SAS® Credit Risk Management for Banking 4.5

Installation Guide

The correct bibliographic citation for this manual is as follows: SAS Institute Inc. 2007. *SAS® Credit Risk Management for Banking 4.5: Installation Guide*. Cary, NC: SAS Institute Inc.

SAS® Credit Risk Management for Banking 4.5: Installation Guide

SAS Institute Inc., SAS Campus Drive, Cary, North Carolina 27513.

1st electronic book, November 2007

SAS® Publishing provides a complete selection of books and electronic products to help customers use SAS software to its fullest potential. For more information about our e-books, e-learning products, CDs, and hard-copy books, visit the SAS Publishing Web site at **support.sas.com/pubs** or call 1-800-727-3228.

Contents

Chapter 1

Introduction

Contents

Audience

This documentation is intended for SAS-trained implementation consultants who are responsible for the installation of SAS Credit Risk Management for Banking. Therefore, the scope of this documentation is limited primarily to the administrative tasks that these users are likely to perform. Moreover, this documentation assumes familiarity with the technical terminology and concepts that are required to perform these tasks.

Where to Find Documentation and More Information

Information about the hardware, software, and database requirements of SAS Credit Risk Management for Banking, as well as links to other sources of related information, is located in the SAS Foundation system requirements documentation for your operating system.

Once you have installed SAS Credit Risk Management for Banking, the following additional documents can be found in PDF format in the `SAS_HOME\Documentation\9.1\en\crriskugpdf.hlp` directory:

- *SAS Credit Risk Management for Banking: Administrator's Guide*
- *SAS Credit Risk Management for Banking: User's Guide*

There are additional documents in this directory in PDF format. It is useful to navigate these many documents using the file `index.htm` which is located in the same directory.

In addition, the *SAS Credit Risk Management for Banking: Installation Guide* can be found in PDF format in the *<install-dir>*`/Config/`*locale* directory. The most recent version of this document, including any late-breaking changes, is located at `http://support.sas.com`.

Some of the tasks that are outlined in this document require that you configure third party software. For detailed instructions about how to complete tasks in a third party product, see that product's documentation. For additional information about third party configuration options that are specific to SAS, see the third party software reference information that is located at http://support.sas.com.

For information about support fixes, see the SAS Notes that are available on the SAS Technical Support Web site. Search for available SAS Notes for SAS Credit Risk Management for Banking at http://support.sas.com.

Chapter 2

Overview of Installation

Contents

The SAS Credit Risk Management for Banking Architecture

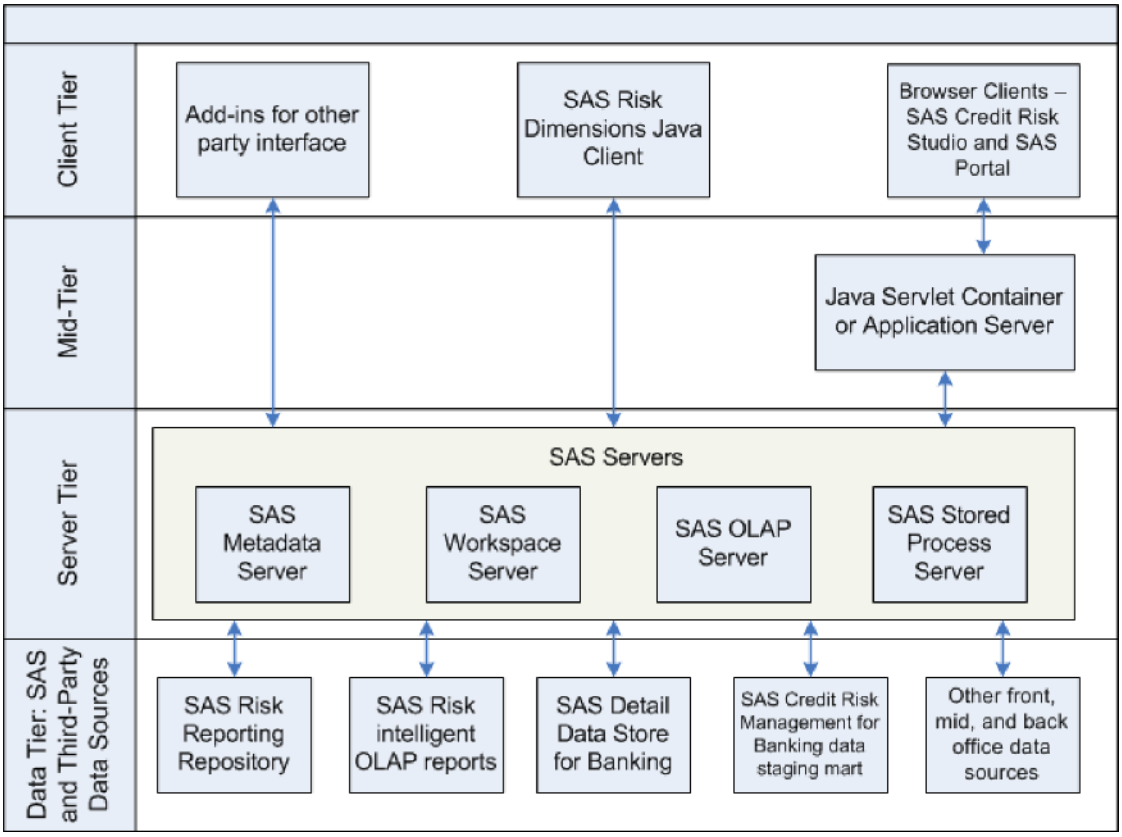
SAS Credit Risk Management for Banking operates in a four-tiered environment. Your existing credit risk data that is maintained in the SAS Detail Data Store for Banking and the credit risk reporting data that is maintained in the SAS Risk Reporting Repository is stored on a data source tier. This data is used by the SAS Credit Risk Management for Banking software components that you install and configure on a server tier and a middle tier. To perform daily credit risk management activities, users can access SAS Credit Risk Studio, a Web application, from machines that are part of a client tier. It is possible to host all tiers on the same machine. However, typically the data source tier, server tier, middle tier, and the client tier are hosted on separate machines. In addition, because the Web application requires little more than access to a Web browser, the client tier can include a number of machines across your organization.

