# Contents

**PART 1** Introduction  1

**Chapter 1 / Documentation and Technical Support Overview**  3
- Purpose of This Document  3
- Target Audience  3
- Technical Support  4

**Chapter 2 / System and Installation Overview**  5
- System Architecture Overview  5
- Migration and Upgrade Support  7
- Installation, Configuration, and Post-Installation
  - Procedures Outline  8
- Installation, Configuration, and Post-Installation Results  11

**PART 2** Installation Preparation  15

**Chapter 3 / Prepare for SAS Installation**  17
- Meet Pre-Installation Requirements for SAS 9.3  17
- Create Server Users  18
- Confirm Use of Correct Java Development Kit  19
- Know Your Web Application Server  19
- Understand JUnit Use If Needed  21
- Verify the Operating System Requirements  21
- Perform SAS Intelligence Platform Pre-Installation Tasks  22

**Chapter 4 / Prepare the Database**  23
- Configure Oracle Databases  24
- Configure MySQL Databases  26
Configure IBM DB2 Databases ........................................ 28
Configure Microsoft SQL Server ........................................ 30
Create Database Users ..................................................... 31
Ensure Proper DB Client and JDBC Driver Setup ...................... 33

PART 3  Installation and Configuration Process  35

Chapter 5  /  Review the Installation and Configuration Process ........................................ 37
Overview of the Install and Configure Sequence ....................... 37

Chapter 6  /  Run the SAS Deployment Wizard ........................................ 39
Run the SAS Deployment Wizard in Install Mode ....................... 40
Run the SAS Deployment Wizard in Configure Mode ................. 42
Recover from JBoss Configuration Failure Message ................... 53

PART 4  Post-Installation Tasks  55

Chapter 7  /  Perform Post-Installation Steps for SAS 9.3 ........................................ 57
Perform Post-Installation Configuration for SAS 9.3 ................... 57

Chapter 8  /  Perform Post-Installation Steps for Databases ........................................ 59
Post-Installation Database Setup Overview ............................ 59
Create Database Tables ..................................................... 60

Chapter 9  /  Perform Post-Installation Steps for SAS Financial Crimes Monitor ...................... 65
Post-Installation Procedure for the SAS Financial Crimes Monitor ........................................ 65
Initialize Users and Groups .................................................. 68

Chapter 10  /  Perform Post-Installation Steps for SAS Social Network Analysis Server .................. 71
| Purpose of Post-Installation Procedures for the SAS Social Network Analysis Server | 72 |
| Import SAS Stored Processes and Deploy Web Services | 73 |
| Initialize Users and Groups | 79 |
| Sample Integration Between SAS Financial Crimes Monitor and SAS Social Network Analysis | 82 |

**PART 5 Setup Tasks 101**

**Chapter 11 / Set Up the SAS Financial Crimes Monitor 103**
- Understanding the Setup Procedure for the SAS Financial Crimes Monitor 104
- Overview of the Post-Installation Setup for the SAS Financial Crimes Monitor 112
- Complete Setup Tasks for the SAS Financial Crimes Monitor 116

**Chapter 12 / Set Up the SAS Social Network Analysis Server 131**
- Setup Tasks for the SAS Social Network Analysis Server 131

**PART 6 Appendixes 133**

**Appendix 1 / Perform Post-Migration Steps 135**
- Understanding SAS Migration 135
- Migration Preparation 136
- Perform Migration 137

**Appendix 2 / Upgrading to the First Maintenance Release of Version 3.1 139**
- Understanding SAS Software Updates 139
- Maintenance Release Update Preparation 141
- Applying the Maintenance Release 142
<table>
<thead>
<tr>
<th>Appendix 3 / Perform Post-Upgrade Steps for Databases</th>
<th>145</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of Post-Upgrade Steps for Databases</td>
<td>146</td>
</tr>
<tr>
<td>Upgrade Approach</td>
<td>146</td>
</tr>
<tr>
<td>Prerequisites and Environments</td>
<td>147</td>
</tr>
<tr>
<td>Restoring Customizations</td>
<td>149</td>
</tr>
<tr>
<td>Upgrade and Alter Scripts</td>
<td>149</td>
</tr>
<tr>
<td>Data Migration Scripts</td>
<td>150</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>154</td>
</tr>
<tr>
<td>Schema Changes for SAS Financial Crimes Monitor</td>
<td>154</td>
</tr>
</tbody>
</table>

Index .............................................................................................................. 171
Introduction

Chapter 1
   Documentation and Technical Support Overview .................. 3

Chapter 2
   System and Installation Overview .................................... 5
Documentation and Technical Support

Overview

Purpose of This Document

This document provides installation and configuration information for the SAS Social Network Analysis Server and the SAS Financial Crimes Monitor.

Target Audience

The target audience for this document includes SAS administrators, database administrators, and system administrators using the SAS Social Network Analysis Server or the SAS Financial Crimes Monitor. For the purpose of this document, the SAS Administrator, the Database Administrator, and the System Administrator tasks are defined as follows:
SAS Administrator
SAS administrators assign investigator roles to investigators for the SAS Social Network Analysis Server and administrator roles to the SAS Financial Crimes Monitor users.

Database Administrator
Database administrators configure schema and database user IDs for use with the SAS Social Network Analysis Server and the SAS Financial Crimes Monitor.

System Administrator
System administrators configure data sources, data stores, and investigation paths.

---

**Technical Support**

SAS Technical Support is the first group to contact regarding installation and configuration issues that are encountered. To contact SAS Technical Support, perform the following steps:

2. Select **Contact Us**.
3. Select the appropriate Web page or telephone number from the **Support Contacts** section of the page.
System and Installation Overview

System Architecture Overview

Migration and Upgrade Support

Installation, Configuration, and Post-Installation Procedures Outline

Installation, Configuration, and Post-Installation Results

System Architecture Overview

The SAS Financial Crimes Monitor and the SAS Social Network Analysis Server are offerings included with the SAS Fraud Framework. The solution is designed to be optimized easily for various industries (for example, banking, insurance, health care, or government).

For purposes of installation and configuration, it is best to think of the system as divided into three sections—a client tier, a middle tier, and a data tier. The relationship of the tiers is shown in the following figure.
After the system is installed and configured and the post-installation tasks are completed, there are two entrance points, depending on the user and the type of access required. Administrators and analysts access the SAS Financial Crimes Monitor to set up projects and to define scenario groups and scenarios (including fraud detection, risk, second pass, scoring, routing, and suppression). Using the SAS Financial Crimes Monitor, users can also apply data enrichment to entities within scenarios, create managed lists, and use calculated fields to optimize project data. Investigators access the SAS Social Network Analysis Server to triage and manage alerts.

The solution includes three essential data models:

- **SASFCMDB**
  SASFCMDB is the default database used by the SAS Financial Crimes Monitor to store initial, development, and saved data.
**SASSNADB**

SASSNADB is the default database for SAS Social Network Analysis Server.

The following section describes the high-level process for installing, configuring, and performing post-installation tasks for the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server.

---

**Migration and Upgrade Support**

In the first maintenance release of version 3.1 for the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server, the following migration and upgrade paths are supported.

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Method</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 3.1 first maintenance release</td>
<td>Version 3.1 first maintenance release</td>
<td>Migration (SAS Migration Utility and SAS Deployment Wizard)</td>
<td>Enables migration to other environments, such as from development to testing or production. See Appendix 1, “Perform Post-Migration Steps,” on page 135.</td>
</tr>
</tbody>
</table>
### Source | Target | Method | Notes
--- | --- | --- | ---

**Note:** Migration involves also migrating database tables. For information migrating database tables from the first maintenance release of version 2.3 to the first maintenance release of version 3.1, see Appendix 3, “Perform Post-Upgrade Steps for Databases,” on page 145.

---

### Installation, Configuration, and Post-Installation Procedures Outline

The SAS Financial Crimes Monitor and the SAS Social Network Analysis Server can be upgraded from version 2.3 to version 3.1, or they can be installed as a first deployment. If you are upgrading to the first maintenance release, refer to “Upgrading to the First Maintenance Release of Version 3.1” on page 139 for detailed information. If you are performing an initial installation, here are the high-level steps for installing, configuring, and performing post-installation tasks for the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server:

#### Installation and Configuration Procedure

1. Confirm that the pre-installation requirements for SAS 9.3, the system requirements for SAS 9.3, and the system requirements for both the SAS Financial Crimes Monitor 3.1 and the SAS Social Network Analysis Server 3.1 have been met.
Note: If your process for running jobs through the SAS Financial Crimes Monitor includes automatic kickoff of projects, then you will need to make sure that you have a compatible scheduler installed that can launch the SAS program required to run jobs. Without a scheduler, jobs must be executed manually.

2 Create an operating system account that will be used to enable the SAS Financial Crimes Monitor to access the needed databases and system resources when a job is executed.

**CAUTION! Avoid delays in the installation process.** In some deployments, requests for user IDs must be submitted. If requests for user IDs need to be made, make the request early and confirm setup before proceeding with the process. Otherwise, delays for installing and configuring SAS software might be encountered.

3 Install third-party software:

   a Install and configure one of the following databases:

      - Oracle Database
      - MySQL Server
      - IBM DB2
      - Microsoft SQL Server

      See “Prepare the Database” on page 24 for additional information about preparation of databases.

   b Install one of the following web application servers:

      - JBoss Application Server. See “Know Your Web Application Server” on page 19 for additional information about supported JBoss versions and configuration requirements.
      - IBM WebSphere Application Server
      - Oracle WebLogic Server

4 Launch the SAS Deployment Wizard and specify **Install SAS Software**.
Note: If you are planning to set up an installation with multiple managed servers, you must select Custom (not Typical) from the SAS Deployment Wizard during the process in order to be presented with the option to install multiple managed servers.

Use the SAS Deployment Wizard to install, but not configure, the following:

a  SAS Foundation

b  SAS/ACCESS

c  SAS Financial Crimes Monitor. This includes the SAS Financial Crimes Monitor middle tier, which can be installed on the same machine as the SAS Financial Crimes Monitor server.

d  SAS Social Network Analysis Server. This includes the SAS Social Network Analysis Server middle tier, which can be installed on the same machine as the SAS Social Network Analysis Server.

5 Run the SAS Deployment Wizard in configure mode to configure the installed SAS software.

Note: Depending on the version of JBoss that you are using, you might have to perform a manual configuration task before the SAS Deployment Wizard configuration procedure can be completed. See “Know Your Web Application Server” on page 19 for additional information about supported JBoss versions and configuration requirements.

Post-Installation Procedure

1 Perform post-installation and configuration tasks for SAS 9.3, the SAS Financial Crimes Monitor, and the SAS Social Network Analysis Server:

SAS 9.3

a  Access the appropriate documentation resources for your operating system as indicated in “Perform Post-Installation Configuration for SAS 9.3” on page 57.

b  Follow the instructions to complete the post-installation steps for SAS 9.3.
c Continue with the post-installation procedures for the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server.

SAS Financial Crimes Monitor

a Confirm that the LIBNAME statement is correct.

b Assign groups to the SAS Financial Crimes Monitor: Admin role.

Note: At the end of the post-installation process for the SAS Financial Crimes Monitor, you will be able to log on to the SAS Financial Crimes Monitor, but you will be unable to create or save items until administration tasks have been completed. See Chapter 10, “Perform Post-Installation Steps for SAS Social Network Analysis Server,” on page 71 for details about the administrative tasks that must be performed.

SAS Social Network Analysis Server

a Import SAS stored processes from a SAS package.

b Deploy the imported SAS stored processes as a web service.

c Add an Investigator group and investigators.

2 Access each application to ensure that the installation, configuration, and post-installation procedures were performed correctly. See “Installation, Configuration, and Post-Installation Results” on page 11 for a description of what to expect when you launch each application after completing the SAS Deployment Wizard installation and configuration process and the post-installation procedures.

Installation, Configuration, and Post-Installation Results

The process of completing the SAS Deployment Wizard installation and configuration procedure and performing the post-installation tasks for the SAS Financial Crimes
Monitor and the SAS Social Network Analysis Server can take hours to complete. The result of completing the process yields a stable fraud detection system that is available to users through the specified web browsers.

The system has two points of entry, based on configured users and the associated permission level. The SAS Financial Crimes Monitor enables users to create projects that generate alerts. Investigators have access to these alerts through the SAS Social Network Analysis Server. The SAS Social Network Analysis Server enables investigators to triage and manage alerts. The following image presents a simplified view of the user components available at the completion of the installation and configuration process.

After the installation, configuration, and post-installation procedures are complete for the SAS Social Network Analysis Server and the SAS Financial Crimes Monitor, each application can be launched from the designated web addresses.

The SAS Financial Crimes Monitor opens to display the interface.

Note: Although you will be able to log on to the SAS Financial Crimes Monitor, you will not be able to create or save items until administration tasks have been completed. See Chapter 10, “Perform Post-Installation Steps for SAS Social Network Analysis Server,” on page 71 for details about the administrative tasks that must be performed.
The SAS Social Network Analysis Server prompts to allow selection of an alert series if the user logging in has been configured for access to more than one alert series. If the user has not been configured to access an alert series or if at least one alert series has not been configured, a warning might be displayed. If all conditions are met, however, then the SAS Social Network Analysis Server opens to display an interface ready to list alerts and show the network diagram associated with entities defined through the SAS Financial Crimes Monitor.

**Note:** The **Disposition** menu must be configured and enabled as a separate procedure. Refer to *SAS Social Network Analysis Server: Administration Guide* for detailed instructions for enabling and configuring the **Disposition** menu.
Note: If post-installation procedures have not been completed properly, including configuration of analytic contexts and deployment of stored processes to populate the interface with data, then an error or warning might be presented after you log on to the SAS Social Network Analysis Server.

Further enhancements can be made to customize the applications. See *SAS Social Network Analysis Server: Administration Guide* for additional configuration and customization features for the SAS Social Network Analysis Server and the SAS Financial Crimes Monitor.
Part 2

Installation Preparation

Chapter 3
Prepare for SAS Installation ........................................... 17

Chapter 4
Prepare the Database .................................................. 23
Meet Pre-Installation Requirements for SAS 9.3

The following table contains URLs to reference documentation for installing SAS 9.3 Foundation on UNIX and Microsoft Windows environments. Go to the URL that corresponds to the appropriate operating system and follow all the applicable steps on those pages.
Create Server Users

The SAS Financial Crimes Monitor and the SAS Social Network Analysis Server rely on an alert generation process to analyze data, perform rule-based and analytic processing, and then generate and display alerts from the analyzed data. To run the alert generation process, the solution requires an operating system user ID. You can assign this user ID operating system credentials or you can create an additional operating system user, such as `fcmctrl`. Since this user ID is an operating system ID, rely on best practices for your enterprise when making this decision.

If you do not already have an operating system account to use for running the alert generation process, then create one, or request one from your system administrator.

As a post-installation task, user IDs must be created in metadata and then the user IDs must be associated with the SAS Financial Crimes Monitor or the SAS Social Network Analysis Server, as appropriate.

For details about database users and access permissions, see “Create Database Users” on page 31.
Confirm Use of Correct Java Development Kit

Use the following URL to identify the version required for the specific hardware and operating environment:


Refer to the Java Development Kits (JDK) section at the URL. Be sure to get the JDK that matches your web application server.

Note: It is not necessary to download a JDK if the IBM WebSphere Application Server is used in the deployment. The IBM WebSphere Application Server includes a specific version of the IBM JDK that is automatically installed and used.

Know Your Web Application Server

The SAS Financial Crimes Monitor and the SAS Social Network Analysis Server support the IBM WebSphere Application Server, Oracle WebLogic Server, and many versions of JBoss Application Server. For more information about these web application servers, see the SAS 9.3 Support for Web Application Servers and HTTP Servers page at the following URL: http://support.sas.com/resources/thirdpartysupport/v93/appservers/index.html.

The SAS Financial Crimes Monitor and the SAS Social Network Analysis Server support a subset of the JBoss Application Servers. Make sure your JBoss Application Server is consistent with one of the ones listed in the following table.
## JBoss Application Server Versions

**Supported by the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server**

<table>
<thead>
<tr>
<th>JBoss Application Server</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>JBoss EAP 5.1.1</td>
<td>For performance optimization and to eliminate the need for manual configuration during the SAS Deployment Wizard configuration procedure, this is the recommended JBoss Application Server version.</td>
</tr>
<tr>
<td>JBoss EAP 4.3.0 CP08 through 4.3.0 CP10</td>
<td></td>
</tr>
<tr>
<td>JBoss EAP 4.3.0 through 4.3.0 CP07</td>
<td>Not recommended. Can be used, but you will receive a Configuration Failure error during the SAS Deployment Wizard configuration procedures. Several manual changes must be performed before the SAS Deployment Wizard configuration procedure can be completed. See “Recover from JBoss Configuration Failure Message” on page 53 for additional information.</td>
</tr>
<tr>
<td>JBoss AS (Community) 4.2.3</td>
<td>Not recommended. Can be used, but you will receive a Configuration Failure error during the SAS Deployment Wizard configuration procedures. Several manual changes must be performed before the SAS Deployment Wizard configuration procedure can be completed. See “Recover from JBoss Configuration Failure Message” on page 53 for additional information.</td>
</tr>
</tbody>
</table>

For more information about JBoss Application Server support for SAS 9.3, see the JBoss Application Server Support for SAS 9.3 page at the following URL:

http://support.sas.com/resources/thirdpartysupport/v93/appservers/jbosssw.html

For more information about the types of changes that are required for deployments including either JBoss AS (Community) 4.2.3 or any of the JBoss EAP versions between 4.3.0 and 4.3.0 CP07, inclusive, see “Recover from JBoss Configuration Failure Message” on page 53.
Understand JUnit Use If Needed

If the SAS Deployment Tester is installed in addition to the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server, then JUnit 4.8.1 is recommended. See the JUnit information that is provided on the SAS 9.3 Support for Additional Software Products page at the following URL:

http://support.sas.com/resources/thirdpartysupport/v93/othersw.html#tab junit

Verify the Operating System Requirements

Before you install the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server, make sure that you meet the minimum system requirements that are described in the system requirements documentation. System requirements are unique for each operating system. Items that are addressed as system requirements include software requirements, hardware requirements, space requirements, specific product requirements, and graphics hardware and software compatibility.

To view system requirements for the SAS Financial Crimes Monitor:


2. Select the SAS 9.3 (TS1M0) System Requirements link.

   The Search page is displayed showing the Results Filter tab having focus with 9.3 selected as the SAS Release option.

3. Perform each of the following:
   a. From the Product menu on that web page, select SAS Financial Crimes Monitor.
The page updates to show linked documents meeting the criteria specified.

b Click the name of the desired link to access the system requirements document.

The page that is displayed includes information about the server tier, the middle tier, and the client tier, as appropriate. Use the drop-down menus to select a target environment for which to display the requirements.

To view system requirements for the SAS Social Network Analysis Server:

1 Access the SAS System Requirements page at http://support.sas.com/resources/sysreq/index.html.

2 Select the SAS 9.3 (TS1M0) System Requirements link.

The Search page is displayed showing the Results Filter tab having focus with 9.3 selected as the SAS Release option.

3 Perform each of the following:

a From the Product menu on that web page, select SAS Social Network Analysis Server.

The page updates to show linked documents meeting the criteria specified.

b Click the name of the desired link to access the system requirements document.

The page that is displayed includes information about the server tier, the middle tier, and the client tier, as appropriate. Use the drop-down menus to select a target environment for which to display the requirements.

---

**Perform SAS Intelligence Platform Pre-Installation Tasks**

For information about pre-installation tasks that are required to install the SAS Intelligence Platform, see the SAS Intelligence Platform: Installation and Configuration Guide at http://support.sas.com/documentation/onlinedoc/intellplatform/index.html.
Prepare the Database

**Configure Oracle Databases** .......................................................... 24
  Product Documentation ................................................................. 24
  Instructions for the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server ............... 24

**Configure MySQL Databases** ..................................................... 26
  Product Documentation ................................................................. 26
  Prerequisites .................................................................................. 26
  Instructions for the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server ............... 27

**Configure IBM DB2 Databases** ..................................................... 28
  Product Documentation ................................................................. 28
  Instructions for the SAS Financial Crimes Monitor .......... 28
  Instructions for the SAS Social Network Analysis Server ........... 29

**Configure Microsoft SQL Server** .................................................. 30
  Product Documentation ................................................................. 30
  Instructions for the SAS Financial Crimes Monitor .......... 30
  Instructions for the SAS Social Network Analysis Server ........... 31

**Create Database Users** ............................................................... 31

**Ensure Proper DB Client and JDBC Driver Setup** ......................... 33
Configure Oracle Databases

Product Documentation

Oracle Database 11g Release 2 Documentation Library: http://www.oracle.com/pls/db112/homepage

CAUTION! Successful installation is driver-dependent. If you are using Oracle Database 11g Release 2, you must use the driver that is delivered with this release. Using any other driver version will result in operating issues and you might see connection errors in the log files.

