Installation Instructions for Hot Fix A5T005

Hot fix **A5T005** addresses the issue(s) in ***Compliance Solutions 7.1*** as documented in the *Issue(s) Addressed* section of the hot fix download page:
http://ftp.sas.com/techsup/download/hotfix/HF2/A5T.html#A5T005

A5T005 is a "container" hot fix that contains the following "member" hot fixes which will update the software components as needed.

A5Q004 updates **SAS Compliance Solutions Mid-Tier 7.1**
A5R005 updates **SAS Compliance Solutions Server 7.1**
A6A003 updates **SAS Compliance Solutions LASR Configuration 7.1**
A6H002 updates **SAS Compliance Solutions Mid-Tier LASR Configuration 7.1**

See What is a container hot fix? in the Hot Fix FAQ for more information about container hot fixes.

Before applying this hot fix, follow the instructions in SAS Note 35968 to generate a SAS Deployment Registry report, then verify that the appropriate product releases are installed on your system. The release number information in the Registry report should match the 'member' release number information provided above for the software components installed on each machine in your deployment.

The hot fix downloaded, A5T005pt.zip, includes the updates required for all components listed above on all applicable operating systems. To apply this hot fix on multiple machines, you can either save A5T005pt.zip on each machine or save it in a network location that is accessible to all machines.

Do NOT extract the contents of A5T005pt.zip. The hot fix installation process will extract the contents as needed.

IMPORTANT NOTES

1. Files delivered in this hot fix will be backed up during the installation process. However, it is good general practice to back up your system before applying updates to software.
2. You must have Administrator Privileges on your CLIENT or SERVER machine.
3. All currently active SAS sessions must be terminated before applying this hot fix.
4. This hot fix should be installed using the same userid who performed the initial software installation.
5. CONFIGURATION: No automatic configuration scripting is included for this hot fix. If you have previously configured software installed, the SAS Deployment Manager may present a screen where you will see "Apply SAS Hot Fixes" and "Configure SAS Hot

Fixes" options. On this screen, you must ensure that the "Configure SAS Hot Fix" option is *__not__* selected. If this option is automatically selected, please de-select it prior to proceeding with the SAS Deployment Manager Screens. Failure to do so could have unintended consequences when applying this hot fix.

INSTALLATION

Hot Fix A5T005 must be installed on each machine where the updated components of the product, listed above, are installed. During the installation process you may see references to all operating systems for which updates are provided in the hot fix. The installation process will determine the operating system and which component(s) of Compliance Solutions 7.1 require updating on the machine. See SAS Note 44810 for more details.

The hot fix will be applied using the SAS Deployment Manager. By default, the SAS Deployment Manager will search in the *<SASHOME>/InstallMisc/HotFixes/New* directory for hot fixes to be applied, but will also prompt for a location if you have downloaded hot fixes to a different directory.

After downloading A5T005pt.zip, follow the instructions for applying hot fixes in the **SAS Deployment Wizard and SAS Deployment Manager 9.4: User's Guide**.

Generally, it is not necessary to shut down any compute tier or metadata servers when executing the hotfix installation and post-installation steps for this hotfix. It is important, however, that SAS is not executing on the compute tier server, because it can lock access to the Compliance Solutions compiled macros library, which cannot be in use when the library gets replaced with the new version. The SAS Deployment Manager will check for files in use by other processes and will issue an error if any are found.

Please review the CONFIGURATION Important Note above concerning proper selection of the "Configure SAS Hot Fix" option in the SAS Deployment Manager.

The hot fix installation process generates the log file:

<SASHOME>/InstallMisc/InstallLogs/IT_date-and-time-stamp.log

for example, IT_2011-10-31-13.18.21.log. Each attempt to apply a hot fix results in the creation of a new log file giving detailed information regarding the installation process.

Postexec log files are created after the installation is completed and identifies the files that were added, backed up, changed and removed. These log files include the 'member' hot fix id in the name of the file and are also written to the <!SASHOME>/InstallMisc/InstallLogs directory. There is one postexec log for each 'member' hot fix applied (member hot fixes are listed at the top of these instructions).

The content of this hot fix is listed in the hot fix manifest.