The server tier consists of a set of SAS servers that are installed as a part of the SAS Intelligence Platform. These servers host the credit risk and reporting data and execute SAS analytical and reporting processes. The server tier also hosts the SAS Risk Engine, which is the core of SAS Risk Dimensions.

The middle tier hosts SAS Credit Risk Studio, which is deployed on a Java application server, such as Apache Tomcat. SAS Credit Risk Studio sends data to and receives data from the Web browsers on the client tier and then organizes the data for storage and use on the server tier and data source tier.

On the client tier, users collect and load data and perform day-to-day credit risk analysis tasks via SAS Credit Risk Studio. In addition, while reports are configured on the server tier, they are visible in the user interface to users who have access to only the machines on the client tier.

Figure 2.1 SAS Credit Risk Management for Banking Architecture



Deployment Outline

To install and deploy SAS Credit Risk Management for Banking:

1. Work with your SAS representative to develop a plan and designate the host machines for your deployment of SAS Credit Risk Management for Banking.
2. Read the SAS Intelligence Platform documentation.
3. Install the SAS Intelligence Platform and SAS Credit Risk Management for Banking on each host machine as outlined in your plan.xml file that you developed with your SAS representative.
4. Complete the post-installation tasks.
5. Define the SAS Credit Risk Management for Banking users and groups.

SAS Intelligence Platform Documentation

Because SAS Credit Risk Management for Banking is designed to work with the SAS Intelligence Platform, it is strongly recommended that you read the SAS Intelligence Platform documentation, which is located at `http://support.sas.com`, before you install SAS Credit Risk Management for Banking. That documentation provides pre-installation tasks and instructions to guide you through a typical installation of the SAS Intelligence Platform.

Default File Locations

This table shows the default locations of the directories and files that are installed with SAS Credit Risk Management for Banking. Use this table as a reference as you proceed through the installation and deployment process.

Table 2.1 Default File Locations

Directory/File	Windows Path	UNIX Path
SAS_HOME	`C:\Program Files\SAS`	*<sas-install-dir>*
!SASROOT	`C:\Program Files\SAS\SAS9.1`	*<sas-install-dir>*`/SAS9.1`
SAS Credit Risk Management for Banking configuration *<config-dir>*	`C:\SAS\`*<plan-file-name>*	`.../SAS/`*<plan-file-name>*

Table 2.1 Default File Locations *continued*

Directory/File	Windows Path	UNIX Path
SAS Credit Risk Management for Banking installation <*install-dir*>	`SAS_HOME\SASCreditRiskManagement\4.5`	`SAS_HOME/SASCreditRiskManagement/4.5`
SAS Risk Reporting Repository installation <*rrr-install-dir*>	`SAS_HOME\SASRiskReportingRepository\1.2`	`SAS_HOME/SASRiskReportingRepository/1.2`
Configuration Wizard summary	<*config-dir*>`\SAS_Configuration_Wizard_InstallLog.xml`	<*config-dir*>`/SAS_Configuration_Wizard_InstallLog.xml`
Configuration Wizard logs	<*config-dir*>`\configure_configure.log` <*config-dir*>`\configure_copyFiles.log` <*config-dir*>`\configure_web.log`	<*config-dir*>`/configure_configure.log` <*config-dir*>`/configure_copyFiles.log` <*config-dir*>`/configure_web.log`
Readme file for installation	`SAS_HOME\SASCreditRiskManagement\4.5`	`SAS_HOME\SASCreditRiskManagement\4.5`
Post-Installation Instructions	<*config-dir*>`\instructions.html`	<*config-dir*>`/instructions.html`

Chapter 3

Installation of SAS Credit Risk Management for Banking

Contents

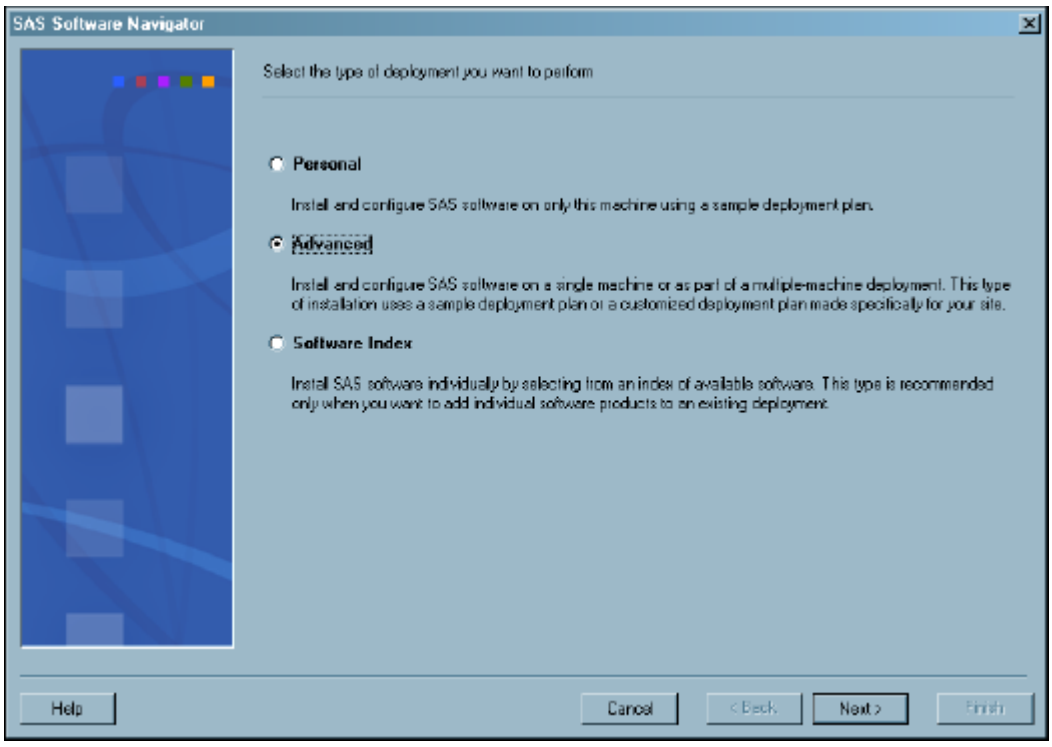
Pre-Installation Tasks

Before you begin to install the SAS Intelligence Platform and SAS Credit Risk Management for Banking, you must complete a set of pre-installation tasks. The SAS Intelligence Platform documentation provides detailed information about the pre-installation tasks that are required to install the SAS Intelligence Platform. There are no additional pre-installation tasks that are required to install SAS Credit Risk Management for Banking.

