Upgrading Cisco IMC Supervisor From Older Versions

This chapter contains the following topics:

- Upgrading Cisco IMC Supervisor , on page 1
- Data Migration, on page 7
- Digitally Signed Images, on page 13
- Requirements for Verifying Digitally Signed Images, on page 14
- Verifying a Digitally Signed Image, on page 14
- Applying a Patch to Cisco IMC Supervisor, on page 15
- Applying a Signed Patch to Cisco IMC Supervisor, on page 16

Upgrading Cisco IMC Supervisor

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.3(8.0)

- From Release 2.3(7.0) to Release 2.3(8.0)
- From Release 2.3(6.0) to Release 2.3(8.0)
- From Release 2.3(5.0) to Release 2.3(8.0)
- From Release 2.3(4.0) to Release 2.3(8.0)
- From Release 2.3(3.0) to Release 2.3(8.0)
- From Release 2.3(2.1) to Release 2.3(8.0)
- From Release 2.3(2.0) to Release 2.3(8.0)
- From Release 2.3(1.0) to Release 2.3(2.0) to Release 2.3(8.0)
- From Release 2.3(0.0) to Release 2.3(2.0) to Release 2.3(8.0)
- From Release 2.2(1.4) to Release 2.3(2.0) to Release 2.3(8.0)
- From Release 2.2(1.3) to Release 2.3(2.0) to Release 2.3(8.0)

Note From Release 2.2(1.3) or Release 2.2(1.4), you should migrate to Release 2.3(x.x).

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.3(7.0)

- From Release 2.3(6.0) to Release 2.3(7.0)
- From Release 2.3(5.0) to Release 2.3(7.0)
- From Release 2.3(4.0) to Release 2.3(7.0)
- From Release 2.3(3.0) to Release 2.3(7.0)
- From Release 2.3(2.1) to Release 2.3(7.0)
- From Release 2.3(2.0) to Release 2.3(7.0)
- From Release 2.3(1.0) to Release 2.3(2.0) to Release 2.3(7.0)
- From Release 2.3(0.0) to Release 2.3(2.0) to Release 2.3(7.0)
- From Release 2.2(1.4) to Release 2.3(2.0) to Release 2.3(7.0)
- From Release 2.2(1.3) to Release 2.3(2.0) to Release 2.3(7.0)

Note From Release 2.2(1.3) or Release 2.2(1.4), you should migrate to Release 2.3(x.x).

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.3(6.0)

- From Release 2.3(5.0) to Release 2.3(6.0)
- From Release 2.3(4.0) to Release 2.3(6.0)
- From Release 2.3(3.0) to Release 2.3(6.0)
- From Release 2.3(2.1) to Release 2.3(6.0)
- From Release 2.3(2.0) to Release 2.3(6.0)
- From Release 2.3(1.0) to Release 2.3(2.0) to Release 2.3(6.0)
- From Release 2.3(0.0) to Release 2.3(2.0) to Release 2.3(6.0)
- From Release 2.2(1.4) to Release 2.3(2.0) to Release 2.3(6.0)
- From Release 2.2(1.3) to Release 2.3(2.0) to Release 2.3(6.0)

Note From Release 2.2(1.3) or Release 2.2(1.4), you should migrate to Release 2.3(x.x).

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.3(5.0)

- From Release 2.3(4.0) to Release 2.3(5.0)

- From Release 2.3(3.0) to Release 2.3(5.0)
- From Release 2.3(2.1) to Release 2.3(5.0)
- From Release 2.3(2.0) to Release 2.3(5.0)
- From Release 2.3(1.0) to Release 2.3(2.0) to Release 2.3(5.0)
- From Release 2.3(0.0) to Release 2.3(2.0) to Release 2.3(5.0)
- From Release 2.2(1.4) to Release 2.3(2.0) to Release 2.3(5.0)
- From Release 2.2(1.3) to Release 2.3(2.0) to Release 2.3(5.0)

Note From Release 2.2(1.3) or Release 2.2(1.4), you should migrate to Release 2.3(x.x).

