IBM Financial Transaction Manager for SWIFT Services for Multiplatforms Version 3.0.0

Readme
Fix Pack 12

This edition applies to Version 3.0.0 of IBM® Financial Transaction Manager for SWIFT Services for Multiplatforms (5725-X92) - Fix Pack 3.0.0.12.

Reference key: 20190829-1000

Contents

General information

Before starting with the installation process, view the online version of this readme file to check if information has changed since the readme file was downloaded.

Download location

You can download FTM SWIFT 3.0.0.12 from Fix Central :

https://www.ibm.com/support/fixcentral/

Search for the Fix ID: 3.0.0-FTM-SWS-MP-fp0012

Prerequisites and co-requisites

Before installing the current fix pack perform the following steps:

- Check the hardware and software requirements of the fix pack you plan to install:
  Go to https://www.ibm.com/support/docview.wss?uid=swg27027034
  and select version **V3.0** and product **FTM for SWIFT Services for Multiplatforms**.

  Updates of pre-requisite software must not be performed during fix pack installation and migration. It is a separate activity:

  – If your software is not at the minimum version required by the new fix pack, upgrade it to a level supported by your current installation and the new fix pack before you start the fix pack installation and migration activity.

  – If the new fix pack provides support for a new software version, install this new version only after you finished the installation and migration activity of the fix pack.
- Review the flashes on the Financial Transaction Manager support web site:
  https://www.ibm.com/support/home/product/W823356Z48952D56/IBM_Financial_Transaction_Manager
- Ensure that you have at least 500 MB of free disk space to contain the uncompressed installation image.
- If you already have FTM SWIFT installed:

  – If you have obtained special fixes, contact IBM Support to determine whether you need an updated version of the fixes before you install this fix pack.

  – Ensure that you have at least fix pack 3.0.0.8 installed and all post-installation steps were finished.

What's new in FTM SWIFT

The following sections summarize what has changed in updates of FTM SWIFT since fix pack 3.0.0.8.

For a list of fixes provided and APARs included in the various product updates refer to:
http://www.ibm.com/support/docview.wss?uid=swg21970097

What's new in FTM SWIFT 3.0.0, Fix Pack 12

The following changes were introduced:

SWIFT Standards Release 2019 (SR2019) added

SR2019 is supported. This includes:

- FIN:

  - Message standards as specified in *Message Format Validation Rules - November 2019 Standards Release*
  - Validation of ISN messages for the mandatory SWIFT gpi services gCCT, gCOV, and gSRP as documented in *SWIFT gpi - Supplementary Message Format Validation Rules, 14 June 2019*
  - MTXML schema files for FIN SR2019. For more details refer to "Summary of changes" on page 29.
- MX
- Funds 5.2

The provided standards release update activates automatically according to the release schedule of SWIFT. However, you can install this fix pack before the SR2019 live date and continue to process messages according to the current standards release. If you want to use the new standards release updates for testing purposes earlier, you can activate them by using FTM SWIFT configuration. For details see Testing a new message definition set.

Removed support for SWIFT Standards
The support for the following SWIFT Standards is removed:

- FIN (SR2016)
- MX (SR2016)
- Funds 4.9

FIN Message Length Check
The length of FIN ISN messages is checked by the MER facility and when using message validation APIs.

What's new in FTM SWIFT 3.0.0, Fix Pack 11

The following changes were introduced:

Support for additional versions of prerequisite software
FTM SWIFT now supports:

- IBM Integration Bus version 10
- IBM Db2® version 11.1
- IBM WebSphere® Application Server version 9

What's new in FTM SWIFT 3.0.0, Fix Pack 10

The following changes were introduced:

SAG 7.3
FIN message transfer services and MSIF transfer services can now use SWIFT Alliance Gateway (SAG) 7.3 and SWIFTNet Link (SNL) 7.3 to send and receive messages or files.

SAG Add-On

- SAG Add-On for SAG 7.3 is available for the following platforms now:
  - AIX®
  - Microsoft Windows
  - Red Hat Enterprise Linux (RHEL x86)

  The existing SAG Add-On for SAG 7.2 and SAG 7.0 is still available.
- SAG Add-On for SAG 7.3 on AIX and RHEL x86 enables users to adapt the runtime environment of the SAG Add-On to installation specific needs.

Data Integrity Checker Utility
The **check** command is enhanced to provide details of suspicious database entries of the FTM SWIFT FIN Service.

The new **dispose** command enables users to delete FTM SWIFT database entries of the FIN Service that are suspected of being manipulated.

What's new in FTM SWIFT 3.0.0, Fix Pack 9

The following changes were introduced:

Data integrity framework
Data integrity problems are now also written to syslog.

Housekeeping improvements

Stored procedures DNI_DI_OPEN and DNI_DI_CLOSE were introduced to enable SQL based maintenance using INSERT and DELETE statements on data integrity protected tables without requiring FTM SWIFT downtime.

Saving and purging configuration and security data was changed to make use of the new DNI_DI_OPEN and DNI_DI_CLOSE procedures.

FIN MTXML format changed

- All schema files were replaced due to a late update of MyStandards Base Libraries for SR2018.
- Type F72Z_148_Type was renamed to Text_4Ec_1_Type. This impacts MT 730 field F72Z.

New directory
The new directory `iFix` was introduced.

Known Problems

For a list of known problems refer to:
http://www.ibm.com/support/docview.wss?uid=swg22017050

Installation information

You can find information about the installation and migration steps mentioned in this document in the FTM SWIFT for Multiplatforms Knowledge Center at:

https://www.ibm.com/support/knowledgecenter/SSRH46_3.0.0_SWS

This readme document uses the following variables:

inst_dir
The installation directory of FTM SWIFT.
The default is: /opt/IBM/ftm/swift/v300.

run_dir
The directory for runtime data.
The default is: /var/ftmswift_v300/run.

cust_dir
The directory for customization data.
The default is: /var/ftmswift_v300/cus.

deployment_dir
The deployment data directory.
The default is: /var/ftmswift_v300/cus/depdata.

instance
The name of the FTM SWIFT instance.
The default is: INST1.

ou
The name of the organizational unit.
Depending on the context this might be SYSOU, DNFSYSOU, or the name of a business OU.

db2_dsn
The name of the FTM SWIFT runtime database.