How to Install SAS Credit Risk Management for Banking

You install SAS Credit Risk Management for Banking on one or several machines as listed in your planning file (plan.xml). In general, you first install SAS Credit Risk Management for Banking on the machines on the data source tier, followed by the machines on the server tier, followed by the machines on the middle tier. However, some machines might host more than one tier.

Figure 3.1 SAS Software Navigator



To install SAS Credit Risk Management for Banking on each machine (Windows or UNIX):

1. Log on to the machine.

   - (Windows) Log on as any user who is in the Administrators group.
   - (UNIX) Log on as a SAS user (for example, *sas*) that you defined in the SAS Intelligence Platform pre-installation tasks.

     NOTE: It is recommended that you do not log on as *root* to perform an installation on a UNIX system.

2. Start the SAS Software Navigator. If you created a SAS Software Depot, then run the navigator from its network location in the depot. Otherwise, use the CD in your SAS Installation Kit to run the program.

3. (If applicable) Select your installation language in the Choose Language dialog box, and click **OK**.

4. Specify that you want to perform an advanced deployment, and click **Next**.

5. Specify the location of the SAS Installation Data (SID), and click **Next**.

   If you choose to obtain the SID from the Web and your site uses a UNIX proxy server to access the Web, then you should verify that the system has your proxy information defined properly.

   - For proxy support of https requests, verify that your HTTPS_PROXY environment variable is defined, using either a host address or an IP address, to point to your proxy server

and port. For example, you could define an HTTPS_PROXY variable in one of two ways:

$ HTTPS_PROXY = “http://proxy.server.com:8080”; export HTTPS_PROXY
$ HTTPS_PROXY = “127.0.0.1:8080”; export HTTPS_PROXY

- If your proxy server requires basic authentication credentials, then define the HTTPS_USERNAME and HTTPS_PASSWORD environment variables. For example, you can define HTTPS_USERNAME and HTTPS_PASSWORD as follows:

  $ HTTPS_USERNAME = “1myaccount”; export HTTPS_USERNAME
  $ HTTPS_PASSWORD = “1mypasswd”; export HTTPS_PASSWORD

6. Verify that the list of software that you are about to install is correct, and click **Next**.
7. Specify that you want to use a customized deployment plan, and then specify the project directory that contains your customized plan (plan.xml). Then, click **Next**.
8. Select your installation options, and click **Next**.
9. Specify the default installation path, and click **Next**.
10. Specify the preferred language of the Help files, and click **Next**.
11. Review your software installation options, and then click **Install**.

    NOTE: If you are using Windows, then the installation might cause your machine to restart. When your machine restarts, then the SAS Software Navigator should resume from where you last ended.
12. The interactive SAS Configuration Wizard opens and configures the software that you installed based on information that you supply. In the Advanced Properties Editor window of the Configuration Wizard, you should review all of the parameters to make sure that they are accurate for your site. You should consult the SAS Intelligence Platform documentation for more information about many of the parameters.

Alternate Installation Using Software Index

If you want to add SAS Credit Risk Management for Banking to an existing SAS deployment, you can perform a software index installation. This type of installation does not use a planning file. Instead, you select the individual SAS products that you want to install from an index of SAS products that are licensed to you.

In addition to SAS Credit Risk Management for Banking, you might want to add other SAS solutions to an existing SAS deployment. For more information about how additional solutions can be used to enhance SAS Credit Risk Management for Banking, see your SAS representative.

For more information about how to perform a software index installation, see the SAS Intelligence Platform documentation.

Chapter 4

Post-Installation Tasks

Contents

Overview of Post-Installation Tasks

At the end of the installation process, provided no installation errors have occurred, the SAS Configuration Wizard produces an HTML document called instructions.html. Follow the post-installation tasks described in the instructions.html file to complete the configuration of the server tier and middle tier. The instructions.html file also indicates when to perform the tasks that are outlined in this chapter. If your server tier and middle tier are hosted on separate machines, you will have an instructions.html file for each machine.

For more detailed information about how to use the instructions.html file to complete post-installation tasks, including supplemental instructions, see the SAS Intelligence Platform documentation.

To install SAS Credit Risk Management for Banking with the SAS Intelligence Platform, perform the post-installation tasks described in the following sections. After you have performed all of the tasks relevant to your site, restart the application server, and then navigate to the page `http://<middle tier host>:<port number>/criskm/jsp/pre_compile.jsp` (for example, `http://localhost:8080/criskm/jsp/pre_compile.jsp`) in your Web browser. After this page finishes loading, post-installation tasks are complete.

Verify Operating System Users and Grant Permissions

As a SAS Intelligence Platform pre-installation task, you created a set of required users at the operating system level. Ensure that these users have read and write permissions on the SAS Credit Risk Management for Banking installation directory. If you have created a user group that contains the SAS Credit Risk Management for Banking users, then give the group these permissions. Any users you create in the future must have read and write permissions for this directory.

Also, ensure that the SAS Web Administrator is associated with the authentication domain (for example, DefaultAuth) that you are using.

If you have created a user group containing the SAS Credit Risk Management for Banking users, ensure that the group contains both the SAS Web Administrator (for example, *saswbadm*) and the user (for example, *sassrv*) who runs the SAS Stored Process Server. In the future, any user that you create who needs to run SAS code in batch mode must be added to this group. In UNIX, this group must also be the primary default user group for the users that belong to it and must, therefore, be associated with these users in the password file.

