IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4

Readme
Fix Pack 9

This edition applies to Version 3.2.4 of IBM Financial Transaction Manager for SWIFT Services for Multiplatforms (5725-X92) - Fix Pack 9 (3.2.4.9).

Reference key: 20230331-1502

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 3.2.4.9 from Fix Central:

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

Search for the Fix ID **3.2.4-FTM-SWS-MP-fp0009**.

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 **V3.2** 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 the Financial Transaction Manager support web site:
  https://www.ibm.com/support/pages/node/6346924
- 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 3.2.4.7 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 4 (3.2.4.7).

For a list of fixes provided and APARs included in the various product updates refer to:
https://www.ibm.com/support/pages/node/6242258

What's new in FTM SWIFT Version 3.2.4 Fix Pack 9

The following changes were introduced:

Expand AO Bank Data Application to manage SWIFTNet remote addresses
The Administration and Operation (AO) web application can now manage SWIFTNet remote addresses for a bank data record.

RM filtering configurable
RM filtering is now configurable and can be made optional. RM filtering done by SWIFT is not affected.

New code signing certificate
A new code signing certificate is provided because a new code signing service provider is used by IBM.

Note: You need to import this certificate into your keystore as part of the migration procedure as described in this readme file.

Security enhancements for Web Applications
Several enhancements are included in FTM SWIFT enterprise applications to further improve the security.

_____

SAG Add-On installation/update considerations:

Update of the installed SAG Add-On required:	☐ YES	☑ NO

What's new in FTM SWIFT Version 3.2.4 Fix Pack 8

The following changes were introduced:

Message Entry and Repair (MER):

Remote address validation for messages in the DNIFINPLUS domain
MER now supports validation of the remote address field according to the SWIFTNet naming and addressing guidelines.

Number format configurable for DNIFINPLUS messages [FTMSWIFT-I-122]
Message Entry and Repair enterprise application supports number formatting for DNIFINPLUS messages, including browser print. You can configure thousands and decimal separators of numbers, for example for amounts.

BIC expansion for fields within messages of the DNIFINPLUS domain [FTMSWIFT-I-124]
Lookup and field expansion of a DNIFINPLUS message which contains BIC information are now supported in message entry and in browser printing. This change excludes the remote address information.

Additional attribute extraction for messages in the DNIFINPLUS domain [FTMSWIFT-I-131]

The values for Reference, Amount and Date are now extracted and displayed for the message types:

- pacs010
- camt029

Find message extended [FTMSWIFT-I-126]
The search criterion for finding messages by reference has been extended to allow dot (".") characters.

Error information for UNPARSABLE messages are now shown during edit
The error information which cause a message be marked as unparsable are now shown in the Unparsable edit dialog.

MSIF
MSIF will no longer reject incoming Store and Forward (SnF) messages from SWIFT if they fail the RM authorization check. Instead, applications will receive a MsgReceived notification with completion code `Partial0k` and reason codes DNFL9430E or DNFL9425I.

Support for IBM App Connect Enterprise (ACE)
FTM SWIFT now supports IBM App Connect Enterprise. The Broker Administration Program (BAP) and other system components have been enhanced to support both IIB and ACE versions. This change includes updated program outputs and changes to error messages issued by BAP. For details of supported versions and required levels, refer to the software requirements.

Message printing service

Number format configurable for DNIFINPLUS messages [FTMSWIFT-I-122]
Printing supports number formatting for DNIFINPLUS messages. You can configure thousands and decimal separators of numbers (for example, amounts) for the message printing service.

BIC expansion for fields within messages of the DNIFINPLUS domain [FTMSWIFT-I-124]
BIC information of messages in the DNIFINPLUS message domain are now expanded if enabled. This change excludes the remote address information.

Print layout changes:

- Line length information is considered when calculating header field offsets.
- Unparsable messages/incorrect header information is marked in printout using delimiter lines (v----v----...-----v-----v).

Timestamp format of history entries configurable [FTMSWIFT-I-141]
The configuration in which format timestamps are to be printed by the message printing service is now also used for history entries.

Security enhancements for Web Applications
Several enhancements are included in FTM SWIFT enterprise applications to further improve the security to prevent of Denial of Service and authorization vulnerability attacks.

New code signing certificate
A new code signing certificate is provided with extended validity period.

Note: You need to import this certificate into your keystore as part of the migration procedure as described in this readme file.