Installing FTM SWIFT 3.0.0.12 - Create a new installation

If you have not installed FTM SWIFT yet:

1. Plan your system as described in Planning.
2. Install fix pack 3.0.0.12 by following the description in Installing FTM SWIFT.
3. Prepare your system as described in Preparing to create an instance.
4. Customize your instance as described in Customizing an instance for which resources have not yet been deployed.

Installing FTM SWIFT 3.0.0.12 - Update an existing installation

Updating an existing environment consists of the phases *Preparing*, *Switching*, *Cleaning up* and optionally *Falling back*.

Depending on how you share your product files there are two installation variants that differ in the amount of migration steps you can prepare before entering the downtime during which you cannot process workload:

Separated file systems
The file systems of the installation system and the customization/runtime systems are separated. The fix pack installation only affects the installation system until you manually share the files with your

customization and runtime system. This helps you to prepare migration steps while your system can still process workload.

Shared file system
Your installation, customization and runtime environment use a single shared file system. The fix pack installation may immediately affect your runtime environment. This reduces the steps you can do to prepare the migration while your system can still process workload.

Choose the subsection that applies to your file system setup.

Separated file systems: Preparing and Switching

Follow the steps required to prepare and switch your environment.

Preparing

Perform the following steps while your runtime system continues to process workload:

1. If you use MER:
   Identify outdated messages and templates using the MER message administration utility. Perform a migration action on the detected templates.
2. Ensure that no customization operation is pending .
3. Ensure that no configuration or security administration change is pending .
4. Create a backup of your customized administrative scripts from *deployment_dir*/*instance*/admin:

   ```
   mkdir ~/admin_scripts_backup
   cp /var/ftmswift_v300/cus/depdata/INST1/admin/* ~/admin_scripts_backup
   ```

5. Use IBM Installation Manager to install the fix pack for FTM SWIFT 3.0.0.12.
6. Share the files in the *inst_dir*/admin directory with your customization system.
7. If your current FTM SWIFT fix pack level is 3.0.0.8 or 3.0.0.9:
   Create and assign new user group:
   a. This fix pack introduces a new customization placeholder that represents an operating system user group that will be granted permissions required to run the new Data Integrity Checker **dispose** command:
      - DNIvDDGRP

      Plan which user group you will assign later in the customization process to the placeholder.
   b. Ask your system administrator to create a missing user group and assign it to the appropriate user id's.
8. If your current FTM SWIFT fix pack level is 3.0.0.8 or 3.0.0.9:
   Provide a value for the new customization placeholder, and create deployment instructions and vehicles:
   a. Log on to your customization system as a customizer (ucust1).
   b. Change to the customization file system, for example:

      ```
      cd /var/ftmswift_v300/cus
      ```

   c. Start the CDP in migration mode and generate a CDD that contains the definitions for your environment:

      ```
      dnicdpm -i instance
      > export cdd/instance_FP3012.cdd
      > supplement cdd/instance_FP3012.cdd cdd/instance_FP3012_supp.cdd
      ```

   d. The new CDD cdd/instance_FP3012_supp.cdd contains the new placeholder *DNIvDDGRP*.

      For more information refer to Customization placeholders.

Edit the CDD and provide an appropriate value for your environment.

e. Import the edited CDD and prepare deployment instructions and vehicles:

```
> import cdd/instance_FP3012_supp.cdd
> prepare
```

This step updates the customized administrative scripts in directory *deployment_dir*/*instance*/admin. It generates deployment instructions in file *deployment_dir*/*instance*/*timestamp*/instructions.txt.

f. Implement the customization definition data and quit the CDP session:

```
> implement
> quit
```

When the message "DNIZ9013I: If you continue, the current CDD will be overwritten by a new CDD." is displayed enter 'y' to continue.

9. If your current FTM SWIFT fix pack level is 3.0.0.10 or 3.0.0.11:
Update customization definition data, and create deployment instructions and vehicles .
10. If you plan manual deployment of the FTM SWIFT BAR files, follow Prepare BAR files for manual deployment .
11. Prepare the migration of configuration entities.

Switching

Perform the following steps during a scheduled downtime:

1. Stop all sessions and services you use.
2. Stop all FTM SWIFT application servers.
3. Back up the FTM SWIFT IBM WebSphere Application Server (WAS) profiles.
4. Restart all FTM SWIFT application servers.
5. Stop all FTM SWIFT enterprise applications.
6. Stop all FTM SWIFT related message flows .
7. Stop all FTM SWIFT message brokers.
8. Share the files in the *inst_dir*/run directory with your runtime system.
9. Back up your runtime database.
10. Open and follow the deployment instructions.
11. Follow the instruction in Verifying the installation of the database routines .
12. Restart all FTM SWIFT message brokers.
13. Deploy BAR files .
14. Verify the deployed BAR files:

```
dniczbap -cmd list -flow DNI_SYSADM
```

The deployment was successful if the displayed version contains 3.0.0.12.

15. Re-activate FTM SWIFT accounting if you use the SIPN FIN or FMT FIN service.
16. Restart all FTM SWIFT related message flows .
17. Migrate the configuration entities.
18. Restart all FTM SWIFT enterprise applications.
19. Restart all sessions and services.
20. Update the IBM Integration Toolkit workstation if you use message set projects containing XML schema definitions that, for example, are utilized by the IBM Integration Toolkit XPath wizard.

Check the impact of SR2019 changes to your routing flows and rebuild and redeploy affected BAR files.

21. Update SAG Add-On for SAG 7.3:
    - After you finished the migration you can upgrade to SAG Add-On for SAG 7.3.
    - If you already use SAG Add-On for SAG 7.3 follow the description in Update an SAG Add-On.

Shared file system: Preparing and Switching

Follow the steps required to prepare and switch your environment.