(UNIX) Set Umask Settings for Newly Created Files

New files are created when you perform SAS Credit Risk Management for Banking tasks, either in batch mode or in SAS Credit Risk Studio. The default umask settings might not allow SAS Credit Risk Management for Banking users to read or write new files. To specify explicit umask settings, add a umask command, such as the string `umask g+rw`, to the sasenv_local file, which is located in the `!SASROOT\bin` directory.

(UNIX) Specify a Display Server

The ActiveX setting that is used to generate graphs in SAS Credit Risk Studio is not supported in UNIX environments. Therefore, for UNIX deployments, you must explicitly specify a valid X Windows System graphics display. For example, if SAS Credit Risk Studio has access to the X server named *ringo.credit.com*, you could submit the following statement:

```
export DISPLAY=ringo.credit.com:0.0
```

The exact steps that are required to specify an X Windows System graphics display vary between systems. For more information, refer to the appropriate system documentation.

Configure the SAS Servers

(Server tier) To configure the SAS Servers for use with SAS Credit Risk Management for Banking:

1. Start the metadata server.
   - (Windows) Select **Control Panel** → **Administrative Tools** → **Services** to navigate to the Services window.
   - (UNIX) Run this script:
     <*config-dir*>`/Lev1/SASApp/MetadataServer/MetadataServer.sh stop`
     <*config-dir*>`/Lev1/SASApp/MetadataServer/MetadataServer.sh start`
2. Make the following case-sensitive changes to one of the two copies of the sasv9.cfg file; a copy of this file is located in both the `!SASROOT\nls\`<*locale*> directory and the <*config-dir*>`Lev1/SASMain` directory:
   a) Add this text to specify variables that are used by SAS Credit Risk Management for Banking:
      `-SET CMHOME "`<*install-dir*>`"`
      `-SET CMINDATA "`<*install-dir*>`"`
      `-SET CMUSER "`<*install-dir*>`"`
      `-SET RRRHOME "`<*rrr-install-dir*>`"`
   b) Add the SAS Credit Risk Management for Banking and SAS Risk Reporting Repository macro folders to the SASAUTOS search path.
      - If you are editing the sasv9.cfg file that is in the `!SASROOT\nls\`<*locale*> directory:
        – (Windows)
          `-SET SASAUTOS ("!SASROOT\core\sasmacro"`
          `"`<*install-dir*>`\sascode\macros"`
          `"`<*rrr-install-dir*>`\DDL\sas")`
        – (UNIX)
          `-SET SASAUTOS ("!SASROOT/sasautos"`
          `"`<*install-dir*>`/sascode/macros"`
          `"`<*rrr-install-dir*>`/DDL/sas")`
      - If you are editing the sasv9.cfg file that is in the <*config-dir*>`Lev1/SASMain` directory:
        – (Windows)
          `-sasautos ('!SASROOT\core\sasmacro'`
          `'`<*install-dir*>`\sascode\macros'`
          `'`<*rrr-install-dir*>`\DDL\sas')`
        – (UNIX)
          `-sasautos ('!SASROOT/sasautos' ...`
          `'`<*install-dir*>`/sascode/macros'`
          `'`<*rrr-install-dir*>`/DDL/sas')`

WARNING: Be sure to list the SAS Credit Risk Management for Banking macro folder first in the SASAUTOS search path. If there are folders listed other than those for SAS Credit Risk Management for Banking and SAS Risk Reporting Repository, ensure that they appear after the SAS Credit Risk Management for Banking macro folder. Otherwise, incorrect macros might be executed.

c) (Optional) If your server does not have a default printer installed, then specify the `-uprint` option. On the Windows operating system, you can also specify the `-uprintmenuswitch` option.

NOTES:

- If you edit the copy of the sasv9.cfg file in the <*config-dir*>`Lev1/SASMain` directory, the changes you make will take effect immediately. If you edit the copy of the sasv9.cfg file in the `!SASROOT/nls/`*locale* directory, you must explicitly invoke the configuration for your changes to take effect in batch mode. To invoke the configuration, use the `-config` option followed by the path of the sasv9.cfg file when you invoke SAS.
- (UNIX) Examine the script that launches SAS to determine which copy of the sasv9.cfg file to edit.

3. In SAS Management Console, ensure that you are logged on as the SAS administrative user (for example, *sasadm*) you defined in the SAS Intelligence Platform pre-installation tasks, and make the following configuration changes to both the SAS Logical Workspace Server and the SAS Stored Process Server:

   a) If the `-memsize` option is specified, use the argument `MAX` to specify the maximum bound on potential memory allocation.

   NOTE: If you have specified the `-memsize` option in the sasv9.cfg file, the specifications you set in that file will override any setting you make for this option in SAS Management Console.

   b) Add the `metaautoinit` option to the Object Server Parameters.

4. (Optional) In SAS Management Console, convert the SAS Logical Workspace Server to connection pooling, and define a new puddle for use by SAS Credit Risk Management for Banking. This step requires that you have defined SAS Credit Risk Management for Banking user groups. For information about users and groups, see Chapter 7, "Administer Users and Groups." If you have not defined SAS Credit Risk Management for Banking user groups, but you intend to, you can return to this step after you have defined the user groups.

   Set these specifications for the new puddle:

   - Name the puddle *CreditRiskPuddle*.
   - (Optional) For performance tuning, enter the minimum and maximum number of available servers.
   - Select SAS Web Administrator and the logon name.
   - Grant access to the CreditRiskAdmin group.