Post-Installation Instructions:

A5R004 Updates SAS Compliance Solutions Server 7.1

Important Note: For ease of completion of post-installation tasks, you can set the following environment variables:

```
UNIX:
# This should be changed to the path where SAS was installed.
export SASHOME=/install/SASHome

# This should be changed to the configuration folder and level for this deployment.
export SASCONFIG=/install/config/Lev1

# This is the base folder where SAS Compliance Solutions and all business units are deployed.
export FCFBASE=${SASCONFIG}/Applications/SASComplianceSolutions

# This will add the location of the SAS ant executable to the PATH.
export PATH=${SASHOME}/SASEnvironmentManagerAgent/2.5/installer/bin:${PATH}

WINDOWS:
# This should be changed to the path where SAS was installed.
set SASHOME=C:\PROGRA~1\SASHOME

# This should be changed to the configuration folder and level for this deployment.
set SASCONFIG=C:\SAS\Config\Lev1

# This is the base folder where SAS Compliance Solutions and all business units are deployed.
set FCFBASE=C:\SAS\Config\Lev1\Applications\SASComplianceSolutions

# This should add the location of ANT executable provided in the SAS installation, to the
PATH.
set PATH=%SASHOME%\SASEnvironmentManagerAgent\2.5\installer\bin;%PATH%
```

Important Note about **ant**: if there is another, competing installation of **ant** on your system, it may not be suitable for the purposes of this procedure. It may use a version of **ant** that does not match the configuration code delivered with SAS, or it may not be configured to include the **ant-apache-regexp** package, which is needed for proper operation of these steps. If you have another installation of **ant** on your system, you need to temporarily remove it from the PATH and clear out the value of the ANT_HOME environment variable, so that the version installed with SAS will be used.

Important Note: The **A5R004** hotfix comprises all changes made for hotfix 1 (A5R001), hotfix 2 (A5R003), hotfix 3 (A5R004), as well as new changes made for hotfix 4 (A5R005). If you previously installed and executed these steps for hotfix 1, and are just now installing hotfix 4, you should ignore all the hotfix 1 steps listed in this document after the keyword **HF1**, and execute those with keywords **HF2, HF3** and **HF4**. If you previously installed and executed these steps for hotfix 2, then you should ignore all the hotfix 1 and 2 steps listed in this document after the keywords **HF1** and **HF2**, and only execute those with the keyword **HF3** and **HF4.** If you are installing all the hotfixes for the first time, you need to execute all the steps, including those marked by the keywords **HF1, HF2, HF3,** and **HF4**.

Hotfix 1 (HF1) delivers Customer Due Diligence for the first time. It contains data model changes that, when executed, will drop the tables listed below.

Important Note about Database Changes: Do not execute HF1 database steps if HF1 has already been installed. All data in the tables will be deleted, and the tables will be created again with new table definitions. This is a destructive process and if these tables contain data from previous releases of CDD, your data should be backed up before these steps are executed.

The following tables will be dropped when the DDL is executed:

```
FCFKC.FSK_CDD_RULE
FCFKC.FSK_CDD_RULE_PARAMETER
FCFKC.FSK_CDD_RULE_GROUP
FCFKC.FSK_CDD_SCORING_EVENT
```

The following tables will be created when the DDL is executed:

```
FCFKC.FSK_CDD_REVIEW
FCFKC.FSK_CDD_REVIEW_EVENT
FCFKC.FSK_CDD_EDD_REVIEW
```

The following table will be altered:

```
FCFKC.FSK_RC_FORM_CONFIG
```

Hotfix 2 (HF2) only alters existing tables, so no data model changes will result in data loss. The following tables will be altered:

```
FCFKC.FSK_RC_REPORT
FCFKC.FSK_CASE
```

Hotfix 3 (HF3) only alters existing tables, so no data model changes will result in data loss. The following table will be altered:

```
FCFKC.FSK_RC_REPORT_ENTITY_INFO
```

Hotfix 4 (HF4) delivers several data model changes. The data model changes, when executed, will drop the tables listed below. **This will result in data loss** that can be restored by baking up the data and restoring it according to the instructions below.

Hotfix 4 will delete all data in the following tables, then it will create the tables again with new table definitions. This is a destructive process and there will be a loss of data that will affect the Alert Triage UI. The tables will be repopulated when the Alert Generation Process (AGP) is executed with HF4 applied.

The following tables will be dropped and recreated:

```
FCFKC.FSK_ALERTED_ENTITY
FCFKC.FSK_ALERT_TRANSACTION
FCFKC.FSK_ENTITY_TRANSACTION
FCFKC.FSK_ENTITY_TX_AGG
FCFKC.FSK_ALERT_TX_AGG
```

The Hotfix 4 (HF4) data model changes replace the ALERTED_ENTITY_KEY with the ALERTED_ENTITY_NUMBER in the Alert Triage Datamart. The Alert Triage Datamart tables contain no historical data except owner assignment for alerted entities (see steps below describing the procedure to save owner assignment information). The tables are rebuilt at the end of each run of the AGP. It is possible to load the Alert Triage Datamart prior to the next execution of the AGP, if you execute the macro %fcf_ent_load_dm_process. Prior to executing this macro, the fcf_autoexec must be executed, the macro %fcf_start_datetime_read must be executed, and the &runasofdate macro variable must be

set. The datamart macros in HF4 are also dependent on the changes to the FSC_EXT_PARTY_ACCOUNT_DIM table described below.