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.3(4.0)

- From Release 2.3(3.0) to Release 2.3(4.0)
- From Release 2.3(2.1) to Release 2.3(4.0)
- From Release 2.3(2.0) to Release 2.3(4.0)
- From Release 2.3(1.0) to Release 2.3(2.0) to Release 2.3(4.0)
- From Release 2.3(0.0) to Release 2.3(2.0) to Release 2.3(4.0)
- From Release 2.2(1.4) to Release 2.3(2.0) to Release 2.3(4.0)
- From Release 2.2(1.3) to Release 2.3(2.0) to Release 2.3(4.0)

Note From Release 2.2(1.3) or Release 2.2(1.4), you should migrate to Release 2.3(x.x).

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.3(3.0)

- From Release 2.3(2.1) to Release 2.3(3.0)
- From Release 2.3(2.0) to Release 2.3(3.0)
- From Release 2.3(1.0) to Release 2.3(2.0) to Release 2.3(3.0)
- From Release 2.3(0.0) to Release 2.3(2.0) to Release 2.3(3.0)
- From Release 2.2(1.4) to Release 2.3(2.0) to Release 2.3(3.0)
- From Release 2.2(1.3) to Release 2.3(2.0) to Release 2.3(3.0)

Note From Release 2.2(1.3) or Release 2.2(1.4), you should migrate to Release 2.3(x.x).

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.3(2.1)

Note Cisco IMC Supervisor 2.3(2.1) includes fixes for security vulnerabilities reported in releases 2.2(1.4), 2.3, 2.3(1.0), and 2.3(2.0). For information on the security vulnerabilities reported in releases 2.2(1.4), 2.3, 2.3(1.0), and 2.3(2.0), see the security advisories for CVE-2021-44228 and CVE-2021-45046 available at this link:

https://tools.cisco.com/security/center/publicationListing.x

- From Release 2.3(2.0) to Release 2.3(2.1)
- From Release 2.3(1.0) to Release 2.3(2.0) to Release 2.3(2.1)
- From Release 2.3(0.0) to Release 2.3(2.0) to Release 2.3(2.1)
- From Release 2.2(1.4) to Release 2.3(2.0) to Release 2.3(2.1)
- From Release 2.2(1.3) to Release 2.3(2.0) to Release 2.3(2.1)

Note From Release 2.2(1.3) or Release 2.2(1.4), you should migrate to Release 2.3(x.x).

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.3(2.0)

Note Ensure that you generate and reinstall the latest CA certificate after data migration.

- From Release 2.3(1.0) to Release 2.3(2.0)
- From Release 2.3(0.0) to Release 2.3(2.0)
- From Release 2.2(1.4) to Release 2.3(2.0)
- From Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3(2.0)
- From Release 2.2(1.1) to Release 2.2(1.4) to Release 2.3(2.0)
- From Release 2.2(1.0) to Release 2.2(1.4) to Release 2.3(2.0)
- From Release 2.2(0.6) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3(2.0)
- From Release 2.2(0.5) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3(2.0)
- From Release 2.2(0.4) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3(2.0)
- From Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3(2.0)
- From Release 2.2(0.2) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3(2.0)
- From Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) Release 2.3(2.0)
- From Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3(2.0)
- From Release 2.1.x.x to Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3(2.0)

- From Release 2.1.x.x to Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3(2.0)
- From Release 2.2(1.3) to Release 2.3(2.0)
- From Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3(2.0)
- From Release 2.2(1.1) to Release 2.2(1.3) to Release 2.3(2.0)
- From Release 2.2(1.0) to Release 2.2(1.3) to Release 2.3(2.0)
- From Release 2.2(0.6) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3(2.0)
- From Release 2.2(0.5) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3(2.0)
- From Release 2.2(0.4) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3(2.0)
- From Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3(2.0)
- From Release 2.2(0.2) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3(2.0)
- From Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3(2.0)
- From Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3(2.0)
- From Release 2.1.x.x to Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3(2.0)
- From Release 2.1.x.x to Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3(2.0)

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.3(1.0)

- From Release 2.3(0.0) to Release 2.3(1.0)
- From Release 2.2(1.4) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(1.1) to Release 2.2(1.4) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(1.0) to Release 2.2(1.4) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.6) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.5) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.4) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.2) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0) to Release 2.3(1.0)

- From Release 2.1.x.x to Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.1.x.x to Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(1.3) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(1.1) to Release 2.2(1.3) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(1.0) to Release 2.2(1.3) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.6) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.5) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.4) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.2) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.1.x.x to Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0) to Release 2.3(1.0)
- From Release 2.1.x.x to Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0) to Release 2.3(1.0)

Supported Upgrade Paths for Cisco IMC Supervisor Release 2.3

Note CentOS 6 Cisco IMC Supervisor appliance with version 2.2.1.3 **or** 2.2.1.4 is considered as the the Source System and CentOS 7 Cisco IMC Supervisor appliance as the Target System.