5. Restart the object spawner.

- (Windows) Select **Control Panel** → **Administrative Tools** → **Services** to navigate to the Services window.
- (UNIX) Run this script:
  `<config-dir>/Lev1/SASApp/ObjectSpawner/ObjectSpawner.sh stop`
  `<config-dir>/Lev1/SASApp/ObjectSpawner/ObjectSpawner.sh start`

6. Restart the SAS OLAP Server.

   - (Windows) Select **Control Panel** → **Administrative Tools** → **Services** to navigate to the Services window.
   - (UNIX) Run this script:
     `<config-dir>/Lev1/SASApp/OLAPServer/OLAPServer.sh stop`
     `<config-dir>/Lev1/SASApp/OLAPServer/OLAPServer.sh start`

7. Launch the SAS Services Application.

   - (Windows) Click **SAS Services Application** in the Credit Risk Management for Banking menu in your Program menu.
   - (UNIX) Issue this command:
     `cd <config-dir>/Lev1/web/Deployments/RemoteServices/WEB-INF`
     `./StartRemoteServices.sh`

NOTE: For additional information about the configuration of the server tier, see the *<install-dir>*`\sascode\macros\autoexec_criskm.sas` and `omr\users\ configuration_settings.xml` files.

Deploy SAS Credit Risk Management for Banking to the Application Server

Overview of the Application Server

It is recommended that you select an application server before you install the SAS Intelligence Platform components. An application server might include WebSphere, WebLogic, or Tomcat. It is best practice that you use the same application server when you install and configure the Web application components.

If it is necessary to change the application server after the initial installation, then you must modify the portal metadata in order to find the SAS Theme_default application. You can modify the portal metadata by using the UpdateThemeConnection.sas job file. The job file is located in the `SAS_HOME\Web\Portal2.0.1\OMR\` directory. For information about redistributing the SAS Themes Web Application, see the Web site: http://support.sas.com/rnd/itech/doc9/portal_admin/deploy/ag_diststhapp.html.

For information about the configuration of the middle tier, see the following configuration files:

- webapps\conf\logging_config_stp.xml
- webapps\conf\login.config
- files that can be accessed from the .war file
  - webapps\criskm\WEB-INF\web.xml
  - webapps\criskm\WEB-INF\conf\sas_metadata_source_client_omr.properties
  - webapps\criskm\WEB-INF\conf\sas_metadata_source_server_omr.properties
  - webapps\criskm\WEB-INF\conf\system_properties.config
  - webapps\criskm\WEB-INF\classes\com\sas\ets\creditrisk\config.properties

NOTE: SAS librefs are not specified in the config.properties file. The SAS librefs are specified only in the autoexec_criskm.sas file in the server tier.

Assignment of Policy Rights to the Application Server

(Middle Tier) To assign policy rights and deploy SAS Credit Risk Management for Banking to the application server:

1. Ensure that your Java Virtual Machine (JVM) startup options are large enough for your site. Because the SAS Intelligence Platform and SAS Web applications make heavy memory demands on the application server, you might need to adjust the JVM startup option values. For information about JVM memory startup options, see the *SAS Intelligence Platform: Web Application Administration Guide*.

   NOTE: If you are using quick start settings for a Sun-based JDK, with any number of users, it is recommended that you use the settings that are specified in the *SAS Intelligence Platform: Web Application Administration Guide* for deployments with more than 10 concurrent users. Additionally, regardless of your operating system, it is recommended that you use the option -Xss256k.

   To enhance performance, it is also recommended that you update parameters in the configuration.properties file, which is located in the configuration directory, to the following values:

   - SERVICES_REMOTE_JVM_INIT_HEAP=512
   - SERVICES_REMOTE_JVM_MAX_HEAP=1024

2. Assign policy rights on the application server.

   - (Apache Tomcat) Add the following text to the catalina.policy file

     ```
     grant codeBase "file:${catalina.home}/webapps/criskm/-" {
     permission java.security.AllPermission;
     };
     ```

- (BEA WebLogic) In the start-up script (for example, startWebLogic.cmd) for the WebLogic domain containing SAS Credit Risk Management for Banking, modify the `-Djava.security.policy` argument to specify a file that contains the following text:

  ```
  grant {
  permission java.security.AllPermission;
  };
  ```

  Alternatively, you first can back up the weblogic.policy file and edit it so that it contains only the following code:

  ```
  grant {
  permission java.security.AllPermission;
  };
  ```

- (IBM WebSphere) You can set policy rights in the next step at deployment time.

3. Deploy SAS Credit Risk Management for Banking to the application server.

   - (Apache Tomcat) Use the Manager Web Application installed with Apache Tomcat. Alternatively, you can copy the war file located in the SAS Credit Risk Management for Banking installation directory to your Apache Tomcat Web application directory, which is typically `$TOMCAT_HOME$/webapps`. If you choose this method of deployment, verify that there are no XML files or folders in this directory that assign the context path */criskm*.
   - (BEA WebLogic) Use the Administrative Console installed with BEA WebLogic.
   - (IBM WebSphere) Follow these steps:
     a) Use the Administration Console installed with IBM WebSphere to install a new application from the war file located in the SAS Credit Risk Management for Banking installation directory. Assign to the application the context root *criskm*.
     b) Add the contents of the `<install.dir>/webapps/conf/login.config` file to the `WAS_ROOT/AppServer/properties/wsjaas.conf` file.
     c) Navigate to the metadata location for the *criskm* application in Websphere, and edit the `deployments/criskm_war/META-INF/was.policy` to read as follows:

        ```
        grant codeBase "file:${application}" {
        permission java.security.AllPermission;
        };
        ```

     d) Restart IBM WebSphere. If necessary, start the SAS Credit Risk Management for Banking application in the Administration Console.

Configure Deployments That Use DBCS Languages

To deploy SAS Credit Risk Management for banking in an environment that uses DBCS languages, edit the config.properties file located in your webapp deployment directory on the machine that hosts the middle tier.

1. (Windows) Change the value of the `lib.pathsep` property from / to \\.

2. (Windows) Change the path separators of the values of all properties that begin with `lib` from / to \\.
3. (Windows) Change the path separators of the value of the `sas.log.directory` property from / to \\.
4. Change the value of the `sas.batch.ods.load` to *load_ods_templates_nls.sas*.

Configure the Reporting and Locale Languages

During the installation of SAS Credit Risk Management for Banking, both the reporting language and the configuration language, also known as the locale language, are set to the same value according to a user selection that is made. In cases where this language is represented by a five-character code (for example, en_us), the locale language is set to the entire code and the reporting language is set to only the first two characters. The exception to this process is traditional Chinese, for which the reporting language is set to `zt` instead of `zh`. These codes that represent the reporting and locale languages are saved in the output_options data set.