The following table will be altered:

```
FCFKC.FSC_EXT_PARTY_ACCOUNT_DIM
```

Hotfix 4 introduces a change to the FSC_EXT_PARTY_ACCOUNT_DIM table. This table has been changed to be a *Slowly Changing Dimensions Type 2* (SCD2) table. This is done to ensure that external party alerts are displayed and triaged correctly in the investigation UI.

The **A5R005** hotfix contains changed files that need to be applied to every business unit that is configured; for example: FCFBU1, FCFBU2, and FCFBU3. The following steps must be repeated for each business unit, substituting the business unit name wherever you see 'FCFBU1' in the steps below. Execute these steps for the first business unit, then change to the second business unit's **config** folder and execute the steps for the second business unit. Repeat as necessary until all business units have been configured.

1. It is vitally important that you back up your business unit databases.

2. It is vitally important that you back up your business unit folder before you proceed with the next step.

   For UNIX, back up $SASCONFIG/Applications/SASComplianceSolutions/FCFBU1 with its subdirectories.

   for Windows, back up %SASCONFIG%\Applications\SASComplianceSolutions\FCFBU1 with its subdirectories.

   Repeat this backup procedure for each business unit in the system.

3. Change the current directory to the $FCFBASE/**FCFBU1**/config folder.

   The Ant build.xml file has been updated in the hotfix release, so you need to copy the new version into your configuration folder.

   for UNIX:

   ```
   cp \
   $SASHOME/SASFoundation/9.4/misc/antimnycmn/deploy/script/build.xml .
   ```

   for Windows:

   ```
   copy ^
   %SASHOME%\SASFoundation\9.4\antimnycmn\sasmisc\deploy\script\build.xml^
    .
   ```

4. There should already exist a file named **build.properties** in the current folder, that was used when configuring the system. The file might have been deleted after the business unit was initially configured, if sensitive login passwords needed to be protected. If that is the case, the build.properties file needs to be created according to the instructions provided in the SAS Anti-

Money Laundering 7.1 Installation and Configuration Guide, Chapter 5, Post-Configuration, in the section titled "Configure Compute Tier Business Units."

You will need to provide a value for the following property:

```
jdbc.driver.dir=/install/jdbc/oracle
```

You should not specify the name of the driver in this variable, just the path; the driver name will be appended automatically depending on the DBMS selected.

In order to connect to the metadata server, you need to provide a value for the following properties:

```
metadata.user=sasadm@saspw
metadata.password=password
```

To connect to the DBMS and execute the HF1 and HF2 DDL, you need to provide a value for the system account:

```
dbms.system.userid=system
dbms.system.passwd=password
```

5. **HF1: For the first business unit (FCFBU1) only:**

   For this step, the metadata server must be running. To start the metadata server, execute:

   ```
   $SASCONFIG/SASMeta/MetadataServer/MetadataServer.sh start
   ```

   In this step you will deploy hotfix changes that are common to all business unit configurations. This step should be run **only one time** for the first business unit, FCFBU1 or whatever it may be named, and this step must be skipped for successive business units. The metadata server must be running in order for this step to succeed. This step should only be performed if you are configuring hotfix 1 (HF1).

   To execute the common code deployment, run **ant** with these parameters:

   ```
   ant hotfix_base -logfile hotfix_base.log
   ```

   When the execution has completed, inspect the hotfix_base.log file and check it for errors. If any errors should occur, please contact SAS Technical Support.

6. **HF1**: In this step you will deploy the hotfix 1 changes to your business unit. This step will replace a large number of files in the business unit configuration folder, including certain files in the custom/source folder, and will execute the hotfix 1 DDL scripts. This step should only be performed if you are configuring hotfix 1 (HF1).

   Execute the hotfix configuration for the current business unit by executing **ant** with these parameters:

   ```
   ant hotfix -logfile hotfix.log
   ```

When the execution has completed, inspect the hotfix.log file and check it for errors. Also check fcf_update.log and rc_update.log for errors. If any errors should occur, please contact SAS Technical Support.

7. **HF2**: In this step you will deploy the hotfix 2 changes to your business unit. This step will replace a large number of files in the business unit configuration folder, including certain files in the custom/source folder, and will execute the hotfix 2 DDL scripts. This step should be performed if you are configuring hotfix 2 (HF2).