Preparing

Perform the following steps while your runtime system continues to process workload:

1. If you use MER:
   Identify outdated messages and templates using the MER message administration utility. Perform a migration action on the detected templates.
2. Ensure that no customization operation is pending .
3. Ensure that no configuration or security administration change is pending .
4. If your current FTM SWIFT fix pack level is 3.0.0.8 or 3.0.0.9:
   Create and assign new user group:
   a. This fix pack introduces a new customization placeholder that represents an operating system user group that will be granted permissions required to run the new Data Integrity Checker **dispose** command:
      - DNIvDDGRP

      Plan which user group you will assign later in the customization process to the placeholder.
   b. Ask your system administrator to create a missing user group and assign it to the appropriate user id's.
5. Create a backup of your customized administrative scripts from *deployment_dir*/*instance*/admin:

```
mkdir ~/admin_scripts_backup
cp /var/ftmswift_v300/cus/depdata/INST1/admin/* ~/admin_scripts_backup
```

Switching

Perform the following steps during a scheduled downtime:

1. Stop all sessions and services you use.
2. Stop all FTM SWIFT application servers.
3. Back up the FTM SWIFT IBM WebSphere Application Server (WAS) profiles.
4. Restart all FTM SWIFT application servers.
5. Stop all FTM SWIFT enterprise applications.
6. Stop all FTM SWIFT related message flows .
7. Stop all FTM SWIFT message brokers.
8. Use IBM Installation Manager to install the fix pack for FTM SWIFT 3.0.0.12.
9. If your current FTM SWIFT fix pack level is 3.0.0.8 or 3.0.0.9:
   Provide a value for the new customization placeholder, and create deployment instructions and vehicles:
   a. Log on to your customization system as a customizer (ucust1).
   b. Change to the customization file system, for example:

```
cd /var/ftmswift_v300/cus
```

c. Start the CDP in migration mode and generate a CDD that contains the definitions for your environment:

```
dnicdpm -i instance
> export cdd/instance_FP3012.cdd
> supplement cdd/instance_FP3012.cdd cdd/instance_FP3012_supp.cdd
```

d. The new CDD cdd/instance_FP3012_supp.cdd contains the new placeholder *DNIvDDGRP*.

For more information refer to Customization placeholders.

Edit the CDD and provide an appropriate value for your environment.

e. Import the edited CDD and prepare deployment instructions and vehicles:

```
> import cdd/instance_FP3012_supp.cdd
> prepare
```

This step updates the customized administrative scripts in directory *deployment_dir*/*instance*/admin. It generates deployment instructions in file *deployment_dir*/*instance*/*timestamp*/instructions.txt.

f. Implement the customization definition data and quit the CDP session:

```
> implement
> quit
```

When the message "DNIZ9013I: If you continue, the current CDD will be overwritten by a new CDD." is displayed enter 'y' to continue.

10. If your current FTM SWIFT fix pack level is 3.0.0.10 or 3.0.0.11:
Update customization definition data, and create deployment instructions and vehicles .
11. Back up your runtime database.
12. Open and follow the deployment instructions.
13. Follow the instruction in Verifying the installation of the database routines .
14. Restart all FTM SWIFT message brokers.
15. If you plan manual deployment of the FTM SWIFT BAR files, follow Prepare BAR files for manual deployment .
16. Deploy BAR files .
17. Verify the deployed BAR files:

```
dniczbap -cmd list -flow DNI_SYSADM
```

The deployment was successful if the displayed version contains 3.0.0.12.

18. Re-activate FTM SWIFT accounting if you use the SIPN FIN or FMT FIN service.
19. Restart all FTM SWIFT related message flows .
20. Prepare the migration of configuration entities.
21. Migrate the configuration entities.
22. Restart all FTM SWIFT enterprise applications.
23. Restart all sessions and services.
24. Update the IBM Integration Toolkit workstation if you use message set projects containing XML schema definitions that, for example, are utilized by the IBM Integration Toolkit XPath wizard.

Check the impact of SR2019 changes to your routing flows and rebuild and redeploy affected BAR files.

25. Update SAG Add-On for SAG 7.3:

- After you finished the migration you can upgrade to SAG Add-On for SAG 7.3.

- If you already use SAG Add-On for SAG 7.3 follow the description in Update an SAG Add-On.

Cleaning up

After you have verified that the migrated environment works as expected and you are sure that no fall back to the previous level of FTM SWIFT is needed, you can remove obsolete resources:

1. Drop the backed up WebSphere Application Server profiles.
2. Drop the backup of the database.
3. Remove the backup of your customized administrative scripts created in step “4” on page 10 (separated file systems) or “5” on page 12 (shared file system):

```
rm -rf ~/admin_scripts_backup
```

Falling back to the previous fix pack level

1. Stop all sessions and services you use.
2. Stop all FTM SWIFT application servers.
3. Stop all FTM SWIFT related message flows .
4. Stop all FTM SWIFT message brokers.
5. Recover the customization system.
6. Roll back the IBM Installation Manager update of the fix pack.
7. Share your files from the installation system with the customization and runtime system, if applicable.
8. Restore the backup of your runtime database.
9. If your migration starting point was FTM SWIFT fix pack level 3.0.0.9 or 3.0.0.10:
   To revert the FTM SWIFT database related changes run the following commands:
   a. `db2 "CONNECT TO DNIvDSN"`
   b. `db2 +c -z fbfp11.log -svf deployment_dir/instance/admin/dnifbfp11.ddl`
10. If your migration starting point was FTM SWIFT fix pack level 3.0.0.8:
    To revert the FTM SWIFT database related changes run the following commands:
    a. `db2 "CONNECT TO DNIvDSN"`
    b. `db2 +c -z fbfp9.log -svf deployment_dir/instance/admin/dnifbfp9.ddl`
11. Restart all FTM SWIFT message brokers.
12. Deploy previous FTM SWIFT BAR files:

```
. /var/ftmswift_v300/run/dniprofile
dniczbap -cmd prepare -update old -deploy [-broker broker_name]
```

13. Verify the deployed BAR files:

```
dniczbap -cmd list -flow DNI_SYSADM
```

    The deployment was successful if the displayed version contains the fix pack that was your migration starting point.
14. Re-activate FTM SWIFT accounting if you use the SIPN FIN or FMT FIN service.
15. Restart all FTM SWIFT related message flows .
16. Restore the IBM WebSphere Application Server profile backups.
17. Restart all FTM SWIFT application servers.
18. Restart all sessions and services.
19. Restore your IBM Integration Toolkit workstation if you updated it during Installation:

a. Restore your Toolkit workspace.

b. Rebuild and deploy your restored message flows.

