SAS® Infrastructure for Risk Management 3.3: Administrator’s Guide
## Contents

### PART 1  Introduction to SAS Infrastructure for Risk Management  
1

**Chapter 1 • Welcome to SAS Infrastructure for Risk Management**  
3

**Chapter 2 • SAS Infrastructure for Risk Management Architecture**  
5
- SAS Infrastructure for Risk Management Architecture 5
- SAS Infrastructure for Risk Management Data Flow 6
- SAS Infrastructure for Risk Management Distributed Development 7

**Chapter 3 • SAS Infrastructure for Risk Management Federated Content**  
9
- Structure of the SAS Infrastructure for Risk Management Federated Area 9
- SAS Infrastructure for Risk Management Federated Content Development 13

**Chapter 4 • What’s New In SAS Infrastructure for Risk Management 3.3**  
17
- What’s New in SAS Infrastructure for Risk Management 3.3 17

### PART 2  Deploying SAS Infrastructure for Risk Management  
19

**Chapter 5 • Performing Pre-installation Tasks**  
21
- Overview of the Pre-installation Tasks 21
- Verify Your System Requirements 22
- Complete the Pre-installation Tasks for SAS Intelligence Platform 22
- Create the SAS Infrastructure for Risk Management User Accounts 23
- Create a SAS Software Depot 23
- Obtain a Deployment Plan 24
- Complete the Pre-installation Checklist That Accompanies Your Deployment Plan 25
- Set SAS Web Application Directory Permissions on UNIX 25
- Check for Installation Notes 25

**Chapter 6 • Installing SAS Infrastructure for Risk Management**  
27
- Overview of the Installation Tasks 27
- Review the File System Structure 27
- Install Hot Fixes 28
- Install SAS Infrastructure for Risk Management 29
- Install Your Solution’s Federated Content 32

**Chapter 7 • Performing Post-installation Tasks**  
33
- Overview of the Post-installation Tasks 33
- Use the Instructions.html File 34
- Groups, Roles, and Capabilities in SAS Infrastructure for Risk Management 34
- Configure the Metadata Accounts for SAS Infrastructure for Risk Management 35
Configure SAS Infrastructure for Risk Management to Use HTTP over an SSL Connection .......................... 37
Access the SAS Infrastructure for Risk Management Solution Web Application ............................. 37
Back Up SAS Content ......................................................... 37

PART 3  Migrating and Upgrading SAS Infrastructure for Risk Management 39

Chapter 8  •  Upgrade and Migration Overview ................................................. 41
About Migrating and Upgrading ................................................................. 41
Releases That Support Migration or Upgrade .................................................. 41

Chapter 9  •  Migrating SAS Infrastructure for Risk Management ................. 43
About the Migration Process ................................................................. 43
Review Additional Documentation ............................................................ 44
Design Your Migration .................................................................................. 45
Create a Migration Package in Your Source Environment .............................. 45
Migrate SAS Infrastructure for Risk Management ........................................... 45
Migrate Federated Content ............................................................................ 47
Troubleshoot Migration Errors ....................................................................... 50

Chapter 10  •  Upgrading SAS Infrastructure for Risk Management .............. 51
About the Upgrade Process ............................................................................ 51
Perform the Pre-upgrade Tasks ...................................................................... 52
Upgrade SAS Infrastructure for Risk Management .......................................... 52
Migrate Federated Content ............................................................................ 53
Troubleshoot Upgrade Errors .......................................................................... 54

PART 4  Administering SAS Infrastructure for Risk Management 57

Chapter 11  •  Managing Federated Areas ...................................................... 59
Overview ........................................................................................................ 59
Add Additional Federated Areas ................................................................. 60

Chapter 12  •  Additional Administrative Tasks ............................................. 63
Configure Middle-Tier Server Clustering on SAS Infrastructure for Risk Management .................................................. 63
Add a Solution to an Existing Deployment .................................................... 63
Load New Data via Live ETL ......................................................................... 64
View the Input and Output Data Sets in SAS Studio ....................................... 65

Chapter 13  •  Troubleshooting ...................................................................... 67
Gather Information ......................................................................................... 67
Enable Detailed Logging ............................................................................... 69
Fix Your Web Application Log File Display .................................................. 70
Log and Configuration File Locations ............................................................ 70
Part 1

Introduction to SAS Infrastructure for Risk Management

Chapter 1

Welcome to SAS Infrastructure for Risk Management ............... 3

Chapter 2

SAS Infrastructure for Risk Management Architecture ............... 5

Chapter 3

SAS Infrastructure for Risk Management Federated Content ........ 9

Chapter 4

What’s New In SAS Infrastructure for Risk Management 3.3 ....... 17
Chapter 1
Welcome to SAS Infrastructure for Risk Management

What Is SAS Infrastructure for Risk Management?