   For this step, the metadata server must be running. To start the metadata server, execute:

   ```
   $SASCONFIG/SASMeta/MetadataServer/MetadataServer.sh start
   ```

   Execute the hotfix configuration for the current business unit by executing **ant** with these parameters:

   ```
   ant hotfix2 -logfile hotfix2.log
   ```

   When the execution has completed, inspect the `hotfix2.log` file and check it for errors. Also check the `rc_update_2.log` for errors. If any errors should occur, please contact SAS Technical Support.

8. **HF3**: In this step you will deploy the hotfix 3 changes to your business unit. This step will replace a large number of files in the business unit configuration folder, including certain files in the custom/source folder, and will execute the hotfix 3 DDL script. This step should be performed if you are configuring hotfix 3 (HF3).

   ```
   ant hotfix3 -logfile hotfix3.log
   ```

   When the execution has completed, inspect the `hotfix3.log` file and check it for errors. Also check the `rc_update_3.log` for errors. If any errors should occur, please contact SAS Technical Support.

9. **HF2 and HF3**: In this step you will execute update programs that refresh the FSK_LOV table with new display and label information.

   Important Note: This step will replace the contents of FSK_LOV and reset the mid-tier application server preferences to default values.

   ```
   ant load_hotfix -logfile hotfix3_load.log
   ```

10. **HF4:** If there is no need to preserve owner assignment for alerted entities then skip this step, the Alert Triage Datamart tables are rebuilt at the end of each run of the AGP or they can be populated by running the `%fcf_ent_load_dm_process` macro as described in one of the steps below.

    To save owner assignment for alerted entities back up the content of FSK_ALERTED_ENTITY table before executing the script in the next step and then restore the table content using the backed-up table as the source. There are many ways that the content of the table can be backed

up, below is an example using SAS code, please consult your DBA for the appropriate solution for your specific deployment:

```
%inc
"/install/config/Lev1/Applications/SASComplianceSolutions/FCFBU1/
custom/config/aml_autoexec.sas";

/* Step 1 - save the data - execute before applying HF4 changes
*/
data cmndata.FSK_ALERTED_ENTITY_SAVE;
    set seg_kc.FSK_ALERTED_ENTITY;
run;


/* Step 2 - restore data - execute after applying HF4 changes */

PROC APPEND BASE=seg_kc.FSK_ALERTED_ENTITY
DATA=cmndata.FSK_ALERTED_ENTITY_SAVE FORCE;
RUN;
```

After the content of the table is restored it is safe to run AGP or the `%fcf_ent_load_dm_process` macro, the owner assignment will be preserved.

11. **HF4:** In this step you will deploy the hotfix 4 changes to your business unit. This step will replace a large number of files in the business unit configuration folder, including certain files in the custom/source folder, and will execute the hotfix 4 DDL script. This step should be performed if you are configuring hotfix 4 (HF4). This step will replace the contents of FSK_LOV and reset the mid-tier application server preferences to default values.

    For this step, the metadata server must be running. To start the metadata server, execute:

    ```
    $SASCONFIG/SASMeta/MetadataServer/MetadataServer.sh start

    ant hotfix4 -logfile hotfix4.log
    ```

12. Start the compute tier servers:

    ```
    ${SASCONFIG}/sas.servers start
    ```

13. Restart the SOLR server after all business units have had the hotfix applied.

    For UNIX, execute:

    ```
    ${SOLR_HOME}/bin/solr restart
    ```

    For Windows, execute:

    ```
    %SOLR_HOME%\bin\solr.cmd restart -port 8983
    ```

14. Rebuild the SOLR index for the 'ewatchlist' entity. Navigate to the Solr Administration console by entering the following URL into your browser:

    http://compute tier server:8983/solr/#/CS-FCFBU1/dataimport//import/aml/entities

Next, set Command to **full-import** and check the **Commit** checkboxes. For Entity, select 'ewatchlist'. Do not check the **Clean** checkbox; it will cause all the indexed data to be dropped. Check the 'Auto-Refresh Status' box if you want to monitor task progress, and press the Execute button.

15. Review the sample program:
`$FCFBASE/FCFBU1/regulatoryConsole/rc_template/rc_fincen_load_sample_data.sas`
Decide if you need to re-execute the program, since the sample data has changed in the hotfix delivery.

    Follow the instructions under "Institution and Branch Setup for FinCEN Forms" in Chapter 6, "Regulatory Reports and E-Filing" from the SAS Anti-Money Laundering 7.1: Administration Guide.

