IBM Financial Transaction Manager for SWIFT Services for Multiplatforms

Version 3.0.0

Readme
Fix Pack 7

IBM Financial Transaction Manager for SWIFT Services for Multiplatforms
Version 3.0.0

Readme
Fix Pack 7

This edition applies to Version 3.0.0 of IBM Financial Transaction Manager for SWIFT Services for Multiplatforms (5725-X92) fix pack 3.0.0.7.

Reference key: @20180515-1751@

Contents

Chapter 1. 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 3.0.0.7 from Fix Central at the following location:

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

Search for the Fix ID: 3.0.0-FTM-SWS-MP-fp0007

Prerequisites and co-requisites

Before installing the current fix pack perform the following steps:

- Ensure that your system meets all of the system requirements: http://www-01.ibm.com/support/docview.wss?uid=swg27027034#V30

  This prevents technical problems that might occur after the installation and configuration 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 3.0.0.4 installed and all post-installation steps were finished.

What's new in FTM SWIFT 3.0.0, Fix Pack 7

The following changes were introduced:

- Support local authentication(LAU) between SAG and FTM SWIFT for the MSIF service.
- Enhanced support for SWIFT Customer Security Program (CSP).
- The parameter *-keystore* of the Data Integrity Utility commands build and check has been deprecated.
- For a list of fixes provided and APARs included refer to: http://www.ibm.com/support/docview.wss?uid=swg21970097

Chapter 2. 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 3.0.0.7 - Create a new installation

If you have not installed FTM SWIFT yet:

1. Plan your system as described in Planning.
2. Install fix pack 3.0.0.7 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 3.0.0.7 - 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. Back up the FTM SWIFT IBM® WebSphere® Application Server (WAS) profiles.
2. If your current FTM SWIFT fix pack level is 3.0.0.4 or 3.0.0.5:
   Ensure that the FTM SWIFT WAS profile is running on Java version 7 or higher.
3. Ensure that no customization operation is pending.
4. Ensure that no configuration or security administration change is pending.
5. Plan your table spaces:
   a. Download the updated table space calculation spreadsheet from:
      http://www.ibm.com/support/docview.wss?uid=swg27047237
   b. Refer to Chapter 3, “Summary of changes,” on page 13 and check if the table space allocation still fits your needs or you have to plan new table spaces.
6. 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
   ```
7. Use IBM Installation Manager to install the fix pack for FTM SWIFT 3.0.0.7.
8. Share the files in the *inst_dir*/admin directory with your customization system.
9. Create and assign new user groups:
   a. This fix pack introduces new customization placeholders that represent operating system user groups that will be granted permissions required to run the Data Integrity Checker commands:
      - DNIvDAGRP
      - DNIvDBGRP
      - DNIvDCGRP

      Plan which user group you will assign later in the customization process to each placeholder.
   b. Ask your system administrator to create missing user groups and assign them to the appropriate user id's.
10. Provide values for new customization placeholders, 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 new placeholders:
```
dnicdpm -i instance
> export cdd/instance_FP3007.cdd
> supplement cdd/instance_FP3007.cdd cdd/instance_FP3007_supp.cdd
```
d. The new CDD `cdd/instance_FP3007_supp.cdd` contains the following new placeholders:
   - DNIvDAGRP
   - DNIvDBGRP
   - DNIvDCGRP

   Placeholders *DNIvD[A|B|C]GRP* represent operating system user groups that you planned earlier already.

   For more information refer to Customization placeholders.

   Edit the CDD and provide appropriate values for your environment.
e. Import the edited CDD and prepare deployment instructions and vehicles:
```
> import cdd/instance_FP3007_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.

