39.tar.gz
```

Backing up a High Availability setup

If the High Availability is currently up and running, since all databases are synced between primary and secondary, taking the backup from primary CMX is enough to save all client data. Simply run **cmxos backup --all --online** command and transfer the files from the primary server.

If High Availability is not currently established between primary and secondary server, first determine which CMX has complete and most recent data and create a backup from it.

Note: If High Availability is established, online backup is supported only on primary server. If High Availability is disabled, online and offline backups are supported on both primary and secondary.

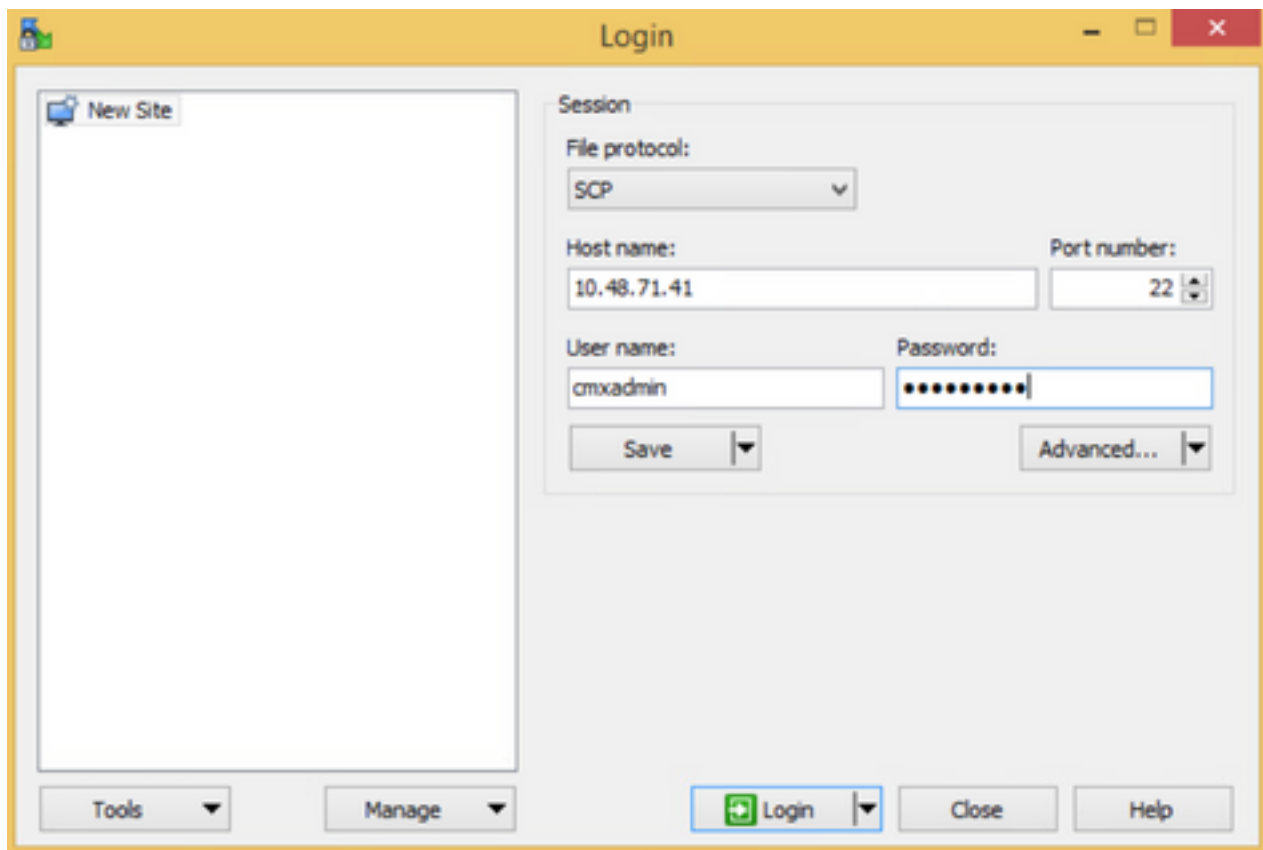
Moving the bundle from CMX to a different machine

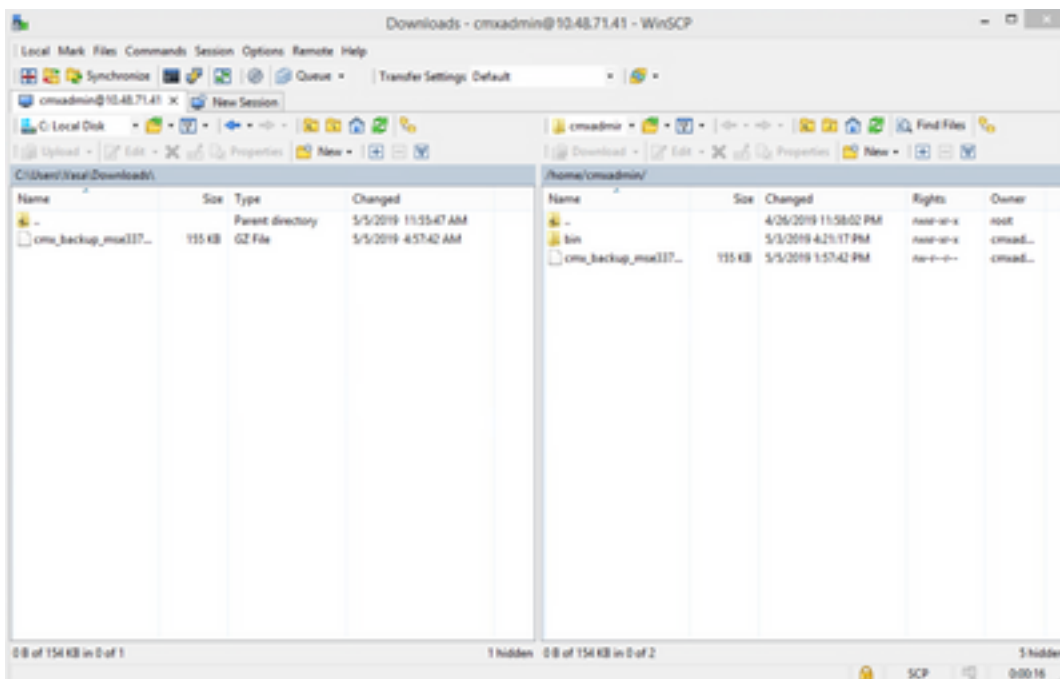
If something happens to the hard drive of the CMX or files get corrupted during the upgrade process, backup files saved on the CMX could be lost. It is recommended to move the data from CMX to another machine using Secure Copy Protocol (SCP). Bellow you can find examples on how to do that on Windows, MacOS and Linux PC:

Windows:

Easiest way to do this on Windows is via [WinSCP](#) program. After installation, enter the IP address and credentials of the cmxadmin user and establish the SCP connection. Navigate to the folder where the backup is saved, find the backup file and drag it to the desired location on your local machine (left window).

Important: Due to root access restrictions in CMX 10.6.x, command `cd` which WinSCP uses to navigate directories is not present. In this situation, using WinSCP is not possible. Contact Cisco TAC to if you want to gain access to the root patch or find an alternate SCP utility.





MacOS and Linux:

MacOS and most Linux distributions come with native scp client. Files can be move using a simple terminal command:

```
scp cmxadmin@<cmx_ip_address>:/<file_path_and_name_on_cmx> <file_path_and_name_on_local_machine>
```

Example:

```
VAPEROVI-M-H1YM:~ vaperovi$ scp
cmxadmin@10.48.71.41:/tmp/cmx_backup_mse33752_2019_04_28_19_38.tar.gz
/Users/vaperovi/cmx_backup_mse33752_2019_04_28_19_38.tar.gz
cmxadmin@10.48.71.41's password:
cmx_backup_mse33752_2019_04_28_19_38.tar.gz                                100%
186KB   1.4MB/s   00:00
```

CMX shows a prompt to enter the credentials of the cmxadmin user, after which the data is transferred to the specified location in your local machine.

Note: Considering that CMX 10.5 and later is running on CentOS 7, this command can be used to move the data from one CMX to a freshly installed one. Since one wireless controller can only be synced with one CMX at the time, make sure to shut down the CMX from which the backup bundle is downloaded.

Deleting the backup archive from CMX

On CMX version 10.5.x, files can be deleted by logging in as root user via `su` command, navigating to the `/tmp` directory where the backup files has been saved and deleting it via `rm -f` command:

```
[cmxadmin@mse33752 ~]$ su
Password:
[root@mse33752 cmxadmin]#
[root@mse33752 cmxadmin]# cd /tmp
```

```
[root@mse33752 tmp]# rm -f cmx_backup_mse33752_2019_04_28_19_38.tar.gz
```

Starting version 10.6.0, root access has been restricted. Without special patch that can only be given out by Cisco TAC, deleting the files like on 10.5 is not possible. Some space can be freed up using the **cmxos clean normal --delete** command:

```
[cmxadmin@mse33752 ~]$ 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/entropy.err
Remove: /opt/cmx/var/log/backup.log.2
Remove: /opt/cmx/var/log/techsupport/cmx_tech_support_2019-04-28.log
Removing files in: /opt/influxdb/shared
Removing files in: /tmp
```

Important: If there is still not enough space to perform the backup after running **cmxos clean normal --delete**, you need to contact Cisco TAC to gain access to root and remove files that are taking up space.

Restoring the backup

If you want to restore the backup, transfer the backup file from the remote machine to CMX. In windows, you can simply drag and drop the files using WinSCP. On MacOS and Linux, use this command:

```
$ scp <file_path_and_name_on_local_machine> cmxadmin@<cmx_ip_address>:/tmp
```

Example:

```
VAPEROVI-M-H1YM:~ vaperovi$ scp /Users/vaperovi/cmx_backup_mse33752_2019_04_28_19_38.tar.gz
cmxadmin@10.48.71.41:/tmp
cmxadmin@10.48.71.41's password:
cmx_backup_mse33752_2019_04_28_19_38_copy.tar.gz          100% 186KB
1.3MB/s 00:00
```

Important: Restoring Cisco CMX data must be done from a device that has the same local time. Otherwise, you are not able to correctly access the analytics data. In addition, the data results in errors or zero values on reports.

To restore data, CMX needs to have free disk space 4 times the size of the backup bundle. If there is not enough space, you can try increasing the space of the VM or by running **cmxos clean normal --delete** command. Restoration process can be initiated using the **cmxos restore** command. Adding the **-i** parameter, you can backup only certain elements (database, cache, cassandra, floormaps, licenses, setup, conf). Its recommended to perform full backups.

Restoration process requires all services to be stopped. Make sure to prepare big enough maintenance window for this process as it can take over an hour.

```
[cmxadmin@mse33752 ~]$ cmxos restore
Please enter the backup file path: /tmp/cmx_backup_mse33752_2019_04_28_22_39.tar.gz
Please enter the path for untar backup file [/tmp]:
Stopping monit (via systemctl): [ OK ]
[23:49:19] Preparing for restore...
```

