Upgrading IoT FND

This section contains the following IoT FND upgrade topics:

Pre-Upgrade Checklist

The section identifies the tasks that can be performed before you begin your upgrade to ensure a successful upgrade and limited downtime.

- Back up application directory. For example, if you want to upgrade **`cgms RPM`**, then you must back up the **`/opt/cgms`** folder. For more information, refer to Installing or Upgrading the SSM Server

Note After upgrade, the manual changes made to the application scripts are lost.

- Back up database. For more information, refer to Creating a Full Backup of the IoT FND Database, Backing Up the IoT FND Database Incrementally

Verifying Certificates and System Requirements

This section describes how to verify certificates and the system requirements for the upgrade procedure.

- Generating and Exporting Certificates
- System Requirements

Upgrading IoT FND and IoT FND TPS Proxy

Note It is not necessary to stop the database during normal upgrades. All upgrades are in-place.

Note For virtual IoT FND installations using custom security certificates, see Managing Custom Certificates before performing upgrade.

Caution Run the following steps sequentially.

To upgrade the IoT FND application:

Step 1 Obtain the new IoT FND ISO from Cisco.

Step 2 Extract the **cgms rpms** into a directory from the FND release ISO file.

Step 3 Run **rpm -qa | grep cgms** to get the list of rpms installed in the application server.

Step 4 Run the following command to stop IoT FND.

RHEL Version	Command
8.x	`systemctl stop cgms`
7.x	`service cgms stop`

Note The application typically takes approximately 10 seconds to stop.

Step 5 Run **ps | grep java** to verify that no Java processes are running.

Step 6 Run the following command to make sure that the **cgms** service has stopped.

RHEL Version	Command
8.x	`systemctl status cgms`
7.x	`service cgms status`

Step 7 Run the following script to upgrade the IoT FND RPM.

IoT FND Release	Command

Upgrade to 4.11.0 from any earlier release.	`rpm -Uvh <new_cgms_rpm_filename> --force`
	For example, to upgrade to IoT FND release 4.11.0, run the following command.
	`rpm -Uvh cgms-4.11.0-46.x86_69.rpm --force`

IoT FND Release	Command
Upgrades prior to release 4.11.0.	`rpm -Uvh <new_cgms_rpm_filename>`

Note We recommend you to upgrade all the installed **rpms** with the same FND version that you will upgrade to. The new *rpm* files overwrite the existing files in **/opt/cgms**.

Note For TPS Proxy, the rpm is bundled in the IoT FND ISO file. Extract the rpm file and copy the rpm to a TPS server. Run the rpm upgrade command `rpm -Uvh cgms-tpsproxy-<fndversion>.rpm` on TPS server.

Step 8 Run **./db-migrate** in **/opt/cgms/bin** directory to upgrade the database.

Note Ensure that you run the **db-migrate** script after each upgrade.

Step 9 Enter the database password when prompted.

Note The default password is **cgms123**.

Step 10 Run the following command to start IoT FND.

RHEL Version	Command
8.x	`systemctl start cgms`
7.x	`service cgms start`

Note You can also use the RHEL (Red Hat Enterprise Linux) GUI to start the IoT FND service (**ADMIN** > **System Management** > **Server Settings** > **Services**).

Post-Upgrade Checklist

This section describes the tasks that you have to perform post upgrade:

Note Any manual changes made to the **cgms** scripts are lost post upgrade; therefore, you have to make the changes again.

- Run **setupCgms** script to reconfigure FND.

Note The **setupCgms** script provides information on new configurations that are part of this FND upgrade.

- Run **DB migrate** script to upgrade the database.
- Start **cgms service** to monitor the status.

Upgrade FND in HA Configuration or Clustered Mode

This section provides the tasks for upgrading IoT FND in high-availability (HA) configuration or clustered mode:

- Upgrade Oracle DB. For more information, refer to Upgrading the IoT FND Database.
- Stop all application servers that are part of the cluster.
- Upgrade all the FND applications.
- Run **`db-migrate`** post upgrade in one of the application servers.
- Start FND service one by one.