11. If your current FTM SWIFT fix pack level is 3.0.0.6 and you already performed the steps in Activating the data integrity framework:
Gather all data integrity trigger modules from the customized administrative scripts directory into a single file:
    a. Log on as a customizer (ucust1).
    b. Create a temporary directory where you want to store the data integrity trigger statements:
```
mkdir -p /tmp/trigger
```
    c. Enter the following command on a single line:
```
inst_dir/admin/bin/dniczdic
       -collect
       -d deployment_dir
       -i instance
       -l /tmp/trigger
```
    This command creates the file /tmp/trigger/dnirundb_dic.ddl.
12. If you plan manual deployment of the FTM SWIFT BAR files, follow Prepare BAR files for manual deployment.
13. If your current FTM SWIFT fix pack level is 3.0.0.4 or 3.0.0.5:
Prepare an updated dniprofile:
    a. Back up your existing dniprofile.

b. Change the CLASSPATH in your current profile or use the delivered sample profile *inst_dir*/run/samples/dniczpro.prf. The CLASSPATH must look like:

```
CLASSPATH=$CLASSPATH:$DNI_WMB_PATH/classes/ConfigManagerProxy.jar
CLASSPATH=$CLASSPATH:$DNI_WMQ_PATH/java/lib/com.ibm.mq.jar
CLASSPATH=$CLASSPATH:$DNI_WMQ_PATH/java/lib/connector.jar
CLASSPATH=$CLASSPATH:$DNI_PATH/run/classes/*
export CLASSPATH
```

14. 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 enterprise applications.
3. Stop all FTM SWIFT related message flows.
4. Stop all FTM SWIFT message brokers.
5. Share the files in the *inst_dir*/run directory with your runtime system.
6. Back up your runtime database.
7. Open and follow the deployment instructions.
8. If your current FTM SWIFT fix pack level is 3.0.0.4 or 3.0.0.5:
   Remove the old Jar files from Db2 function folder:
   ```
   rm /home/db2inst1/sqllib/function/jar/dnicsl.*
   ```
9. Follow the instruction in Verifying the installation of the database routines.
10. Restart all FTM SWIFT message brokers.
11. Deploy BAR files.
12. Verify the deployed BAR files:
    ```
    dniczbap -cmd list -flow DNI_SYSADM
    ```

    The deployment was successful if the displayed version contains 3.0.0.7.
13. Re-activate FTM SWIFT accounting if you use the SIPN FIN or FMT FIN service.
14. Restart all FTM SWIFT related message flows.
15. Migrate the configuration entities.
16. If your current FTM SWIFT fix pack level is 3.0.0.6 and you already performed the steps in Activating the data integrity framework:
    Update the data integrity framework:
    a. Create and update data integrity triggers:
       1) Log on as Db2 administrator (udb2adm1).
       2) Run the data integrity trigger creation statements:
          ```
          cd /tmp/trigger
          db2 connect to db2_dsn
          db2 +c -svtd# -z trig.log -f dnirundb_dic.ddl
          ```
    b. Run the DIC **build** command:
       1) Log on as a data integrity operator.
       2) Run the data integrity checker command build, for example:
          ```
          dnpdic -Djava.security.policy=/var/ftmswift_v300/run/ftmswift.policy
                 -keystore /var/ftmswift_v300/run/ftmswift_vault.jceks
                 -passphrase my_passphrase
                 -dsn DSN1 -schema DNI -uid helen -pw helens_password
                 -build
          ```
    c. Add configuration object DniVault:

1) Log on as System configuration administrator (sa1).
2) Run your dniprofile:
```
. /var/ftmswift_v300/run/dniprofile
```
3) Create a new configuration object:
```
dnicli -ou SYSOU -s DNI_SYSADM
> add -ou SYSOU -ct DniFileDir -co DniVault -attr Path -val vault_path
> add -ou SYSOU -ct DniFileDir -co DniVault -attr read
```
where *vault_path* represents the directory you specified in the **dir** parameter of the DIC **init** command when activating the data integrity framework.
4) Commit, approve and deploy SYSOU.