16. When the HF4 deployment script was executed it added three additional columns to the FSC_EXT_PARTY_ACCOUNT_DIM table with default values. You need to ensure that the table contains correct data for the AGP and UI to use and that it is also SCD2 compliant. To accomplish this, a couple of additional steps are required:

    a. The ETL process needs to be modified to make sure that entity resolution is performed for external parties and the FSC_EXT_PARTY_ACCOUNT_DIM table is updated correctly. The AGP and UI code assumes that EXTERNAL_PARTY_NUMBER column values are unique for each party and all the records with the same value in EXTERNAL_PARTY_NUMBER are for the same party and only one record for each party has CHANGE_CURRENT_IND = 'Y'. All UI and AGP queries will use the record with CHANGE_CURRENT_IND = 'Y' as the current record for the party.

    b. Review your data in the FSC_EXT_PARTY_ACCOUNT_DIM table and make sure that there is only one record with CHANGE_CURRENT_IND = 'Y' for each party number in EXTERNAL_PARTY_NUMBER. For example, execute the query below:

```
select count(*) as DUP_COUNT, EXTERNAL_PARTY_NUMBER
from FCFCORE.FSC_EXT_PARTY_ACCOUNT_DIM
where CHANGE_CURRENT_IND='Y'
group by EXTERNAL_PARTY_NUMBER;
```

    Analyze and fix records where DUP_COUNT > 1. Because EXTERNAL_PARTY_NUMBER is used as a foreign key for the FSC_CASH_FLOW_FACT table, such records cannot be simply deleted without deleting the transactions first. The easiest workaround is to set CHANGE_CURRENT_IND='N' for all records but one, for example one where EXT_PARTY_ACCOUNT_KEY has the max value.

    Oracle workaround example:

```
update
  FCFCORE.FSC_EXT_PARTY_ACCOUNT_DIM e
set
  CHANGE_CURRENT_IND = 'N',
```

```
  CHANGE_BEGIN_DATE = CREATE_DTTM,
  CHANGE_END_DATE = CURRENT_DATE
where
  CHANGE_CURRENT_IND='Y' and
  exists (
    select *
    from FCFCORE.FSC_EXT_PARTY_ACCOUNT_DIM e1
    where
      e1.CHANGE_CURRENT_IND='Y' and
      e.EXT_PARTY_ACCOUNT_KEY < e1.EXT_PARTY_ACCOUNT_KEY and
      e.EXTERNAL_PARTY_NUMBER = e1.EXTERNAL_PARTY_NUMBER
  );
```

This change does not guarantee that the data will be valid because entity resolution was not performed but it will make the data SCD2 compliant for AGP and UI queries. Completing step #1 above ensures that all the future data in the table will be valid.

As an alternative to the workaround described above, you can back up the FSC_CASH_FLOW_BANK_BRIDGE, FSC_CASH_FLOW_FACT and FSC_EXT_PARTY_ACCOUNT_DIM tables, delete all the records from FSC_CASH_FLOW_BANK_BRIDGE and from FSC_CASH_FLOW_FACT. Then perform proper entity resolution on FSC_EXT_PARTY_ACCOUNT_DIM and fix the EXTERNAL_PARTY_NUMBER values if necessary by making them unique for each party. Re-populate FSC_CASH_FLOW_FACT and FSC_CASH_FLOW_BANK_BRIDGE using new party keys if necessary.

17. If you wish to reload the Alert Triage Datamart prior to the next execution of the AGP, you must execute the macro %fcf_ent_load_dm_process as part of a SAS program like the following:

```
%include "<SASCONFIG>/Applications/SASComplianceSolutions/
          FCFBU1/custom/config/fcf_autoexec.sas";
%fcf_get_runsasofdate
%fcf_start_datetime_read
%fcf_ent_load_dm_process
```

    If you choose not to reload the datamart tables, they will be reloaded during the next AGP execution. The SAS Compliance Solutions web application will not display information correctly until the datamart is updated.

18. For security reasons, you should modify your build.properties file to erase any clear text passwords stored in the file.

For any additional business units, you must repeat all these steps (except #5), for each business unit.

This concludes the compute tier portion of the hotfix configuration.