To upgrade to Cisco IMC Supervisor 2.3 we can deploy either through VMware vSphere or Micrsoft Hyper -V and follow the below upgrade path to migrate data from old system to new system.

- From Release 2.2(1.4) to Release 2.3 (0.0)
- From Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0)
- From Release 2.2(1.1) to Release 2.2(1.4) to Release 2.3 (0.0)
- From Release 2.2(1.0) to Release 2.2(1.4) to Release 2.3 (0.0)
- From Release 2.2(0.6) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0)
- From Release 2.2(0.5) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0)

- From Release 2.2(0.4) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0)
- From Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0)
- From Release 2.2(0.2) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0)
- From Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0)
- From Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0)
- From Release 2.1.x.x to Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0)
- From Release 2.1.x.x to Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.4) to Release 2.3 (0.0)
- From Release 2.2(1.3) to Release 2.3 (0.0)
- From Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0)
- From Release 2.2(1.1) to Release 2.2(1.3) to Release 2.3 (0.0)
- From Release 2.2(1.0) to Release 2.2(1.3) to Release 2.3 (0.0)
- From Release 2.2(0.6) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0)
- From Release 2.2(0.5) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0)
- From Release 2.2(0.4) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0)
- From Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0)
- From Release 2.2(0.2) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0)
- From Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0)
- From Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0)
- From Release 2.1.x.x to Release 2.2(0.1) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0)
- From Release 2.1.x.x to Release 2.2(0.0) to Release 2.2(0.3) to Release 2.2(1.2) to Release 2.2(1.3) to Release 2.3 (0.0)

CentOS 7 migration is possible only from platform versions 6.7.4.x (6.7.4.0, 6.7.4.1, 6.7.4.2, 6.7.4.3). As Cisco IMC Supervisor Release 2.2.1.3 is based on platform version 6.7.4.0 and Cisco IMC Supervisor Release 2.2.1.4 is based on platform version 6.7.4.2 ,and you should upgrade your appliance first to either Cisco IMC Supervisor versions 2.2.1.3 or 2.2.1.4 and try CentOS 7 migration.

Data Migration

Data Migration has two options

- Online Migration
- Offline Migration

Online Migration

Procedure

Step 1 Login to SSH with root credentials of the target system.

Step 2 Navigate to the migration folder with the following command.

```
cd /opt/infra/migration
```

Step 3 Run the **./performMigration.sh** script.

```
[root@localhost migration]# sh performMigration.sh
********************************************************************************
  ******************   IMC Supervisor CentOS 7.0 Migration  ********************
********************************************************************************

Current IMC Supervisor Version       :  2.3.2.0
Deployment Type                      :  standalone
Note: Before migrating data to the latest version of Cisco IMC Supervisor,
ensure that you run the CSA tool in the current version to identify and resolve the
incompatibilities.
Have you resolved the incompatibilities [y/n]?
```

Step 4 Enter y and press Enter.

The following sample information will be displayed.

```
Please proceed to migration...................

Services will be stopped before migration. Any existing data in this appliance database
will be deleted as part of migration.
Do you want to continue [y/n]? :
```

Step 5 Enter y and press Enter.

Step 6 Specify the IP address and root password details of the source system and press Enter.