The locale and reporting languages are used for different purposes in SAS Credit Risk Management for Banking. The locale language is associated with the stored process configuration data sets, which are used to define the stored processes. The reporting language is used to support multi-lingual reporting. To change the reporting or locale language from the value that is set during installation, edit the appropriate values in the output_options data set, which is located in either the `master` or `<entity>\users\<user ID>` subdirectory of the <*install-dir*>`\groups\<entity>` directory. In addition, you must create a localized version of the stored processes configuration data sets and save them in the <*install-dir*>`\omr\stp` directory. Append the file names of the localized files with the locale language code. Similarly, you must create a localized version of the reporting data sets and save them in the <*install-dir*>`\nls\stp` directory. Append the file names of the localized files with the reporting language code.

NOTE: A change in the reporting language or locale language is effective only if the corresponding localized configuration data sets exist. If each of the data sets is not defined for a particular language, then the English version is used for all of them.

For more information about configuration of the locale language, multi-lingual reporting, and localized data sets, see the *SAS Credit Risk Management for Banking: Administrator's Guide*.

Customize the SAS Information Delivery Portal

The installation of the SAS Credit Risk Management for Banking application includes a deployment of the SAS Information Delivery Portal configured for use with SAS Credit Risk Management for Banking. Two types of scripts are used to configure the SAS Information Delivery Portal: portal page definition and appearance scripts and portal authentication and authorization scripts.

Edit the following XML scripts to define the portal pages, as well as the portlets and graphs that populate the portal pages:

portalpages.xml
: defines the portal pages, their placement, as well as their titles and descriptions.

defineportlets.xml
: defines the portlets that are on each portal page, their titles, placement, dimensions, and descriptions.

dashboard_graphs_panel_config.xml
: defines the graph panels that are on each portal page, their titles, placement, and dimensions.

riskstudio_collection_portlets.xml
: defines the collection of links that appears.

Additionally, when the metadata server is loaded, two XML scripts for each existing user group are created: riskstudio_pagesto_create.xml and riskstudio_portlets_create.xml. Edit these XML files to define the authentication and user-access information that is required for pages and portlets to surface in the SAS Information Delivery Portal for each user.

To remove all portal definitions, execute the remove_riskstudio_page.sas, program. Use caution when removing portal definitions; this process is irreversible.

You can configure the title displayed in the SAS Information Delivery Portal. To do so, in the install_defaults.properties file, which is located in the SAS Information Delivery Portal installation directory, set the value of `NAME_IN_BANNER` to the custom name (for example, *Risk Studio*). Then, execute the configure_wik.bat script that is in the same directory to refresh the SAS Information Delivery Portal war file. Finally, redeploy the SAS Information Delivery Portal war file to your application server.

Define a Content Area on the WebDAV Server

If you wish to define a content area on the WebDAV Server for SAS Credit Risk Management for Banking, follow these steps:

1. Create a subdirectory of the base directory, sasdav, for SAS Credit Risk Management for Banking content. Name this subdirectory *crisk*.

2. Grant the server tier read and write permissions on the crisk directory. Also, ensure that the SAS Web Administrator has permission to create folders in this directory.

   NOTE: If you are using Xythos, you must also grant these permissions to *Public* and *Users with accounts*.

3. In SAS Management Console, ensure that you are logged on as the SAS Administrator. Verify that the local BIP information service has the WebDAV repository configured for auto-connect. You must verify this setting in three locations:

- **Repositories** field in the Properties window of the BIP Information Service node
- Server Manager
- Properties window of the BIP Tree in Business Report Manager

4. (Xythos) In SAS Management Console, verify that the SAS Web Administrator uses the same Authentication Domain as the HTTP DAV Server.

Initialize the SAS Credit Risk Management for Banking Data

To load and initialize the SAS Credit Risk Management for Banking data, execute a series of SAS jobs on the server tier. If you are using UNIX, you must be logged on as a user who is a member of the primary default group. Run the following SAS jobs in order:

1. To load the SAS Credit Risk Studio metadata, for most languages execute <*install-dir*>`/omr/load_credit_risk_metadata.sas`.

   For Double Byte Character Set (DBCS) languages, execute <*install-dir*>`/omr/load_credit_risk_metadata_nls.sas`.

2. To load the SAS Information Delivery Portal metadata, execute <*install.dir*>`/omr/Portal/Load_risk_studio_metadata.sas`.

   NOTE: The SAS Information Delivery Portal must be initialized before you execute this job. If it is not initialized, log on to the SAS Information Delivery Portal as the SAS Web Administrator and ensure that its war file is deployed. Alternatively, run the script initPortalData located in the `SAS_HOME/Web/Portal2.0.1/Tools` directory to create the metadata structure and initialize the SAS Information Delivery Portal.

3. To initialize the data, execute <*install.dir*>`/sascode/batch/installation_batch_job.sas`.

   NOTE: You can also execute this SAS job when you run Valuation Project in SAS Credit Risk Studio.

Reconfigure the SAS Credit Risk Management for Banking

To reconfigure SAS Credit Risk Management for Banking, use the run_config_ant_script that are located in the <*install-dir*>`/Config` directory. For more information about running this script, see the readme file that is located in the same directory.

In addition, you can edit the required.ant.properties file that is located in the <*install-dir*>`/Config` directory. Information about editing this file is located in the <*install-dir*>`/Config/<locale>` directory.

Chapter 5

ETL Job Deployment

Contents

Overview of the ETL Jobs

ETL jobs are used to extract data from the tables in the SAS Detail Store for Banking, transform that data, and then load it into the tables in the SAS Credit Risk Management for Banking data mart.

Four types of ETL jobs are used:

Configuration table jobs
: directly populate the configuration tables in the SAS Credit Risk Management for Banking data mart with the most recent, valid records in the SAS Detail Data Store for Banking tables.