A5Q003 Updates SAS Compliance Solutions Mid-Tier 7.1

Important Note: For ease of completion of post-installation tasks, you can set the following environment variables:

```
UNIX:
# This should be changed to the path where SAS was installed.
export SASHOME=/install/SASHome

# This should be changed to the configuration folder and level for this deployment.
export SASCONFIG=/install/config/Lev1

# This is the base folder where SAS Compliance Solutions and all business units are deployed.
export FCFBASE=${SASCONFIG}/Applications/SASComplianceSolutions

# This will add the location of the SAS ant executable to the PATH.
export PATH=${SASHOME}/SASEnvironmentManagerAgent/2.5/installer/bin:${PATH}

WINDOWS:
# This should be changed to the path where SAS was installed.
set SASHOME=C:\PROGRA~1\SASHOME

# This should be changed to the configuration folder and level for this deployment.
set SASCONFIG=C:\SAS\Config\Lev1

# This is the base folder where SAS Compliance Solutions and all business units are deployed.
set FCFBASE=C:\SAS\Config\Lev1\Applications\SASComplianceSolutions

# This should add the location of ANT executable provided in the SAS installation, to the
PATH.
set PATH=%SASHOME%\SASEnvironmentManagerAgent\2.5\installer\bin;%PATH%
```

The **A5Q003** hotfix requires that the WebApps be rebuilt and redeployed. Use the following steps to perform this post-installation task:

Step 1: Re-build Web Applications

Note: For this step to execute correctly, at the very least the Metadata Server must be running. It is okay if all other servers are still running.

1. Invoke the SAS Deployment Manager 9.4.
   For UNIX, from $SASHOME/SASDeploymentManager/9.4, execute sasdm.sh.
   For Windows, from %SASHOME%\SASDeploymentManager\9.4, execute sasdm.exe.
2. Select a language in the Choose Language box
3. Select Rebuild Web Applications
4. Select Configuration Directory or enter the Configuration Directory and Level that needs to be updated
5. Specify Connection Information, including the sasadm User ID and Password
6. Select the following WebApps:
   SAS Compliance Solutions Mid 7.1
7. Verify the information on the Summary screen and select Start
8. Select Finish when the deployment is complete.
   This process will update the ear files in <SASCONFIGDIR>/Web/Staging. A backup of the original ear files will be placed in the directory below:
   <SASCONFIGDIR>/Web/Staging/Backup

Step 2: Re-deploy Web Applications

Note: In order for this step to execute correctly, everything should be running: the Metadata Server, the compute tier servers, and all Mid-Tier web application servers.

1. Invoke the SAS Deployment Manager 9.4.
   For UNIX, from $SASHOME/SASDeploymentManager/9.4, execute sasdm.sh.
   For Windows, from %SASHOME%\SASDeploymentManager\9.4, execute sasdm.exe.
2. Select a language in the Choose Language box
3. Select Deploy Web Applications
4. Select Configuration Directory or enter the Configuration Directory and Level that needs to be updated
5. Specify Connection Information, including the sasadm User ID and Password
6. Select the following WebApps:
   SAS Compliance Solutions Mid 7.1
7. Verify the information on the Summary screen and select Start
8. Select Finish when the deployment is complete

Step 3: Apply New Groups and Capabilities to Metadata

This hotfix contains changed metadata import data that needs to be applied to the first business unit that was configured when the product was deployed, usually FCFBU1. To configure the mid-tier, you need to execute an Ant script that deploys the antimnylndin.appxml file, token-substitutes it, and then loads it into the SAS Metadata Server. This step needs to be accomplished one time, for FCFBU1.

1. On the mid-tier server machine, create the folder $FCFBASE/**FCFBU1**/configmid, if it doesn't already exist.

2. Copy $SASHOME/SASComplianceSolutionsMidTier/7.1/deploy/script/build.xml there.

3. Create a build.properties file with these contents:

```
sasconfig.dir=/install/config/Lev1
jdbc.driver.dir=/install/jdbc/oracle
metadata.user=sasadm@saspw
metadata.password=password
dbms.segkc.userid=FCFBU1
dbms.segkc.passwd=password
```

   Note: On Windows platforms, all paths in the ANT property files must use double backslashes, or a single forward slash, in place of the single backslash character. These are both valid examples:

```
sasconfig.dir=C:/install/config/Lev1
sasconfig.dir=C:\\install\\config\\Lev1
```

4. Whether you are configuring HF1 only, or HF2 plus HF1, or HF3 plus HF2 and HF1, or HF4 plus HF3, HF2 and HF1, configure the Mid-Tier metadata for FCFBU1 using the command:

```
ant hotfix -logfile hotfix4.log
```

Step 4: Reapply Business Unit Datasource Definitions

When the Deployment Manager rebuilds and redeploys the web application WAR file, it overwrites all changes made to the following two files:

```
infrastructure_config.xml
spring-config.properties
```

The files are found in the following folder:

```
$SASCONFIG/Web/WebAppServer/SASServer8_1/sas_webapps/sas.financialservices.aml.war/
WEB-INF/spring-config
```

After the Deployment Manager redeploys the web application, only datasource definitions for the first bank (FCFBU1) will exist in the files listed above. You need to reapply the datasource information for the remaining business units back into the files. To do this, you will need to execute the following commands:

For UNIX:

```
  cd $FCFBASE/FCFBU2/configmid
  cp $SASHOME/SASComplianceSolutionsMidTier/7.1/deploy/script/build.xml .
  ant context_xml spring_xml spring_properties –logfile hotfix4.log
```

For Windows:

```
  cd %FCFBASE%\FCFBU2\configmid
  copy %SASHOME%\SASComplianceSolutionsMidTier\7.1\deploy\script\build.xml
.
  ant context_xml spring_xml spring_properties -logfile hotfix4_web.log
```

Perform Step 4 for FCFBU2, FCFBU3, and every other business unit except for the first.