The following sample information is displayed:

```
Enter IMC Supervisor 2.2.1.3 [or] 2.2.1.4 appliance IP address : 10.105.219.111
Enter root password for 10.105.219.111               :
Trying to connect to database on 10.105.219.111 : UP
Checking for available free disk space for 10.105.219.111
Required disk space : 237 MB
Available free disk space : 98272 MB
Initiating database backup on remote node. This process will take some time depending on
the database size.
............ done
Extracting the database backup archive file to validate the DB files.
. done

Validating the exported file is complete.
Exported database successfully.
Restoring database. This process will take some time depending on the database size.
Extracting database backup archive /opt/infra/migration/backup-ucsd/database_backup.tar.gz...
Initializing Database...
.............. done
Restoring data from db_private_admin.sql
.................................................................................. done
Restoring data from confmgr_production.sql
. done
```

```
Database restored successfully.
Product name from old appliance: Cisco IMC Supervisor
Bigdata specific upgrade is not required
Migrated property files successfully.
Updating multisite xml file...
Restore Open automation files...
Running database migration scripts [ Source : 6.7.4.2 ]
Upgrading database query...
Ending database upgrade process...
The database schema initialization has been triggered. This will take some time. Please
wait until schema initialization is complete.
..................................... done
Schema Initialization has been completed.
Started encrypting all password field using dynamic AES key.

SLF4J: Class path contains multiple SLF4J bindings.
SLF4J: Found binding in
[jar:file:/opt/infra/lib/slf4j-log4j12-1.7.2.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in
[jar:file:/opt/infra/lib/common/slf4j-log4j12-1.7.25.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
SLF4J: Actual binding is of type [org.slf4j.impl.Log4jLoggerFactory]
Completed encrypting all password field using dynamic AES Key.

Starting services. Use the "Display Services Status" option to check the status.
Migration completed successfully.
Migration log file available at /var/log/ucsd/migrateCentOS7.log
[root@localhost migration]#
```

Once the migration process is completed, the source system services get turned off, and the target system will be up with the migrated information. However, the source appliance and its IP address will be available for you to use it.

Offline Migration

Procedure

Step 1 Login to SSH with root credentials of the target system.

Step 2 Navigate to the migration folder with the following command.

```
cd /opt/infra/migration
```

Step 3 Execute the command **/performMigration.sh offline copyMigrationScript**command to copy the migration script **(/opt/infra/migration)** of the target system to the source system (opt/infra/migration).

```
  ******************   IMC Supervisor CentOS 7.0 Migration  ********************
********************************************************************************

Current IMC Supervisor Version       :  2.3.2.0
Deployment Type                      :  standalone
Note: Before migrating data to the latest version of Cisco IMC Supervisor,
ensure that you run the CSA tool in the current version to identify and resolve the
incompatibilities.
Have you resolved the incompatibilities [y/n]?
```

Step 4 Enter y and press Enter.

```
Please proceed to migration...................
```

Step 5 Specify the IP address and root password details of the source system and press Enter.

The following information will be displayed.

```
Enter IMC Supervisor 2.2.1.3 [or] 2.2.1.4 appliance IP address : 10.105.219.111
Enter root password for 10.105.219.111               :
Transferred centOS7 migration files successfully.
[root@localhost migration]#
```

Step 6 SSH into the source system and navigate to the /**opt/infra/migration** folder.

Step 7 Executing the command backs up the data **./performMigration.sh offline backup**.The following command is displayed:

```
******************   IMC Supervisor CentOS 7.0 Migration  ******************
********************************************************************************

Current IMC Supervisor Version       :  2.2.1.4
Deployment Type                      :  standalone
Note: Before migrating data to the latest version of Cisco IMC Supervisor,
ensure that you run the CSA tool in the current version to identify and resolve the
incompatibilities.
Have you resolved the incompatibilities [y/n]?
```

Step 8 Enter y and press Enter.

The following command will be displayed.

```
Please proceed to migration...................
Services will be stopped before migration. Do you want to continue [y/n]? :
```

Step 9 Enter y and press Enter.

The following command will be displayed.

```
Copying config files...
Starting config file migration...
No Open Automation feature found in existing appliance.
Required disk space : 71 MB
Available free disk space : 25888 MB
Initiating database backup on remote node. This process will take some time depending on
the database size.
Taking backup of db_private_admin database............ done
Taking backup of confmgr_production database.... done
Creating database backup archive... done
Database backup archive: /opt/infra/migration/backup-ucsd/database_backup.tar.gz
LOG_FILE=/var/log/ucsd/migrateCentOS7.log
Extracting the database backup archive file to validate the DB files.
. done

Validating the exported file is complete.
Exported database successfully.
Migrating script module process...
Generated /opt/infra/migration/backup-ucsd/backup-ucsd.tar.gz file with the backup contents.
Do you want to copy the IMC Supervisor backup file to a remote location [y/n]?
```

Step 10 Specify the transfer mode and press Enter.

```
Specify the transfer mode [FTP/SFTP/SCP]:
```

Step 11 Specify the IP and login credentials, and press Enter.