Known Problems

For a list of known problems refer to:
https://www.ibm.com/support/pages/node/6242088

Installation information

You can find information about the installation and migration steps mentioned in this document in the IBM Documentation for FTM SWIFT for Multiplatforms:

http://www.ibm.com/docs/en/ftmswsfm324

This readme document uses the following variables:

Variable	Description	Default
inst_dir	The installation directory of FTM SWIFT.	/opt/IBM/ftm/swift/v324
run_dir	The directory for runtime data.	/var/ftmswift_v324/run
cust_dir	The directory for customization data.	/var/ftmswift_v324/cus
deployment_dir	The deployment data directory.	/var/ftmswift_v324/cus/depdata
instance	The name of the FTM SWIFT instance.	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 3.2.4.9 – Create a new installation

If you have not yet installed FTM SWIFT, follow the description in the IBM Documentation for FTM SWIFT to install and customize a new instance instead of using this readme file.

Installing FTM SWIFT 3.2.4.9 – 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. Ensure that no customization operation is pending.
2. Ensure that no configuration or security administration change is pending.
3. Create a backup of your customized administrative scripts from *deployment_dir*/*instance*/admin:

```
mkdir ~/admin_scripts_backup
cp /var/ftmswift_v324/cus/depdata/INST1/admin/* ~/admin_scripts_backup
```

4. Use IBM Installation Manager to install the fix pack for FTM SWIFT 3.2.4.9.
5. Share the files in the *inst_dir*/admin directory with your customization system.
6. Update customization definition data, and create deployment instructions and vehicles.
7. If you plan manual deployment of the FTM SWIFT BAR files, follow Prepare BAR files for manual deployment.
8. Prepare the migration of configuration entities.
9. Backup your certificate keystore, for example:

```
cp -p /var/ftmswift_v324/run/ftmswift_keystore.jks /your_backup_directory
```

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. Replace the Public Key certificate for signed Java components using the *keytool* program from a Java Developement Kit (JDK):
   a. Delete the previous version of the certificate from your keystore:

```
keytool -delete -alias ftmswift -keystore ks.jks
```

   where **ks.jks** refers to your keystore, e.g. /var/ftmswift_v324/run/ftmswift_keystore.jks. When prompted, enter the password of your keystore.

   b. Import the new version of the certificate into your keystore:

```
keytool -importcert -alias ftmswift -file FTMSWIFT.cer -keystore ks.jks
```

   where:

   ks.jks
   Your certificate keystore, e.g. /var/ftmswift_v324/run/ftmswift_keystore.jks

   FTMSWIFT.cer
   The Public Key certificate from your FTM SWIFT installation directory, e.g. /opt/IBM/ftm/swift/v324/run/cert/FTMSWIFT.cer

   When prompted, enter the password of your keystore. Check if the displayed certificate information is identical with the one provided below. Especially, check if the certificate fingerprints match.

```
Owner: CN=International Business Machines Corporation, OU=IBM CCSS, O=International Business
Machines Corporation, L=Armonk, ST=New York, C=US
```

```
Issuer: CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1, O="DigiCert, Inc.", C=US
Serial number: 9ae51c9cfb701bc6f01688fab2acfc9
Valid from: 1/10/23 1:00 AM until: 11/15/24 12:59 AM
Certificate fingerprints:
         MD5:  4E:A5:C4:0B:73:EA:23:54:24:A8:44:0F:07:06:16:70
         SHA1: F6:DB:01:1C:A3:D9:F2:80:00:2A:29:56:52:4B:9E:43:F9:EE:EF:7A
         SHA256:
85:F7:23:4A:9E:A6:38:7D:C8:90:16:CD:CF:21:80:98:02:92:E9:87:9F:04:22:47:9A:3A:5B:5F:4A:0E:DE:E0
         Signature algorithm name: SHA256withRSA
         Version: 3
```

If the displayed information is correct, confirm that you trust this certificate to finish the import.

10. To verify that the certificate was replaced successfully, run the Software Integrity Checker (SIC):

    ```
    dnpsic -Djava.security.policy=/var/ftmswift_v324/run/ftmswift.policy
    ```

    The check needs to finish successfully.
11. Back up your runtime database.
12. Open and follow the deployment instructions.
    If you do not plan to use generated deployment vehicles for resource class CFGPF, you need to manually update the following enterprise applications:

Table 1. IBM WebSphere Application Server applications to be updated

Application	Migrating from FP7	Migrating from FP8
Administration and Operation (AO)	Yes	Yes
Message Entry and Repair (MER)	Yes	Yes
Relationship Management Application (RMA)	Yes	Yes
WebHome enterprise application	Yes	Yes

13. Follow the instruction in Verifying the installation of the database routines.
14. Restart all FTM SWIFT message brokers.
15. Deploy BAR files.
16. Verify the deployed BAR files:

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

    The deployment was successful if the displayed version contains 3.2.4.9.
17. Re-activate FTM SWIFT accounting if you use the SIPN FIN or FMT FIN service.
18. Restart all FTM SWIFT related message flows.
19. Migrate the configuration entities.
20. Run the following script files if you have both MSIF and MER facility deployed:
    - dnqctos.cli
    - dnqctosrole.cli

    See Configuring transfer option set field for details.
21. Restart all FTM SWIFT enterprise applications.
22. Restart all sessions and services.