When all business units have been reconfigured, restart the Compliance Solutions Mid-Tier web application server (usually SASServer8_1).

Step 5: Import AML Scenarios and CDD Rules Packages.

For Hotfix 4, there are changes to AML Scenarios and CDD delivers new Beneficial Ownership rules. There are two updated files located on the Compute Tier:

$SASHOME/SASFoundation/9.4/misc/antimnycmn/deploy/data/AMLScenarios.json
$SASHOME/SASFoundation/9.4/misc/antimnycmn/deploy/data/CDDRules.json

Open a browser session from the compute tier server, or copy the two files to your local machine and use a local browser. Log on to the Anti-Money Laundering web application as a user that has access to the first business unit and has Scenario Administrator and Rule Administrator capabilities.

Make sure, if you have changed the default AML Scenarios or their parameters, that you back up those changes before you proceed. It is not a good practice to change the default scenarios, but

instead we recommend making a copy and modifying the copy so that when hotfixes are applied, none of your customizations are lost or overwritten.

Click **Admin** on the Entity Triage window and then click **Scenarios** on the toolbar. Click **Import**. When prompted for a JSON file to import, click **Choose File** and navigate to the AMLScenarios.json file at the location shown above. Click **Import**. A message will be displayed stating that the import is in progress. Wait until a dialog window pops up showing the status of the import. Scroll through the information to make sure there was no failure during import. Click **Close** to finish the import.

Make sure, if you have changed the default CDD Rules or their parameters, that you back up those changes before you proceed. It is not a good practice to change the default rules, but instead we recommend making a copy and modifying the copy so that when hotfixes are applied, none of your customizations are lost or overwritten.

Click **Admin** on the Entity Triage window and then click **Rules** on the toolbar. Click **Import**. When prompted for a JSON file to import, click **Choose File** and navigate to the CDDRules.json file at the location shown above. Click **Import**. A message will be displayed stating that the import is in progress. Wait until a dialog window pops up showing the status of the import. Scroll through the information to make sure there was no failure during import. Click **Close** to finish the import.

Repeat these steps for each business unit on your system.

Concluding Steps:

For security reasons, you should modify your build.properties file to erase any clear text passwords stored in the file.

This concludes the metadata update portion of the mid-tier configuration.

A6A002 Updates SAS Compliance Solutions LASR Configuration 7.1

Important Note: For ease of completion of post-installation tasks, you can set the following environment variables:

```
UNIX:
# This should be changed to the path where SAS was installed.
export SASHOME=/install/SASHome

# This should be changed to the configuration folder and level for this deployment.
export SASCONFIG=/install/config/Lev1

# This is the base folder where SAS Compliance Solutions and all business units are deployed.
export FCFBASE=${SASCONFIG}/Applications/SASComplianceSolutions

# This will add the location of the SAS ant executable to the PATH.
export PATH=${SASHOME}/SASEnvironmentManagerAgent/2.5/installer/bin:${PATH}

WINDOWS:
# This should be changed to the path where SAS was installed.
set SASHOME=C:\PROGRA~1\SASHOME

# This should be changed to the configuration folder and level for this deployment.
```

```
set SASCONFIG=C:\SAS\Config\Lev1

# This is the base folder where SAS Compliance Solutions and all business units are deployed.
set FCFBASE=C:\SAS\Config\Lev1\Applications\SASComplianceSolutions

# This should add the location of ANT executable provided in the SAS installation, to the
PATH.
set PATH=%SASHOME%\SASEnvironmentManagerAgent\2.5\installer\bin;%PATH%
```

The **A5R004** hotfix contains changed files that need to be applied to every business unit that is configured; for example: FCFBU1, FCFBU2, and FCFBU3. The following steps must be repeated for each business unit, substituting the business unit name wherever you see 'FCFBU1' in the steps below. Execute these steps for the first business unit, then change to the second business unit's **configrpt** folder and execute the steps for the second business unit. Repeat as necessary until all business units have been configured.