Oracle Database 10g Release 2 Documentation Library: http://www.oracle.com/pls/db102/homepage

Instructions for the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server

1 Install Oracle Database, and record the location of the Oracle JDBC drivers.

   The location is typically $ORACLE_HOME/jdbc/lib.

   Note: The location must be provided to the SAS Deployment Wizard.

   If the SAS middle-tier software will be installed on a different machine, then copy the drivers to the machine that will be used for the SAS middle tier.

2 Create and configure a database and schema within Oracle Database.

   During this process, the hardware sizing, hardware configuration, global database settings, table space creation, and data files specification are performed.

   Note: The SAS Deployment Wizard defaults to a database that is named FINCRMDB for the SAS Financial Crimes Monitor and to a database that is named
SASSNADS for the SAS Social Network Analysis Server, but the names referenced by the SAS Deployment Wizard can be changed during the installation.

The creation of the databases is usually performed with the Oracle Database Configuration Assistant (DBCA).

**Table 4.1**  *Field Values for the SAS Financial Crimes Monitor Configured with DBCA*

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Database Name</td>
<td>FINCRMDB.my.domain.com</td>
</tr>
<tr>
<td>SID</td>
<td>FINCRMDB</td>
</tr>
</tbody>
</table>

**Display 4.1**  *Example of DBCA Dialog Box Showing Values for Fields*

![Example of DBCA Dialog Box](image)

**Table 4.2**  *Field Values for the SAS Social Network Analysis Server Configured with DBCA*

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Database Name</td>
<td>SASSNADS.my.domain.com</td>
</tr>
<tr>
<td>SID</td>
<td>SASSNADS</td>
</tr>
</tbody>
</table>
For the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server, the SID will be used in the URL for the database connection:

url: jdbc:oracle:thin:@serverName.unx.example.com:1521:FINCRMDB

Configure MySQL Databases

Product Documentation


Select the appropriate version from left navigation pane at the web site indicated previously.

Prerequisites

If the JDBC driver has not already been installed on the middle-tier machine, then download Connector/J from the following link:

http://dev.mysql.com/downloads/connector/j/
Record the location of the JDBC drivers.

**Note:** The location must be provided to the SAS Deployment Wizard.

---

**Instructions for the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server**

1. **Install MySQL version 5.1 or 5.5.**

   **Note:** Although the middle tier for the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server supports MySQL 5.0, 5.1, and 5.5, the SAS (data tier) infrastructure supports 5.1 and 5.5 only. For maximum compatibility, installation of MySQL 5.1 or 5.5 is recommended. For more information about SAS/ACCESS Interface to MySQL software, please see the MySQL chapter in SAS/ACCESS Software for Relational Databases: Reference.

2. **Create and configure a database within MySQL, paying attention to the following:**

   - In the my.ini file, configure the database so that the default engine type is InnoDB.
   - In the my.ini file, verify that the appropriate character set is specified.

     **Note:** Because UTF-8 encoding generally allows for the proper display and saving of characters related to a wide variety of languages, UTF-8 is the recommended Unicode setting.

   - SAS also suggests setting `innodb_flush_log_at_trx_commit` to 1 so that the transaction logs are flushed to disk after each transaction is committed.

     **Note:** The SAS Deployment Wizard defaults to a database that is named FINCRMDB for the SAS Financial Crimes Monitor and to a database that is named SASSNADS for the SAS Social Network Analysis Server, but the names referenced by the SAS Deployment Wizard can be changed during the installation.
Configure IBM DB2 Databases

Product Documentation


IBM DB2 Database for Linux, UNIX, and Windows Information Center: http://publib.boulder.ibm.com/infocenter/db2luw/v9r7/index.jsp

Instructions for the SAS Financial Crimes Monitor

1. Install DB2, and record the location of the JDBC drivers.

   The location is typically in the DB2 installation directory, in a directory that is named java. Identify which JDBC driver JAR file applies to the JDK that is used by the web application server, and then copy that JAR file to a separate directory.

   **Note:** The directory name must be provided to the SAS Deployment Wizard. Make sure that this directory contains only the JAR file that will be needed.

   If the SAS middle-tier software will be installed on a different machine, then copy the JDBC driver JAR file to that machine.

2. Create and configure a database.

   The SAS Financial Crimes Monitor requires that the table space for the database uses a 32-kilobyte page size.

   The following command is a sample SQL statement for creating the SAS Financial Crimes Monitor database instance:

   ```sql
   create database FINCRMDB
   pagesize 32 k user tablespace
   managed by database
   using (file '/data01/fincrmdb/fincrmdb.dbf' 16184)
   ```
autoresize yes
temporary tablespace
managed by system
using ('/data01/fincrmdb/user_tmp')
extentsize 32

Note: The SAS Deployment Wizard defaults to a database that is named FINCRMDB for the SAS Financial Crimes Monitor, but the names referenced by the SAS Deployment Wizard can be changed during the installation.

Instructions for the SAS Social Network Analysis Server

1 Install DB2, and record the location of the JDBC drivers.

The location is typically in the DB2 installation directory, in a directory that is named java. Identify which JDBC driver JAR file applies to the JDK that is used by the web application server, and then copy that JAR file to a separate directory.

Note: The directory name must be provided to the SAS Deployment Wizard. Make sure that this directory contains only the JAR file that will be needed.

If the SAS middle-tier software will be installed on a different machine, then copy the JDBC driver JAR file to that machine.

2 Create and configure a database.

The SAS Social Network Analysis Server requires that the table space for the database uses a 32-kilobyte page size.

The following command is a sample SQL statement for creating the SAS Social Network Analysis Server database instance:

create database SASSNADS
pagesize 32 k user tablespace
managed by database
using (file '/../data01/sassnads/sassnads.dbf' 16184)
autoresize yes
temporary tablespace
managed by system
using ('/data01/sassnads/user_tmp')
extentsize 32
Note: The SAS Deployment Wizard defaults to a database that is named SASSNADS for the SAS Social Network Analysis Server, but the name referenced by the SAS Deployment Wizard can be changed during the installation.