20. If you use SAG Add-On for SAG 7.3, roll back the SAG Add-On to the previous level. Follow the description in “Roll back an SAG Add-On” on page 26.
21. Restore the backup of your customized administrative scripts created in step “4” on page 10 (separated file systems) or “5” on page 12 (shared file system):

```
rm -rf /var/ftmswift_v300/cus/depdata/INST1/admin/*
cp ~/admin_scripts_backup/* /var/ftmswift_v300/cus/depdata/INST1/admin/
```

Maintenance tasks

The following sections provide detailed instructions for selected installation steps of a fix pack. Refer to "Installing FTM SWIFT 3.0.0.12 - Update an existing installation" on page 9 to find out which steps you have to perform and to determine the sequence.

Ensure that no customization operation is pending

When you apply maintenance fixes to FTM SWIFT, no customization operation must be pending. That is, all previously prepared deployment instructions were carried out and the CDP **implement** command was used before you can apply an update.

To check that all previous CDD changes were implemented using the CDP:

1. Log on to your customization system as a customizer (ucust1).
2. Enter the following command:

   ```
   inst_dir/admin/bin/dnicdpst -i instance -cdefs cust_defs_dir
   ```

   where:

   inst_dir
   The FTM SWIFT installation directory

   instance
   The name of the FTM SWIFT instance

   cust_defs_dir
   The name of the customization definitions directory as specified in the CDP ini file, for example: `/var/ftmswift_v300/cus/defs`
3. Check whether the response indicates that a customization operation is still pending.
4. If a operation was pending in customization mode (dnicdp), implement it before continuing.
5. If a operation was pending in migration mode (dnicdpm):
   - Ensure that you have not yet shared the new files contained in this or any other product update with the customization system.
   - Implement the pending operation before continuing.

Note: Ensure that no changes are made to the currently implemented CDD until the migration for the current product update has been completely finished.

Ensure that no configuration or security administration change is pending

When you apply maintenance fixes to FTM SWIFT, no configuration or security administration changes must be pending.

To ensure that all configuration administration changes have been deployed and that all security administration changes have been approved:

1. Log on to your runtime system as a system configuration administrator (sa1).
2. Run the `dniprofile` by entering:

   ```
   . /var/ftmswift_v300/run/dniprofile
   ```
3. Enter the following commands:

```
dnicli -s DNI_SYSADM -ou SYSOU -c "list -ou % -qo amorz"
dnicli -s DNI_SYSADM -ou SYSOU -c "list -cos % -qo amorz"
dnicli -s DNI_SYSADM -ou SYSOU -c "list -ct % -qo amorz"
```

4. Check that each list command did result in 'No [OU/COS/CT] match search criteria'.
5. Log on to your runtime system as a security administrator (ua1).
6. Run the `dniprofile` by entering:

```
. /var/ftmswift_v300/run/dniprofile
```

7. Enter the following commands:

```
dnicli -s DNI_SECADM -ou SYSOU -c "list -ro % -qo mor"
dnicli -s DNI_SECADM -ou SYSOU -c "list -rg % -qo mor"
```

8. Check that each list command did result in 'No roles/role groups found that match specified criteria'.
9. Enter the following command for each OU:

```
dnicli -s DNI_SECADM -ou OU -c "list -user % -qo mor"
```

10. Check that each list command did result in 'No users found that match specified criteria'.

Note: Ensure that no changes are made to configuration and security administration until the migration for the current product update has been completely finished.

Use IBM Installation Manager to install the fix pack

Extract the fix pack repository from the TAR archive you downloaded from Fix Central to a temporary directory, for example `/tmp/FTM_SWS_MP_3.0.0.9_fp009`.

After you have successfully applied the fix pack using IBM Installation Manager follow the instructions in “Granting access permissions to FTM SWIFT users” on page 19.

IBM Installation Manager offers different modes. The following two sections provide examples using wizard mode (graphical user interface or web) or command line driven installations. Choose one of the IBM Installation Manager modes.

Install a fix pack using wizard mode

To install a fix pack using wizard mode:

1. Start Installation Manager in graphical user interface or web mode.
2. Add the fix pack repository:
   a. Go to **File** > **Preferences** > **Repository** > **Add repository**.
   b. Enter the path of the extracted fix pack repository's `diskTag.inf` file, for example: `/tmp/FTM_SWS_MP_3.0.0.9_fp009/disk1/diskTag.inf`.
   c. Click **OK**.
3. Test the repository connection.
4. Close the Preferences dialog.
5. In the Installation Manager main window, click **Update**.
6. Select the package group of the FTM SWIFT installation to update with the fix pack.
7. Click **Next**.
8. Ensure the correct fix pack is displayed and selected.
9. Click **Next**.
10. Accept the license agreement.
11. Click **Next**

12. Review the summary information and click **Update**.
13. Click **Finish**.
14. Close the Installation Manager:
    - In graphical user interface mode, click **File** > **Exit**.
    - In web mode, click **File** > **Stop server**

Install a fix pack using command line mode

To install a fix pack on the command line:

1. Go to the Installation Manager tools directory, for example:

   ```
   cd /opt/IBM/InstallationManager/eclipse/tools
   ```

2. Run the command:

   ```
   ./imcl install com.ibm.ftmswift.mp.v300 -repositories fix_pack_repo -acceptLicense
   ```

   where *fix_pack_repo* is the fix pack repository's `diskTag.inf` file, for example: `/tmp/FTM_SWS_MP_3.0.0.9_fp009/disk1/diskTag.inf`.

3. Verify the installation result by issuing the following command:

   ```
   ./imcl listInstalledPackages -long |grep com.ibm.ftmswift
   ```

   The output includes the version of the installed fix pack, for example `3.0.0.9` for fix pack 9. Ensure that this version matches the fix pack you are currently installing.

Granting access permissions to FTM SWIFT users

This description assumes that you use the following group names:

- dniadmin
- dnilpp

To ease access for these groups, issue the following commands:

```
chgrp -R dniadmin inst_dir/admin
chgrp -R dnilpp inst_dir/run
chmod 755 inst_dir
chmod -R 750 inst_dir/admin
chmod -R 750 inst_dir/run
chmod -R 755 inst_dir/iFix
```

This gives the users in each of the specified groups access to the specified directories and all their subdirectories.