The following command will be displayed.

```
Specify the login credentials

Server IP Address: 10.105.219.110
Server Login: root
Server Password:
Sub-directory (from Home directory) to store the file. Press enter to select the Home
directory: /home
Warning: Permanently added '10.105.219.110' (ECDSA) to the list of known hosts.
File is copied successfully
[root@localhost migration]#
```

Step 12 Login to SSH with root credentials of the target system.

Step 13 Navigate to the folder **/opt/infra/migration**.

Step 14 Execute the command **./performMigration.sh offline restore**.

Step 15 Remote backup file copy will be prompted.

The following command will be displayed.

```
[root@localhost migration]# sh performMigration.sh offline restore
********************************************************************************
  ******************   IMC Supervisor CentOS 7.0 Migration  ********************
********************************************************************************

Current IMC Supervisor Version       :  2.3.2.0
Deployment Type                      :  standalone

Note: Before migrating data to the latest version of Cisco IMC Supervisor,
ensure that you run the CSA tool in the current version to identify and resolve the
incompatibilities.
Have you resolved the incompatibilities [y/n]?
```

Step 16 Enter y and press Enter.

The following command will be displayed.

```
Please proceed to migration...................

Services will be stopped before migration. Any existing data in this appliance database
will be deleted as part of migration.
Do you want to continue [y/n]? :
```

Step 17 Enter y and press Enter.

The following command will be displayed.

```
Do you want to copy the IMC Supervisor backup file from a remote location [y/n]? :
```

Step 18 Enter y and press Enter.

Step 19 Specify the transfer mode and press Enter.

```
Specify the transfer mode [FTP/SFTP/SCP]:
```

Step 20 Enter y and press Enter.

The following command will be displayed.

```
Please proceed to migration...................

Services will be stopped before migration. Any existing data in this appliance database
will be deleted as part of migration.
Do you want to continue [y/n]? :
```

Step 21 Specify the IP and login credentials, and press Enter.

The following command will be displayed.

```
Specify the login credentials

Server IP Address: 10.105.219.111
Server Login: root
Server Password:
Remote Backup File (Absolute Path to File backup-ucsd.tar.gz ):
/opt/infra/migration/backup-ucsd/backup-ucsd.tar.gz

File is fetched successfully.
Extracting the backup archive file....
Required disk space : 237 MB
Available free disk space : 98342 MB
Restoring database. This process will take some time depending on the database size.
Extracting database backup archive /opt/infra/migration/backup-ucsd/database_backup.tar.gz...
Initializing Database...
.......... done
Restoring data from db_private_admin.sql
.....................................................................................
 done
Restoring data from confmgr_production.sql
. done
Database restored successfully.
Migrating config files...
Product name from old appliance: Cisco IMC Supervisor
Bigdata specific upgrade is not required
Migrating open automation files...
Running database migration scripts [ Source : 6.7.4.2 ]
Upgrading database query...
Ending database upgrade process...
The database schema initialization has been triggered. This will take some time. Please
wait until schema initialization is complete.
..................................... done
Schema Initialization has been completed.
Started encrypting all password field using dynamic AES key.

SLF4J: Class path contains multiple SLF4J bindings.
SLF4J: Found binding in
[jar:file:/opt/infra/lib/slf4j-log4j12-1.7.2.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in
[jar:file:/opt/infra/lib/common/slf4j-log4j12-1.7.25.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
SLF4J: Actual binding is of type [org.slf4j.impl.Log4jLoggerFactory]
Completed encrypting all password field using dynamic AES Key.

Starting services. Use the "Display Services Status" option to check the status.
Migration completed successfully.
Migration log file available at /var/log/ucsd/migrateCentOS7.log
[root@localhost migration]#
```

Note Migration is performed by exporting the backed up data from the source system to target system, **/opt/infra/migration/backup-ucsd/backup-ucsd.tar.gz**to the backup data located in the target system during the backup process.

Note Customers who failed to export the backup data from source machine to target machine in backup operation can use the above mentioned option to move backed up data from remote location.

Migration Checklist

As part of CentOS7 migration you will be migrating all configurations and data from source system to target system and below mentioned exceptions would not migrate for IMCS 2.3(2.0).