Configure Microsoft SQL Server

Product Documentation


Instructions for the SAS Financial Crimes Monitor

1 Install SQL Server.

2 Create and configure a database.

   The following command is a sample SQL statement for creating the SAS Financial Crimes Monitor database instance:

```
create database fincrmdb
   on
   ( name = fincrmdbdat,
     filename = 'c:\sqlserver\datafiles\fincrmbdb.mdf',
     size = 5120,
     maxsize = 8192,
     filegrowth = 50 )
log on
   ( name = fincrmbdblog,
     filename = 'c:\sqlserver\transaction_logs\fincrmbdblog.1df',
     size = 5120MB,
     maxsize = 8192MB,
     filegrowth = 50MB )
;```
Note: The SAS Deployment Wizard defaults to a database that is named FINCRMDB for the SAS Financial Crimes Monitor, but the name referenced by the SAS Deployment Wizard can be changed during the installation.

Instructions for the SAS Social Network Analysis Server

1 Install SQL Server.

2 Create and configure a database.

   The following command is a sample SQL statement for creating the SAS Social Network Analysis Server database instance:

   ```sql
   create database SASSNADS
   on
   ( name = snadat,
     filename = 'c:\sqlserver\datafiles\snadat.mdf',
     size = 5120,
     maxsize = 8192,
     filegrowth = 50 )
   log on
   ( name = snalog,
     filename = 'c:\sqlserver\transaction_logs\snalog.1df',
     size = 5120MB,
     maxsize = 8192MB,
     filegrowth = 50MB )
   ;
   ```

Note: The SAS Deployment Wizard defaults to a database that is named SASSNADS for the SAS Social Network Analysis Server, but the name referenced by the SAS Deployment Wizard can be changed during the installation.

Create Database Users

Creating database user IDs before running the SAS Deployment Wizard is an optional task. The SAS Deployment Wizard requires information about how to connect to the
database with JDBC, including user credentials, but it installs and configures the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server without connecting to the database. As a result, you can create database user IDs before running the SAS Deployment Wizard if it is more convenient or you prefer to do so.

The following tables list the default values for the user IDs and schemas.

### Table 4.3  SAS Financial Crimes Monitor User ID and Schema

<table>
<thead>
<tr>
<th>User ID</th>
<th>FINCRMDB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schema</td>
<td>FINCRMDB</td>
</tr>
</tbody>
</table>

**Note:** The `fincrmdb` user will be set up to authenticate into the database in a procedure defined in the SAS Social Network Analysis Server: Administration Guide. You can assign this user ID operating system credentials or you can create an additional operating system user, such as `fcmctrl`. Creating unique user IDs to enable one (for example, `fincrmdb`, the default User ID created during installation) to have standard permissions to access data and another (for example, `fcmctrl`) to enable the solution to access and execute the SAS code enables you to separate access controls.

### Table 4.4  SAS Social Network Analysis User ID and Schema

<table>
<thead>
<tr>
<th>User ID</th>
<th>SNAUSER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schema</td>
<td>SASSNADS</td>
</tr>
</tbody>
</table>

**Note:** If you are using IBM DB2 and the database uses operating system user IDs for authentication, then you need to create a user ID named `snauser` to enable proper operation of the Social Network Analysis Server. See Table 4.5 on page 33 for details about the access permissions.

The SNAUSER needs access to certain tables in the SAS Financial Crimes Monitor to be able to perform alert dispositioning through the SAS Social Network Analysis Server. The permissions required for the SNAUSER are outlined in the following table.
Table 4.5  Access Permissions for SNAUSER

<table>
<thead>
<tr>
<th>Access Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SELECT or READ</td>
<td>Enables access to the FCM_ALERT* tables.</td>
</tr>
<tr>
<td>INSERT</td>
<td>Enables access to the FCM_ALERT_EVENT table.</td>
</tr>
<tr>
<td>UPDATE</td>
<td>Enables access to the FCM_ALERT table. Must be able to update FCM_SEQUENCE table.</td>
</tr>
</tbody>
</table>

Ensure Proper DB Client and JDBC Driver Setup

As a post-installation task, you must run several database scripts provided with the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server to prepare and initialize your databases. These database scripts assume that a database client application is installed and available on the PATH.

If the database is not installed on the same machine as the server tiers for the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server, then install the database client on the server-tier machine.

The SAS Financial Crimes Monitor and the SAS Social Network Analysis Server middle-tier web applications require access to the databases through JDBC. If the database is installed on a different machine than the middle tier applications, then install the JDBC driver for the databases on the middle-tier machine.

The following table identifies the JDBC drivers for the databases that the SAS Social Network Analysis Server and the SAS Financial Crimes Monitor support.
### Table 4.6  JDBC Driver and Java Version Support

<table>
<thead>
<tr>
<th>Database</th>
<th>Driver</th>
<th>Java Version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Database</td>
<td>ojdbc6.jar</td>
<td>Java 6</td>
<td>This includes a compatible version of JBoss 4.3 and Oracle WebLogic Server 11g.</td>
</tr>
<tr>
<td></td>
<td>Minimum version</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>– 11.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MySQL Database</td>
<td>mysql-connector-java-5.1.13-bin.jar</td>
<td>Java 6</td>
<td>This includes a compatible version of JBoss 4.3 and Oracle WebLogic Server 11g.</td>
</tr>
<tr>
<td>IBM DB2</td>
<td>db2jcc4.jar; Version v9.5fp6a_jdbc_sqlj</td>
<td>Java 6</td>
<td>Failure to use v9.5fp6a_jdbc_sqlj will result in Hibernate exceptions being written to the log files.</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>sqljdbc4.jar</td>
<td>Java 6</td>
<td>Provides support for JDBC 4.0.</td>
</tr>
</tbody>
</table>

Because the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server support a subset of the JBoss Application Servers, you must make sure your JBoss Application Server is consistent with one of the supported versions. See “Know Your Web Application Server” on page 19 for additional information about compatible JBoss versions.
Part 3

Installation and Configuration Process

Chapter 5
Review the Installation and Configuration Process ............ 37

Chapter 6
Run the SAS Deployment Wizard ..................................... 39
Overview of the Install and Configure Sequence

The SAS Deployment Wizard has two modes: install and configure. It is important to run the wizard in install mode and then run the wizard a second time in configure mode. The following steps describe the sequence for a single-machine deployment and then for a multiple-machine deployment.

**Single-Machine Deployment**

1. Run the SAS Deployment Wizard in install mode.

2. Run the SAS Deployment Wizard in configure mode.

**Multiple-Machine Deployment**

In a multiple-machine deployment, start with the server-tier machine and follow the same order of install and then configure:

1. Run the SAS Deployment Wizard in install mode on the server-tier machine, and then on the middle-tier machine.
2 Run the SAS Deployment Wizard in configure mode on the server-tier machine, and then on the middle-tier machine.

After the SAS Deployment Wizard installation and configuration process has completed successfully, a series of post-installation tasks must be performed before the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server can be launched without error.
Run the SAS Deployment Wizard

Run the SAS Deployment Wizard in Install Mode ........................................ 40

Run the SAS Deployment Wizard in Configure Mode ............................ 42
  Start the SAS Deployment Wizard in Configure Mode ....................... 42
  Indicate Preference for Anonymous Web Access ............................... 43
  Configure the SAS Financial Crimes Monitor ................................. 43
  Configure the SAS Social Network Analysis Server ......................... 48

Recover from JBoss Configuration Failure Message .......................... 53
Run the SAS Deployment Wizard in Install Mode

As described in the previous section, it is important to run the SAS Deployment Wizard in install mode, and to specifically disable the configure mode. The following figure shows the wizard with only the install mode enabled.

Display 6.1  SAS Deployment Wizard: Install SAS Software

**Note:** During the installation process, when given the choice of either a custom or a typical installation, if you are performing a multiple-machine deployment, then you must select **Custom** (as opposed to **Typical**) to be presented with the appropriate multiple-deployment options during the process.
After you have completed the installation procedure, you can launch the SAS Deployment Wizard and enter the configure mode to configure the software. This process is detailed in the following section.
Run the SAS Deployment Wizard in Configure Mode

Start the SAS Deployment Wizard in Configure Mode

The following figure shows the wizard with only the configure mode enabled.

Display 6.3  SAS Deployment Wizard: Configure SAS Software

The following sections describe the wizard pages that are used for configuring the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server during the configuration process of the SAS Deployment Wizard.
Indicate Preference for Anonymous Web Access

The SAS Deployment Wizard offers an option to enable anonymous web access. The consequence of enabling this option is that the web services and stored processes that are used in the SAS Social Network Analysis Server and the SAS Financial Crimes Monitor will not require authenticated credentials to be used. If this option is not selected, then all requests for the web services and stored processes require credentials. This second option results in a more secure deployment.

Display 6.4  Anonymous Web Access

The SAS Financial Crimes Monitor and the SAS Social Network Analysis Server do not require anonymous web access, so unless some other SAS software is deployed on the machine and requires it, do not enable this option.

Configure the SAS Financial Crimes Monitor

Within the SAS Deployment Wizard, you are asked a series of questions regarding the database required by the SAS Financial Crimes Monitor. Complete the following instructions.

1. Select the server database product from the Database Type list.
Click **Next** to continue.

The SAS Financial Crimes Monitor Server Database Properties page is displayed, with default values.

2 At the SAS Financial Crimes Monitor Server Database Properties page, enter the appropriate values or accept the default values.

**Note:** For Oracle servers, the entry in the **Database Name** field corresponds to the System ID (SID).
**Display 6.6  Database Properties Specific to MySQL Selection**

**Note:** The fields displayed on this page are specific to the server database type selected on the previous page. So, for example, selecting Oracle as the server database type would present a new field, **Schema Name**, on the page.

Click **Next** to continue.

The SAS Financial Crimes Monitor Server Database Connection Properties page is displayed, showing the default value for the **Database Authentication Domain** field.
3 At the SAS Financial Crimes Monitor Server Database Connection Properties page, either accept the default value or enter a new value in the Database Authentication Domain field.

**Display 6.7  Database Authentication Domain**

Click **Next** to continue.

The SAS Financial Crimes Monitor Mid-Tier page is displayed.

4 At the SAS Financial Crimes Monitor Mid-Tier page, indicate the location of the JDBC driver JAR files necessary to access your database server.

When you provide the directory that contains the JDBC driver JAR files, you need to browse to the directory that contains the JAR file. You do not need to select the JAR file, and the JAR filename does not appear in the text field on the wizard page.

**Note:** Make sure that the directory contains only the JAR file that is appropriate for the JDK version that is used by the web application server. For more information about the JDBC driver JAR files, see “Ensure Proper DB Client and JDBC Driver Setup” on page 33.
After indicating the directory containing the JAR file, click **Next** to continue.

The SAS Financial Crimes Monitor Mid-Tier Database User page is displayed, with the **User ID** field populated with a default value.

5 At the SAS Financial Crimes Monitor Mid-Tier Database User page, specify the user information for the database connection and then click **Next** to continue.
This is the final page for the SAS Financial Crimes Monitor and, after clicking Next, the initial page for configuring the SAS Social Network Analysis Server is displayed.

**Configure the SAS Social Network Analysis Server**

Within the SAS Deployment Wizard, you are asked a series of questions regarding the JDBC database connection information required by the Social Network Analysis middle tier. Complete the following instructions:

1. Select the database product from the **Database Type** list.
Display 6.10  Database Type

Click **Next**.

The SAS Social Network Database JDBC Properties page is displayed, with default values populating several fields.

2 Enter appropriate values or ensure that the default values are correct. Indicate the directory that contains the JDBC driver JAR files for the database.

**Note:** For Oracle servers, the entry in the **Database Name** field corresponds to the System ID (SID).
**Display 6.11  JDBC Properties (Specific to MySQL Selection)**

![Image of the SAS Deployment Wizard with JDBC Properties page]

**Note:** The fields displayed on this page are specific to the server database type selected on the previous page. So, for example, selecting *Oracle* as the server database type would present a new field, *Schema Name*, on the page.

When you provide the directory that contains the JDBC driver JAR files, you need to browse to the directory that contains the JAR file. You do not need to select the JAR file, and the JAR filename does not appear in the text field on the wizard page. Also, make sure that the directory contains only the JAR file that is appropriate for the JDK version that is used by the web application server. For more information about the
JDBC driver JAR files, see “Ensure Proper DB Client and JDBC Driver Setup” on page 33.

Click Next.

The SAS Social Network Analysis Mid-Tier Database User page is displayed, with the User ID field populated with a default value.

3 Specify the user information for the JDBC connection and then click Next to continue.

Note: Depending on your database selection, a default user ID might be displayed. If the default user ID is displayed, accept this user ID.

**Display 6.12 JDBC Database User**

![SAS Deployment Wizard](image)

This is the final page for the SAS Social Network Analysis middle tier.

At this point in the process, follow the instructions in the appropriate operating system-specific SAS 9.3 Foundation guide. See “Meet Pre-Installation Requirements for SAS 9.3” on page 17 for links to operation-specific documentation resources.

4 At the end of the prompting phase of the SAS Deployment Wizard configuration process, the Deployment Summary page is displayed.
Click **Start** to begin the actual configuration process.

The configuration process begins with indicators displayed to show the progress of the configuration.

**Note:** If you have indicated use of JBoss AS (Community) 4.2.3 or JBoss EAP 4.3.0 through 4.3.0 CP07 for the SAS Financial Crimes Monitor, then the configuration process is interrupted and you are presented with a Configuration Failure error. If this occurs, follow the instructions in “Recover from JBoss Configuration Failure Message” on page 53 to complete the SAS Deployment Wizard configuration process.

**CAUTION!** For an initial installation, complete the post-installation procedures for the solution. Before you can launch the SAS Financial Crimes Monitor or the SAS Social Network Analysis Server without error or issues, you must complete the post-installation instructions for each application. Failure to do so will yield unpredictable results.
Recover from JBoss Configuration Failure Message

At the end of the prompting phase of the SAS Deployment Wizard configuration process, you will click **Start** to begin the actual configuration process. If you have indicated use of JBoss AS (Community) 4.2.3 or JBoss EAP 4.3.0 through 4.3.0 CP07 for the SAS Financial Crimes Monitor, then you will be presented with a Configuration Failure message.

The following figure shows the Configuration Failure message displayed during the SAS Deployment Wizard configuration phase of the Installation and Configuration process.

**Display 6.14  SAS Deployment Wizard: Configuration Failure Message**

You will have to modify a specific directory to remove several files before the SAS Deployment Wizard can complete the configuration process successfully.

**Note:** These file deletions are not needed for JBoss EAP 4.3.0 CP08 (and later) Cumulative Patch releases.

1. For the installations including the JBoss Application Server versions mentioned previously, when the Configuration Failure error is displayed during the SAS Deployment Wizard configuration process, navigate to the following directory.
2 Delete the following files:
   - ejb3-persistence.jar
   - hibernate-annotations.jar
   - hibernate-commons-annotations.jar
   - hibernate-validator.jar
   - hibernate3.jar

3 Navigate to the following directory.
   `<JBOSS_HOME>/server/SASServer8/deploy_sas/sas.socialnetworkanalysis2.3.ear/sas.sso.snaserver.war/WEB-INF/lib/`

4 Delete the following files:
   - ejb3-persistence.jar
   - hibernate-annotations.jar
   - hibernate-commons-annotations.jar
   - hibernate-validator.jar
   - hibernate3.jar

5 At the Configuration Failure message, click **Retry** to continue with the SAS Deployment Wizard configuration procedure.
Part 4

Post-Installation Tasks

Chapter 7
Perfom Post-Installation Steps for SAS 9.3 .......................... 57

Chapter 8
Perfom Post-Installation Steps for Databases ..................... 59

Chapter 9
Perfom Post-Installation Steps for SAS
Financial Crimes Monitor ................................................. 65

Chapter 10
Perfom Post-Installation Steps for SAS
Social Network Analysis Server ........................................ 71
Perform Post-Installation Steps for SAS 9.3

Perform Post-Installation Configuration for SAS 9.3

Table 7.1  SAS 9.3 Configuration References

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Document</th>
<th>URL</th>
</tr>
</thead>
</table>
Post-Installation Database Setup Overview

This chapter describes the process for creating tables to allow the proper operation of the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server. During installation and configuration, database schemas and database users were defined. These databases and users must be created. If necessary, work with the Database Administrator to ensure that these tasks have been completed. See “Create Database Users” on page 31 for the permissions that must be granted to the SAS Social Network Analysis Server database user role. This user requires access to several of the SAS Financial Crimes Monitor tables to be able to manage and triage alerts.

To continue with the table creation procedure in the following section, make sure you have the following information:
SAS Financial Crimes Monitor Database User (FINCRMDB by default) account details

SAS Social Network Analysis Server Database User (SNAUSER by default) account details

SAS Financial Crimes Monitor Schema (FINCRMDB by default) details, if necessary

SAS Social Network Analysis Server Schema (SASSNADS by default) details, if necessary

Database details

---

Create Database Tables

**SAS Financial Crimes Monitor Tables and Sequences**

SAS provides a set of scripts, based on database type, to create the tables and sequences required by SAS Financial Crimes Monitor.

When performing an initial installation (not an upgrade), run the appropriate script for the database used at your site.

<table>
<thead>
<tr>
<th>Database Type</th>
<th>Create Table Scripts</th>
<th>Drop Table Scripts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>fcm_ddl_oracle.sql</td>
<td>fcm_drop_scripts_oracle.sql</td>
</tr>
<tr>
<td>MySQL</td>
<td>fcm_ddl_mysql.sql</td>
<td>fcm_drop_scripts_mysql.sql</td>
</tr>
<tr>
<td>IBM DB2</td>
<td>fcm_ddl_db2.sql</td>
<td>fcm_drop_scripts_db2.sql</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>fcm_ddl_ms_sql.sql</td>
<td>fcm_drop_scripts_ms_sql.sql</td>
</tr>
</tbody>
</table>

These database scripts are available for each supported database in the following location:
Windows:

SAS-install-dir\fincrmmva\sasmisc\dbmc\ddl\fcm

UNIX:

SAS-install-dir/misc/fincrmmva/dbmc/ddl/fcm

Note: Executing the fcm_ddl_*.sql script creates the needed tables, including the alert_summary template table. Additional information about the alert_summary template table can be found in the SAS Social Network Analysis Server: Administration Guide.

Additional Step: Specify Database Name

An additional step must be performed in order for drop table operations to work properly. Open drop_objects_trans_db2.sql, specify the name of your database, and save this change. The drop_objects_trans_db2.sql file resides in /
SAS-installation_directory/SASFoundation/9.3/misc/snamva/dbmsc/ddl/.

In the following line, replace DATABASENAME with the name of your database:

set @database = 'DATABASENAME' /*Enter database name*/

For example:

set @database = 'myDBname' /*Enter database name*/

Additional Step for AIX Sites

For sites that run DB2 on AIX, an additional step must be performed in order for drop table operations to work properly. Open fcm_drop_scripts_db2.sql, uncomment the AIX-specific statements, comment the previously uncommented DROP statements, and save these changes. The fcm_drop_scripts_db2.sql file resides in /
SAS-installation_directory/SASFoundation/9.3/misc/snafcm/dbmsc/ddl/.

Comment the lines that begin and end with these DROP and GO statements:

DROP TABLE SNA_TABLE_METADATA;
GO
DROP TABLE SNA_COLORMODEL;
GO

Comment this series of statements by inserting comment tags /* and */. For example:

/*DROP TABLE SNA_TABLE_METADATA;
GO
.
.
DROP TABLE SNA_COLORMODEL;
GO*/

Uncomment the lines starting and ending with these DROP statements:

/********** AIX Format ******************/
/*
ALTER TABLE SNA_COLUMN_DISPLAY
.
.
DROP TABLE SNA_CONTEXT_PREFERENCE;
*/

Uncomment this series of statements by removing the lines containing only /* and */. For example:

/********** AIX Format ******************/
ALTER TABLE SNA_COLUMN_DISPLAY
.
.
DROP TABLE SNA_CONTEXT_PREFERENCE;

SAS Social Network Analysis Server Tables and Sequences

SAS provides a set of scripts, based on database type, to create the tables and sequences required by SAS Social Network Analysis Server.

When performing an initial installation (not an upgrade), run the appropriate script for the database used at your site.
<table>
<thead>
<tr>
<th>Database Type</th>
<th>Create Table Script</th>
<th>Drop Table Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td><code>create_table_trans_orcl.sql</code></td>
<td><code>drop_objects_trans_orcl.sql</code></td>
</tr>
<tr>
<td>MySQL</td>
<td><code>create_table_trans_mysql.sql</code></td>
<td><code>drop_objects_trans_mysql.sql</code></td>
</tr>
<tr>
<td>IBM DB2</td>
<td><code>create_table_trans_db2.sql</code></td>
<td><code>drop_objects_trans_db2.sql</code></td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td><code>create_table_trans_sqlserver.sql</code></td>
<td><code>drop_objects_trans_sqlserver.sql</code></td>
</tr>
</tbody>
</table>

These database scripts are available for each supported database in the following location:

- **Windows:**
  
  `$SAS-install-dir\snamva\sasmisc\dbmc\ddl\fcm`

- **UNIX:**
  
  `$SAS-install-dir/misc/snamva/dbmc/ddl/fcm`

### Additional Resources

Within the directories containing the scripts for the SAS Financial Crimes Monitor, you will also find the following comprehensive database documentation:

- Data dictionary for the SAS Financial Crimes Monitor database
  
  `SAS_Financial_Crimes_Monitor_DataDictionary.rtf`

- Data model for the SAS Financial Crimes Monitor database:
  
  `SAS_Financial_Crimes_Monitor_DataModel.pdf`
Perform Post-Installation Steps for SAS Financial Crimes Monitor

**Post-Installation Procedure for the SAS Financial Crimes Monitor**

- Confirm That the LIBNAME Statement Is Correct
- Configure LIBNAME for Parallel Processing

**Initialize Users and Groups**

- Metadata Group Naming Convention
- Assign Groups to the SAS Financial Crimes Monitor:Admin Role

---

**Post-Installation Procedure for the SAS Financial Crimes Monitor**

At the successful completion of the SAS Deployment Wizard installation and configuration procedures, the application is installed, the default Administrator role is created, and the application server context (either SASApp by default or a user-assigned name), is created. At this point, it is not possible to successfully log on to the SAS Financial Crimes Monitor without performing the procedure described in the following section.
Confirm That the LIBNAME Statement Is Correct

During installation and configuration, you are prompted to accept default values or, in some cases, to specify unique values for your deployment. The entries added to the SAS Deployment Wizard are used to create a LIBNAME statement that is written to the SAS autoexec.sas file. Before you can access the SAS Financial Crimes Monitor, you must confirm that the LIBNAME statement written to the SAS autoexec.sas file is correct. If the LIBNAME statement is incorrect, you must edit the statement to ensure that it is accurate. If this statement is not correct, then the SAS Financial Crimes Monitor will be unable to connect to the database and users will be unable to create projects.

The autoexec.sas file is located in the following directory: `SAS-Configuration-directory/Lev1/Applications/SASFinancialCrimesMonitor3.1/

To confirm or modify the LIBNAME specification:

1. Locate the autoexec.sas file in the appropriate directory listed above.
2. Open the autoexec.sas file using SAS 9.3.
3. Locate the LIBNAME specification line that is preceded by the following comment:
   
   /* FCM model tables */

   **Note:** The line written to the file is consistent with the database type that was installed and configured. The following example shows a sample for a MySQL database installation and configuration.
Display 9.1  Example of the LIBNAME Entry in the SAS autoexec.sas File

4  Ensure that the LIBNAME statement is written correctly and that the values specified are accurate for your deployment.

5  If you modified the file, make sure that you save it before closing the file and exiting SAS 9.3.

**Configure LIBNAME for Parallel Processing**

For SAS Financial Crimes Monitor to perform parallel processing, the following options must be added onto the SAS Financial Crimes Monitor LIBNAME statement in autoexec.sas:

- **MySQL:**
  
  ```
  libname fcm MYSQL database=XXXX authdomain=XXXX port=XXXX reread_expansion=yes;
  ```

- **Oracle:**
  
  ```
  libname fcm ORACLE path=XXXX authdomain=XXXX schema=XXXX reread_expansion=yes read_lock_type=row update_lock_type=row connection=unique;
  ```

- **DB2:**
  
  ```
  libname fcm DB2 DSN=XXXX authdomain=XXXX schema=XXXX reread_expansion=yes read_lock_type=row update_lock_type=row connection=unique;
  ```
Initialize Users and Groups

Administrators use the SAS Financial Crimes monitor to manage projects and scenarios. Investigators use the SAS Social Network Analysis Server to triage and manage alerts. Access to the SAS Social Network Analysis Server and to the SAS Financial Crimes Monitor is controlled by SAS metadata permissions on metadata folders.

Metadata Group Naming Convention

SAS metadata group names must begin with FCM for SAS to display them for routing scenarios (for example, 'FCM DB Auth').

Assign Groups to the SAS Financial Crimes Monitor:Admin Role

At the completion of the installation process, SAS Financial Crimes Monitor is installed with a default role named Financial Crimes Monitor:Admin added to metadata. This is a universal role without limitations to tasks that can be performed. Only groups (or users) assigned to this role are able to access the SAS Financial Crimes Monitor and perform tasks.

Note: Initializing users and groups as described in the following procedure allows the users to log on to the SAS Financial Crimes Monitor. The users will be unable to create projects or to execute jobs until the setup procedure, as described in Chapter 11, “Set Up the SAS Financial Crimes Monitor,” on page 103, is completed.
1 Use the User Manager plug-in to SAS Management Console to create a group that will be assigned membership to the SAS Financial Crimes Monitor:Admin role.

This group needs to be assigned the Financial Crimes Monitor:Admin role so that administrators have Read and Write access to the database used by the SAS Financial Crimes Monitor.

2 At the User Manager plug-in, select the group that you created, right-click and select Properties.

3 Select the **Groups and Roles** tab, and assign this group to the Financial Crimes Monitor:Admin role.

If additional groups are needed, create the groups and add them to the role as well. Only group members and users with assignment to this role will be granted access to the SAS Financial Crimes Monitor.

At the completion of the entire installation procedure, you can now log on to the SAS Financial Crimes Monitor, generally by accessing a URL that is similar to the following examples:

<table>
<thead>
<tr>
<th>Application Server</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>JBoss Application Server</td>
<td><a href="http://hostname.example.com:8780/SASFINCRM">http://hostname.example.com:8780/SASFINCRM</a></td>
</tr>
<tr>
<td>Oracle WebLogic Server</td>
<td><a href="http://hostname.example.com:7801/SASFINCRM">http://hostname.example.com:7801/SASFINCRM</a></td>
</tr>
<tr>
<td>IBM WebSphere Application Server</td>
<td><a href="http://hostname.example.com:9087/SASFINCRM">http://hostname.example.com:9087/SASFINCRM</a></td>
</tr>
</tbody>
</table>

See “Installation, Configuration, and Post-Installation Results” on page 11 for a description of what to expect upon logging on to the solution for the first time.
Perform Post-Installation Steps for SAS Social Network Analysis Server

Purpose of Post-Installation Procedures for the SAS Social Network Analysis Server .................................................. 72

Import SAS Stored Processes and Deploy Web Services .............. 73
  Overview .................................................................................. 73
  Import SAS Stored Processes from a SAS Package .................. 73
  Deploy the Imported SAS Stored Processes as a Web Service .......................................................... 76

Initialize Users and Groups ......................................................... 79
  Add an Investigator Group and Investigators ........................... 80

Sample Integration Between SAS Financial Crimes Monitor and SAS Social Network Analysis ..................... 82
  Overview .................................................................................. 82
  Prepare Your Environment ........................................................ 82
  Run metadata_script.sas ............................................................ 85
  Import Sample Data ................................................................. 90
  Generate Alerts .................................................................... 91
  Using Data Sets Instead of a Database ..................................... 92
  Import SAS Stored Processes from a SAS Package ................. 93
  Deploy the Imported SAS Stored Processes as a Web Service .......................................................... 96
  Set Up Advanced Search and Disposition Files ....................... 99
  Considerations for SAS Enterprise Case Management ............. 100
Purpose of Post-Installation Procedures for the SAS Social Network Analysis Server

The SAS Social Network Analysis Server is a customizable offering included within the SAS Fraud Framework solution. Administrators and analysts work together to create an environment consistent with the needs of the business user.

The procedures outlined in the following sections include setting up the SAS Social Network Analysis Server with sample content provided by SAS. Instructions are also provided to enable you to define users and groups that will be created to access the sample content.

The users and groups defined in this chapter are created specifically to perform the following actions:

- access the provided sample content
- log on to the SAS Social Network Analysis Server

In practice, however, the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server are designed to work together and, for certain operations, share the FCM schema, as outlined in “Sample Integration Between SAS Financial Crimes Monitor and SAS Social Network Analysis” on page 82. To use the offerings in conjunction with one another, you must follow the guidance provided in the SAS Social Network Analysis Server: Administration Guide. The information in this chapter is provided as a way of demonstrating the success of the installation of the SAS Social Network Analysis Server. It is not intended as a procedure to allow full user access (of both offerings) or full use of the SAS Social Network Analysis Server.

The following figure shows the stand-alone operation of the SAS Social Network Analysis Server as configured for the purpose of validating the installation.
As shown in the preceding image, the installation and configuration procedure does not include integration with the SAS Financial Crimes Monitor. The following procedures are described in this chapter.

- importing SAS Stored Processes from a SAS package
- deploying the imported SAS Stored Process as a web service
- initializing users and groups

## Import SAS Stored Processes and Deploy Web Services

### Overview

The SAS Social Network Analysis Server shows alerts that are generated by the alert generation process. For alert viewing, SAS Stored Processes are deployed as web services, and the SAS Social Network Analysis Server displays the alerts that are read by the SAS Stored Processes.

### Import SAS Stored Processes from a SAS Package

SAS provides template SAS Stored Process metadata in a SAS package file. To import a template SAS package, perform the following steps:
1. Using SAS Management Console, select the **Folders** tab and navigate to `/System/Applications/SAS Social Network Analysis/Social Network Analysis 3.1`

2. Right-click the **Social Network Analysis 3.1** folder and select **Import SAS Package**.

   **Display 10.1 Import SAS Package**

3. Select the **Browse** button and navigate to the location of the template SAS package file:

   **UNIX Specifics:** `!SASROOT/misc/snamva/Template.spk`
   **Windows Specifics:** `!SASROOT\snamva\sasmisc\Template.spk`

   a. Ensure that the **Include access controls** check box is **not** selected.
   b. Select **Next**.
4 At the Select Objects to Import page, make sure each stored process is selected.

**Display 10.2 Import SAS Package: Select Objects to Import**

Click **Next** to continue.

**Note:** You might be presented with an Import Warning dialog box that displays a caution message regarding not importing entries and associations related to access control entries (ACEs) or an access control template (ACT). Click **Yes** to continue. Your installation will continue without an error related to this warning.

**Display 10.3 Template Warning Dialog Box That Might Appear during SAS Package (SPK) File Import**

5 Select **Next** on the About Metadata Connections page.

6 Select **SASApp** as the target application server on the SAS Application Servers page, and then click **Next**.

7 Select **Add** on the Source Code Repositories page, and provide the directory name:

UNIX Specifics: `<SASHome>/SASFoundation/9.3/sasstp/snامva`

Windows Specifics: `<SASHome>\SASFoundation\9.3\snамva\sasstp`
8 Use the **Target** menu to select the directory that was just added, and then click **Next**.

9 Review the Summary page, and then click **Next**.

10 Confirm that the import process completed successfully, and then click **Finish**.

11 After you have imported the Template.spk file, you have to manually add the message parameter as a property to processAlertResponse.

   a In the **Folders** tab of SAS Management Console, locate **Template** and the **processAlertResponse** stored process.

   b Right-click on **processAlertResponse** and select **Properties**.

   c In the Properties dialog box, select the **Parameters** tab.

   d In the **Output Parameters** list box, click **New**.

   e In the New Output Parameters dialog box, enter **Message** in the **Name** field and **String** in the **Type** field, and click **OK**.

### Deploy the Imported SAS Stored Processes
as a Web Service

After the SAS package file is imported, metadata is associated with the SAS program code for the stored processes in the SAS installation directory. The code for the stored processes can be modified at any time to configure the display of alerts and social networks on the investigator user interface. However, they are deployed as a web service now, even though the SAS program code can be customized later. To deploy these stored processes as a web service, follow these steps:

1 Use the **Folders** tab of SAS Management Console to navigate to the folder that was just imported to the */System/Applications/SAS Social Network Analysis/Social Network Analysis 3.1* folder.
2 Select the Template folder, unless it has been renamed. If the folder has been renamed, select the renamed folder. The stored process icons appear in the right pane.

3 Deploy the alerts-related web service. Hold down the CTRL key and click to select the following stored process icons:

- `getActionableEntities`
- `getChartSeries`
- `getAlertTransactions`
- `getSubAlerts`
- `processAlertResponse`

4 Right-click one of the selected icons and select **Deploy As Web Service**. The Deploy As Web Service wizard starts.

5 On the Web Service Information page, confirm or set the following values:

- Select the default value for **Web Service Maker URL** from the menu.
- Make sure that **New Web Service Name** is set to the value of `TemplateAlerts`. However, if the folder was renamed to a value such as `Healthcare`, then the **New Web Service Name** must be `HealthcareAlerts`.

  **Note:** The web service name is case sensitive. That is, if the Template folder was renamed Healthcare, then the new web service name must be HealthcareAlerts. However, if the Template folder was renamed healthcare, then the new web service name must be healthcareAlerts.

- The choice of credentials to use does not matter.

  Click **Next**.

6 On the Web Service Keywords and Namespace page, provide the following value for the **Namespace** field:

  `http://sas.com/sso/fraud/alerts`
Click **Next**.

7 Confirm the settings and then click **Finish**.

8 Deploy the social network-related web service using a method that is similar to deploying the alerts-related web service. Hold down the CTRL key and click to select the following stored process icons:

- `getSocialNetwork`
- `getSocialNetworkNodeDetails`
- `growSocialNetworkNode`

9 Right-click one of the selected icons and select **Deploy As Web Service**.

   The Deploy As Web Service Wizard starts.

10 On the Web Service Information page, confirm or set the following values:

   - Use the default value for **Web Service Maker URL**.
   - Make sure that **New Web Service Name** is set to the value of `TemplateSocialNetworkAnalysis`. However, if the folder was renamed to a value such as `Healthcare`, then the **New Web Service Name** must be `HealthcareSocialNetworkAnalysis`.

   **Note:** The web service name is case sensitive. That is, if the Template folder was renamed `Healthcare`, then the new web service name must be `HealthcareSocialNetworkAnalysis`. However, if the Template folder was renamed `healthcare`, then the new web service name must be `healthcareSocialNetworkAnalysis`.

   - The choice of credentials to use does not matter.

   Click **Next**.

11 On the Web Service Keywords and Namespace page, provide the following value for the Namespace field:

   `http://sas.com/sso/fraud/sna`

   Click **Next**.
12 Confirm the settings and then click **Finish**.

If the deployment completes successfully, two new web services (*TemplateAlerts* and *TemplateSocialNetworkAnalysis*) are deployed. You can confirm successful deployment by reviewing the entries under the Configuration Manager within SAS Application Infrastructure at the BI Webservices for Java 9.3 node.

**Display 10.4  SAS Management Console Showing Successful Deployment of Services**

---

**Initialize Users and Groups**

Investigators use the SAS Social Network Analysis Server to review, triage, or manage alerts. Administrators use the SAS Financial Crimes monitor to manage projects and scenarios. Access to the SAS Financial Crimes Monitor and to the SAS Social Network Analysis Server is controlled by SAS metadata permissions on metadata folders.
Add an Investigator Group and Investigators

Investigators access the SAS Social Network Analysis Server to view alerts. Access to the SAS Social Network Analysis Server is controlled with explicit ReadMetadata permission on a metadata folder. A metadata folder is created when a SAS package file (SPK file) is imported into metadata (or metadata folders can be created through the SAS Management Console for each analytic domain). The metadata folder contains metadata for the SAS Stored Processes that read the alerts generated by the alert generation process and display them through the SAS Social Network Analysis Server. Users can be added and removed from an investigator group at any time.

**Note:** Creation of the Investigator Group and the addition of investigator users enables the defined groups and investigators to log on to the SAS Social Network Analysis Server within the permissioned analytic domain. Perform this procedure to complete the installation and log on to the SAS Social Network Analysis Server. This enables you to verify successful installation and configuration. The logged-on user will not be able to perform alert disposition tasks. Rely on the information in Chapter 12, “Set Up the SAS Social Network Analysis Server,” on page 131 to set up and define true solution users.

1 Use the User Manager plug-in to SAS Management Console to create a group for the investigators. The group can be named according to the type of activity that the group investigates, or perhaps by geographical location. For example, you might create a group named SNA Investigators.

2 Click the **Folders** tab and navigate to `/System/Applications/SAS Social Network Analysis/Social Network Analysis 3.1/Template`. If the folder was renamed when the Template.spk file was imported, then the folder name will be different.

3 Right-click the folder icon and select **Properties**.

4 Select the **Authorization** tab and click **Add**.

   The Add Users and Groups dialog box appears.

5 Select the group name, such as **SNA Investigators**, from the list, select the right-arrow icon, and click **OK**. The Add Users and Groups dialog box closes.
6. Select the group that you just added to the **Users and Groups** list.

7. In the **Effective Permissions** area, confirm that the **ReadMetadata** permission is set to **Grant** and click **OK**.

8. Select the **Plug-ins** tab and use the User Manager plug-in to add investigative users. As each user is added, use the **Groups and Roles** tab to make the user a member of the investigative group.

Investigative users can belong to more than one investigative group. For example, an investigator can be a member of a group that investigates check fraud and a member of a group that investigates wire fraud. However, when creating and assigning groups, do not nest groups because this is might result in unpredictable results.

At the completion of the entire installation procedure, you can log on to the SAS Social Network Analysis Server (but you will not be able to disposition alerts). You log on by accessing a URL that is similar to the following examples:

<table>
<thead>
<tr>
<th>Application Server</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>JBoss Application Server</td>
<td><a href="http://hostname.example.com:8780/SASSNA">http://hostname.example.com:8780/SASSNA</a></td>
</tr>
<tr>
<td>Oracle WebLogic Server</td>
<td><a href="http://hostname.example.com:7801/SASSNA">http://hostname.example.com:7801/SASSNA</a></td>
</tr>
<tr>
<td>IBM WebSphere Application Server</td>
<td><a href="http://hostname.example.com:9087/SASSNA">http://hostname.example.com:9087/SASSNA</a></td>
</tr>
</tbody>
</table>

See “Installation, Configuration, and Post-Installation Results” on page 11 for a description of what to expect upon logging in to the solution for the first time.
Sample Integration Between SAS Financial Crimes Monitor and SAS Social Network Analysis

Overview

This is a link “Create Database Tables” on page 60. SAS enables you to validate your SNA and FCM deployments with the sample.spk package. This package consists of several SAS stored processes that contain logic to process alerts generated with SAS Financial Crimes Monitor and display them in SAS Social Network Analysis.

Implementing the sample.spk package is an alternative to implementing template.spk described earlier in “Import SAS Stored Processes and Deploy Web Services” on page 73. In the case of sample.spk, you are able to validate both your FCM and SNA deployments.

Prepare Your Environment

Overview of Prepare Your Environment

Preparing your environment, consists of the following steps:

1. Back up your metadata.
2. Set your environment variables.
3. Create required operating system users.
4. Encode the password for the users.

Backup Your Metadata

Before creating your new metadata, please backup your current metadata using SAS Management Console. For more information, refer to Instructions.html that reside in SAS-configuration-directory/Levn/Documents.
Set Your Environment Variables

Before beginning the execution of the metadata script, you must set your $PATH and SASCONFIG environment variables. Confirm that both these environment variables are properly set.

First, set your $PATH environment variable to have the MakeFolder command located in your !sasroot/SASHome/SASPlatformObjectFramework/9.3 directory available.

For example, to update your $PATH variable on a LINUX machine, execute this command: `export PATH=$PATH:/SASHome/SASPlatformObjectFramework/9.3`

**TIP** You can add your SAS execution location to the PATH variable so that it can be used by FCMMain.sas.

Test your command by entering: `MakeFolder`.

(Executing MakeFolder enables you to see the different options available for MakeFolder.)

If your SASCONFIG environment variable does not already exist on your system, create it.

For example, create a SASCONFIG environment variable on a LINUX machine by executing the following command: `export SASCONFIG=SAS-configuration-directory/Lev`.n

Test SASCONFIG by entering: `echo $SASCONFIG` (on UNIX) and `echo %SASCONFIG%` (on Windows). Executing this command should display the path that you entered on your export command.

Create Six Operating System User Accounts

The metadata_script.sas script that you will eventually run, requires that the following six user accounts be defined on your operating system:

- fcmuser1
- fcmuser2
If these user accounts are not present, create them, assigning the same password for all six accounts. For more information, refer to the documentation for your respective operating system.

**Note:** Add fcmuser1 to the FCM DB Auth Group.

### Encrypt User Passwords with SAS

The metadata_script.sas script requires that the password for all six user accounts (referenced in “Create Six Operating System User Accounts” on page 83), be encrypted with PROC PWENCODE. Use the following code to encrypt your password to a text file in your sample library.

**Note:** The code sample that follows uses a Windows path.