Table 1. Required access permissions to the customization programs, runtime programs, and data

Directory	Owner permissions	Owner group permissions	Other permissions	Owner group
inst_dir	r w x	r - x	r - x	Primary group of installer
inst_dir/admin	r w x	r - x	- - -	dniadmin
inst_dir/run	r w x	r - x	- - -	dnilpp
inst_dir/iFix	r w x	r - x	r - x	Primary group of installer

Update customization definition data, and create deployment instructions and vehicles

FTM SWIFT maintenance may require to update resources for an instance. The customization definition program (CDP) detects which resources are affected and prepares the necessary deployment data.

To execute the CDP in migration mode:

1. Log on to your customization system as a customizer (ucust1).
2. Change to the customization file system, for example:

```
cd /var/ftmswift_v300/cus
```

3. Run your customization profile:

```
. ./dnicus_instance
```

4. Start the CDP in migration mode and use the following commands to migrate customization data:

```
dnicdpm -i instance
> export cdd/instance_FPxxxx.cdd
> import cdd/instance_FPxxxx.cdd
> prepare
```

where

instance
The name of the FTM SWIFT instance.

xxxx
The version of the fix pack, for example 3002.

deployment_dir
The name of the customization deployment directory, for example: `/var/ftmswift_v300/cus/depdata`

This step updates the customized administrative scripts in the directory '*deployment_dir*/*instance*/admin'. It generates deployment instructions and record it in the file '*deployment_dir*/*instance*/*timestamp*/instructions.txt'. Dependent on the fix pack migration it generates the deployment data and vehicles.

5. Implement the customization definition data and quit the CDP session:

```
> implement
```

When the message "DNIZ9013I: If you continue, the current CDD will be overwritten by a new CDD." is displayed enter 'y' to continue.

```
> quit
```

Prepare BAR files for manual deployment

If you want to use the Toolkit or `mqsideploy` command to manually deploy the updated BAR files, you can customize them as soon as you have shared the FTM SWIFT installation directory's `run/flows` subdirectory with the message broker runtime system.

To customize BAR files for manual deployment:

1. Ensure that the updated BAR files are available.

If your installation and runtime systems are different:
Share the `run/flows` subdirectory of the FTM SWIFT installation directory from the installation system with the runtime system.

If your installation and runtime systems are identical:
Install the update using IBM Installation Manager as described in "Use IBM Installation Manager to install the fix pack" on page 18 during the switching phase.

2. On the runtime system where the message broker runs, log on as IBM Integration Bus administrator (uwmba1).
3. Run the `dniprofile` by entering:

```
. /var/ftmswift_v300/run/dniprofile
```

4. Create a sub-directory `ftmswift_`*xxxx* where *xxxx* is the version of the fix pack. You need read and write access and it must have at least 50 MB of free space. This is the directory in which dniczbap will store the customized BAR files.
5. Issue the following command to let the BAP identify the BAR files that are to be updated and customize them:

```
dniczbap -cmd prepare -update new -dir output_dir
```

where *output_dir* represents the directory you created in step "4" on page 21.

Each customized BAR file in the output directory has a name of the form:
instance`.`*broker*`.`*exec_group*`.`*BAR_file*`.bar` where

instance
The name of your FTM SWIFT instance.

broker
The name of the broker to which the BAR file is to be deployed.

exec_group
The name of the execution group to which the BAR file is to be deployed.

BAR_file
The name of the BAR file as provided by FTM SWIFT.

6. Transfer, in binary mode, the customized BAR files in the output directory to the system where you need to deploy them, for example your Toolkit system.
7. If you use the Toolkit to deploy the customized BAR files, import them now into your workspace.

Stop all FTM SWIFT related message flows

FTM SWIFT related message flows are based on FTM SWIFT provided IBM Integration Bus plugins. To ensure that both are updated before new messages are processed you need to stop the flows.

FTM SWIFT related message flows include:

- Flows provided by FTM SWIFT
- Flows you developed based on FTM SWIFT APIs

Use the Toolkit or the command `mqsistopmsgflow` to stop all FTM SWIFT related message flows.

Verifying the installation of the database routines

To verify the installation of the database routines:

1. On the runtime system, log on as a DB2® administrator (udb2adm1). The access rights of this user are described in *FTM SWIFT: Planning, Installation, and Customization*.
2. Ensure that you have access to a Java™ runtime environment.
3. Run the `dniprofile` by entering:

```
. /var/ftmswift_v300/run/dniprofile
```

4. Enter the following command on a single line:

```
jre_dir/bin/java
-cp inst_dir/run/classes/dnicddbm.jar:db2_inst_dir/java/db2jcc4.jar:$CLASSPATH
com.ibm.dni.dbm.DniGetSpInfo DNIvDSN DNIvSN
```

where:

jre_dir
The directory where your Java Runtime Environment (JRE) is installed.

inst_dir
The installation directory.

db2_inst_dir
The DB2 installation directory (for example, `/opt/ibm/db2/V10.5`).

DNIvDSN
The name of the runtime database, for example, DNIDBRUN.

DNIvSN
Name of the schema to be used, for example, DNI.

5. Examine the output and ensure that the following messages are displayed:

```
DNID0001I Correct stored procedures for 'SYSADM' are installed
DNID0001I Correct stored procedures for 'SECADM' are installed
```

Deploy BAR files

During the switching phase you need to update the message flows running in IBM Integration Bus. If you use multiple broker servers, you must perform the following steps for each.

If you have created customized BAR files as described in “Prepare BAR files for manual deployment” on page 20, use the Toolkit or `mqsideploy` now to deploy them.

To use the BAP to automatically customize and deploy updated BAR files:

1. Ensure that your brokers and execution groups are running.
2. On the runtime system, log on as IBM Integration Bus administrator (uwmba1).
3. Run the `dniprofile` by entering:

```
. /var/ftmswift_v300/run/dniprofile
```

4. Ensure that you have at least 50 MB of free space in the current directory.
5. Issue the following command:

```
dniczbap -cmd prepare -update new -deploy -broker brokername
```

The parameter -broker is only required if you use multiple broker servers.

The BAP will identify all BAR files for which the message flows deployed in the broker need to be updated and automatically customize and deploy them.

Re-activate FTM SWIFT accounting

If you use the SIPN FIN or FMT FIN service, re-activate FTM SWIFT accounting.