17. Restart all FTM SWIFT enterprise applications.
18. Restart all sessions and services.
19. Update the IBM Integration Toolkit workstation if you use either of the following:
    - FTM SWIFT sample message flows as foundation for your own flow development
    - FTM SWIFT nodes in your own message flows
    - FTM SWIFT message set projects containing XML schema definitions that, for example, are utilized by the IBM Integration Toolkit XPath wizard
20. If your current FTM SWIFT fix pack level is 3.0.0.4 or 3.0.0.5:
    If you use the SAG Add-On, 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. Back up the FTM SWIFT IBM WebSphere Application Server (WAS) profiles.
2. If your current FTM SWIFT fix pack level is 3.0.0.4 or 3.0.0.5:
   Ensure that the FTM SWIFT WAS profile is running on Java version 7 or higher.
3. Ensure that no customization operation is pending.
4. Ensure that no configuration or security administration change is pending.
5. If your current FTM SWIFT fix pack level is 3.0.0.4 or 3.0.0.5:
   Prepare an updated dniprofile:
   a. Back up your existing dniprofile.
   b. Change the CLASSPATH in your current profile or use the delivered sample profile *inst_dir*/run/samples/dniczpro.prf. The CLASSPATH must look like:
```
CLASSPATH=$CLASSPATH:$DNI_WMB_PATH/classes/ConfigManagerProxy.jar
CLASSPATH=$CLASSPATH:$DNI_WMQ_PATH/java/lib/com.ibm.mq.jar
CLASSPATH=$CLASSPATH:$DNI_WMQ_PATH/java/lib/connector.jar
CLASSPATH=$CLASSPATH:$DNI_PATH/run/classes/*
export CLASSPATH
```
6. Plan your table spaces:
   a. Download the updated table space calculation spreadsheet from:
   http://www.ibm.com/support/docview.wss?uid=swg27047237

b. Refer to Chapter 3, "Summary of changes," on page 13 and check if the table space allocation still fits your needs or you have to plan new table spaces.

7. Create and assign new user groups:
   a. This fix pack introduces new customization placeholders that represent operating system user groups that will be granted permissions required to run the Data Integrity Checker commands:
      - DNIvDAGRP
      - DNIvDBGRP
      - DNIvDCGRP

      Plan which user group you will assign later in the customization process to each placeholder.
   b. Ask your system administrator to create missing user groups and assign them to the appropriate user id's.
8. 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 enterprise applications.
3. Stop all FTM SWIFT related message flows.
4. Stop all FTM SWIFT message brokers.
5. Use IBM Installation Manager to install the fix pack for FTM SWIFT 3.0.0.7.
6. Provide values for new customization placeholders, 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 new placeholders:

```
dnicdpm -i instance
> export cdd/instance_FP3007.cdd
> supplement cdd/instance_FP3007.cdd cdd/instance_FP3007_supp.cdd
```

   d. The new CDD cdd/instance_FP3007_supp.cdd contains the following new placeholders:
      - DNIvDAGRP
      - DNIvDBGRP
      - DNIvDCGRP

      Placeholders *DNIvD[A|B|C]GRP* represent operating system user groups that you planned earlier already.

      For more information refer to Customization placeholders.

      Edit the CDD and provide appropriate values for your environment.
   e. Import the edited CDD and prepare deployment instructions and vehicles:

```
> import cdd/instance_FP3007_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.

7. Back up your runtime database.
8. Open and follow the deployment instructions.
9. If your current FTM SWIFT fix pack level is 3.0.0.4 or 3.0.0.5:
   Remove the old Jar files from Db2 function folder:

```
rm /home/db2inst1/sqllib/function/jar/dnicsl.*
```

10. Follow the instruction in Verifying the installation of the database routines.
11. Restart all FTM SWIFT message brokers.
12. If you plan manual deployment of the FTM SWIFT BAR files, follow Prepare BAR files for manual deployment.
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 3.0.0.7.

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. Prepare the migration of configuration entities.
18. Migrate the configuration entities.
19. If your current FTM SWIFT fix pack level is 3.0.0.6 and you already performed the steps in Activating the data integrity framework:
    Update the data integrity framework:
    a. Create and update data integrity triggers:
       1) Log on as a customizer (ucust1).
       2) Create a temporary directory where you want to store the data integrity trigger statements:

```
mkdir -p /tmp/trigger
```

       3) Enter the following command on a single line:

```
inst_dir/admin/bin/dniczdic
       -collect
       -d deployment_dir
       -i instance
       -l /tmp/trigger
```

This command creates the file /tmp/trigger/dnirundb_dic.ddl.

       4) Log on as Db2 administrator (udb2adm1).
       5) Run the data integrity trigger creation statements:

```
cd /tmp/trigger
db2 connect to db2_dsn
db2 +c -svtd# -z trig.log -f dnirundb_dic.ddl
```

    b. Run the DIC **build** command:
       1) Log on as a data integrity operator.

2) Run the data integrity checker command build, for example:

```
dnpdic -Djava.security.policy=/var/ftmswift_v300/run/ftmswift.policy
       -keystore /var/ftmswift_v300/run/ftmswift_vault.jceks
       -passphrase my_passphrase
       -dsn DSN1 -schema DNI -uid helen -pw helens_password
       -build
```

c. Add configuration object DniVault:

1) Log on as System configuration administrator (sa1).

2) Run your dniprofile:

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

3) Create a new configuration object:

```
dnicli -ou SYSOU -s DNI_SYSADM
> add -ou SYSOU -ct DniFileDir -co DniVault -attr Path -val vault_path
> add -ou SYSOU -ct DniFileDir -co DniVault -attr read
```

where *vault_path* represents the directory you specified in the **dir** parameter of the DIC **init** command when activating the data integrity framework.

4) Commit, approve and deploy SYSOU.

20. Restart all FTM SWIFT enterprise applications.
21. Restart all sessions and services.
22. Update the IBM Integration Toolkit workstation if you use either of the following:
    - FTM SWIFT sample message flows as foundation for your own flow development
    - FTM SWIFT nodes in your own message flows
    - FTM SWIFT message set projects containing XML schema definitions that, for example, are utilized by the IBM Integration Toolkit XPath wizard
23. If your current FTM SWIFT fix pack level is 3.0.0.4 or 3.0.0.5:
    If you use the SAG Add-On, 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. If your migration starting point was FTM SWIFT fix pack level 3.0.0.4 or 3.0.0.5:
   Free the obsolete packages and drop the unused SQLJ based stored procedures:
   a. Log on as a Db2 administrator (udb2adm1).
   b. Change to the directory of the customized administrative scripts (*deployment_dir*/*instance*/admin):

```
cd  /var/ftmswift_v300/cus/depdata/INST1/admin
```

   c. Connect to your runtime database *db2_dsn* and run the Db2 commands included in the file dnicdmc0.ddl. For example, issue the following commands:

```
db2 connect to DNIDBRUN
db2 -t -n -s -f /var/ftmswift_v300/cus/depdata/INST1/admin/dnicdmc0.ddl
```

4. If your migration starting point was FTM SWIFT fix pack level 3.0.0.6:
   Clean up unnecessary permissions for group *DNIvSGRP*:

a. Log on as a Db2 administrator (udb2adm1).
b. Run the following statement in an SQL processor:

```
REVOKE INSERT,UPDATE,DELETE ON DNIvSN.DNI_CCTRL FROM GROUP DNIvSGRP;
```

5. If your migration starting point was FTM SWIFT fix pack level 3.0.0.4 or 3.0.0.5: Clean up your Db2 administrator profile by removing the routines-instance directory entry from the CLASSPATH statement. For example, remove `/var/ftmswift_v300/run/routines/INST1`.
6. If your migration starting point was FTM SWIFT fix pack level 3.0.0.4 or 3.0.0.5: Clean up the routines directory:
   a. Change to the routines-instance directory:

      ```
      cd /var/ftmswift_v300/run/routines
      ```

   b. Remove the *instance* sub-directory:

      ```
      rm -R INST1
      ```

   c. After all FTM SWIFT instances are migrated remove the routines directory:

      ```
      cd /var/ftmswift_v300/run
      rm -R routines
      ```

7. Remove the backup of your customized administrative scripts created in step 6 on page 4 (separated file systems) or 8 on page 8 (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 your runtime database.
9. If your migration starting point was FTM SWIFT fix pack level 3.0.0.4 or 3.0.0.5:
   Restore the previous FTM SWIFT system and security administration routine JAR files:

   ```
   db2 "CALL SQLJ.REPLACE_JAR('file:/opt/IBM/ftm/swift/v300/run/classes/dnicdcfg.jar','dni.dnicdcfg')"
   db2 "CALL SQLJ.REPLACE_JAR('file:/opt/IBM/ftm/swift/v300/run/classes/dnicdusr.jar','dni.dnicdusr')"
   db2 "CALL SQLJ.REFRESH_CLASSES()"
   ```

10. If your migration starting point was FTM SWIFT fix pack level 3.0.0.4 or 3.0.0.5:
    Restore the previous Db2 functions folder content:
    a. Copy the previous libraries into the Db2 function JAR directory.
    b. Remove the installed libraries from the Db2 function subdirectory DNI:

       ```
       cp /opt/IBM/ftm/swift/v300/run/classes/dnicsl.* /home/db2inst1/sqllib/function/jar/
       chmod 750 /home/db2inst1/sqllib/function/jar/dnicsl.*
       chgrp dnilpp /home/db2inst1/sqllib/function/jar/dnicsl.*
       rm /home/db2inst1/sqllib/function/jar/DNI/DNICS*.jar
       ```

11. If your migration starting point was FTM SWIFT fix pack level 3.0.0.4 or 3.0.0.5:
    Restore the previous FTM SWIFT User Defined Functions by removing the installed function JAR files:

    ```
    rm /home/db2inst1/sqllib/function/jar/DNI/*RTN.jar
    ```

12. If your migration starting point was FTM SWIFT fix pack level 3.0.0.4 or 3.0.0.5:
    Stop and restart the database.
13. Restart all FTM SWIFT message brokers.
14. Deploy previous FTM SWIFT BAR files:
    ```
    . /var/ftmswift_v300/run/dniprofile
    dniczbap -cmd prepare -update old -deploy [-broker broker_name]
    ```
15. Verify the deployed BAR files:
    ```
    dniczbap -cmd list -flow DNI_SYSADM
    ```

    The deployment was successful if the displayed version contains the fixpack that was your migration starting point.
16. Re-activate FTM SWIFT accounting if you use the SIPN FIN or FMT FIN service.
17. Restart all FTM SWIFT related message flows.
18. Restore the IBM WebSphere Application Server profile backups.
19. Restart all FTM SWIFT application servers.
20. Restart all sessions and services.
21. Restore your IBM Integration Toolkit workstation if you updated it during Installation:
    a. Restore your Toolkit `dropins` directory.
    b. Restore your Toolkit workspace.
    c. Deploy your restored message flows.
22. If you use SAG Add-On, roll back the SAG Add-On to the previous level.
23. Restore the backup of your customized administrative scripts created in step 6 on page 4 (separated file systems) or 8 on page 8 (shared file system):
    ```
    rm -rf /var/ftmswift_v300/cus/depdata/INST1/admin/*
    cp ~/admin_scripts_backup/* /var/ftmswift_v300/cus/depdata/INST1/admin/
    ```

Chapter 3. Summary of changes

3.0.0.7

- New customization placeholders
  - DNIvDAGRP
  - DNIvDBGRP
  - DNIvDCGRP
- Resource class DB
  - New alias
    - DNI_COS_CT_CON_REL_CTRL
    - DNI_CT_ATTR_VALUE_CTRL
    - DNI_OU_CTRL
    - DNI_RO_CT_ATTR_REL_CTRL
    - DNI_ROLE_CTRL
    - DNI_ROLEGROUP_CTRL
    - DNI_RG_ROLE_REL_CTRL
    - DNI_USR_RG_REL_CTRL
    - DNI_USER_CTRL
    - DNI_USR_ROLE_REL_CTRL
    - DNI_ROLE_RESOLVED_CTRL
    - DNI_USER_RESOLVED_CTRL
    - DNIMWH_PT_DNIvOU_CTRL
    - DNI_A_MSG_DNIvOU_CTRL
    - DNI_A_USR_DNIvOU_CTRL
    - DNI_EVENT_CTRL
    - DNFO_FSM_STATE_CTRL
    - DNFO_MSG_PART_CTRL
    - DNFO_LOB_DATA_CTRL
    - DNFO_FSM_RCV_MSG_CTRL
    - DNFO_FSM_SND_MSG_CTRL
    - DNFO_FSM_SEND_CTRL
    - DNFO_FSM_RECEIVE_CTRL
    - DNFO_FSM_PROVDL_CTRL
    - DNFO_FSM_RSPDL_CTRL
    - DNFO_FSM_DOWNLOAD_CTRL
    - DNFO_CONFIG_DATA_CTRL
    - DNFO_MWH_DATA_CTRL
    - DNF_IAMS_CTRL
    - DNF_OAMS_CTRL
    - DNFMWHFIN_DNIvOU_CTRL
    - DNF_RMAD_CTRL
    - DNF_RMAP_CTRL
    - DNF_RMAH_CTRL

- DNF_RMQS_CTRL
- DNF_RMQH_CTRL

– New tables
- DNI_COS_CT_CON_REL_CTRLA / DNI_COS_CT_CON_REL_CTRLB
- DNI_CT_ATTR_VALUE_CTRLA / DNI_CT_ATTR_VALUE_CTRLB
- DNI_OU_CTRLA / DNI_OU_CTRLB
- DNI_RO_CT_ATTR_REL_CTRLA / DNI_RO_CT_ATTR_REL_CTRLB
- DNI_ROLE_CTRLA / DNI_ROLE_CTRLB
- DNI_ROLEGROUP_CTRLA / DNI_ROLEGROUP_CTRLB
- DNI_RG_ROLE_REL_CTRLA / DNI_RG_ROLE_REL_CTRLB
- DNI_USR_RG_REL_CTRLA / DNI_USR_RG_REL_CTRLB
- DNI_USER_CTRLA / DNI_USER_CTRLB
- DNI_USR_ROLE_REL_CTRLA / DNI_USR_ROLE_REL_CTRLB
- DNI_ROLE_RESOLVED_CTRLA / DNI_ROLE_RESOLVED_CTRLB
- DNI_USER_RESOLVED_CTRLA / DNI_USER_RESOLVED_CTRLB
- DNIMWH_PT_DNIvOU_CTRLB
- DNI_A_MSG_DNIvOU_CTRLA / DNI_A_MSG_DNIvOU_CTRLB
- DNI_A_USR_DNIvOU_CTRLA / DNI_A_USR_DNIvOU_CTRLB
- DNI_EVENT_CTRLA / DNI_EVENT_CTRLB
- DNFO_FSM_STATE_CTRLA / DNFO_FSM_STATE_CTRLB
- DNFO_MSG_PART_CTRLA / DNFO_MSG_PART_CTRLB
- DNFO_LOB_DATA_CTRLA / DNFO_LOB_DATA_CTRLB
- DNFO_FSM_RCV_MSG_CTRLA / DNFO_FSM_RCV_MSG_CTRLB
- DNFO_FSM_SND_MSG_CTRLA / DNFO_FSM_SND_MSG_CTRLB
- DNFO_FSM_SEND_CTRLA / DNFO_FSM_SEND_CTRLB
- DNFO_FSM_RECEIVE_CTRLA / DNFO_FSM_RECEIVE_CTRLB
- DNFO_FSM_PROVDL_CTRLA / DNFO_FSM_PROVDL_CTRLB
- DNFO_FSM_RSPDL_CTRLA / DNFO_FSM_RSPDL_CTRLB
- DNFO_FSM_DOWNLOAD_CTRLA / DNFO_FSM_DOWNLOAD_CTRLB
- DNFO_CONFIG_DATA_CTRLA / DNFO_CONFIG_DATA_CTRLB
- DNFO_MWH_DATA_CTRLA / DNFO_MWH_DATA_CTRLB
- DNF_IAMS_CTRLB
- DNF_OAMS_CTRLB
- DNFMWHFIN_DNIvOU_CTRLB
- DNF_RMAD_CTRLA / DNF_RMAD_CTRLB
- DNF_RMAP_CTRLA / DNF_RMAP_CTRLB
- DNF_RMAH_CTRLA / DNF_RMAH_CTRLB
- DNF_RMQS_CTRLA / DNF_RMQS_CTRLB
- DNF_RMQH_CTRLA / DNF_RMQH_CTRLB

– Modified table structure
- Added columns DI_ID and DI_CHG_TS