Intermediate table jobs
: populate intermediate tables in the SAS Credit Risk Management for Banking data mart with the valid records that have been most recently extracted from SAS Detail Data Store for Banking. SAS Credit Risk Management for Banking does not access the data that is in the intermediate tables; rather, the intermediate tables are used to restructure the extracted data.

Staging table jobs
: populate the staging (input) tables in the SAS Credit Risk Management for Banking data mart. Primarily, these jobs extract data from the intermediate tables. In some cases, the jobs extract data from the SAS Detail Data Store for Banking tables. Staging jobs with names that start with ETL01 or ETL02 populate intermediate tables. Staging jobs with names that start with ETL03 or ETL04 prepare the extracted data and then populate the staging tables in the SAS Credit Risk Management for Banking data mart.

Internal table jobs
: populate additional tables with information about the execution of the staging jobs and any associated errors. Installation of these jobs is optional.

How to Install the ETL Jobs

Installation of the SAS Credit Risk Management for Banking ETL jobs relies on an existing deployment of SAS Detail Data Store for Banking. For information about how to install SAS Detail Data Store for Banking, see *SAS Detail Data Store for Banking: Implementation and Administration Guide*.

Use SAS Data Integration Studio to install the SAS Credit Risk Management for Banking ETL jobs. For specific information about how to perform the following actions in SAS Data Integration Studio, see *SAS Data Integration Studio: User's Guide*.

NOTE: Package files that are located in the <*install-dir*>\ETL\packages directory of the server tier machine are used to install the ETL jobs. If you are using an installation of SAS Data Integration Studio that is on a different machine, you must make the package files available to that machine before you attempt to install the ETL jobs.

To install the SAS Credit Risk Management for Banking ETL jobs:

1. Create a custom repository, which is dependent on the Foundation repository that is used for the SAS Detail Data Store for Banking deployment. The SAS Credit Risk Management for Banking ETL jobs and table definitions are installed in this custom repository. It is recommended that you give the custom repository a meaningful name (for example, *CreditRisk4.5*).

2. Ensure that the physical locations to which you want the SAS Credit Risk Management for Banking libraries to point exist. Capacity planning should be completed at your site. To enhance system performance, it is recommended that the libraries that are defined for SAS Credit Risk Management for Banking point to different physical disks, if possible.

3. Use the Import Wizard to import the SAS Credit Risk Management for Banking library package file (CRISKM_Libraries.spk) into the custom repository. After you import the package file, three libraries are registered, and the metadata for the associated tables is created. Importing the CRISKM_Libraries.spk package file registers these libraries:

Library Name	libref	Contains
Configuration Mart	CfgTbls*	33 configuration tables
Intermediate Mart	DDSInt	82 intermediate tables
Staging Mart	RD_STAGE	46 staging tables

*The SAS Credit Risk Management for Banking analytic processes access this library with the libref RD_STAT.

4. Use the Import Wizard to import the SAS Credit Risk Management for Banking package files (CRISKM_Configuration.spk, CRISKM_Intermediate.spk, CRISKM_Staging.spk) for the configuration, intermediate, and staging ETL jobs into the custom repository.

   NOTE: Relevant physical target tables are created when each job is executed for the first time.

5. (Optional) Use the Import Wizard to import the SAS Credit Risk Management for Banking package file (CRISKM_Internal.spk) for the internal library, internal table metadata, and internal ETL jobs into the custom repository.

If the data sets already exist, you might need to manually set an option in the **Select the objects to import** window of the Import Wizard. In this window, highlight the name of each internal table, and then select **Include/replace physical table** on the **Options** tab.

After you import the package file, one library is registered, and the metadata for the associated tables is created. Importing the CRISKM_Internal.spk package file registers this library:

Library Name	libref	Contains
Internal Monitoring	INT_TAB	3 internal jobs

NOTE: To enhance system performance, select a target location in the **Physical Location** window of the Import Wizard that is on a different physical disk than the locations of the libraries that you have already registered.

Configure the Preprocessor and the Internal ETL Jobs

To configure the ETL preprocessor that defines the library for the user-supplied run-time and date information, which is used by the internal jobs, edit the launch command option of either the Workspace Server (interactive mode) or the Batch Server (batch mode) in SAS Management Console. Add the option `-autoexec` and, in double quotes, the path of the preprocessor file. If you are operating in interactive mode, then restart the object spawner after you have made this change.

In SAS Data Integration Studio, you can specify that the code for each of the internal ETL processes will be retrieved from a specified location, rather than generated by SAS Data Integration Studio. To do so, edit the properties of each internal ETL process.

ETL Process	Location of Code
D_Update_etlstart.sas	Update_etlstart.sas
D_Update_etlerrorlog	Update_etlerrorlog.sas
D_Update_etlend	Update_etlend.sas

Configure Scheduling of ETL Jobs

In SAS Management Console, you can use the Schedule Manager to create job flows that schedule the execution of ETL jobs. If you configure scheduling for the SAS Credit Risk Management for Banking ETL jobs, you should define a job flow that includes the configuration jobs (these begin with *POPULATE_CONFIG*) and a separate job flow that includes the staging jobs (these jobs begin with *ETL*), intermediate jobs (these jobs begin with *Populate_I*), and internal jobs (these jobs begin with *D_Update*). There are no job dependencies within the former job flow. However, for the later job flow, you need to set the job dependency *ends with exit code less than 2* for each of the solution mart jobs and for the D_Update_etlend internal job. Also, set the job dependency *ends with exit code less than 1* for the D_Update_etlerrorlog internal job.

For a listing of the ETL jobs and illustrations of their flows, see the appendix about ETL jobs.