```sas
%let SASCONFIG=%sysget(SASCONFIG);
%let samplib=&SASCONFIG\Applications\SASFinancialCrimesMonitor3.1\sample ;
%let _user=;
%let _pass= ;
data _null_; call symput("password_file",compress("&samplib/%lowcase(&_USER).txt") ); run;
filename pw "&password_file";
proc pwencode in="&_pass" out=pw; run;
quit;
```

Define fcmuser1 to your `%let _user=;` statement.

Provide a password for the `%let _pass=;` statement. After running the code, secure this file according to the security policies defined for your site. metadata_script.sas reads your password information from this text file. Your SASCONFIG environment variable should be defined to the proper install location. (See “Set Your Environment Variables” on page 83 for more information.)
Repeat this encoding procedure for your database user account password. Create a second file using the SAS code listed earlier with the necessary specifics for your database user account.

Each password file in your sample library is prepended with your username.

**Run metadata_script.sas**

**Overview of Running metadata_script.sas**

The metadata_script.sas file includes four scripts to create all the required metadata for your SAS Financial Crimes Monitor and SAS Social Network Analysis integration:

```sas
%include samplib(load_users_groups_roles);
%include samplib(make_folder);
%include samplib(make_library);
%include samplib(register_tables);
```

You must set some script macro variables first, and then you run each individual script in the order listed above. After you validate the script, you run the next script:

1. Set macro variables.
2. Run `load_users_groups_roles` and validate.
3. Run `make_folder` and validate.
4. Run `make_library` and validate.
5. Run `register_tables` and validate.

**Set Macro Variables**

Start a SAS Session, and include the metadata_script.sas file.

**Note:** If you are running on Microsoft Windows, you must update the macro variable `WindowsDomain` in the metadata_script program. This is used to prepend your Windows domain (or machine name) to your defined operating system users.

For all platforms, set the following macro variables:

```sas
%let metaserver = ;
%let metapass = ;
```
Enter the following for each macro variable:

metaserver
   Enter a fully qualified machine name for your metadata server.

metapass
   Enter the password for your metadata user.

FCMDBUser
   Do not change this value unless you specified a non-default value during installation. (The database user contains the default configuration value of FINCRMDB.)

DBPasswd
   Enter the SAS encoded password that you created earlier for the six user accounts.

fcmDBAuth
   Do not change this value unless you specified a non-default value during the product configuration. (fcmDBAuth contains the default value of the installation.)

Run load_users_groups_roles Script
The load_users_groups_roles script creates six metadata users, two groups, and assigns various metadata roles. To run load_users_groups_roles, follow these steps:

1. Comment out all %include lines in metadata_script.sas except, %include(load_users_groups_roles);.

2. Execute metadata_script.sas either through interactive or batch SAS.

3. Check there are no errors in your SAS log.

4. Start a SAS Management Console using your sasadm@saspw profile, and verify that there are three fcmusers and three snausers present.

5. Right-click the first user and select Properties ➤ Accounts to verify there is a user login.

6. If you are on Microsoft Windows:
Validate that the login contains a prepended domain (or machine name).

Validate there are two FCM groups that were created: FCM DB Auth Group and FCM Default Group.

Open the properties of the FCM DB Auth Group and verify the database user ID login is specified along with its password under the **Accounts** tab.

Open the properties of the Financial Crimes Monitor: Admin Role, and validate that both FCM groups are members under the **Members** tab.

Verify that the one SNA group called SAS Investigator was created.

Open the properties of the Social Network Analysis Report: Viewer Role, and under the **Members** tab, verify that snauser3 is present.

**Run make_folder Script**

The make_folder script creates four metadata folders. To run make_folder, follow these steps:

1. Comment out all `%include` lines in `metadata_script.sas` except, `%include samplib(make_folder);`.

2. Execute `metadata_script.sas` either through interactive or batch SAS.

3. Check there are no errors in your SAS log.

4. Start a SAS Management Console using your sasadm@saspw profile, and select the **Folders** tab.

   This script creates a **Financial Crimes Monitor** folder beneath the **Shared Data** tree.

5. Open the properties of the **Financial Crimes Monitor** folder. On the **Authorization** tab verify that ReadMetadata, WriteMetadata, WriteMemberMetadata, and Read permissions are granted.
6 Expand the Financial Crimes Monitor Folder to display four folders created for FCM consumption: FCM Alert Template, FCM Scenario Library, FCM Prep Data, FCM Enrichment.

These subfolders inherit the permissions from the Financial Crimes Monitor parent folder.

Run make_library script

The make_library script creates four libraries with their appropriate SAS librefs, paths, and locations. To run make_library, follow these steps:

1 Comment out all %include lines in metadata_script.sas except, %include samplib(make_library);

2 Execute metadata_script.sas either through interactive or batch SAS.

3 Check there are no errors in your SAS log.

4 Start a SAS Management Console using your sasadm@saspw profile, and select the Plug-ins tab.

5 Expand your Data Library Manager tree. Underneath the Libraries directory, you should find four libraries that were created by the script: FCM Alert Template, FCM Enrichment, FCM Prep Data, and FCM Scenario Library.

6 Open the properties of the FCM Alert Template. Validate that Location reveals the /Shared Data/Financial Crimes Monitor/FCM Alert Template directory.

7 The Assign tab should have the SASApp server selected.

8 The Options tab should display the FCMATEMP libref and a selected path specification that points to your sample alert_template.

9 Validate the remaining libraries in the same manner.
Run register_table script

The register_table script registers prep tables for three of the libraries created in “Run make_library script” on page 88. To run register_table, follow these steps:

1. Comment out all %include lines in metadata_script.sas except, %include samplib(register_table);

2. Execute metadata_script.sas either through interactive or batch SAS.

3. Check there are no errors in your SAS log.

4. Start a SAS Management Console using your sasadm@saspw profile, and select the Plug-ins tab.

5. Expand your Data Library Manager tree.

   Underneath the Libraries directory, you should see the FCM libraries: FCM Alert Template, FCM Enrichment, FCM Prep Data, and FCM Scenario Library.

6. Verify that each library, except the FCM Scenario Library, has its appropriate registered tables. Select the FCM library name and note the table name listed in the panel to the right of the library. Confirm the tables registered as listed below. If you do not find a registered table consult your SAS log for errors:

   - FCM Alert Template
     - alert_summary_sample
   - FCM Prep Data
     - sample_contractor_revenue
     - sample_employer_ratio
   - FCM Enrichment
     - details_contractor
     - details_employer
## Import Sample Data

To import the sample data, follow these steps:

1. Make sure that the fcm * _ddl_* .sql script for your database has been executed for your database has been executed to create the database FCM tables.  
   For more information, see “Create Database Tables” on page 60.

2. Log on to the Financial Crimes Monitor Web application on the same machine that your sample_tax_fraud.xml exists with the fcmuser1 credentials.

3. Log on to the Financial Crimes Monitor Web application on the same machine that your sample_tax_fraud.xml exists with the fcmuser1 credentials.

4. After the application appears in your browser, you can import the Sample Tax Fraud project. To do this, first make a note of the URL shown in the browser's address bar. The beginning of the URL will follow this format: http://hostname:portname/SASFINCRM/ (for example: http://myhostname.mycompany.com:8780/SASFINCRM/).

5. In the address bar, enter this same URL, adding ProjectImport after the trailing slash character. For example, following from the earlier example, you might enter http://myhostname.mycompany.com:8780/SASFINCRM/ProjectImport.

6. At this point, the page will prompt you, "Please choose an XML file to upload." Click the Browse button and navigate to the sample_tax_fraud.xml file in the sample subdirectory.

7. Select the file and click the **Upload** button.  
   When complete, the page displays the following:
   
   Parsing 1 project(s) from uploaded file.  
   About to load project "Sample Tax Fraud" project imported.  
   Done. Imported 1 project(s).

8. Next, load the Financial Crimes Monitor Web application again, and verify that the project **Sample Tax Fraud** is visible in the **Configured Projects** list.
Generate Alerts

Follow these steps to generate alerts:

1. You must update the job calendar, before generating alerts. Log on to the Financial Crimes Monitor Web application with the fcmuser1 credentials.

   **Note:** By default, the Job Calendar fields are not populated. A script (fcm_job_calendar_holiday_seed_data.sql), to enable populating the holiday table with United States holidays is delivered with your installation and can be executed to populate the table with seed data. The input file can be customized for other locales. For more information, see SAS Social Network Analysis Server: Administration Guide.

2. Highlight the Sample Tax Fraud project, and scroll to the bottom of the screen to update the job calendar.

   All the scenarios imported are ‘Daily’ scenarios.

3. Generate a job calendar for a daily run today. For more information, see SAS Social Network Analysis Server: Administration Guide.

4. Execute the alert generation process (AGP) with the FCMMain.sas batch command. For more information, see “Manage Project Scheduling and Execution” in the SAS Social Network Analysis Server: Administration Guide.

5. Verify the number of alerts generated by the AGP process.

   The following table validates the number of alerts generated per scenario. Please review your log to validate the number of alerts generated per scenario:

   **Table 10.1 Number of Alerts Generated Per Scenario**

<table>
<thead>
<tr>
<th>Scenario Name</th>
<th>Purpose</th>
<th>STAGE.Alert_summary</th>
<th>FCM.FCM_ALERT</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1:Employee Ratio vs Peer Group</td>
<td>Fraud Detection</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Scenario Name</td>
<td>Purpose</td>
<td>STAGE.Alert_summary</td>
<td>FCM.FCM_ALERT</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>F2:Pct Contractor Annual Rev From One Employer</td>
<td>Fraud Detection</td>
<td>154</td>
<td>154</td>
</tr>
<tr>
<td>F3:Pct Contractor Total Rev from One Employer</td>
<td>Fraud Detection</td>
<td>45</td>
<td>45</td>
</tr>
<tr>
<td>F4:Num of Contractors per Employer</td>
<td>Risk</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>FSP:Rev from One Employer and High Loss Amt</td>
<td>Second Pass</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>225</strong></td>
<td><strong>224</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Using Data Sets Instead of a Database**

For sites where a SAS Financial Crimes Monitor database connection is not available for use, SAS data sets generated from the initial run of the alert generation process (AGP) can be used instead. To use data sets, follow these steps:

1. Use a text editor to load the file, Disposition_Alerts.sas, located in: SAS-configuration-directory/Lev1/Applications/SASFinancialCrimesMonitor3.1/sample.

2. Comment out the FCM libname statement.

3. Use instead, the static data sets of the alerts resulting in the sample_output directory.

   For example, add a line similar to:

   ```sql
   libname fcm
   "/local/install/cfgsas93/config/Lev1/Applications`
   ```
Repeat steps 2–4 for Tax_Demo_Tables.sas and sample_getSubAlerts.sas.

Import SAS Stored Processes from a SAS Package

SAS provides sample SAS Stored Process metadata in a SAS package file. To import a sample SAS package, perform the following steps:


2. Right-click the Financial Crimes Monitor 3.1 folder and select Import SAS Package.

Display 10.5  Import SAS Package
3 Select the **Browse** button and navigate to the location of the template SAS package file:

**UNIX Specifics:** `SAS-config-dir/Applications/SASFinancialMonitor3.1/sample/Sample.spk`

**Windows Specifics:** `SAS-config-dir\Applications\SASFinancialMonitor3.1\sample\Sample.spk`

- Ensure that the **Include access controls** check box is **not** selected.
- Select **Next**.

4 At the Select Objects to Import page, make sure each stored process is selected.

**Display 10.6 Import SAS Package: Select Objects to Import**

Click **Next** to continue.

**Note:** You might be presented with an Import Warning dialog box that displays a caution message regarding not importing entries and associations related to access control entries (ACEs) or an access control template (ACT). Click **Yes** to continue. Your installation will continue without an error related to this warning.
5 Select **Next** on the About Metadata Connections page.

6 Select **SASApp** as the target application server on the SAS Application Servers page, and then click **Next**.

7 Copy the sample* stored procedures from `SAS-config-dir/Applicatons/SASFinancialMonitor3.1/sample` to:

   - **Windows**:
     ```
     SAS-install-dir/SASFoundation/9.3/snamva/sasstp
     ```
   - **UNIX**:
     ```
     SAS-install-dir/SASFoundation/9.3/sasstp/snamva
     ```

8 Select **Add** on the Source Code Repositories page, and provide the directory name:

   **UNIX Specifics**: `<SASHome>/SASFoundation/9.3/sasstp/snamva`
   
   **Windows Specifics**: `<SASHome>/SASFoundation/9.3/snamva/sasstp`

9 Use the **Target** menu to select the directory that was just added, and then click **Next**.

10 Review the Summary page, and then click **Next**.

11 Confirm that the import process completed successfully, and then click **Finish**.

12 After you have imported the Sample.spk file, you have to manually add the message parameter as a property to `processAlertResponse`.

---

**Display 10.7  Template Warning Dialog Box That Might Appear during SAS Package (SPK) File Import**
a In the Folders tab of SAS Management Console, locate Sample and the processAlertResponse stored process.

b Right-click on processAlertResponse and choose Properties.

c In the Properties dialog box, choose the Parameters tab.

d In the Output Parameters list box, click New.

e In the New Output Parameters dialog box, enter Message in the Name field, and String in the Type field, and click OK.

Deploy the Imported SAS Stored Processes as a Web Service

After the SAS package file is imported, metadata is associated with the SAS program code for the stored processes in the SAS installation directory. The code for the stored processes can be modified at any time to configure the display of alerts and social networks on the investigator user interface. However, they are deployed as a Web service now, even though the SAS program code can be customized later. To deploy these stored processes as a web service, follow these steps:

1 Use the Folders tab of SAS Management Console to navigate to the folder that was just imported to the /System/Applications/SAS Social Network Analysis/Social Network Analysis 3.1/Sample folder.

2 Deploy the alerts-related Web service. In the right panel, hold down the CTRL key and click to select the following stored processes:

   - sample_getActionableEntities.sas
   - sample_getAlertCharts.sas
   - sample_getAlertTransactions.sas
   - sample_getSocialNetworkNodeAndLinks.sas
   - sample_getMoreSocialNetworkNodesAndLinks.sas
Right-click one of the selected icons and select **Deploy As Web Service.** The Deploy As Web Service wizard starts.

On the Web Service Information page, confirm or set the following values:

- Select the default value for **Web Service Maker URL** from the menu.
- Make sure that **New Web Service Name** is set to the value of `SampleAlerts`. However, if the folder was renamed to a value such as `Healthcare`, then the **New Web Service Name** must be `HealthcareAlerts`.

**Note:** The web service name is case sensitive. That is, if the Sample was renamed Healthcare, then the new web service name must be HealthcareAlerts. However, if the Sample folder was renamed healthcare, then the new web service name must be healthcareAlerts.

- The choice of credentials to use does not matter. Click **Next**.

On the Web Service Keywords and Namespace page, provide the following value for the **Namespace** field:

- `http://sas.com/sso/fraud/alerts`

Click **Next**.

Confirm the settings and then click **Finish**.

Deploy the social network-related Web service using a method that is similar to deploying the alerts-related Web service. Hold down the CTRL key and click to select the following stored process icons:

- `getSocialNetwork`
- `getSocialNetworkNodeDetails`
- `growSocialNetworkNode`
8 Right-click one of the selected icons and select **Deploy As Web Service**.

The Deploy As Web Service Wizard starts.

9 On the Web Service Information page, confirm or set the following values:

- Use the default value for **Web Service Maker URL**.
- Make sure that **New Web Service Name** is set to the value of **SampleSocialNetworkAnalysis**. However, if the folder was renamed to a value such as **Healthcare**, then the **New Web Service Name** must be **HealthcareSocialNetworkAnalysis**.

  **Note:** The web service name is case sensitive. That is, if the Template folder was renamed Healthcare, then the new web service name must be HealthcareSocialNetworkAnalysis. However, if the Template folder was renamed healthcare, then the new web service name must be healthcareSocialNetworkAnalysis.

- The choice of credentials to use does not matter.

  Click **Next**.

10 On the Web Service Keywords and Namespace page, provide the following value for the Namespace field:

- **http://sas.com/sso/fraud/sna**

  Click **Next**.

11 Confirm the settings and then click **Finish**.

If the deployment completes successfully, two new Web services (**sampleAlerts** and **sampleSocialNetworkAnalysis**) are deployed. You can confirm successful deployment by reviewing the entries under the Configuration Manager within SAS Application Infrastructure at the BI Webservices for Java 9.3 node. (You must refresh your session to see these entries.)
Add the SAS Investigator group to the sample folder in SAS Management Console, so that snauser1 has access to the sample domain. For more information, see “Add an Investigator Group and Investigators” on page 80.

**Set Up Advanced Search and Disposition Files**

Copy samplesearch_config.xml and esearch_config.xml from the SAS-config-dir \Applications\SASFinancialMonitor3.1\sample to the configuration directory for your web application server:

- JBoss:
  

- UNIX:
  

  JBOSS_HOME/server/SASServer8/deploy_sas/sas.socialnetworkanalysis3.1.ear/sas.sso.snaserver.war
Windows: `JBOSS_HOME\server\SASServer8\deploy\sas\sas.socialnetworkanalysis3.1.ear\sas.sso.snaserver.war`

UNIX: `WebSphereHome\AppServer\profiles\SAS01Node\installedApps\SASDmgr01Cell\SASSNA3.1.ear\sas.sso.snaserver.war`

Windows: `WebSphereHome\AppServer\profiles\SAS01Node\installedApps\SASDmgr01Cell\SASSNA3.1.ear\sas.sso.snaserver.war`

WebSphere:

You must restart your managed server containing SAS Social Network, typically SASServer8, before you will see the Sample Analytic Domain's search and disposition panels.

Add snauser1 to the fcmDBAuth group using SAS Management Console, so that the FCM libref in the stored processes is assigned correctly. For more information, see “Initialize Users and Groups” on page 68.

Considerations for SAS Enterprise Case Management

Customers who also license SAS Enterprise Case Management, are able to add further customizations. These customers can communicate information through alerts displayed in the Social Network Analysis alert viewer to SAS Enterprise Case Management.

For more information, see “SAS Social Network Analysis Server Expanded Features” in SAS Social Network Analysis Server: Administration Guide.
Part 5

Setup Tasks

Chapter 11
Set Up the SAS Financial Crimes Monitor .................. 103

Chapter 12
Set Up the SAS Social Network Analysis Server .......... 131
Set Up the SAS Financial Crimes Monitor

Understanding the Setup Procedure for the SAS Financial Crimes Monitor .......................... 104
- Operation of the SAS Financial Crimes Monitor .................................................. 104
- Source File Location ..................................................................................... 105
- Groups, Roles, and Group Memberships .......................................................... 105

Overview of the Post-Installation Setup for the SAS Financial Crimes Monitor .................. 112
- Special Considerations for the WebSphere Application Server with IBM DB2 on AIX Installation ................................................................. 113
- Verify the Authentication Domain ..................................................................... 113
- Create and Configure an Authentication Domain Access Group .................. 113
- Modify UNIX Directory and File Permissions for Trusted User Account .......... 114
- Grant Permission for User Group Access to the Data ..................................... 114
- Define Libraries and Register Tables ............................................................... 115
- Establish a Connection to the Metadata Server ............................................... 116

Complete Setup Tasks for the SAS Financial Crimes Monitor ................................. 116
- Perform Post-Installation Setup of the SAS Financial Crimes Monitor ........... 116
Understanding the Setup Procedure for the SAS Financial Crimes Monitor

The SAS Financial Crimes Monitor operation is based on a specific deployment and its associated projects. In order to complete a successful setup, you must understand the objective of each process in the procedure. The balance of this chapter uses examples to demonstrate each task; you must adjust these examples, based on your understanding of your data and your projects, to suit your deployment.

Operation of the SAS Financial Crimes Monitor

To support project development, the SAS Financial Crimes Monitor uses a hierarchy method that represents jobs that will be executed to produce an alerts table. The SAS Financial Crimes Monitor must have access to the libraries and scenario code indicated in each project as well as to the databases that house the data that will be used for analysis. When a job is executed, the SAS Financial Crimes Monitor uses the metadata engine to retrieve data from the metadata repository about specific libraries. The metadata engine requires that the solution supply the credentials and connection information for the metadata repository to which it will be connecting.

To enable the SAS Financial Crimes Monitor to access the resources required and perform the tasks needed, it must be associated with an account that connects to the metadata server using the inherent trusted user mechanism. For this to occur, the following two criteria must be met:

- An operating system user account must be defined.
- The user account identified for access must be a metadata user that uses the default authentication domain.

In addition, the following connection system options for metadata must be supplied (either in a configuration file or through the use of the SAS autoexec.sas file).