  - DNI_COS_CT_CON_REL
  - DNI_CT_ATTR_VALUE
  - DNI_OU
  - DNI_RO_CT_ATTR_REL

        - DNI_ROLE
        - DNI_ROLEGROUP
        - DNI_RG_ROLE_REL
        - DNI_USR_RG_REL
        - DNI_USER
        - DNI_USR_ROLE_REL
        - DNI_ROLE_RESOLVED
        - DNI_USER_RESOLVED
        - DNI_A_MSG_DNIvOU
        - DNI_A_USR_DNIvOU
        - DNI_EVENT
        - DNFO_FSM_STATE
        - DNFO_MSG_PART
        - DNFO_LOB_DATA
        - DNFO_FSM_RCV_MSG
        - DNFO_FSM_SND_MSG
        - DNFO_FSM_SEND
        - DNFO_FSM_RECEIVE
        - DNFO_FSM_PROVDL
        - DNFO_FSM_RSPDL
        - DNFO_FSM_DOWNLOAD
        - DNFO_CONFIG_DATA
        - DNFO_MWH_DATA
        - DNF_RMAD
        - DNF_RMAP
        - DNF_RMAH
        - DNF_RMQS
        - DNF_RMQH
      - Dropped unique constraint OAMS_UN from DNF_OAMS
      - Dropped foreign key constraint FK_DNF_OAMS_ID from DNF_OAMS_CTRLA
    - Renamed tables
      - DNIMWH_PT_DNIvOU_CTRL to DNIMWH_PT_DNIvOU_CTRLA
      - DNF_IAMS_CTRL to DNF_IAMS_CTRLA
      - DNF_OAMS_CTRL to DNF_OAMS_CTRLA
      - DNFMWHFIN_DNIvOU_CTRL to DNFMWHFIN_DNIvOU_CTRLA
    - New sequence: SEQIAMS
    - Updated Jar files for stored procedures
      - dnicsl.boots.jar
      - dnicsl.impl.jar
      - dnicdcfg.jar
      - dnicdusr.jar
    - New stored procedure
      - DNI_INSTALL_DI_TRIGGER
- Resource class CFGPF: Modified enterprise applications

  - MER facility: dnq.app.main.ear
  - RMA: dnf.rma.web.ear
  - AO facility: dnp.ado.web.ear
  - WebHome facility: dni.home.ear
- Modified role
  - add -ro DnfRmCfg -ct DniFileDir -co DniVault -attr *
- Modified configuration type
  - If you use MSIF: add -ct DnfEfaSagMPOptionSet -attr lkn
- Changed Toolkit resources
  - Toolkit dropins: com.ibm.dni.api.jar and com.ibm.dnq.api.jar

3.0.0.6

- Resource class DB
  - New table space: DNICNTRL
  - New tables
    - DNI_CCTRL
    - DNIMWH_PT_DNIvOU_CTRL
    - DNFMWHFIN_DNIvOU_CTRL
    - DNF_IAMS_CTRL (FIN only)
    - DNF_OAMS_CTRL (FIN only)
  - Modified table structure
    - Added columns DI_ID and DI_CHG_TS
      - DNIMWH_PT_DNIvOU
      - DNFMWHFIN_DNIvOU
      - DNF_IAMS (FIN only)
      - DNF_OAMS (FIN only)
  - New procedures
    - DNI_DIC_INS
    - DNI_DIC_UPD
    - DNI_DIC_DEL
    - DNI_CHECK_CTRL_ROW
    - All System and Security Administration procedures, e.g. DNI_CREATE_CT
  - Dropped procedures: old System and Security Administration procedures, e.g. DNI9CREATE9CT (removed in Cleanup phase)
  - Updated functions
    - DNIBLOB2VARCHAR
    - DNFMWHFINMSG
- Modified enterprise applications
  - MER facility: dnq.app.main.ear
  - RMA: dnf.rma.web.ear
  - AO facility: dnp.ado.web.ear
- Changed Toolkit resources
  - Message set: dni.schemas.comibmdni.zip
  - Message set projects: DNI_DniMsgSetEnv contained in dni.project.interchange.zip
- The sample profile dniczpro.prf is changed.

3.0.0.5

- Resource class DB
  - Altered tables
    - DNF_ASP
- Message updates
  - New messages
    - DNFO3612E

Chapter 4. Copyright and trademark information

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

Chapter 5. Document change history

Date	Description of change
May 16, 2018	Initial publication date

Product Number: 5725-X92

Printed in USA