1. Log on as a IBM Integration Bus administrator (uwmba1).
2. Issue the following commands:

```
mqsichangeflowstats broker -a -e eg -f 'DNF_ILS_FIN' -c active -b basic -o "xml"
mqsichangeflowstats broker -a -e eg -f 'DNF_ILS_ACK' -c active -b basic -o "xml"
```

where:

broker
The name of the broker.

eg
The name of the execution group.

If you deployed the above mentioned bar files to multiple execution groups, repeat the steps for each execution group in which the bar files are deployed.

Restart all FTM SWIFT related message flows

After the updated message flows have been deployed as described in "Deploy BAR files" on page 22 you need to restart your message flows.

You can use either the BAP, the Toolkit or the command `mqsistartmsgflow` to start message flows provided by FTM SWIFT. For flows that you have developed you have to use the Toolkit or `mqsistartmsgflow`.

To use the BAP to start the message flows provided by FTM SWIFT on each broker server:

1. Ensure that your brokers and execution groups are running.
2. On the runtime system, log on as IBM Integration Bus administrator (uwmba1).
3. Run the `dniprofile` by entering:

```
. /var/ftmswift_v300/run/dniprofile
```

4. Issue the following command to start all message flows provided by FTM SWIFT on the current broker:

```
dniczbap -cmd start
```

Recover the customization system

Recover former service bundles, and restore the current definition directory and the deployment directory for administrative resources *deployment_dir*/*instance*/admin.

1. Log on to your customization system as a customizer (ucust1).
2. Change to the customization file system, for example:

```
cd /var/ftmswift_v300/cus
```

3. Run your customization profile:

```
. ./dnicus_instance
```

4. Start the CDP in migration mode and use the following commands to recover customization data:

```
dnicdpm -i instance
> recover
```

where *instance* is the name of the FTM SWIFT instance.

Roll back the IBM Installation Manager update of the fix pack

Use the roll back feature of IBM Installation Manager to remove an update and revert to a previous fix pack of FTM SWIFT.

After having reverted to a previous version of FTM SWIFT, follow the instructions in "Granting access permissions to FTM SWIFT users" on page 19.

IBM Installation Manager offers different modes. The following two sections are examples using wizard mode (graphical user interface or web) or command line driven roll backs. Choose one of the IBM Installation Manager modes.

Roll back using wizard mode

To roll back a fix pack using wizard mode:

1. Start Installation Manager in graphical user interface or web mode.
2. Click **Roll Back**.
3. Select the package group of FTM SWIFT and click **Next**.
4. Select the fix pack level to roll back to.
5. Click **Next**.
6. Review the summary information and click **Roll Back**.
7. Click **Finish**.
8. Close the Installation Manager:
   - In graphical user interface mode, click **File** > **Exit**.
   - In web mode, click **File** > **Stop server**

Roll back using command line mode

To roll back FTM SWIFT to the previously installed fix pack on the command line:

1. Go to the Installation Manager tools directory, for example:

   ```
   cd /opt/IBM/InstallationManager/eclipse/tools
   ```

2. Run the command:

   ```
   ./imcl rollback com.ibm.ftmswift.mp.v300
   ```

3. Verify the roll back result:

   ```
   ./imcl listInstalledPackages -long |grep com.ibm.ftmswift
   ```

   The output includes the version of the installed fix pack, for example `3.0.0.9` for fix pack 9. Ensure that this version matches the fix pack you are rolling back to.

Upgrade to SAG Add-On for SAG 7.3

Starting with version 3.0.0.10 FTM SWIFT provides an SAG Add-On for SAG 7.3 in the following directory: `/opt/IBM/ftm/swift/v300/admin/SAG73AddOn`

To migrate to SAG Add-On for SAG 7.3:

1. Stop your SAG Add-On for SAG 7.2.
2. Create a backup of your current SAG Add-On profile (dnfcssao.cfg).
3. Uninstall your current SAG Add-On.
4. Upgrade your SWIFT software (SAG and SNL) to version 7.3.
5. Install SAG Add-On for SAG 7.3.
6. Restore the backup of your SAG Add-On profile (dnfcssao.cfg).
7. Use the SAG Add-On password utility **dnfcspwd** to add the LAU key to the profile:

- On AIX and RHEL, enter:

```
./dnfcspwd -hk1 hk1
./dnfcspwd -hk2 hk2
```

- On Windows, enter:

```
dnfcspwd -hk1 hk1
dnfcspwd -hk2 hk2
```

where *hk1* and *hk2* represent the left and right half key used for local authentication between SAG Add-On and SAG.

8. Start SNL and SAG.
9. Start SAG Add-On.
10. Assign a local authentication (LAU) key to all message partners that are configured with message format **Sag:Relaxed** in the FTM SWIFT database:
    a. Issue the following command to get a list of all configured message partners:

```
listMessagePartner -sag sag -src cfg
```

    where *sag* is the name of your SAG configuration object.
    b. For each of the listed message partners *msg_partner*:
        1) Issue the following command to display the configuration data for *msg_partner*:

```
readMessagePartner -sag sag -mpn msg_partner -src cfg
```

        2) Check if the following message is displayed for *msg_partner*:

```
DNFG2028I SupportedMessageFormat (mfm1) 'Sag:RelaxedSNL'
```

        3) If this message is not displayed, no further action is required.

        Otherwise, check if the following message is also displayed for *msg_partner*:

```
DNFG2028I LAUKeyName (lkn) 'lau_key'
```

        where *lau_key* can have any value.
        4) If this message is displayed, a LAU key is already assigned to message partner *msg_partner* and no further action is required.

        Otherwise, assign a LAU key to message partner *msg_partner* by issuing the following command:

```
updateMessagePartner -sag sag -mpn msg_partner -lkn lau_key
```

        where:

        - *sag* is the name of your SAG configuration object
        - *lau_key* is a CO of type DnfLAUKeyMP that provides the LAU key to be used
11. Run a DNFSAGCFG **deploy** command to create or update the message partners used for communication between SAG Add-On and SAG:

```
deploy -sag sag
```

where *sag* is the name of your SAG configuration object.