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. Ensure that no customization operation is pending.

2. Ensure that no configuration or security administration change is pending.
3. Create a backup of your customized administrative scripts from *deployment_dir*/*instance*/admin:

```
mkdir ~/admin_scripts_backup
cp /var/ftmswift_v324/cus/depdata/INST1/admin/* ~/admin_scripts_backup
```

4. Backup your certificate keystore, for example:

```
cp -p /var/ftmswift_v324/run/ftmswift_keystore.jks /your_backup_directory
```

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 3.2.4.9.
9. Replace the Public Key certificate for signed Java components using the *keytool* program from a Java Developement Kit (JDK):
   a. Delete the previous version of the certificate from your keystore:

```
keytool -delete -alias ftmswift -keystore ks.jks
```

   where **ks.jks** refers to your keystore, e.g. /var/ftmswift_v324/run/ftmswift_keystore.jks. When prompted, enter the password of your keystore.

   b. Import the new version of the certificate into your keystore:

```
keytool -importcert -alias ftmswift -file FTMSWIFT.cer -keystore ks.jks
```

   where:

   ks.jks
   Your certificate keystore, e.g. /var/ftmswift_v324/run/ftmswift_keystore.jks

   FTMSWIFT.cer
   The Public Key certificate from your FTM SWIFT installation directory, e.g. /opt/IBM/ftm/swift/v324/run/cert/FTMSWIFT.cer

   When prompted, enter the password of your keystore. Check if the displayed certificate information is identical with the one provided below. Especially, check if the certificate fingerprints match.

```
Owner: CN=International Business Machines Corporation, OU=IBM CCSS, O=International Business
Machines Corporation, L=Armonk, ST=New York, C=US
Issuer: CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1, O="DigiCert, Inc.", C=US
Serial number: 9ae51c9cfb701bc6f01688fab2acfc9
Valid from: 1/10/23 1:00 AM until: 11/15/24 12:59 AM
Certificate fingerprints:
         MD5:  4E:A5:C4:0B:73:EA:23:54:24:A8:44:0F:07:06:16:70
         SHA1: F6:DB:01:1C:A3:D9:F2:80:00:2A:29:56:52:4B:9E:43:F9:EE:EF:7A
         SHA256:
85:F7:23:4A:9E:A6:38:7D:C8:90:16:CD:CF:21:80:98:02:92:E9:87:9F:04:22:47:9A:3A:5B:5F:4A:0E:DE:E0
         Signature algorithm name: SHA256withRSA
         Version: 3
```

   If the displayed information is correct, confirm that you trust this certificate to finish the import.

10. To verify that the certificate was replaced successfully, run the Software Integrity Checker (SIC):

    ```
    dnpsic -Djava.security.policy=/var/ftmswift_v324/run/ftmswift.policy
    ```

    The check needs to finish successfully.
11. Update customization definition data, and create deployment instructions and vehicles.
12. Back up your runtime database.
13. Open and follow the deployment instructions.
    If you do not plan to use generated deployment vehicles for resource class CFGPF, you need to manually update the following enterprise applications:

    Table 2. IBM WebSphere Application Server applications to be updated

Application	**Migrating from FP7**	**Migrating from FP8**
Administration and Operation (AO)	Yes	Yes
Message Entry and Repair (MER)	Yes	Yes
Relationship Management Application (RMA)	Yes	Yes
WebHome enterprise application	Yes	Yes

14. Follow the instruction in Verifying the installation of the database routines.
15. Restart all FTM SWIFT message brokers.
16. If you plan manual deployment of the FTM SWIFT BAR files, follow Prepare BAR files for manual deployment.
17. Deploy BAR files.
18. Verify the deployed BAR files:

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

    The deployment was successful if the displayed version contains 3.2.4.9.
19. Re-activate FTM SWIFT accounting if you use the SIPN FIN or FMT FIN service.
20. Restart all FTM SWIFT related message flows.
21. Prepare the migration of configuration entities.
22. Migrate the configuration entities.
23. Run the following script files if you have both MSIF and MER facility deployed:
    - dnqctos.cli
    - dnqctosrole.cli

    See Configuring transfer option set field for details.
24. Restart all FTM SWIFT enterprise applications.
25. Restart all sessions and services.