1. Create the $FCFBASE/**FCFBU1**/configrpt folder and change directory to that folder:
   For UNIX:
   ```
   mkdir $FCFBASE/FCFBU1/configrpt
   cd $FCFBASE/FCFBU1/configrpt
   ```
   For Windows:
   ```
   mkdir %FCFBASE%\FCFBU1\configrpt
   cd %FCFBASE%\FCFBU1\configrpt
   ```

2. Copy the cslasrc.properties file from <FCFBASE>.
   For UNIX:
   ```
   cp  $FCFBASE/cslasrc.properties  $FCFBASE/FCFBU1/configrpt
   ```
   For Windows:
   ```
   copy  %FCFBASE%\cslasrc.properties  %FCFBASE%\FCFBU1\configrpt
   ```

3. Copy the build.xml file from the SASComplianceSolutionsLASRConfiguration folder:
   For UNIX:
   cp
   $SASHOME/SASComplianceSolutionsLASRConfiguration/7.1/Configurable/deploy/script/build.xml .
   For Windows:
   copy
   %SASHOME%\SASComplianceSolutionsLASRConfiguration\7.1\Configurable\deploy\script\build.xml

   Create a file in the current directory called **build.properties** and add the following properties to the file:

   ```
   host.name=machine.company.com
   ```

   The host.name value above must refer to the middle tier server.

   Because of a defect in the software deployment wizard that causes it to write 8 extra spaces to the value of dbms.segkc.userid in the cslasrc.properties file, you need to provide a property in the build.properties file to override it with a value that contains no trailing spaces:

```
dbms.segkc.userid=FCFBU1
```

If you are configuring an Oracle database, make the following additions to the build.properties:

```
dbms.engine=oracle
dbms.oracle.sid=ORCL
dbms.oracle.servicename=ORCL.COMPANY.COM
dbms.system.userid=system
dbms.system.password=password
dbms.core.userid=FCFCORE
dbms.kc.userid=FCFKC
dbms.segkc.userid=FCFBU1
```

If you are configuring a DB2 database, make the following additions to the build.properties:

```
dbms.engine=db2
dbms.database=database
dbms.system.userid=db2admin
```

If you are configuring a Teradata database, make the following additions to the build.properties:

```
dbms.engine=teradata
dbms.host=dbms.company.com
dbms.teradata.database=database
dbms.system.userid=dbc
dbms.teradata.perm.size=1000000000
dbms.teradata.spool.size=50000000
```

If you are configuring a SQLServer database, make the following additions to the build.properties:

```
dbms.engine=odbc
dbms.sqlserver.instance=database
dbms.system.userid=sa
```

If the metadata server is located on a different machine from the mid-tier server, make the following additions to the build.properties file:

```
metadata.host=metadata.company.com
```

If the metadata server operates on a different port from the default, specify the changed port number in the build.properties file:

```
metadata.port=9999
```

4. Execute **ant** to configure the report files and create empty extraction datasets:

```
ant -logfile reports.log
```

5. Validate that the reporting installer created empty report data sets.

You can confirm that the reporting installer ran correctly by looking in $SASCONFIG/AppData/SASComplianceSolutions/FCFBU1/AutoLoad. The following files should be there:

```
active_headers_data.sas7bdat
alert_investigation_extract.sas7bdat
cs_user_info_groups.sas7bdat
```

```
jobs_stats_detail.sas7bdat
jobs_stats_summary.sas7bdat
list_report_data.sas7bdat
risk_classifier_report_data.sas7bdat
scenario_audit.sas7bdat
scenario_change_history_data.sas7bdat
scenarios_and_risk_data.sas7bdat
user_group_role_totals.sas7bdat
```

6. Execute $FCFBASE/FCFBU1/AutoLoad/runsas.sh, to upload empty datasets to LASR.

   Validate that the Autoload program executed correctly and copied the datasets to LASR. The Autoload log file is located in $FCFBASE/FCFBU1/AutoLoad/Logs.

7. For security reasons, you should modify your build.properties file to erase any clear text passwords stored in the file.

This concludes the LASR configuration portion of the configuration.

A6H002 Updates SAS Compliance Solutions Mid-Tier LASR Configuration 7.1

The **A6H002** hotfix contains an updated version of the AMLReports.spk file located in the following folder:

```
$SASHOME/SASComplianceSolutionsMidTierLASRConfiguration/7.1/Config/Deployment
/Packages
```

From SAS Metadata Console, you need to re-import the AMLReports.spk package. For more detailed information on how to accomplish this, refer to the SAS Anti-Money Laundering 7.1: Installation and Configuration Guide, under Post-Configuration in the section “Configure Report Tier,” step 5.

This concludes the Mid-Tier LASR configuration portion of the configuration.