Update an SAG Add-On

If a fix pack contains an update of SAG Add-On, use IBM Installation Manager to install the update. How to obtain the Installation Manager repository is described in *FTM SWIFT: Planning, installation, and customization / Preparing the SAG Add-On*. You do not need to stop the SAG in order to update the SAG Add-On.

1. If your SAG workstation is running on:
   - AIX: Stop the SAG Add-On subsystem.
   - Solaris: Stop the SAG Add-On daemon process.
   - Windows: Stop the SAG Add-On service.
   - RHEL x86: Stop the SAG Add-On service.

   If the SAG Add-On cannot be stopped, stop the SAG Add-On process manually. How to do these things is described in *FTM SWIFT: System Administration*.
2. Update the SAG Add-On with the corresponding fix pack level using IBM Installation Manager.
3. Start the SAG Add-On.

Roll back an SAG Add-On

If there are problems with a new level of an SAG Add-On, you can roll back to your previous level by carrying out the following steps:

1. If your SAG workstation is running on:
   - AIX: Stop the SAG Add-On subsystem.
   - Solaris: Stop the SAG Add-On daemon process.
   - Windows: Stop the SAG Add-On service.
   - RHEL x86: Stop the SAG Add-On service.

   If the SAG Add-On cannot be stopped, stop the SAG Add-On process manually. How to do these things is described in *FTM SWIFT: System Administration*.
2. Roll back your current SAG Add-On to the previous level using IBM Installation Manager.
3. Start the SAG Add-On.

Prepare the migration of configuration entities

FTM SWIFT maintenance may require to update configuration entities. The program dnfczmlc compares your current configuration with the target configuration. If it detects differences it creates CLI command files which will contain the configuration migration statements.

To prepare the migration of configuration entities:

1. If your installation and runtime systems are different:

   Share the `run/data` subdirectory of the FTM SWIFT installation directory from the installation system with the runtime system.
2. On the runtime system, log on as the system configuration administrator (sa1), and run the profile for your runtime environment by entering:

   ```
   . /var/ftmswift_v300/run/dniprofile
   ```
3. Create a sub-directory `ftmswift_`*xxxx* where *xxxx* is the version of the fix pack, for example 3002.
4. Switch to this directory and enter the following command:

```
dnfczmlc -i instance [-dual YES|NO] [-to timeout]
```

where

-i *instance*
The name of the FTM SWIFT instance.

-dual YES|NO
Specifies whether files are to be created for a system that uses dual authorization for SYSOU. The default is -dual YES. Specify -dual NO only if dual authorization is turned off for both DNI_SYSADM and DNI_SECADM in SYSOU at the time when the created files are executed. Whether dual authorization is switched on or off for other OUs is irrelevant.

-to timeout
The number of milliseconds that the CLI waits for a response to this command before it issues an error message. The default is 100000 (100 seconds). It must be a whole number between 20000 and 9999999.

The command dnfczmlc creates the CLI command files which will contain the configuration migration statements and stores it in the current directory.

Note: This command starts a long-running task that might take several minutes to complete. Check the file dnfczmlc.log to ensure that it completed successfully.

Migrate the configuration entities

FTM SWIFT maintenance may require to update configuration entities. In section "Prepare the migration of configuration entities" on page 26 you created some of the following CLI command files that need to be executed with the indicated user authorization:

- If dual authorization was not used (-dual NO):
  1. dnfczmlc_1_ua_rem_ro_all.cli by any UA
  2. dnfczmlc_2_sa_ent_all.cli by any SA
  3. dnfczmlc_3_ua_cre_ro_all.cli by any UA
- If dual authorization was used (-dual YES):
  1. dnfczmlc_1_ua_rem_ro_com.cli by the first UA (for example, ua1)
  2. dnfczmlc_1_ua_rem_ro_app.cli by the second UA (for example, ua2)
  3. dnfczmlc_2_sa_rem_cos_com.cli by the first SA (for example, sa1)
  4. dnfczmlc_2_sa_rem_cos_dep.cli by the second SA (for example, sa2)
  5. dnfczmlc_3_sa_rem_co_com.cli by the first SA
  6. dnfczmlc_3_sa_rem_co_dep.cli by the second SA
  7. dnfczmlc_4_sa_rem_ct_com.cli by the first SA
  8. dnfczmlc_4_sa_rem_ct_dep.cli by the second SA
  9. dnfczmlc_5_sa_cre_ct_com.cli by the first SA
  10. dnfczmlc_5_sa_cre_ct_dep.cli by the second SA
  11. dnfczmlc_6_sa_cre_co_com.cli by the first SA
  12. dnfczmlc_6_sa_cre_co_dep.cli by the second SA
  13. dnfczmlc_7_sa_cre_cos_com.cli by the first SA
  14. dnfczmlc_7_sa_cre_cos_dep.cli by the second SA
  15. dnfczmlc_8_ua_cre_ro_com.cli by the first UA
  16. dnfczmlc_8_ua_cre_ro_app.cli by the second UA

To migrate the configuration entities:

1. On the runtime system, log on as the indicated user, and run the profile for your runtime environment by entering:

   ```
   . /var/ftmswift_v300/run/dniprofile
   ```

2. Switch to the sub-directory ftmswift_*xxxx* you created in section “Prepare the migration of configuration entities” on page 26, step “3” on page 26.
3. Run the generated CLI command files in the numbered-sequence by entering the following command:

   ```
   dnicli -s svc -ou SYSOU -cft file | tee -a dnfczmlc_cli_xxxx.log
   ```

   where

   svc

   DNI_SYSADM
   For files executed by the system configuration administrators, abbreviated as SA.

   DNI_SECADM
   For files executed by the security administrators, abbreviated as UA.

   file
   The CLI command file name, for example dnfczmlc_5_sa_cre_ct_com.cli.

   xxxx
   The version of the fix pack, for example 3002.

Check the log-file to see if any error occurred.