Cleaning up

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

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

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

4. Remove the backed up certificate keystore.

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 certificate keystore, for example:

```
cp -p /your_backup_directory/ftmswift_keystore.jks /var/ftmswift_v324/run/ftmswift_keystore.jks
```

9. Restore the backup of your runtime database.
10. Run the following commands to revert the FTM SWIFT database related changes :
    a. Open file *deployment_dir*/*instance*/admin/dnicommon_inst_sp_fb02.ddl.
    b. Replace DNIvOLDINSTPATH with your FTM SWIFT installation directory.
    c. Save your changes.
    d. db2 "CONNECT TO *db2_dsn*"
    e. db2 +c -z fp9_fallback_jar.log -svf *deployment_dir*/*instance*/admin/dnicommon_inst_sp_fb02.ddl
11. Restart all FTM SWIFT message brokers.
12. Deploy previous FTM SWIFT BAR files:

```
. /var/ftmswift_v324/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 the backup of your customized administrative scripts created in step “3” on page 10 (separated file systems) or “3” on page 12 (shared file system):

```
rm -rf /var/ftmswift_v324/cus/depdata/INST1/admin/*
cp -p ~/admin_scripts_backup/* /var/ftmswift_v324/cus/depdata/INST1/admin/
```

Re-migrating after a previous fallback

After you fall back to an earlier level, plan for re-migration only after you have identified the reason for the fallback and have corrected the problem.

To re-migrate, follow the steps described in this readme document.

Maintenance tasks

The following sections provide detailed instructions for selected installation steps of a fix pack. Refer to "Installing FTM SWIFT 3.2.4.9 – 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_v324/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_v324/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_v324/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_3.2.4.0_fp001`.

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 17.

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 the IBM 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_3.2.4.0_fp001/disk1/diskTag.inf`.
   c. Click **OK**
3. Test the repository connection
4. Close the Preferences dialog
5. In the IBM 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 IBM 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. Check what is currently installed for FTM SWIFT:

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

   The output includes a line for the installed fix pack. There may be additional lines for installed iFixes. All lines have the format:

```
inst_dir : package_id : name : version
```

   Note the value for *inst_dir*, which is identical in all lines of the output.

3. Run the following command:

```
./imcl install com.ibm.ftmswift.mp.v324
-installationDirectory inst_dir -repositories fix_pack_repo
-acceptLicense
```

   where

   inst_dir
   is the value determined in step “2” on page 17

   fix_pack_repo
   is the fix pack repository's `diskTag.inf` file, for example: `/tmp/FTM_SWS_MP_3.2.4.0_fp001/disk1/diskTag.inf`.

4. 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 `3.2.4.1` for fix pack 1. 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 3. 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_v324/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 3241.

   deployment_dir
   The name of the customization deployment directory, for example: /var/ftmswift_v324/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 16 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_v324/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 19.

   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

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

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

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

```
. /var/ftmswift_v324/run/dniprofile
```

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

```
dniczbap -cmd stop
```

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).
2. Ensure that you have access to a Java™ runtime environment.
3. Run the dniprofile by entering:

```
. /var/ftmswift_v324/run/dniprofile
```

4. Issue the **dnimaintinfo** command, for example:

```
dnimaintinfo -dsn MYDB -schema DNI
```

   For details about the **dnimaintinfo** command, see Maintenance Information command .
5. Examine the output and ensure that the following message is displayed:

```
DNID0001I Jar file version verification successful
```

   If you did not assign the **DNFFIN** service bundle (SVB) to any OU, the output should be:

```
DNID0015E JAR file 'dnfcdrtn.jar' for jarId 'dnfcdrtn' is either not installed or has an
unexpected version.
```

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 19, 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_v324/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 20 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_v324/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_v324/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 17.

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 following command:

   ```
   ./imcl rollback com.ibm.ftmswift.mp.v324
   ```

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 `3.2.4.1` for fix pack 1. Ensure that this version matches the fix pack you are rolling back to.

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 Installing the SAG Add-On / Pre-installation steps. You do not need to stop the SAG in order to update the SAG Add-On.

To update an SAG Add-On:

1. Stop the SAG Add-On.

   How to do this depends on the operating system of your SAG workstation:

   - On AIX®: Stop the SAG Add-On subsystems as described in Stopping an SAG Add-On on AIX
   - On RHEL x86: Stop the SAG Add-On service as described in Stopping an SAG Add-On on RHEL x86
   - On Windows: Stop the SAG Add-On service as described in Starting, stopping, or displaying the status of an SAG Add-On

   If the SAG Add-On cannot be stopped, stop the SAG Add-On process manually. How to do this depends on the operating system of your SAG workstation and is described here:

   - For AIX: Killing the SAG Add-On process on AIX (use only if the process is deadlocked)
   - For RHEL x86: Killing the SAG Add-On process on RHEL x86 (use only if the process is deadlocked)
   - For Windows: Starting, stopping, or displaying the status of an SAG Add-On
2. Create a backup of your SAG Add-On profile `dnfcssao.cfg` that is located in the SAG Add-On runtime directory:

   - On AIX and RHEL x86: `/var/ftmswift_v324/sao`
   - On Windows: `%PROGRAMDATA%\ftmswift_v324\sao`

   Note: Do not store the backup file in the SAG Add-On runtime directory, but in a different location.
3. Uninstall the currently installed version of the SAG Add-On using IBM Installation Manager.
4. Install the SAG Add-On with the new fix pack level using IBM Installation Manager.
5. Copy the backup of the SAG Add-On profile `dnfcssao.cfg` (that you created in step "2" on page 23) to the SAG Add-On runtime directory:

   - On AIX and RHEL x86: `/var/ftmswift_v324/sao`
   - On Windows: `%PROGRAMDATA%\ftmswift_v324\sao`
6. 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 bring your environment to the target configuration.

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_v324/run/dniprofile
   ```
3. Create a sub-directory `ftmswift_`*xxxx* where *xxxx* is the version of the fix pack, for example 3241.
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 lists the CLI command files that it created in the current directory, for example:

```
Generating the command files for migration ...
The following files are generated and need to be executed for migration:

Seq  User    File
---  ------  ------------------------------
001  Any UA  dnfczmlc_1_ua_rem_ro_all.cli
002  Any SA  dnfczmlc_2_sa_ent_all.cli
003  Any UA  dnfczmlc_3_ua_cre_ro_all.cli

DnfInfo: Script /opt/IBM/ftm/swift/v324/run/bin/dnfczmlc completed successfully.
```

Note: The command dnfczmlc starts a long-running task that might take several minutes to complete.

5. Save the output of dnfczmlc which tells you the sequence and the user ID you have to use later when you submit the CLI command files in “Migrate the configuration entities” on page 24.

Migrate the configuration entities

FTM SWIFT maintenance may require to update configuration entities. In section “Prepare the migration of configuration entities” on page 23 you created the required CLI command files that now need to be executed.

To migrate the configuration entities:

1. For each CLI command file listed in the output of dnfczmlc in “Prepare the migration of configuration entities” on page 23, log on as the user specified for the current file.

   The user IDs are:

   1st, 2nd, or Any SA
   The first system configuration administrator (sa1), the second system configuration administrator (sa2), or any system configuration administrator.

   1st, 2nd, or Any UA
   The first user administrator (ua1), the second user administrator (ua2), or any user administrator.

2. Run the profile for your runtime environment by entering:

   ```
   . /var/ftmswift_v324/run/dniprofile
   ```

3. Switch to the sub-directory ftmswift_*xxxx* you created in section “Prepare the migration of configuration entities” on page 23, step “3” on page 23.

4. Run the current CLI command file by issuing the following command:

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

   where:

   svc

   DNI_SYSADM
   For files executed by a system configuration administrator.

   DNI_SECADM
   For files executed by a security administrator.

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

xxxx
The version of the fix pack, for example 3241.

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

Update the IBM Integration Toolkit workstation

To install the new versions of the Toolkit resources, follow the instructions listed in:

- Transferring the FTM SWIFT Toolkit resources
- Installing the FTM SWIFT Eclipse plug-ins

If you use FTM SWIFT sample message flows as foundation for your own flow development follow the instructions provided in Using the sample routing flows.

Otherwise, continue with the instructions provided in:

- Importing FTM SWIFT sample projects
- Importing the message sets and sample routing flows

Additionally, if you use FTM SWIFT message set projects containing XML schema definitions for your own flow development follow the instructions provided in: Importing XSD files for SWIFT message payloads.

Furthermore, you have to rebuild and redeploy your message flows if they are based on the FTM SWIFT API.

Copyright and trademark information

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

Document change history

Date	Description of change
2023-03-31	Initial publication date

Product Number: 5725-X92