```
metaport=
metaprotocol=
```
See SAS Language Interfaces to Metadata for information about system options for metadata.

Setting up an account through which the SAS Financial Crimes Monitor can operate is a required post-installation setup task.

Source File Location

The interface of the SAS Financial Crimes Monitor contains several areas to enable you to indicate the location of the source files for SAS code (for example, processing code (pre or post), scenario code, enrichment code). The SAS Financial Crimes Monitor points to the directory established by the FCM_SLIB libref, as indicated in the autoexec.sas file. The solution sees this as the top directory and enables you to drill down from this directory into subdirectories that have been created. Source files that are not within this libref are not accessible by the solution.

For example, suppose FCM_SLIB libref is defined as C:\FCMFiles\FCMSource\fcm_slib. In this example, if you create a directory named enrichment beneath fcm_slib, then it will be displayed by the user interface.

However, if you create a directory structure of C:\FCMFFiles\FCMTSource\enrichment, the user interface will not display the enrichment directory or any files within it.

Groups, Roles, and Group Memberships

During the installation and configuration process, the default Financial Crimes Monitor:Admin role is created. Administrators must be assigned to this role either as individuals or as group members. In addition, other group memberships are required to allow the solution and users of the solution to access the resources required. The following table lists the typical user types and displays the access permissions that must be granted to allow the user to perform the typical tasks, also outlined in the following table.
### Table 11.1  
**Overview of Typical User Types and Associated Permissions for Typical Tasks**

<table>
<thead>
<tr>
<th>Example User Type</th>
<th>Typical Tasks</th>
<th>Access Permissions</th>
<th>Notes</th>
</tr>
</thead>
</table>
| SAS Financial Crimes Monitor Administrator | - Access the SAS Financial Crimes Monitor  
- Create or manage projects and related items  
- Run the AGP to execute projects | - Assign to Financial Crimes Monitor: Admin role.  
- Make member of a group that has access rights to appropriate data sources.  
- Grant R/W permissions on FCM schema. | Only users who are included in the Financial Crimes Monitor: Admin role (as users or within a group) can log on. As a best practice, care must be taken to provide the appropriate level of access to the required data sources. For example, since prep data is not modified by the SAS Financial Crimes Monitor, RO permission to the prep table data source would be sufficient. |
<table>
<thead>
<tr>
<th>Example User Type</th>
<th>Typical Tasks</th>
<th>Access Permissions</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS Social Network Analysis User: Alert Recipient (that is, SAS Social Network Analysis user who performs alert disposition)</td>
<td>- Does not access the SAS Financial Crimes Monitor</td>
<td>- Include in an FCM* routing group.</td>
<td>Many routing groups can be defined. Creating a default routing group (such as FCM Default, suggested during the installation procedure) is recommended to allow project creation.</td>
</tr>
<tr>
<td></td>
<td>- Is responsible for triaging alerts through the SAS Social Network Analysis Server</td>
<td>- Grant R/W permissions on the FCM schema to allow disposition of alerts.</td>
<td>If ReadMetadata permission is granted to a group to allow user access, the group cannot be a default SAS group; it must be a uniquely created group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Set ReadMetadata permission to the user (or group to which the user belongs) on the analytic domain (metadata folder) to which the user or group has been granted rights to access.</td>
<td></td>
</tr>
</tbody>
</table>

For example, if you configured the Template example during installation, you created the SNA Investigator group with this criteria. The group or members are not viewable through the interface.
<table>
<thead>
<tr>
<th>Example User Type</th>
<th>Typical Tasks</th>
<th>Access Permissions</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS (Operating System) Account</td>
<td>Valid account required to run the SAS Financial Crimes Monitor</td>
<td>Include in a group with RO access to data sources (for example, prep table)</td>
<td>The user ID fcmctrl is suggested later in this guide.</td>
</tr>
<tr>
<td></td>
<td>Requires access credentials including database user ID, password, and authentication domain for external data such as the prep table, enrichment data, and alerts.</td>
<td>Include in a group with R/W access to FCM schema.</td>
<td>The SAS Financial Crimes Monitor needs to access solution code and defined databases to execute jobs.</td>
</tr>
</tbody>
</table>

In addition, one or more authentication groups (for example, FCM DB Auth, as suggested later in this guide) must be defined. This group can have potentially one entry for each supported database to which the solution must connect under the user ID of the host account. The SAS Financial Crimes Monitor needs to access solution code and defined databases to execute jobs. The credentials required for access include database user ID, password, and authentication domain for external data such as the prep table, enrichment data, and alerts. A user ID, such as fcmctrl defined as suggested in the SAS Social Network Analysis Server: Installation and Configuration Guide, must be a member of this group.

The following diagram demonstrates the relationships between the users identified in the previous table and the remaining elements in the structure.
The Authentication group definition plays a key role in successful project execution. If the permissions are not granted properly, then the job will not execute properly or, in some cases, might not execute at all.

The following example demonstrates the correct use and setup of authentication domains for a specific job.

**Issue Description**

- There are several Oracle servers (instances) that require access for a specific project.
Each Oracle server (instance) requires a unique user ID and password combination (that is, the instances cannot be accessed by the same credentials).

Assume that the user ID `fcmctrl` has been set up as an operating system-level account, as suggested in the SAS Social Network Analysis Server: Installation and Configuration Guide. Assume also that this user ID has been configured as a trusted user account to allow access to metadata, as described later in this chapter.

**Issue Resolution**

For this example, two unique authentication domains, one for each Oracle server (instance), must be configured. Configure each one using the following parameters and credentials.

<table>
<thead>
<tr>
<th>Authentication Domain 1</th>
<th>Authentication Domain 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name = oracleDBAuth1</td>
<td>Name = oracleDBAuth2</td>
</tr>
<tr>
<td>User ID = OracleUser1</td>
<td>User ID = oracleUser2</td>
</tr>
<tr>
<td>Password = OraclePW1</td>
<td>Password = oraclePW2</td>
</tr>
</tbody>
</table>

The following options can be used for specifying the authentication domain for each instance.

- **Option 1 - Add both accounts to an existing account**
  
  In this instance, the oracleDBAuth1 and the oracleDBAuth2 accounts can be added to the account. This would allow the solution to execute jobs and access the data in both accounts as needed.

- **Option 2 - Create two groups, adding one account to each group**
  
  In this instance, two separate groups are created, with each having just one of these authentication domains, but both listing a trusted user, (for example, `fcmctrl`) as a member.

  The advantage of this implementation method is that you can then create additional groups, such as FCM Prep DB, FCM Enrichment DB, and FCM Alert Templates DB. This would mean that the FCM DB Auth group would be used strictly to enable
access to the database (instance) that has the FCM schema tables so that the SAS Financial Crimes Monitor can run the code required to execute jobs.

The following figure shows the setup of a deployment consistent with the criteria of Option 1.

**Figure 11.2 Example of Adding Multiple Accounts to an Existing Account**

![Diagram showing the setup of a deployment consistent with the criteria of Option 1.](image)

The following figure shows the setup of a deployment consistent with the criteria of Option 2.

![Diagram showing the setup of a deployment consistent with the criteria of Option 2.](image)
The method that you use to configure your deployment should be the best for your circumstances and should take access controls into consideration.

Overview of the Post-Installation Setup for the SAS Financial Crimes Monitor

At the completion of the SAS Financial Crimes Monitor installation and configuration process, the application has been installed, the default Administrator role has been created, and the application server context (either SASApp by default or a user-assigned name), has been defined. At this point, you can log on to the SAS Financial Crimes Monitor, but you cannot create or save projects. You must perform the post-installation setup tasks described in this chapter to enable the use of the solution. The post-installation setup procedure connects all of the pieces, including defining the correct permissions for users and resources. At the completion of the post-installation
setup steps, the SAS Financial Crimes Monitor can be accessed by a user with the defined role, and projects and project components can be created and managed.

**Special Considerations for the WebSphere Application Server with IBM DB2 on AIX Installation**

If your installation includes the WebSphere Application Server (Version 7 or 8), IBM DB2 database, and AIX, then additional post-installation steps are required. The steps enable you to save data; without completing the setup steps specific to this deployment configuration, you will receive an endless ‘Please Wait’ message after attempting to save a project. For these configurations, you must access the WebSphere Application Server Console to modify the connection pool definitions.

See “Special Considerations for the WebSphere Application Server with IBM DB2 on AIX Installation” on page 113 for details.

**Verify the Authentication Domain**

As a prerequisite, if the database in use is either MySQL or Oracle, then create the server context (SASApp is used throughout this document) and point the server context to the back-end database. If the database is either Microsoft SQL Server or IBM DB2, then these steps were completed during the installation, and they do not have to be revisited as post-installation setup tasks.

For all database types, make sure that the authentication domain is valid and make a note of the domain as it will be used throughout the post-installation process.

See “Verify Authentication Domain” on page 119 for details.

**Create and Configure an Authentication Domain Access Group**

A group that will access the authentication domain must be created and configured. By design, the only users who will be able to access the data in the database are those users who are either members of this group or users who have login credentials within that specific domain.
Create a group that will be used to access the authentication domain.

Ensure that the group created has login credentials that use the authentication domain referenced by the server context.

See “Create and Configure an Authentication Domain Access Group” on page 121 for details.

Modify UNIX Directory and File Permissions for Trusted User Account

When a project is executed, the code that runs behind the solution to generate alerts must have Read, Write, and Execute access to several directories and files. In most instances, the correct permissions are set during the setup and installation procedure. On UNIX systems, this step must be performed manually.

See “Modify UNIX Directory and File Permissions for Trusted User Account” on page 122 for details.

Grant Permission for User Group Access to the Data

Users and groups have to be granted explicit permission to access the data. At the end of the installation and configuration process, the user sasdemo, for example, is created (if you indicated or accepted this name as the SAS user account). You can either configure this user or you can create a new user (such as fcmctrl, as suggested in the SAS Social Network Analysis: Installation and Configuration Guide). This is performed by adding the user to the group and ensuring the correct credentials, as follows:

Create or identify the user ID that you want to permission for access to the data.

**Note:** The only account that needs to read the data is the account that is used to connect to the metadata when the job is executed. This is defined in the SAS autoexec.sas file using the LIBNAME options statement or a configuration file, as described in “Establish a Connection to the Metadata Server” on page 116.
Ensure that the user ID is associated with an operating system account. That is, confirm that the user has login credentials specific to the default authentication domain (DefaultAuth) indicated.

- Add the user to the group defined in “Create and Configure an Authentication Domain Access Group” on page 113.

See “Grant Permission for User Group Access to the Data” on page 123 for details.

**Define Libraries and Register Tables**

Regardless of the database type (DB2, Microsoft SQL Server, MySQL, or Oracle), you must define the connection and the default login as the one specified during server context setup.

- Create your library (generally recommended to be located under the metadata path /Shared Data/FCM/Libraries)

  Configure your library to have connection and the default login set to the one specified in “Create and Configure an Authentication Domain Access Group” on page 113.

- Add the group created in “Create and Configure an Authentication Domain Access Group” on page 113 to the library authentication, making sure the group has Read permission assigned to the group set to Grant.

- For tables, especially prep tables, define each table to have the same group added to its authentication tab that was added to the library that you created.

- Ensure that each table has the Read permission set to Grant for the group that was created in “Create and Configure an Authentication Domain Access Group” on page 113.

See “Define Libraries and Register Tables” on page 124 for details.
Establish a Connection to the Metadata Server

Using either an OPTIONS statement or an external configuration file, properly secured, you must specify the metadata server connection and make it available to the system for access.

See “Establish a Connection to the Metadata Server” on page 129 for details.

Complete Setup Tasks for the SAS Financial Crimes Monitor

After the SAS Financial Crimes Monitor is installed and configured, a series of steps, outlined in the SAS Social Network Analysis Server: Installation and Configuration Guide, must be completed before the application can be launched successfully. This section contains detailed procedures for completing the post-installation setup tasks. The completion of the post-installation setup tasks enables you to launch the SAS Financial Crimes Monitor and to create and save projects.

Perform Post-Installation Setup of the SAS Financial Crimes Monitor

Special Considerations for the WebSphere Application Server with IBM DB2 on AIX Installation

If your installation includes the WebSphere Application Server (Version 7 or 8), IBM DB2 database, and AIX, then additional post-installation steps are required. The steps enable you to save data; without completing the setup steps specific to this deployment configuration, you will receive an endless ‘Please Wait’ message after attempting to save a project. For these configurations, you must access the WebSphere Application Server Console to modify the connection pool definitions.

In general, you must perform the following tasks.

- Access the WebSphere Application Server Administration Console.
- Delete the **FinancialCrimes** entry from the JDBC, Data Sources area, generally accessible from within the Resources panel.

- Delete the **FCM JDBC Provider** entry from the JDBC, JDBC providers area, generally accessible from within the Resources panel.

- Review your changes and make sure you indicate **Synchronize changes with Nodes** before saving.

- Select the SAS Financial Crimes Monitor server (generally this is SASServer8) from under the **Scope** of the JDBC Provider area and create a new JDBC provider with the following settings:
  - Database type = User-defined
  - Implementation class name = com.ibm.db2.jcc.DB2ConnectionPoolDataSource
  - Name = FCM JDBC Provider
  - Class path = Full path to the db2jcc4.jar

- Select **Data sources**, make sure you are within the SAS Financial Crimes Monitor server (generally this is SASServer8) and create a new data source with the following settings:
  - Data source name = Financial Crimes
  - JNDI name = sas/jdbc/SASFCMDS
  - JDBC provider = FCM JDBC Provider (Select from existing )
  - Data store helper class name = com.ibm.websphere.rsadapter.GenericDataStoreHelper
- Make sure the option **Use this data source in container managed persistence (CMP)** is not selected.

- Specify the following security aliases:
  - Component-managed authentication alias = SASDmgr01Cell/Financial Crimes
  - Mapping-configuration alias = DefaultPrincipalMapping
  - Container-managed authentication alias = SASDmgr01Cell/FinancialCrimes

- For the FinancialCrimes data source (generally accessible through the Data Sources page), configure the following custom properties:
  - `databaseName` Value = The name of your database. Contact your DBA if you are unsure.
  - `serverName` Value = The name of your server.
  - `portNumber` Value = The port number of the database server.
  - `driverType` Value = 4

- Review your changes and make sure you indicate **Synchronize changes with Nodes** before saving.
Test your connection to ensure proper configuration and then stop and restart the SAS Financial Crimes Monitor server (generally this is SASServer8).

If you require assistance completing this process, contact SAS Technical Support.

**Verify Authentication Domain**

Before you can verify the authentication domain, you must make sure the server context has been created. Make sure that the server context pointing to the back-end server is created and that the server context has a valid authentication domain (this will be common across libraries, users, and groups).

**Note:** If the database in use is either MySQL or Oracle, then create the server context (SASApp is used throughout this document) and point the server context to the back-end database. If the database is either Microsoft SQL Server or IBM DB2, then these steps were completed during the installation.

**Note:** During installation, a default server authentication domain is identified as described in the *SAS Social Network Analysis Server: Installation and Configuration Guide*. If you did not accept the default and instead entered a different authentication domain, then you should select the authentication domain established during installation and configuration.
The authentication domain indicated for the installation is also the same authentication domain entry that you are instructed to confirm is correct at the LIBNAME specification line in the SAS autoexec.sas file during the SAS Financial Crimes Monitor post-installation steps in the SAS Social Network Analysis Server: Installation and Configuration Guide.

Through SAS Management Console, ensure that the authentication domain is specified correctly for the server context related to this deployment.
The authentication domain for the server is the same authentication domain that a user will need to be associated with in order to access data. Make a note of the authentication domain for later reference and use.

**Create and Configure an Authentication Domain Access Group**

Only users (or groups) that have valid credentials (user name and password) for the selected authentication domain will be allowed to access the data. In addition, the user or group account must be associated with an operating system account.

**Note:** As explained in the *SAS Social Network Analysis Server: Installation and Configuration Guide*, the operating system association enables the user ID to execute SAS code initiated by the solution. If you created a unique user ID, such as `fcmctrl`, to be used as the ID under which to execute SAS Code and another user ID, such as `fincrmdb`, for general access, then substitute the appropriate users in the following procedure.

1. Identify or create a group that will be allowed to access data within the server context identified.
Make sure the group created or identified is associated with the server context and has access to the authentication domain specified.

In the following screen, for example, the group FCM GEN DB has been created. Viewing the properties of the group shows that the user ID *fincrmdb* is included in the *fcmDBAuth* authentication domain and has a valid login defined for the FCM GEN DB group.

**Note:** The *fincrmdb* account does not need operating system account credentials. The *fincrmdb* ID must have access to the FCM schema for each database server being used (for example, Oracle, MySQL, IBM DB2, or Microsoft SQL Server).

<table>
<thead>
<tr>
<th>FCM GEN DB Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
</tr>
<tr>
<td>Logins defined for FCM GEN DB</td>
</tr>
<tr>
<td>Authentication Domain</td>
</tr>
<tr>
<td>fcmDBAuth</td>
</tr>
</tbody>
</table>

**Modify UNIX Directory and File Permissions for Trusted User Account**

When a project is executed, the code that runs to generate alerts must have Read, Write, and Execute access to several directories and files. In most instances, the correct permissions are set during the setup and installation procedure. On UNIX systems, this step must be performed manually.

Make sure the permissions on the following directories are set for Read/Write/Execute for the user ID that executes project runs. The permissions must include the directories, the subdirectories, and all files in the subdirectories.

- `/SASConfig/Lev1/Applications/SASFinancialCrimesMonitor3.1/
- `/SASHome/SASFoundation/9.3/misc/fincrmvma/formats/
- `/SASConfig/Lev1/Applications/SASFinancialCrimesMonitor3.1/ stage/`
Grant Permission for User Group Access to the Data

Users added to the authentication domain are able to access data within the server context. Users added must have operating system level accounts.

1. Create or identify an existing user with operating system credentials.

2. Ensure that the user also has a login specific to the default authentication domain (DefaultAuth) defined.

So, for example, during installation, the user sasdemo is created and assigned to the DefaultAuth authentication domain, which is an operating system level domain.

Note: Using sasdemo in your production environment is not recommended. You should create a user with the proper access rights for your deployment and with consideration to access controls in your organization.

Display 11.3 Example Showing a User with Operating System Account Access

For the Microsoft Windows operating system, generally the User ID is displayed as either MachineName\UserID or MicrosoftWindowsDomain\UserID. For UNIX deployments, generally only the user ID is required.
The user sasdemo is a member of several groups, including the FCM GEN DB group, created after the installation specifically for this example.

**Note:** A password is not required because this account will be recognized as a trusted user account. Additional metaoptions will be configured in a process described later in this document.

**Display 11.4**  Example Group Membership for SAS Demo User

The group to which the user ID (ideally, this would be something like fcmctrl) with operating system-level credentials belongs must have access to the authentication domain identified in “Verify Authentication Domain” on page 119.

**Define Libraries and Register Tables**

Libraries must be created and then the groups, such as the one created in “Create and Configure an Authentication Domain Access Group” on page 121, must be added to the library’s authorization list.

It is recommended that you create your libraries under the metadata path /Shared Data/FCM/Libraries. To enable the SAS Financial Crimes Monitor scenario Library panel to display scenarios, you must create a SAS library with the name FCM_SLIB that points to the directory in which the scenario library files (SAS and XML) are located. See “Create and Manage a Custom Scenario Library” in Chapter 13 of SAS Social

**Note:** The SAS Financial Crimes Monitor looks for libraries defined with librefs beginning with “FCM” when loading projects. Therefore, all of your library librefs should be prefixed with “FCM” to be identified and selected by the SAS Financial Crimes Monitor.

**Note:** Do not create libraries with the LIBNAME FCM_PREP or the LIBNAME FCM because these names are reserved for use by the SAS Financial Crimes Monitor. Creating a library with the LIBNAME FCM_PREP or a library with the LIBNAME FCM will result in system issues that might prevent scenarios from running.

**CAUTION! Unexpected results or erroneous data might result from using duplicate names across libraries.** The SAS Financial Crimes Monitor uses concatenation to create one library named FCM_PREP that includes the tables that you indicate. If tables across libraries have the same name as one another, the SAS Financial Crimes Monitor will be unable to distinguish one from the other and will use the first one it encounters. This might result in unexpected or erroneous results.

**TIP** If you set the permissions at the top level, then you will not have to access each table in the library to set the permissions at the individual table levels.

1. Create and define libraries through SAS Management Console.
   Libraries created through SAS Management Console must specify the default login that the library will use as the authentication domain as specified in “Verify Authentication Domain” on page 119. In addition, the database server and the connection information must be specified and must be the same as that defined in “Verify Authentication Domain” on page 119.
If you are defining a SAS BASE library, you do not have to associate it with a MySQL or an Oracle database.
When you define your library, however, you must use the UNC path of the repository on a Microsoft Windows system. If the repository is on a Linux system, then administrators must use Samba to make it appear as if it is running on a Microsoft Windows system. See “File Path Resolution Consideration” in Chapter 14 of SAS Social Network Analysis Server: Administration Guide for suggestions to resolve file path specification issues.

**Display 11.7  Example Showing UNC Path Specification**

![Example Showing UNC Path Specification](image)

2 After the library is created, add the groups created during this post-installation procedure to each library’s authorization list, making sure the **Read** permission is set to **Grant**.

For example, the image below shows the FCM GEN DB group added to the authorizations for the FCM – MySQL GEN PrepData library, and the **Read** permissions set to **Grant**.
3 Register the tables in the library by right-clicking a library, selecting **Register Tables**, and completing the Register Tables wizard.

**Note:** For a UNIX deployment, you must use a Microsoft Windows version of SAS Management Console to register tables. The UNIX SAS Management Console does not support the Register Tables feature.

When registering the tables, make sure you select the **Enable case-sensitive DBMS object names** option.

4 After the tables have been registered, for each table in the library, add the same group to its authorization list as was added to the library in a previous step.
Note: If you did not set the permissions at the top level, then you must perform the following sequence to set the permissions for each table individually to update the authorizations.

Display 11.10  Example Showing Library Table Authorizations

Establish a Connection to the Metadata Server

The SAS Financial Crimes Monitor uses the metadata engine to retrieve information from the metadata repository about specific libraries. To enable the SAS Financial Crimes Monitor to establish a connection to the metadata server, you must specify your connection properties directly. This can be done by either using a configuration file or by using an OPTIONS statement added to the SAS autoexec.sas program. The Example Code 11.1 on page 129 shows a configuration file example; this is the recommended method. The Example Code 11.2 on page 129 shows an OPTIONS statement example that is added to a SAS autoexec.sas file.

Example Code 11.1  Configuration File

    -METAPORT 9999
    -METAREPOSITORY "myrepos"
    -METASERVER "a123.us.company.com"

Example Code 11.2  OPTIONS Statement

    options metaport=8561
The metadata user, sasdemo in our examples, was created with an operating system-level account. Because the metadata user has an operating system-level account, the metadata server will log on as this user (a trusted user).

See *SAS Language Interfaces to Metadata* for information about system options for metadata.
Set Up the SAS Social Network Analysis Server

Setup Tasks for the SAS Social Network Analysis Server

Setup Tasks for the SAS Social Network Analysis Server

The SAS Social Network Analysis Server is an investigator interface that enables users to manage and triage alerts. The interface is customizable, and the alert types and severity indicators are driven by the development and implementation of projects by administrative users who access the SAS Financial Crimes Monitor. Investigators use the SAS Social Network Analysis Server: Investigator Guide for information about using the solution.

The SAS Social Network Analysis Server: Installation and Configuration Guide contains detailed information about the installation and post-installation tasks that need to be performed to enable users with investigator credentials to access and use the solution. The SAS Social Network Analysis Server: Installation and Configuration Guide also provides an example that defines setting up an alert series. Rely on the information in the SAS Social Network Analysis Server: Installation and Configuration Guide for details relevant to installation and configuration of the SAS Social Network Analysis Server.

Beyond installation, configuration, and setup of the SAS Social Network Analysis Server, administrative users can perform the following tasks to implement customized
features that are documented in the *SAS Social Network Analysis Server: Administration Guide*:

- enable and customize an Advanced Search panel. See “Configure the Advanced Search Window” in Chapter 17 of *SAS Social Network Analysis Server: Administration Guide* for additional information.


Appendixes

Appendix 1

Perform Post-Migration Steps .................................................. 135

Appendix 2

Upgrading to the First Maintenance Release
of Version 3.1 ........................................................................ 139

Appendix 3

Perform Post-Upgrade Steps for Databases ............................. 145
Appendix 1

Perform Post-Migration Steps

Understanding SAS Migration ................................................................. 135

Migration Preparation ............................................................................. 136
  Data Stored Outside the SAS Configuration Directory ...................... 136

Perform Migration .................................................................................... 137

Understanding SAS Migration

Migration is a process in which your SAS content and configuration from an earlier SAS release is upgraded to run in a later SAS release. When performed successfully, migration attempts to preserve as much of your current content and configuration as possible, reduce the number of manual migration tasks, and minimize system downtime.

SAS provides the following tools to automate most of the tasks necessary to migrate to SAS 9.3:

- SAS Migration Utility
- SAS Deployment Wizard

The SAS Migration Utility is a cross-platform framework and set of SAS product extensions whose primary purpose is to create a package of content from an earlier SAS version and configuration that the SAS Deployment Wizard will use when it installs and configures SAS 9.3.
The SAS Deployment Wizard is a cross-platform utility that installs and initially configures SAS 9.3 products. Using a SAS installation data file and a deployment plan for its initial input, the wizard is designed to prompt the customer for all the remaining input at the start of the session so that the customer does not have to monitor an entire deployment. During a migration, the wizard reads the migration package created by the SAS Migration Utility and upgrades SAS content and configuration to run in SAS 9.3.

Before you begin a SAS software migration, read and make sure you understand the information in the following sources:

- the installation preparation sections of this document, specifically “Prepare for SAS Installation” on page 17. Make sure that you are familiar with requirements and any procedural changes needed as a result of the version 3.1 deployment.

## Migration Preparation

### Data Stored Outside the SAS Configuration Directory

There are many vital assets stored outside of the SAS configuration directory that are not migrated. For example:

- SAS Financial Crimes Monitor Alert table must be recreated.
- Any enrichment code must be manually moved.
- SAS Financial Crimes Monitor SLIB contents and the prep table data must be manually moved.
Perform Migration

To learn about the features provided by the update, see the “What's New in the SAS Social Network Analysis Server 3.1” chapter in the SAS Social Network Analysis Server: Administration Guide.

To migrate from the first maintenance release of SAS Financial Crimes Monitor 2.3 and SAS Social Network Analysis Server 2.3 to the first maintenance release of version 3.1, follow these steps:

1. Review the bimig documentation recommended in “Understanding SAS Software Updates” on page 139 and make a note of all relevant items pertaining to your deployment as directed in “Prepare for SAS Installation” on page 17.


3. Perform all tasks indicated in the Instructions.html file.

4. Refer to Chapter 9, “Perform Post-Installation Steps for SAS Financial Crimes Monitor,” on page 65 to complete any additional post-installation (administration) steps, such as confirming the LIBNAME statement, reconfiguring for Parallel Processing (optional).

5. Refer to Chapter 10, “Perform Post-Installation Steps for SAS Social Network Analysis Server,” on page 71 to complete any additional post-installation (administration) steps, such as importing SAS Stored Processes and deploying web services.

6. Refer to Chapter 11, “Set Up the SAS Financial Crimes Monitor,” on page 103 to complete any additional post-installation (administration) steps, such as setting up connection information to the metadata repository, modifying UNIX directory and file permissions for the trusted user account, or performing tasks specific to deployment using the WebSphere Application Server with IBM DB2 on AIX.
Refer to Appendix 3, “Perform Post-Upgrade Steps for Databases,” on page 145 in order to upgrade the database.
Appendix 2

Upgrading to the First Maintenance Release of Version 3.1

Understanding SAS Software Updates ........................................... 139

Maintenance Release Update Preparation ................................. 141
  Gather Information from Existing Deployment ..................... 141
  Be Prepared to Restore Customizations ............................... 141
  Rename or Relocate Files .................................................. 142

Applying the Maintenance Release ........................................... 142

Understanding SAS Software Updates

The SAS Deployment Wizard is the mechanism through which SAS software updates are initiated. If product updates are required when the SAS Deployment Wizard is launched, the SAS Deployment Wizard goes into Update mode. This enables updates to be applied to installed software. New software is not installed during the update procedure. After the updates have been applied, the SAS Deployment Wizard allows selection of the configuration directory to which to apply the maintenance release.
Before you begin a SAS software update, read and make sure you understand the information in the following sources:

- the installation preparation sections of this document, specifically “Prepare for SAS Installation” on page 17. Make sure that you are familiar with requirements and any procedural changes needed as a result of the version 3.1 deployment.


Completing the installation and configuration procedure for the upgrade enables you to launch each application from the designated web address. You might, however, have to perform post-installation procedures, as described in Chapter 9, “Perform Post-Installation Steps for SAS Financial Crimes Monitor,” on page 65 and Chapter 10, “Perform Post-Installation Steps for SAS Social Network Analysis Server,” on page 71.
Maintenance Release Update Preparation

To complete the upgrade to version 3.1, you will have to resupply some information that was provided for the version 2.3 deployment. You might also have to reconfigure features that were customized for the version 2.3 installation (for example, re-implement geographic map services), and you might have to perform manual steps during the maintenance update if your environment requires manual configuration either during or after the SAS Deployment Wizard installation and configuration process. You must also upgrade your database content. For more information, see Appendix 3, “Perform Post-Upgrade Steps for Databases,” on page 145. The following sections outline the considerations for preparing to update.

Gather Information from Existing Deployment

When you used the SAS Deployment Manager to install and configure version 2.3 of the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server, you either accepted the default schemas when prompted or you indicated your preferred schemas. To apply the maintenance update, you must specify the same schema information as you did in the version 2.3 installation and configuration.

Make sure you have this information available for the maintenance update.

**CAUTION! Incorrect specification of schemas results in a deployment failure.** During the maintenance upgrade, if you do not specify the correct information during the installation and configuration, a deployment failure results and you will not be able to run the affected solution.

Be Prepared to Restore Customizations

You can customize the deployment of the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server to provide optimum solutions for your intended purpose. If the solutions were customized, it is possible that some of the customizations might be overwritten. For example, if your SAS Social Network Analysis Server 2.3 instance...
implemented the optional Comments or Geographic Map feature, then you will have to re-implement those features before they can be used again.

**Rename or Relocate Files**

With the first maintenance release of the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server, you can perform either an initial installation or you can upgrade from version 2.3. During the SAS Deployment Wizard installation and configuration process, directories are created and files are added to the directories. In some instances, if the files already exist, the new files will not overwrite the existing files. This will result in an unsuccessful upgrade. Therefore, before you begin the upgrade procedure, you must relocate or rename certain files as follows:

1. Navigate to the following directory:
   - **UNIX Specifics:** `<SASHome>/SASFoundation/9.3/sasstp/snamva/
   - **Windows Specifics:** `<SASHome>\SASFoundation\9.3\snamva\sasstp`

2. Rename or relocate the following files:
   - `getSubAlerts.sas`
   - `getActionableEntities.sas`
   - `getMoreSocialNetworkNodesAndLinks.sas`
   - `getSocialNetworkNodesAndLinks.sas`

---

**Applying the Maintenance Release**

Applying the maintenance release for the SAS Financial Crimes Monitor and the SAS Social Network Analysis Server updates your current version of 2.3 to version 3.1 of the offerings. To learn about the features provided by this update, see the “What's New in the SAS Social Network Analysis Server 3.1” chapter in the SAS Social Network Analysis Server: Administration Guide.
To apply version 3.1:

1. Review the documentation recommended in “Understanding SAS Software Updates” on page 139 and make a note of all relevant items pertaining to your deployment as directed in “Prepare for SAS Installation” on page 17.

2. Rename or relocate the appropriate files as directed in “Rename or Relocate Files” on page 142.


   Keep the following in mind as you perform the installation and configuration for the maintenance release:

   - During the process, the SAS Deployment Wizard launches in Update mode to facilitate performing any updates.
   - The SAS Deployment Manager opens to guide you through the configuration steps for the maintenance update.
   - As phases of the configuration procedure are completed for the maintenance application, updateinstructions.html files are presented and provide post-installation instructions that must be performed.

4. Perform all instructions indicated in the updateinstructions.html files.

5. Refer to Chapter 9, “Perform Post-Installation Steps for SAS Financial Crimes Monitor,” on page 65 to complete any additional post-installation (administration) steps, such as confirming the LIBNAME statement, reconfiguring for Parallel Processing (optional).

6. Refer to Chapter 10, “Perform Post-Installation Steps for SAS Social Network Analysis Server,” on page 71 to complete any additional post-installation (administration) steps, if you have previously deployed the Template.spk package, please carefully review the section “Import SAS Stored Processes and Deploy Web Services” on page 73 for more information about adding the message parameter.
7 Refer to Chapter 11, “Set Up the SAS Financial Crimes Monitor,” on page 103 to complete any additional post-installation (administration) steps such as setting up connection information to the metadata repository, modifying UNIX directory and file permissions for the trusted user account or performing tasks specific to deployment using the WebSphere Application Server with IBM DB2 on AIX.

8 Refer to Appendix 3, “Perform Post-Upgrade Steps for Databases,” on page 145 in order to upgrade the database.
Appendix 3

Perform Post-Upgrade Steps for Databases

Overview of Post-Upgrade Steps for Databases ........................................ 146
Upgrade Approach ....................................................................................... 146
Prerequisites and Environments .................................................................. 147
  Overview of Prerequisites and Environments ........................................ 147
  Oracle ...................................................................................................... 148
  DB2 ........................................................................................................ 148
  MySQL ................................................................................................... 148
  Microsoft SQL Server ............................................................................ 149
Restoring Customizations ......................................................................... 149
Upgrade and Alter Scripts .......................................................................... 149
Data Migration Scripts ............................................................................... 150
  Overview of Data Migration Scripts ..................................................... 150
  More about Data Migration Scripts ..................................................... 151
  Running a Script .................................................................................... 152
  Rerunning a Script ................................................................................ 152
  Oracle Required Database Engine Parameters ................................... 152
  MySQL Required Database Engine Parameters ................................ 153
  DB2 Required Database Engine Parameters ....................................... 153
  ODBC (SQL Server) Required Database Engine Parameters .............. 153
Additional Resources ................................................................................ 154
Overview of Post-Upgrade Steps for Databases

This series of topics describes how to perform the following tasks:

- upgrade your SAS Financial Crimes Monitor 3.1 to the version 3.1 first maintenance release schema
- upgrade or migrate your SAS Financial Crimes Monitor 2.3 first maintenance release schema and data to the version 3.1 first maintenance release schema

The upgrade is a multi-step process. Upgrade and migration paths provided in this guide are available for Oracle, DB2, MySQL and Microsoft SQLServer.

You will have to modify the migration scripts based your data profile.

Data migration in these topics refers to migration of existing data from SAS Financial Crimes Monitor 2.3 first maintenance release to the version 3.1 first maintenance release. Customizations made to the data model are supported.

Upgrade Approach

The recommended data migration approach is to first perform the upgrade steps in a test environment that is a copy of the production environment. The upgrade is a multi-step process.

- If you have installed the SAS Financial Crimes Monitor 3.1 schema, apply the version 3.1 first maintenance release alter scripts to upgrade your schema.
- Edit the migration script by defining your database connection options.
- Migrate and populate the version 3.1 first maintenance release configuration and alert tables.
After SAS Financial Crimes Monitor has been upgraded and your data has been migrated, verify the upgrade and migration results and move the test environment into production. The upgrade scripts do not attempt to decrease the length of any existing columns. Migration includes dropping some tables and columns. Please work in a test environment until you are satisfied with the results.

**Note:** The data migration script applies to the SAS Financial Crimes Monitor 3.1 first maintenance release schema only. It is necessary to apply the alter table scripts provided bring the schema up-to-date.

**Note:** The configuration tables and the alert tables have been separated into two sections in the migration script. This adds to the ease of use in cases where there is a need for one migration and not the other.

---

**Prerequisites and Environments**

**Overview of Prerequisites and Environments**

This section describes the environment, setup, required tools, and processes that are needed for the upgrade and data migration process.

- Begin the upgrade process by preparing a test environment.
- SAS 9.3 must be installed and available.
- The SAS Financial Crimes Monitor 2.3 first maintenance release physical tables must be available on the appropriate database and accessible using the appropriate SAS/ACCESS engine.
- The SAS Financial Crimes Monitor 3.1 first maintenance release physical tables must be available on the appropriate database and accessible using the appropriate SAS/ACCESS engine. For more information, see Chapter 8, “Perform Post-Installation Steps for Databases,” on page 59.
- Verify that all appropriate SAS hot fixes are applied before beginning the deployment. Hot fixes can be obtained from support.sas.com.
Both the SAS Financial Crimes Monitor 2.3 first maintenance release and SAS Financial Crimes Monitor 3.1 first maintenance release schemas must exist.

When performing the migration in a database environment, it might be necessary to adjust some of the environment settings to realize the most efficient system performance. SAS white papers are available that address these issues and can be helpful in setting up a scalable, efficient environment. For more information, see the SAS Technical Papers database at http://support.sas.com/resources/papers/tnote/tnote_database.html.

Oracle

Oracle clients must be installed and available. Ensure that your Oracle tnsnames.ora file contains the appropriate client-side network configuration parameters.


DB2

DB2 clients must be installed and available. Ensure that your installed DB2 is version 9.7 or later and the appropriate client-side network configuration parameters have been set.


MySQL

MySQL clients must be installed and available. Ensure that your MySQL installation contains the appropriate client-side network configuration parameters.


**Microsoft SQL Server**

SQL Server clients must be installed and available. Ensure that your SQL Server installation contains the appropriate client-side network configuration parameters.


---

**Restoring Customizations**

If the SAS Financial Crimes Monitor 2.3 first maintenance release database schema has been customized, it is likely that the customizations will be overwritten.

A suggested means to avoid loss of data, customizations, or schema structure is to create backup, or history, tables.

For example, in Oracle, your statement should resemble the following:

```sql
data FCM.FCM_PROJECT_HIS; set FCM.FCM_PROJECT; run;
data FCM.FCM_SCENARIO_HIS; set FCM.SCENARIO; run;
```

---

**Upgrade and Alter Scripts**

SAS Financial Crimes Monitor 3.1 alter scripts (fcm_alter_script_*_.sql) are available to upgrade the 3.1 database schema to the version 3.1 first maintenance release schema.
The alter scripts are run after the SAS Financial Crimes Monitor 3.1 database installation. The alter scripts modify the physical tables only and do not migrate data.

Scripts are available for each supported database in the following locations:

- **Windows:**
  \[SAS\text{-}install\text{-}dir\fincrmmva\sasmisc\dbmc\ddl\fcm\]

- **UNIX:**
  \[SAS\text{-}install\text{-}dir\misc\fincrmmva\dbmc\ddl\fcm\]

---

**Data Migration Scripts**

**Overview of Data Migration Scripts**

The migration scripts provide a way to update the SAS Financial Crimes Monitor 2.3 first maintenance release schema and data to the new SAS Financial Crimes Monitor 3.1 first maintenance release structures. A primary change to the SAS Financial Crimes Monitor 2.3 first maintenance release schema involves a change to slowly changing dimension columns.

SAS Financial Crimes Monitor 3.1 no longer supports the type-2 slowly changing dimension columns (that is, validity dates). They have been removed. In addition, the SAS Financial Crimes Monitor 3.1 schema migrates the current LOGICAL_RK columns to their respective *_SK columns.

Special consideration needs to be taken with the LOGICAL_RK modifications. In SAS Financial Crimes Monitor 2.3, it was possible to have a LOGICAL_SK value of 0 in the FCM_PROJECT table. In SAS Financial Crimes Monitor 3.1, the LOGICAL_RK values become the PROJECT_SK values. Because primary keys are not allowed to have values of 0, these values need to be changed. The migration script will modify any values of 0 with a value of your choice. Review the current values for the LOGICAL_RK columns in the version 2.3 FCM_PROJECT table and select a value that does not currently exist. Set the macro variable PROJECT_SK_REP to this value.

**Note:** In the script provided, the value "9999" is used to populate a value of 0.
More about Data Migration Scripts

The migration scripts are divided into three distinct parts:

- database connection options
- migration for SAS Financial Crimes Monitor 3.1 first maintenance release configuration tables
- migration for the SAS Financial Crimes Monitor 3.1 first maintenance release alert generation process (AGP) tables

Provide the database-specific library connection information in the `fcm_migration_.sas` script. The migration script has clearly marked the configuration tables and alert tables in separate sections. This makes it easier to migrate all of the tables or just the areas you require. It is your decision to run all or part of the migration script. For example, if you have no need to upgrade the alert tables, simply remove the section called "Populate 3.1 Alert Tables." The configuration table section and the alert table section are independent of each other.

As stated earlier, in the first maintenance release of SAS Financial Crimes Monitor 2.3, it was possible to have a LOGICAL_SK value of 0 in the FCM_PROJECT table. In version 3.1, the LOGICAL_RK values become the PROJECT_SK values. Because primary keys are not allowed to have values of 0, these values need to be changed. You need to look at the current values for LOGICAL_RK in the SAS Financial Crimes Monitor 2.3 first maintenance release FCM_PROJECT table and select a value that does not currently exist. The macro variable PROJECT_SKREP should be set to this value. The script uses the value of 9999 to represent the PROJECT_SK value of 0.

Set the PROJECT_SK replacement value as follows:

```sas
/* Set replacement value for project_sk when equal to 0 */
%let project_sk_rep = 9999;
```

Two libraries are used to distinguish the SAS Financial Crimes Monitor 2.3 first maintenance release schema and the SAS Financial Crimes Monitor 3.1 first maintenance release schema. You will have to provide the database-specific information necessary to connect to the database engine for your installation. Ensure
that the &DBENGINE parameter is set to one of the following values: ODBC, ORACLE, MYSQL, or DB2. Set the DBENGINE value by editing the last line in the program:

```sas
%migrate(dbengine=);
```

For more information, see the required database engine parameters later in this document.

**Running a Script**

After you are satisfied with installations of the SAS Financial Crimes Monitor 2.3 first maintenance release and SAS Financial Crimes Monitor 3.1 first maintenance release, start a SAS session.

Edit the `fcm_migration_.sas` script. The script contains macro parameters for all the supported engines. Provide the library parameters appropriate for your installation. There should be no other edits required, unless you choose not to run both the configuration table and the alert table scripts during the same session.

**Rerunning a Script**

In the event a migration script has to be rerun, it is essential that any affected tables and data should be deleted from the migrated library. Failure to remove the tables can cause undesired behavior.

**Oracle Required Database Engine Parameters**

Here are the required parameters for the Oracle database engine:

```sas
%if ( %sysfunc(upcase(&dbengine;)) = ORACLE ) %then %do;
    %let user=;
    %let password=;
    %let path23=;
    %let schema23=;
    %let path31=;
    %let schema31=;
    libname fcm23 &dbengine; path=&path23; schema=&schema23; user=&user;
    password=&user;
    libname fcm31 &dbengine; path=&path31; schema=&schema31; user=&user;
```

152 Appendix 3 / Perform Post-Upgrade Steps for Databases
MySQL Required Database Engine Parameters

Here are the required parameters for the MySQL database engine:

```sas
%if ( %sysfunc(upcase(&dbengine;)) = MYSQL ) %then %do;
  %let database23=;
  %let database31=;
  %let user=;
  %let password=;
  %let port=;
  %let server=;
libname fcm23 &dbengine; database=&database23; user=&user; password=&password;
  %let port=;
libname fcm31 &dbengine; database=&database31; user=&user; password=&password;
  server="&server";
```

DB2 Required Database Engine Parameters

Here are the required parameters for the DB2 database engine:

```sas
%if ( %sysfunc(upcase(&dbengine;)) = DB2 ) %then %do;
  %let dsn=;
  %let user=;
  %let password=;
  %let schema23=;
  %let schema31=;
libname fcm23 &dbengine; dsn=&dsn23; user=&user; password=&password;
  %let schema23=;
libname fcm31 &dbengine; dsn=&dsn31; user=&user; password=&password;
  schema=&schema23;
```

ODBC (SQL Server) Required Database Engine Parameters

Here are the required parameters for the ODBC database engine:

```sas
%if ( %sysfunc(upcase(&dbengine;)) = ODBC ) %then %do;
  %let datasrc23=;
  %let datasrc31=;
  %let user=;
  %let password=;
```
Additional Resources

The SAS Financial Crimes Monitor package includes the following sets of additional documentation:

- Data dictionary for the SAS Financial Crimes Monitor database
- Data model for the SAS Financial Crimes Monitor database

Schema Changes for SAS Financial Crimes Monitor

Table A3.1  Dropped Table

<table>
<thead>
<tr>
<th>Dropped Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM_ALERT_REMINDER</td>
</tr>
</tbody>
</table>

Table A3.2  New Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Object Referenced</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM_PROJECT_X_PARAMETER</td>
<td></td>
<td>ADDITIONAL TABLE</td>
</tr>
<tr>
<td>FCM_SCENARIO_X_PARAMETER</td>
<td></td>
<td>ADDITIONAL TABLE</td>
</tr>
<tr>
<td>FCM_EXCLUSIONCALENDAR</td>
<td></td>
<td>ADDITIONAL TABLE</td>
</tr>
<tr>
<td>FCM_JOBCALENDAR_HOLIDAY</td>
<td></td>
<td>ADDITIONAL TABLE</td>
</tr>
<tr>
<td>FCM_ALERT_ENRICHMENT_HISTORY</td>
<td></td>
<td>ADDITIONAL TABLE</td>
</tr>
</tbody>
</table>
### Table A3.3  Existing Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Object Referenced</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM_PROJECT</td>
<td>SUPPRESSION_GROUP_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_PROJECT</td>
<td>ROUTING_GROUP_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_PROJECT</td>
<td>PROJ_STATUS_CD</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_PREP_TABLE</td>
<td>PROJECT_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_ENTITY</td>
<td>PROJECT_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>PREP_TABLE_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>ENTITY_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>ENTITY_VAR_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>ROUTING_GROUP_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>Table</td>
<td>Object Referenced</td>
<td>Difference</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>SUPPRESSION_GROUP_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>SCENARIO_GROUP_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>PROJECT_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>SUPPRESSION_GROUP_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>ROUTING_GROUP_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>SG_STATUS_CD</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_SCENARIO_CALC_VAR</td>
<td>SCENARIO_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_ENTITY_VAR</td>
<td>ENTITY_VAR_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_ENTITY_VAR</td>
<td>ENTITY_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_PARAMETER</td>
<td>PROJECT_PARAMETER_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_FORM_ITEM</td>
<td>PARAMETER_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_FORM_ITEM_OPTION</td>
<td>FORM_ITEM_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_ALERT_ENTITY</td>
<td>ENTITY_VAR_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_ALERT_ENRICHMENT</td>
<td>RECORD_VERSION_NO</td>
<td>ADDITIONAL COLUMN</td>
</tr>
</tbody>
</table>
### Table

<table>
<thead>
<tr>
<th>Table</th>
<th>Object Referenced</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM_SCENARIO_BY_VARIABLE</td>
<td>SCENARIO_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>ALERT_SUMMARY</td>
<td>SCENARIO_GROUP_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_JOB CALENDAR</td>
<td>JOB_CALENDAR_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
<tr>
<td>FCM_JOB CALENDAR</td>
<td>PROJECT_SK</td>
<td>ADDITIONAL COLUMN</td>
</tr>
</tbody>
</table>

**Table A3.4  Data Type Changes**

<table>
<thead>
<tr>
<th>Table</th>
<th>Column</th>
<th>Previous Data Type</th>
<th>New Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM_PROJECT</td>
<td>PROJECT_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_PREP_TABLE</td>
<td>PREP_TABLE_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ENTITY</td>
<td>ENTITY_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>SCENARIO_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>SCENARIO_GROUP_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_SCENARIO_CALC_VAR</td>
<td>SCENARIO_CALC_VAR_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_PARAMETER</td>
<td>PARAMETER_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_FORM_ITEM</td>
<td>FORM_ITEM_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_FORM_ITEM_OPTION</td>
<td>FORM_ITEM_OPTION_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT</td>
<td>PROJECT_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
</tbody>
</table>
### Appendix 3 / Perform Post-Upgrade Steps for Databases

<table>
<thead>
<tr>
<th>Table</th>
<th>Column</th>
<th>Previous Data Type</th>
<th>New Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM_ALERT</td>
<td>SCENARIO_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT</td>
<td>ENTITY_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT_ENTITY</td>
<td>ENTITY_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT_ENRICHMENT</td>
<td>PROJECT_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_SCENARIO_BY_VARIABLE</td>
<td>SCENARIO_BY_VARIABLE_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_MANAGED_LIST</td>
<td>MANAGED_LIST_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>ALERT_SUMMARY</td>
<td>SCENARIO_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>ALERT_SUMMARY</td>
<td>PROJECT_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>ALERT_SUMMARY</td>
<td>ENTITY_SK</td>
<td>NUMBER(10)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT</td>
<td>ENTITY_VARIABLE_SK</td>
<td>NUMBER(10)</td>
<td>VARCHAR(64)</td>
</tr>
<tr>
<td>FCM_ALERT_ENTITY</td>
<td>ENTITY_VARIABLE_SK</td>
<td>NUMBER(10)</td>
<td>VARCHAR(64)</td>
</tr>
<tr>
<td>ALERT_SUMMARY</td>
<td>ENTITY_VARIABLE_SK</td>
<td>NUMBER(10)</td>
<td>VARCHAR(64)</td>
</tr>
<tr>
<td>FCM_ALERT_ENTITY</td>
<td>ALERT_ENTITY_SK</td>
<td>NUMERIC(19)</td>
<td>NUMBER(20)</td>
</tr>
<tr>
<td>FCM_ALERT</td>
<td>ALERT_SK</td>
<td>NUMERIC(19)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT_COMMENT</td>
<td>COMMENT_SK</td>
<td>NUMERIC(19)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT_COMMENT</td>
<td>ALERT_SK</td>
<td>NUMERIC(19)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT_DOCUMENT</td>
<td>DOCUMENT_SK</td>
<td>NUMERIC(19)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT_DOCUMENT</td>
<td>FCM_ALERT_DOCUMENT_SK</td>
<td>NUMERIC(19)</td>
<td>NUMERIC(20)</td>
</tr>
</tbody>
</table>
### Table

<table>
<thead>
<tr>
<th>Table</th>
<th>Column</th>
<th>Previous Data Type</th>
<th>New Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM_ALERT_EMAIL</td>
<td>EMAIL_SK</td>
<td>NUMERIC(19)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT_EMAIL</td>
<td>ALERT_SK</td>
<td>NUMERIC(19)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT_EVENT</td>
<td>EVENT_SK</td>
<td>NUMERIC(19)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT_EVENT</td>
<td>ALERT_SK</td>
<td>NUMERIC(19)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT_ENRICHMENT</td>
<td>ALERT_ENRICHMENT_SK</td>
<td>NUMERIC(19)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT_ENRICHMENT</td>
<td>ALERT_SK</td>
<td>NUMERIC(19)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>ALERT_SUMMARY</td>
<td>ALERT_SK</td>
<td>NUMERIC(19)</td>
<td>NUMERIC(20)</td>
</tr>
<tr>
<td>FCM_ALERT_ENTITY</td>
<td>SEGMENT_ID</td>
<td>VARCHAR(128)</td>
<td>VARCHAR2(128)</td>
</tr>
<tr>
<td>FCM_PROJECT</td>
<td>RECIPIENT_ID</td>
<td>VARCHAR(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_FORM_ITEM</td>
<td>CREATED_USER_ID</td>
<td>VARCHAR(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_FORM_ITEM</td>
<td>MODIFIED_USER_ID</td>
<td>VARCHAR(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_FORM_ITEM_OPTION</td>
<td>CREATED_USER_ID</td>
<td>VARCHAR(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_FORM_ITEM_OPTION</td>
<td>MODIFIED_USER_ID</td>
<td>VARCHAR(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_ALERT</td>
<td>RECIPIENT_ID</td>
<td>VARCHAR(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>ALERT_SUMMARY</td>
<td>RECIPIENT_ID</td>
<td>VARCHAR(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_PROJECT</td>
<td>ALERT_TEMPLATE_DATASET_NM</td>
<td>VARCHAR(40)</td>
<td>VARCHAR(255)</td>
</tr>
<tr>
<td>ALERT_SUMMARY</td>
<td>SCENARIO_DESC</td>
<td>VARCHAR2(100)</td>
<td>VARCHAR2(1000)</td>
</tr>
<tr>
<td>Table</td>
<td>Column</td>
<td>Previous Data Type</td>
<td>New Data Type</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------</td>
<td>--------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>ALERT_SUMMARY</td>
<td>SCENARIO_NM</td>
<td>VARCHAR2(100)</td>
<td>VARCHAR2(255)</td>
</tr>
<tr>
<td>FCM_PROJECT</td>
<td>CREATED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_PROJECT</td>
<td>MODIFIED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_PREP_TABLE</td>
<td>CREATED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_PREP_TABLE</td>
<td>MODIFIED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_ENTITY</td>
<td>CREATED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_ENTITY</td>
<td>MODIFIED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>RECIPIENT_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>CREATED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>MODIFIED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>RECIPIENT_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>CREATED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>MODIFIED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_SCENARIO_CALC_VAR</td>
<td>CREATED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_SCENARIO_CALC_VAR</td>
<td>MODIFIED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_ENTITY_VAR</td>
<td>CREATED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_ENTITY_VAR</td>
<td>MODIFIED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
<tr>
<td>FCM_PARAMETER</td>
<td>CREATED_USER_ID</td>
<td>VARCHAR2(32)</td>
<td>VARCHAR(60)</td>
</tr>
</tbody>
</table>
### Table A.3.5  Dropped Columns

<table>
<thead>
<tr>
<th>Table</th>
<th>Dropped Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALERT_SUMMARY</td>
<td>VALID_FROM_DTTM</td>
</tr>
<tr>
<td>ALERT_SUMMARY</td>
<td>VALID_TO_DTTM</td>
</tr>
<tr>
<td>FCM_MANAGED_LIST</td>
<td></td>
</tr>
<tr>
<td>FCM_MANAGED_LIST</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>Dropped Column</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>FCM_ALERT_ENRICHMENT</td>
<td>RECIPIENT_ID</td>
</tr>
<tr>
<td>FCM_ALERT_ENRICHMENT</td>
<td>RECIPIENT_TYPE_CD</td>
</tr>
<tr>
<td>FCM_ENTITY</td>
<td>VALID_FROM_DTTM</td>
</tr>
<tr>
<td>FCM_ENTITY</td>
<td>VALID_TO_DTTM</td>
</tr>
<tr>
<td>FCM_ENTITY</td>
<td>LOGICAL_DELETE_FLG</td>
</tr>
<tr>
<td>FCM_ENTITY_VAR</td>
<td>ENTITY_VARIABLE_SK</td>
</tr>
<tr>
<td>FCM_ENTITY_VAR</td>
<td>VALID_FROM_DTTM</td>
</tr>
<tr>
<td>FCM_ENTITY_VAR</td>
<td>VALID_TO_DTTM</td>
</tr>
<tr>
<td>FCM_ENTITY_VAR</td>
<td>LOGICAL_DELETE_FLG</td>
</tr>
<tr>
<td>FCM_FORM_ITEM</td>
<td>VALID_FROM_DTTM</td>
</tr>
<tr>
<td>FCM_FORM_ITEM</td>
<td>VALID_TO_DTTM</td>
</tr>
<tr>
<td>FCM_FORM_ITEM</td>
<td>LOGICAL_DELETE_FLG</td>
</tr>
<tr>
<td>FCM_FORM_ITEM_OPTION</td>
<td>VALID_FROM_DTTM</td>
</tr>
<tr>
<td>FCM_FORM_ITEM_OPTION</td>
<td>VALID_TO_DTTM</td>
</tr>
<tr>
<td>FCM_FORM_ITEM_OPTION</td>
<td>LOGICAL_DELETE_FLG</td>
</tr>
<tr>
<td>FCM_JOBCALENDAR</td>
<td>JOB CALENDAR_ID</td>
</tr>
<tr>
<td>FCM_MANAGED_LIST</td>
<td>VALID_FROM_DTTM</td>
</tr>
<tr>
<td>FCM_MANAGED_LIST</td>
<td>VALID_TO_DTTM</td>
</tr>
<tr>
<td>FCM_MANAGED_LIST</td>
<td>LOGICAL_DELETE_FLG</td>
</tr>
<tr>
<td>FCM_PARAMETER</td>
<td>VALID_FROM_DTTM</td>
</tr>
<tr>
<td>Table</td>
<td>Dropped Column</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>FCM_PARAMETER</td>
<td>VALID_TO_DTTM</td>
</tr>
<tr>
<td>FCM_PARAMETER</td>
<td>LOGICAL_DELETE_FLG</td>
</tr>
<tr>
<td>FCM_PREP_TABLE</td>
<td>VALID_FROM_DTTM</td>
</tr>
<tr>
<td>FCM_PREP_TABLE</td>
<td>VALID_TO_DTTM</td>
</tr>
<tr>
<td>FCM_PREP_TABLE</td>
<td>LOGICAL_DELETE_FLG</td>
</tr>
<tr>
<td>FCM_PROJECT</td>
<td>RUN_FREQUENCY_TYPE_CD</td>
</tr>
<tr>
<td>FCM_PROJECT</td>
<td>VALID_FROM_DTTM</td>
</tr>
<tr>
<td>FCM_PROJECT</td>
<td>VALID_TO_DTTM</td>
</tr>
<tr>
<td>FCM_PROJECT</td>
<td>LOGICAL_DELETE_FLG</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>VALID_FROM_DTTM</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>VALID_TO_DTTM</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>LOGICAL_DELETE_FLG</td>
</tr>
<tr>
<td>FCM_SCENARIO_BY_VARIABLE</td>
<td>VALID_FROM_DTTM</td>
</tr>
<tr>
<td>FCM_SCENARIO_BY_VARIABLE</td>
<td>VALID_TO_DTTM</td>
</tr>
<tr>
<td>FCM_SCENARIO_BY_VARIABLE</td>
<td>LOGICAL_DELETE_FLG</td>
</tr>
<tr>
<td>FCM_SCENARIO_CALC_VAR</td>
<td>VALID_FROM_DTTM</td>
</tr>
<tr>
<td>FCM_SCENARIO_CALC_VAR</td>
<td>VALID_TO_DTTM</td>
</tr>
<tr>
<td>FCM_SCENARIO_CALC_VAR</td>
<td>LOGICAL_DELETE_FLG</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>RUN_FREQUENCY_TYPE_CD</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>VALID_FROM_DTTM</td>
</tr>
</tbody>
</table>
### Table A3.6  Column Null Modifications

<table>
<thead>
<tr>
<th>Table</th>
<th>Column</th>
<th>NULL to NOT NULL</th>
<th>NOT NULL to NULL</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM_ALERT</td>
<td>RECORD_VERSION_NO</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>FCM_ALERT_ENTITY</td>
<td>RECORD_VERSION_NO</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>FCM_ALERT_ENRICHMENT</td>
<td>PROJECT_SK</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FCM_JOBCALENDAR</td>
<td>CALENDAR_DT</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FCM_PROJECT</td>
<td>SEGMENT_ID</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FCM_ENTITY</td>
<td>SEGMENT_ID</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>SEGMENT_ID</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FCM_ENTITY_VAR</td>
<td>SEGMENT_ID</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FCM_ALERT_ENTITY</td>
<td>ENTITY_SK</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FCM_SCENARIO_BY_VARIABLE</td>
<td>SEGMENT_ID</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FCM_JOBCALENDAR</td>
<td>MONTHLY_RUN_FLG</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Table A3.7  Modifications to Foreign Keys and Relationships

<table>
<thead>
<tr>
<th>Table and Column</th>
<th>Column Defined By</th>
<th>Column References</th>
<th>Foreign Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM_ENTITY</td>
<td>FCM_ENTITY</td>
<td>FCM_PROJECT</td>
<td>Dropped</td>
</tr>
<tr>
<td>XIF3FCM_ENTITY</td>
<td></td>
<td>FCM_PROJECT(LOGICAL_RK)</td>
<td></td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>FCM_SCENARIO</td>
<td>FCM_PROJECT</td>
<td></td>
</tr>
<tr>
<td>INDEX_XIF1FCM_SCENARIO</td>
<td>FCM_SCENARIO(SCENARIO_GROUP_RK)</td>
<td>FCM_SCENARIO_GROUP(LOGICAL_RK)</td>
<td>Dropped</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FCM_ENTITY</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FCM_ENTITY_VAR</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FCM_ENTITY_VAR(LOGICAL_RK)</td>
<td></td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>FCM_SCENARIO</td>
<td>FCM_PROJECT</td>
<td></td>
</tr>
<tr>
<td>INDEX_XIF2FCM_SCENARIO</td>
<td>FCM_SCENARIO_GROUP(PROJECT_RK)</td>
<td>FCM_PROJECT(LOGICAL_RK)</td>
<td>Dropped</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>FCM_SCENARIO_GROUP</td>
<td>FCM_PROJECT</td>
<td></td>
</tr>
<tr>
<td>XIF2FCM_SCENARIO_GROUP</td>
<td></td>
<td>FCM_PROJECT(LOGICAL_RK)</td>
<td></td>
</tr>
<tr>
<td>FCM_SCENARIO_CALC_VAR</td>
<td>FCM_SCENARIO_CALC_VAR(SCENARIO_RK)</td>
<td>FCM_SCENARIO</td>
<td>Dropped</td>
</tr>
<tr>
<td>XIF1FCM_CALCULATED_FIELD</td>
<td></td>
<td>FCM_SCENARIO</td>
<td></td>
</tr>
<tr>
<td>FCM_PARAMETER</td>
<td>FCM_PARAMETER</td>
<td>FCM_PARAMETER</td>
<td>Dropped</td>
</tr>
<tr>
<td>XIF4FCM_PARAMETER</td>
<td></td>
<td>FCM_PARAMETER</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FCM_PARAMETER(LOGICAL_RK)</td>
<td></td>
</tr>
<tr>
<td>FCM_ALERT</td>
<td>FCM_ALERT</td>
<td>FCM_ALERT</td>
<td>Dropped</td>
</tr>
<tr>
<td>XIF8FCM_ALERT</td>
<td></td>
<td>FCM_ALERT</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ENTITY(Entity_SK, ENTITY_VARIABLE_SK)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ENTITY(Entity_SK, ENTITY_VARIABLE_SK)</td>
<td></td>
</tr>
<tr>
<td>FCM_ALERT</td>
<td>FCM_ALERT</td>
<td>FCM_PROJECT</td>
<td>Dropped</td>
</tr>
<tr>
<td>FK1_ALERT</td>
<td></td>
<td>FCM_PROJECT</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(PROJECT_SK)</td>
<td></td>
</tr>
<tr>
<td>FCM_ALERT</td>
<td>FCM_ALERT</td>
<td>FCM_ALERT</td>
<td>Dropped</td>
</tr>
<tr>
<td>R_273</td>
<td></td>
<td>FCM_ALERT</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(ALERT_SK)</td>
<td></td>
</tr>
<tr>
<td>Table and Column</td>
<td>Column Defined By</td>
<td>Column References</td>
<td>Foreign Key</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>FCM_ALERT_ENRICHMENT</td>
<td>FCM_ALERT_ENRICHMENT(PROJECT_SK)</td>
<td>FCM_ALERT(PROJECT_SK)</td>
<td>Dropped</td>
</tr>
<tr>
<td>XIF2FCM_ALERT_ENRICHMENT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCM_ENTITY</td>
<td>FCM_ENTITY(PROJECT_SK)</td>
<td>FCM_PROJECT(PROJECT_SK)</td>
<td>Added</td>
</tr>
<tr>
<td>XIF1FCM_ENTITY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>FCM_SCENARIO(SCENARIO_GROUP_SK)</td>
<td>FCM_SCENARIO_GROUP(SCENARIO_GROUP_SK)</td>
<td>Added</td>
</tr>
<tr>
<td>XIF14FCM_SCENARIO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>FCM_SCENARIO(ENTITY_SK)</td>
<td>FCM_ENTITY(ENTITY_SK)</td>
<td>Added</td>
</tr>
<tr>
<td>XIF15FCM_SCENARIO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>FCM_SCENARIO(ENTITY_VAR_SK)</td>
<td>FCM_ENTITY_VAR(ENTITY_VAR_SK)</td>
<td>Added</td>
</tr>
<tr>
<td>XIF16FCM_SCENARIO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>FCM_SCENARIO(PREP_TABLE_SK)</td>
<td>FCM_PREP_TABLE(PREP_TABLE_SK)</td>
<td>Added</td>
</tr>
<tr>
<td>XIF17FCM_SCENARIO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>FCM_SCENARIO_GROUP(PROJECT_SK)</td>
<td>FCM_PROJECT(PROJECT_SK)</td>
<td>Added</td>
</tr>
<tr>
<td>XIF1FCM_SCENARIO_GROUP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCM_SCENARIO_CALC_VAR</td>
<td>FCM_SCENARIO_CALC_VAR(SCENARIO.SK)</td>
<td>FCM_SCENARIO(SCENARIO.SK)</td>
<td>Added</td>
</tr>
<tr>
<td>XIF1FCM_SCENARIO_CALC_VAR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCM_PARAMETER</td>
<td>FCM_PARAMETER(PROJECT_PARAMETER_SK)</td>
<td>FCM_PARAMETER(PARAMETER_SK)</td>
<td>Added</td>
</tr>
<tr>
<td>XIF1FCM_PARAMETER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table and Column

<table>
<thead>
<tr>
<th>Table and Column</th>
<th>Column Defined By</th>
<th>Column References</th>
<th>Foreign Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM_ALERT_ENTITY XIF1FCM_ALERT_ENTITY</td>
<td>FCM_ALERT_ENTITY(ENTITY_VAR_SK)</td>
<td>FCM_ENTITY_VAR(ENTITY_VAR_SK)</td>
<td>Added</td>
</tr>
<tr>
<td>FCM_ALERT_ENTITY XIF2FCM_ALERT_ENTITY</td>
<td>FCM_ALERT_ENTITY(ENTITY_SK)</td>
<td>FCM_ENTITY(ENTITY_SK)</td>
<td>Added</td>
</tr>
<tr>
<td>FCM_JOB CALENDAR XIF1FCM_JOB CALENDAR</td>
<td>FCM_JOB CALENDAR(PROJECT_SK)</td>
<td>FCM_PROJECT(PROJECT_SK)</td>
<td>Added</td>
</tr>
</tbody>
</table>

### Table A3.8  Renamed Columns

<table>
<thead>
<tr>
<th>Table</th>
<th>Renamed Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM_PROJECT</td>
<td>ROUTING_GROUP_RK</td>
</tr>
<tr>
<td>FCM_PROJECT</td>
<td>SUPPRESSION_GROUP_RK</td>
</tr>
<tr>
<td>FCM_ENTITY</td>
<td>PROJECT_RK</td>
</tr>
<tr>
<td>FCM_ENTITY</td>
<td>LOGICAL_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>PREP_TABLE_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>ENTITY_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>ENTITY_VARIABLE_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>SCENARIO_GROUP_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>ROUTING_GROUP_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>SUPPRESSION_GROUP_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>PROJECT_RK</td>
</tr>
<tr>
<td>Table</td>
<td>Renamed Column</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>ROUTING_GROUP_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>SUPPRESSION_GROUP_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO_CALC_VAR</td>
<td>SCENARIO_RK</td>
</tr>
<tr>
<td>FCM_ENTITY_VAR</td>
<td>ENTITY_RK</td>
</tr>
<tr>
<td>FCM_PARAMETER</td>
<td>PROJECT_PARAMETER_RK</td>
</tr>
<tr>
<td>FCM_FORM_ITEM</td>
<td>PARAMETER_RK</td>
</tr>
<tr>
<td>FCM_FORM_ITEM_OPTION</td>
<td>FORM_ITEM_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO_BY_VARIABLE</td>
<td>SCENARIO_RK</td>
</tr>
<tr>
<td>ALERT_SUMMARY</td>
<td>SCENARIO_GROUP_RK</td>
</tr>
<tr>
<td>ALERT_SUMMARY</td>
<td>PROJECT_RK</td>
</tr>
<tr>
<td>FCM_PREP_TABLE</td>
<td>PROJECT_RK</td>
</tr>
<tr>
<td>FCM_PARAMETER</td>
<td>PARENT_RK</td>
</tr>
</tbody>
</table>

Table A3.9  LOGICAL_RK Columns Migrated and Dropped

<table>
<thead>
<tr>
<th>Table</th>
<th>Dropped Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM_PREP_TABLE</td>
<td>LOGICAL_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO</td>
<td>LOGICAL_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO_GROUP</td>
<td>LOGICAL_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO_CALC_VAR</td>
<td>LOGICAL_RK</td>
</tr>
<tr>
<td>FCM_ENTITY_VAR</td>
<td>LOGICAL_RK</td>
</tr>
<tr>
<td>Table</td>
<td>Dropped Column</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>FCM_PARAMETER</td>
<td>LOGICAL_RK</td>
</tr>
<tr>
<td>FCM_FORM_ITEM</td>
<td>LOGICAL_RK</td>
</tr>
<tr>
<td>FCM_FORM_ITEM_OPTION</td>
<td>LOGICAL_RK</td>
</tr>
<tr>
<td>FCM_SCENARIO_BY_VARIABLE</td>
<td>LOGICAL_RK</td>
</tr>
<tr>
<td>FCM_MANAGED_LIST</td>
<td>LOGICAL_RK</td>
</tr>
<tr>
<td>FCM_PROJECT</td>
<td>LOGICAL_RK</td>
</tr>
</tbody>
</table>
Index

A
anonymous web access 43
architecture, system 5
audience 3

C
configuration
DB2 databases 28
Microsoft SQL Server 30
middle tier 48
MySQL databases 26
Oracle databases 24
overview 8, 37
post-installation for SAS 57
results 11
running SAS Deployment Wizard 42

D
data models 6
database administrator 4
databases
configuring DB2 databases 28

configuring Microsoft SQL Server 30
configuring MySQL databases 26
configuring Oracle databases 24
creating tables 62
JDBC drivers 33, 50
post-installation setup 59
DB2 databases
configuring 28

E
error, configuration
running SAS Deployment Wizard 53

F
FINCRMDB data model 6

G
groups
adding an investigator group 80
assigning to Financial Crimes Monitor: Admin role 68

IBM Websphere Application Server 19

installation
creating database user IDs 31
creating system user IDs 18
overview 8, 37
pre-installation requirements 17, 21
results 11
running SAS Deployment Wizard 40
SAS Intelligence Platform 22
investigator access 80

Java Development Kit (JDK) 19
JBoss Application Server 19
JDBC drivers 33, 50
JUnit 21

LIBNAME statement 66

Microsoft SQL Server
configuring 30
middle tier configuration 48
MySQL databases
configuring 26

Oracle databases
configuring 24
Oracle WebLogic Server 19

post-installation
creating database tables 62
databases 59
deploying stored processes 76
importing stored processes 73
initializing users and groups 68, 80
overview 8
results 11
SAS Social Network Analysis Server 73
tasks for SAS 57
verifying LIBNAME statement 66
pre-installation requirements
17, 21

requirements for pre-installing
SAS 17

SAS administrator 4
SAS Deployment Wizard
configuration error 53
running in configure mode 42
running in install mode 40
SAS Financial Crimes Monitor
overview, groups 105
overview, memberships 105
overview, roles 105
overview, setup 104, 113
setup 113, 116
setup example 109
special considerations 113, 116
system architecture 5
SAS Intelligence Platform 22
SAS Social Network Analysis
Server
setup 131
system architecture 5
SAS Technical Support 4
SASSNADS data model 7
setup

SAS Financial Crimes Monitor
113, 116
SAS Social Network Analysis
Server 131
special considerations 113
stored processes
deploying as web service 76
importing 73
support 4
system administrator 4
system architecture 5

tables
creating for databases 62

user IDs
See also users
creating for databases 31
creating for system 18
users
access for administrative
users 68
access for investigator users 80

web access, anonymous 43
web application servers 19
web service

deploying stored processes as

76