Summary of changes

3.0.0.12

- Resource class FNCON: Configuration
  - CT/CO DnfExceptMsgAttr removed
  - CT/CO DnfExceptMsgAttr removed from COS DnfIlcFinCos and DnfIlsFinCos
  - attributes FIN106, FIN121, FIN206, FIN207, FIN256, FIN303, FIN307, FIN308, FIN405, FIN528, FIN529, FIN574, FIN577, FIN579, FIN582, FIN584, FIN587, FIN588, FIN589, FIN609, FIN643, FIN644, FIN645, FIN646, FIN649, FIN810, FIN812, FIN813, FIN820, FIN821, FIN822, FIN823, GPA074, and GPA094 removed from CT DnqERMessageRightsDNIFIN and CO ALL
  - attribute reda.003.001, setr.048.001, setr.050.001, setr.052.001, setr.054.001 and setr.056.001 removed from CT DnqERMessageRightsDNIFUNDS and CO ALL
  - attribute head.001.001, semt.010.001, semt.011.001 removed from CT DnqERMessageRightsDNIMX and CO ALL
  - attribute semt.041.001 and semt.042.001 added to CT DnqERMessageRightsDNIFUNDS and CO ALL
  - attribute admi.005.001, admi.006.001, admi.007.001, reda.014.001, reda.015.001, reda.016.001, reda.017.001, reda.022.001, reda.031.001, reda.041.001, reda.042.001, reda.043.001 and supl.034.001 added to CT DnqERMessageRightsDNIMX and CO ALL
- Resource class CFGPF: Modified enterprise applications
  - AO facility: dnp.ado.web.ear
  - MER facility: dnq.app.main.ear
  - RMA facility: dnf.rma.web.ear
- Toolkit resources: schema files
  - dni.schemas.swiftFin2019.zip
  - dni.schemas.swiftFin2018.zip
  - dni.schemas.swiftFin2017.zip
- Modified MTXML schema files

  For SR2019 a set of new schema files for the MTXML representation of FIN messages is provided. If you have customer implementations, for example Routing logic, you might have to adapt this logic. You might use the SWIFT UHB or MyStandards to identify the SR2019 related changes.

  In addition to the SR2019 related changes introduced to satisfy business requirements, SWIFT published the following changes for MTXML.

Table 2. Additional MTXML changes

Description	Impacted Fields	Impacted Messages
Type F22F_346_Type changed to F22F_265_Type.	F22F	524
Type F22H_105_Type changed to F22H_102_Type.	F22H	503, 504, 505, 506, 507
Type F41D_5_Type changed to F41D_3_Type.	F41D	700, 705, 707, 710, 720, 740
Type F57A_16_Type changed to F57A_9_Type.	F57A	516

Table 2. Additional MTXML changes (continued)		
Description	**Impacted Fields**	**Impacted Messages**
Type F58D_4_Type changed to F58D_Type.	F58D	700, 707, 710, 720
Type F71B_x_Type changed to F71B_18_Type.	F71B	102, 103, 103.REMIT, 103.STP, 104, 107, 200, 201, 202, 202.COV, 203, 204, 205, 205.COV, 341
Type F72_x_Type changed to F72_85_Type.	F72	n90, n91, 400
Type F72_x_Type changed to F72_117_Type.	F72	n90, n91, 410, 412, 420, 422, 430, 450, 456, 516, 526, 581, 600, 601, 604, 605, 606, 607, 769, 802, 900, 910, 935
Type F72_x_Type changed to F72_106_Type.	F72	304, 305
Type F72_x_Type changed to F72_113_Type.	F72	350, 62
Type F72Z_175_Type changed to F72Z_148_Type.	F72Z	732, 734, 740, 742, 744, 747, 750, 752, 754, 756
TypeF73_23_Type changed to F73_17_Type.	F73	801
Type F75_x_Type changed to F75_10_Type.	F75	n95, 422
Type F77B_x_Type changed to F77B_17_Type.	F77B	102, 103, 103.REMIT, 107, 734
Type F87A_5_Type changed to F87A_4_Type.	F87A	516, 526
Type F92C_3_Type changed to F92C_2_Type.	F92C	527, 558
Type F95C_x_Type changed to F95C_2_Type.	F95C	513, 514, 515, 517, 536, 537, 540, 541, 542, 543, 544, 545, 546, 547, 569, 575, 578, 586
Type F95P_x_Type changed to F95P_9_Type.	F95P	370, 380, 381, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 513, 514, 515, 517, 518, 519, 524, 527, 530, 535, 536, 537, 538, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 558, 564, 565, 566, 567, 568, 569, 575, 576, 578, 586, 670, 671
Type F95R_x_Type changed to F95R_3_Type.	F95R	321, 370, 380, 381, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 513, 514, 515, 517, 518, 519, 524, 527, 530, 535, 536, 537, 538, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 558, 564, 565, 566, 567, 568, 569, 575, 576, 578, 586, 670, 671

Table 2. Additional MTXML changes (continued)		
Description	**Impacted Fields**	**Impacted Messages**
Type F95S_x_Type changed to F95S_18_Type.	F95S	670, 671, 519
Type F95S_x_Type changed to F95S_16_Type.	F95S	540, 541, 542, 543, 544, 545, 546, 547, 548, 566, 578, 586
Type F99B_2_Type rename F99B_1_Type.	F99B	514

3.0.0.11

- Resource class DB
  - Updated Jar files for stored procedures
    - dnicdcfg.jar

3.0.0.10

- New customization placeholder
  - DNIvDDGRP (including new grants in resource class DBGNT and IBM MQ authorizations in resource class MQAUT)
- Resource class CFGPF: Modified enterprise applications
  - AO facility: dnp.ado.web.ear

3.0.0.9

- Resource class DB
  - New variable
    - DI_SESSION_INFO
  - New stored procedures
    - DNI_DI_OPEN
    - DNI_DI_CLOSE
    - DNI_DI_CHECK
    - DNI_DI_CHECK_INSERT
    - DNI_DI_CHECK_UPDATE
    - DNI_WRITE_SYSLOG
    - DNI_WRITE_SYSLOG_CODE
  - Modified stored procedures
    - DNI_DIC_INS
    - DNI_DIC_UPD
    - DNI_DIC_DEL
    - DNI_CHECK_CTRL_ROW
  - New Jar file for stored procedures
    - dni.sec.jar
  - Updated Jar files for stored procedures
    - dnicdrtn.jar

- dnicdcfg.jar

- Resource class CFGPF: Modified enterprise applications
  - MER facility: dnq.app.main.ear

Copyright and trademark information

http://www.ibm.com/legal/copytrade.shtml

Document change history

Date	Description of change
2019-08-30	Initial publication date