Chapter 6

How to Install and Configure the SAS Risk Reporting Repository Data

To install and configure the SAS Risk Reporting Repository data:

1. In a SAS session, run the following SAS programs, which are located in the `C:\Program Files\TBD` directory, to define the table structures:

Macro	Description
ddlrrr.sas	creates the table data definitions
rrr_ic.sas	creates the table integrity constraint definitions

   Each of these programs contains an %INCLUDE statement that references <*table-name*>_data.sas or <*tablename*>_ic.sas files, which contains the DATA step code or ALTER TABLE statements. If necessary, you can edit the programs to configure the format of the following variables for your site:

Variable	Default SAS Format	Description
DTFMT	DATE9.	applies formats/informats to date fields
DTTMFMT	NLDATM21.	applies formats/informats to datetime fields
TMFMT	NLTIMAP10.	applies formats/informats to time fields
FMTRK	12.	applies formats/informats to fields for retained surrogate keys
NUMW_D	18.5	indicates the width and decimal precision in format statements for currency amount fields. (See this format statement: `FORMAT=NLNUM&NUMW_D`.)

2. Edit the ddlall.sas macro to include the file locations that are relevant to your site. Then, submit this macro in a SAS session.

3. To verify that the tables were created correctly, submit the code below in a SAS session. Then compare the output to the SAS Risk Reporting Repository physical data structure, which is included in this document as an appendix.

```
proc datasets lib=RRR;
quit;
```

Chapter 7

Administer Users and Groups

Contents

Overview of Users and Groups

Each SAS Credit Risk Management for Banking user is assigned a role that determines what functions that user is able to perform in SAS Credit Risk Studio. These are the default user roles in SAS Credit Risk Management for Banking:

User
: can view the results of the master calculations.

Analyst
: can view the results of the master calculations and run their own sets of calculations. Analysts who are working in their user directory cannot execute certain stored processes that they are able to execute when they are working in their master directory.

Admin
: can run the master calculations, view the results of the master calculations, load and manage data, and create user profiles.

You can group users. The name of each user group must begin with the keyword *CreditRisk*. The default, case-sensitive user groups in SAS Credit Risk Management for Banking are CreditRiskUser, CreditRiskAnalyst, and CreditRiskAdmin. If you create user groups, ensure that the SAS Web Administrator (for example, *saswbadm*) is a member of the CreditRiskAdmin group.

To further limit the access that users have to data in SAS Credit Risk Studio, you can associate any user with one or more entities, which define the parts of the organization that user is able to analyze. Users who are associated with multiple entities can specify which entity to analyze after they have logged on to SAS Credit Risk Studio. To associate a group of users with an entity, you append an underscore and the name of the entity to the user group name. For example, a user who

belongs to the group CreditRiskUser_CorporateLending would be able to view master results for only calculations that are performed for the parts of your organization that are defined by the entity CorporateLending.

Visibility of Tabs

Any user is able to view each page on the **Results** tab, the **Inputs** tab, and the **Profile** tab in SAS Credit Risk Studio. However, the visibility of the **Analysis** tab is governed by the role of a user and, for Analysts, the directory in which the user is working. The **Analysis** tab is not visible to either Analysts who are working in their user directory or to Users. The **Analysis** tab is visible both to Analysts who are working in a master directory and to Admins.

Create Users and Groups for the First Time

You create users and groups on the metadata server for SAS Credit Risk Management for Banking. First, create the users and groups at the operating system level, and administer their local security policies. Then, define the users in the SAS Metadata Repository. To define the users in the SAS Metadata Repository, you can manually enter each user and group definition in SAS Management Console. However, to create multiple SAS Credit Risk Management for Banking users at once, it is less cumbersome to develop an automated process that populates xml files. You can then use a SAS script to load the data that is in the xml files into the SAS Metadata Repository.

SAS Credit Risk Management for Banking includes both the SAS script createcriskusers.sas, which you can use to load user and group definitions and three sample xml files that have the data structure that the script expects. These files are located in the <*install- dir*>\omr\users directory. Before you use createcriskusers.sas to load the user definitions, you must update these sample xml files with content that is relevant to the users and groups for your organization:

criskuser.xml
: contains user information.

authdomain.xml
: contains the available authentication domains.

criskgroupmembers.xml
: maps users to previously defined user groups.

In the xml files, the following fields require non-missing values:

- keyid
- name

- description
- userid
- password
- authdomkeyid
- authDomName
- grpkeyid
- memkeyid

Authorization to Access Files

Authorization to access files is defined by access permissions in the <*install-dir*>\sascode\macros directory.

SAS Server Users, which include *sassrv*, are granted Full Control permissions for the SAS Credit Risk Management for Banking installation directory. SAS Users, which include *sasadm*, *saswbadm*, and *sasdemo*, are included in the SAS Server Users group. SAS Users are granted Full Control permissions to the macros through inheritance from the macro directory's parent directory, except in one case. SAS Server User permissions for the autoexec_criskm.sas macro are not inherited; you must set these permissions explicitly.

It is recommended that you ensure that all of the files and directories in the SAS Credit Risk Management for Banking installation directory can inherit the permissions that are granted to the SAS Credit Risk Management for Banking installation directory. Verify that the **Allow inheritable permissions from the parent to propagate to this object and all child objects** is enabled on the **Security** tab of the Advanced file properties.

Constraints When You Define Users and Groups

The following constraints apply when you load users and groups in SAS Credit Risk Management for Banking:

- User and group names must be unique.
- A user or group can have multiple user names, but each user name must be associated with only one user.
- Each user name must be unique within the authentication domain in which it is used.

- User names in a Windows environment must be qualified with the Windows domain name that owns the account.
- If the user name is intended for a network domain, the user name should be in the form *domain/userid*.
- You cannot simultaneously add and remove a definition for a person or group.

Remove or Update Users and Groups

To permanently remove all SAS Credit Risk Management for Banking users and groups, run the remove_credit_risk_user.sas script that is located in the <*install-dir*>\omr\users directory.

To update users and groups, you must first run the remove_credit_risk_user.sas script to delete all existing users and groups and then follow the process for creating users and groups for the first time.

CAUTION: Failing to run the remove_credit_risk_user.sas script prior to reloading users and groups will compromise the integrity of your user metadata.

Your Turn

We want your feedback.

- If you have comments about this book, please send them to **yourturn@sas.com**. Include the full title and page numbers (if applicable).
- If you have comments about the software, please send them to **suggest@sas.com**.