- Diagnostics ISO Images
- Local Firmware Upgrade ISO Images
- IMC Supervisor Patch Images
- Host Mapping Images
- Server Diagnotics Report
- Techsupport Report

Table 1: List of Exceptions

Menu	Module	Component	Migration Status
Systems	Firmware Management	Images Local	Not Applicable
Systems	Firmware Management	Firmware Upgrades	Not Applicable
Systems	Firmware Management	Host Image Mapping	Not Applicable
Systems	Server Diagnostics	SCU Image Profiles	Not Applicable
Systems	Server Diagnostics	Server Diagnostics	Not Applicable
Systems	Inventory and Faults	Rack Servers – Tech Support	Not Applicable
Administration	Update IMCS	IMCS Update Report	Not Applicable

Digitally Signed Images

Cisco IMC Supervisor release 2.2(1.2) images are delivered in digitally signed zip files. These signed zip files are wrapped in a container zip file that includes the following:

- Digitally signed zip file—Contains the Cisco IMC Supervisor installation or upgrade image
- Verification program—Verifies the certificate chain and signature. During certificate chain validation, the program verifies the authenticity of the end-entity certificate using Cisco's SubCA and root CA certificates. Then, the authenticated end-entity certificate is used to verify the signature.
- Digital signature file—Contains the signature that you can verify before installation or upgrade.
- Certificate file—Enables you to verify the digital signature. This Cisco-signed x.509 end-entity certificate contains a public key that can be used to verify the signature. This certificate is chained to the Cisco root posted on http://www.cisco.com/security/pki/certs/crcam2.cer.
- ReadMe file—Provides the information and instructions required to verify the digitally signed zip file.

Verify the image offline. Once the image is verified, you can begin the installation or upgrade of Cisco IMC Supervisor.

Requirements for Verifying Digitally Signed Images

Before you verify a Cisco IMC Supervisor digitally signed image, ensure that you have the following on your local machine:

- Connectivity to https://www.cisco.com during the verification process.
- Python 3.6.8
- OpenSSL

Verifying a Digitally Signed Image

Before you begin

Download the Cisco IMC Supervisor image from Cisco.com.

Procedure

Step 1 Unzip the file you downloaded from Cisco.com and verify that it contains the following files:

- ReadMe file
- Digitally signed zip file.
- Certificate file, for example `UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer`
- Digital signature generated for the image.
- Signature verification program, for example `cisco_x509_verify_release.py3`

Step 2 Review the instructions in the ReadMe file.

Note If there are any differences between these instructions and those in the ReadMe, follow the ones in the ReadMe.

Step 3 Run the signature verification program from the directory where you have unzipped the downloaded content.

Example: Signature Verification for Upgrade Patch

```
python3 ./cisco_x509_verify_release.py3 -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
-i cimcs_patch_2_3_2_0_67198.zip -s cimcs_patch_2_3_2_0_67198.zip.signature -v dgst -sha512
```

Step 4 Review the output and ensure that the verification has succeeded.

Example: Expected Output for Upgrade

```
Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully downloaded and verified crcam2.cer.
Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer
```

```
...
Successfully downloaded and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully verified the signature of cimcs_patch_2_3_2_0_67198.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```

Applying a Patch to Cisco IMC Supervisor

Choose this option to apply a patch to the appliance in **shelladmin**.

Note The patch file (zip file) is provided by Cisco IMC Supervisor. Before applying a patch:

- Review the patch release notes and the Readme file.
- Take a snapshot of your VM.
- Make a backup of your database prior to taking the patch. The **`Apply Patch`** option enables you to make a backup as part of the **`Apply Patch`** procedure; but the best practice is to create a backup immediately before using the **`Apply Patch`** option.
- Stop the appliance services.

Before you begin

- Download the patch file.
- Place the file in a web server or an FTP server.
- Choose **`Apply Patch`** from the Cisco IMC Supervisor Shell menu.
- Provide patch URL (http://WebServer/TestPkg.zip)

Procedure

Step 1 From the **Cisco IMC Supervisor Shell Menu**, choose **`Apply Patch`** and press **`Enter`**.

Information similar to the following is displayed:

```
Applying Patch...
Do you want to take database backup before applying patch (y/n)?
```

Step 2 If you entered **`y`**, enter the requested FTP server IP address and login data, then press **`Enter`**.