```
Restore size 30383753
Available disk space in /tmp is 1812541169664
Available disk space is 1817753817088
[23:49:19] Untarring backup file...
Backing up existing licenses on the system...
Successfully saved existing licenses
Stopping all services...
Pre restore took: 41.672647953 seconds
[23:50:00] Restoring Database...
Created temporary database temp_mse
Running command /usr/bin/sudo -u postgres pg_restore -j 8 -d temp_mse -Fc
/tmp/cmx_backup_mse33752_2019_04_28_22_39/postgres/mse.dump
Restored temporary database temp_mse
Dropping database mse
Renaming database temp_mse to mse
Restarting database...
Starting database...
Restore database took: 10.2765719891 seconds
[23:50:11] Restoring Cache...
Stopping cache_6378...
Restarting cache_6378...
Stopping cache_6379...
Restarting cache_6379...
Stopping cache_6385...
Restarting cache_6385...
Stopping cache_6380...
Restarting cache_6380...
Stopping cache_6381...
Restarting cache_6381...
Stopping cache_6382...
Restarting cache_6382...
Stopping cache_6383...
Restarting cache_6383...
Stopping cache_6384...
Restarting cache_6384...
Restore Cache took: 61.1865711212 seconds
[23:51:12] Restoring Cassandra...
Stopping Cassandra...
Starting Cassandra after wipe...
starting cassandra
Creating empty cassandra schemas
Stopping Cassandra...
Starting Cassandra after restore ...
starting cassandra
Restore Cassandra took: 117.123826981 seconds
[23:53:09] Restoring floormaps...
Restore floor maps took: 0.0736980438232 seconds
[23:53:09] Restoring licenses...
Restore licenses took: 0.000176906585693 seconds
[23:53:09] Restoring setup...
Restore setup took: 0.00758194923401 seconds
[23:53:09] Restoring connect images...
Restore connect images took: 0.000188827514648 seconds
[23:53:09] Running Post Restore Tasks...
[23:53:09] Migrating Schemas...
[23:53:10] Migrating Cassandra Schemas...
stopping cassandra
Local licenses wont be retained.
Running full vacuum command on postgres
Performing cleanup of redis cache 6378 and 6383 to evict bloom filter stale entries.
Performing cleanup of redis cache 6378 to evict stale records by glesspyworker.
Update CMX default certificate
Post restore took: 61.7358779907 seconds
[23:54:11] Starting all services...
```

Additional information

Restrictions of backup and restoration process

- Backups from CMX 10.3 or older cannot be imported into CMX 10.5.x and later. Backups from 10.5.x can be imported into CMX 10.6.x
- In order to stay compliant with GDPR, backup of database, floor maps, licenses and setup components needs to be performed
- Make sure that the port 22 is not blocked between CMX and the machine which is used to access it
- If restoring backups from a different type of CMX deployment, refer to the table to check if they are compatible:

Restore from...	Restore to...	Recommendations
Same machine specs	Same machine specs	OK
Cisco MSE 3365 appliance	Cisco 3375 appliance	OK
Cisco MSE 3365 appliance	High-end MSE virtual (vMSE)	OK
High-end vMSE	Cisco 3375 and Cisco MSE 3365 appliances	OK unless the high-end machine has more RAM allocated than the recommended specs
Standard vMSE	Cisco 3375 and Cisco MSE 3365 appliances	OK
Standard vMSE	High-end vMSE	OK
Low-end vMSE	Cisco 3375 and Cisco MSE 3365 appliances	OK
Low-end vMSE	High-end vMSE	OK
Low-end vMSE	Standard vMSE	OK
Cisco 3375 appliance	Cisco MSE 3365 appliance	Not Recommended
Cisco MSE 3365 appliance	Standard vMSE	Not Recommended
Cisco MSE 3365 appliance	Low-end vMSE	Not Recommended
High-end vMSE	Standard vMSE	Not Recommended
High-end vMSE	Low-end vMSE	Not Recommended
Standard vMSE	Low-end vMSE	Not Recommended

Difference between backup and virtual machine snapshot

Virtual Machine snapshots cannot be considered a backup tool as they do not do anything to preserve the integrity of the VMDK file that the Virtual Machine uses for its data storage. Snapshots operate by "freezing" the original VMDK storage file and creating additional snapshot files which capture the changes made to the original VMDK file (so called disk chain). This way the state of the disk file can be preserved in time and rolled back to if needed after some changes are made.

Therefore, If the original (parent) VMDK file is lost or is corrupted in any way, snapshot data

cannot be used to restore it back to its previous state and the stored data is effectively lost.

VMware best practices for using snapshots in the vSphere environment mentions the following:

- **Do not use snapshots as backups** (reasons outlined)
- VMware recommends not to use a single snapshot for more than 72 hours (The snapshot file continues to grow in size when it is retained for a longer period. This can cause the snapshot storage location to run out of space and impact the system performance).
- Maximum of 32 snapshots are supported in a chain. However, for a better performance, limit the use only 2 to 3 snapshots.

For more information, refer to the [VMware snapshot best practices article](#).