```
y
Backup will upload file to an FTP server.
Provide the necessary access credentials.
   FTP Server IP Address:
   FTP Server Login:
```

Step 3 If you entered **n**, enter the mode of transfer, and press **Enter** and provide the required information, as follows:

- SFTP—Enter the SFTP server IP address, server login name and password, and the path to the location where you have stored the upgrade file.
- SCP—Enter the SCP server IP address, server login name and password, and the path to the location where you have stored the upgrade file.
- FTP—Enter the FTP server IP address, server login name and password, and the path to the location where you have stored the upgrade file. For example,

  ftp://username:password@hostname\IP_address/software_location_and_name.
- HTTP—Enter the URL for the location where you stored the upgrade file.
- FILE—Enter the path to the local directory where you have stored the upgrade file.

```
n
User selected option not to take backup, proceeding with applying patch
Specify the Transfer mode [SFTP/SCP/FTP/HTTP/FILE]: SFTP
Server IP Address: XXX.XX.XXX.XXX
Server Username: XXXXX
Server Password:
SFTP Path to Patch Zip file:TestPkg.zip
Applying the Patch TestPkg.zip [y/n]? y
```

Note Refer to the Readme file for information about the patches.

Step 4 If you are prompted to confirm that you want to apply the patch, enter **y**, then press **Enter**.

Step 5 Follow the onscreen prompts to complete the process.

What to do next

After the patch is applied, choose **Stop Services** and **Start Services**.

Applying a Signed Patch to Cisco IMC Supervisor

Procedure

Step 1 From the Cisco IMC Supervisor Shell menu, choose **Apply Signed Patch** and press Enter.

The following information is displayed:

```
Applying Patch...
Services will be stopped before upgrade. Do you want to continue? [y/N]:
```

Step 2 Enter **y** and press **Enter**.

The following information is displayed:

```
Stopping services...
Do you want to take database backup before applying patch? [Y/n]:
```

Step 3 If you entered **Y** and press **Enter** the backup process starts. Enter the transfer mode and press **Enter**.

```
The backup process creates a <filename>.tar.gz file on the system running Cisco IMC
Supervisor.
You can copy this file to another server using the FTP/SFTP/SCP mode.
Specify the transfer mode and login credentials
Specify the transfer mode [FTP/SFTP/SCP]:
```

Note Refer to the ReadMe file for information about the patches.

Step 4 If you entered **n**, enter the desired patch file download protocol and press **Enter** and provide the required information, as follows:

- SFTP—Enter the SFTP server IP address, server login name and password, and the path to the location where you have stored the signed zip file.
- SCP—Enter the SCP server IP address, server login name and password, and the path to the location where you have stored the signed zip file.
- FTP—Enter the FTP server IP address, server login name and password, and the path to the location where you have stored the signed zip file. For example, **ftp**:*//username:password@hostname\IP_address/software_location_and_name*.
- HTTP—Enter the URL for the location where you stored the signed zip file.
- FILE—Enter the path to the local directory where you have stored the signed zip file.

```
n
User selected option not to take backup, proceeding with applying patch.
Enter patch file download protocol [SFTP/SCP/FTP/HTTP/FILE]: SCP
Server IP Address: 172.29.109.134
Server Username: root
Server Password:
Full Patch to Patch Zip File: /opt/mytest123/cimcs_patch_2_2_1_1_xxxx_signed.zip
Apply the patch '/opt/mytest123/cimcs_patch_2_2_1_1_xxxx_signed.zip? [y/N]:
```

Step 5 If you are prompted to confirm that you want to apply the patch, enter **y**, then press **Enter**.

The following information is displayed:

```
y
Checking if database is running ...yes
Downloading the patch...
Successfully Connected to 172.29.109.134
Completed downloading the patch.
Verifying patch signature...
Successfully verified the signature of patch file
/opt/mytest123/cimcs_patch_2_2_1_1_xxxx_signed.zip
Proceeding with patch installation
```

Note You can use the **Apply Signed Patch** option in the Shell menu to apply a signed patch for release 2.2(1.2) and later. If you want to upgrade to release 2.2(1.1), you should apply the patch zip file using the **Apply Patch** option.