SAS Infrastructure for Risk Management is a job execution engine with a web-based user interface that is deployed along with one or more SAS solutions. SAS Infrastructure for Risk Management solutions are delivered as industry-specific content release products.

Calculations are performed using transparent job flows that facilitate auditing of your risk practices. The entire platform is designed to be customizable and flexible, so that you can rapidly adapt to changing regulations.

The architecture of SAS Infrastructure for Risk Management enables a simplified and easy way to develop and run the fastest analytics.

Using SAS Infrastructure for Risk Management: Administrator’s Guide

SAS Infrastructure for Risk Management: Administrator’s Guide is written for administrators who are responsible for installing and configuring solutions that use SAS Infrastructure for Risk Management as a platform.

The administrator must have the skills to perform the following tasks:

• Use SAS Download Manager to download the SAS Software Depot to each machine on which the installation is performed.

• Install and configure SAS Intelligence Platform and the solution platform and associated content modules.

• Use the SAS Management Console to maintain the metadata for the servers, users, and other global resources that are required by the solution.

For information about how to use the SAS Infrastructure for Risk Management user interface, see SAS Infrastructure for Risk Management: User’s Guide.
Chapter 2

SAS Infrastructure for Risk Management Architecture

SAS Infrastructure for Risk Management Architecture

SAS Infrastructure for Risk Management Data Flow

SAS Infrastructure for Risk Management Distributed Development

Overview

Contributors

Federated Content

SAS Infrastructure for Risk Management

Architecture

SAS Infrastructure for Risk Management operates in a three-tiered environment, as shown in the following figure:
• **Server Tier**

The server tier handles requests from the client tier and the middle tier, and serves as an abstract layer between the data tier and the middle tier or between the data tier and the client tier. The server tier consists of SAS applications, such as the SAS Metadata Server and SAS Application Servers.

• **Middle Tier**

The middle tier receives and processes web requests from the client tier and passes these requests to the server tier and the data tier. The middle tier contains a web application server in addition to web applications such as the SAS Infrastructure for Risk Management web application.

• **Client Tier**

The client tier initiates requests to perform the necessary work and to view formatted output. Desktop client applications or web browsers send these requests. For daily activities, you access the SAS Infrastructure for Risk Management web application from systems that are part of the client tier. The client tier GUI is developed in HTML5.

---

### SAS Infrastructure for Risk Management Data Flow

The following figure shows the flow of data in SAS Infrastructure for Risk Management solutions.
Note the following about the SAS Infrastructure for Risk Management data flow:

1. Data is supplied to a solution in one of the following ways:
   - The customer submits data directly to the input area.
   - When the system is running, the customer submits data directly to the landing area of a federated area.
   - If the SAS Detail Data Store is in place, data can be drawn from the SAS Detail Data Store into the input area.

2. Subsets of the input data are created in separate folders, for each reporting period. These subsets of input data are created in the read-only staging or read-only landing area of the SAS Infrastructure for Risk Management solution. The tables are versioned by date (8-character string – mmdyyy) or date and time (14-character string – mmdyyyyhhmms).

3. The output of the job flow is placed in the persistent area. The persistent area is a read/write area for inputs and outputs (files in XLSX format, files in XBRL format, and SAS data sets).

---

**SAS Infrastructure for Risk Management Distributed Development**

**Overview**

SAS Infrastructure for Risk Management solutions are designed to support distributed development. Distributed development means that developers in different locations can independently develop code to refine the functionality of a SAS Infrastructure for Risk Management solution.

Note that distributed development has the following implications:

- Code that is developed in one location must not break code that is developed in another location.
- Subsequent releases of a SAS Infrastructure for Risk Management solution must support all changes or fixes that are deployed since the prior release, including additions to flows, code, and data.
- Developers are responsible for the integrity of their code.
• If you modify a subflow that is used by other flows, then you can break these flows. For example, you might break the flows if you changed the number or nature of the outputs of a subflow. Therefore, coordination of the development group is necessary.

• With the exception of the ability to load data, all installed federated areas are read-only.

• Once installed, a federated area must not be removed.

**Contributors**

Contributors to the distributed development of SAS Infrastructure for Risk Management solutions include the following:

• SAS Research & Development
  SAS Research & Development provides the content that is included with your SAS Infrastructure for Risk Management solution.

• SAS Consultants
  SAS Consultants provide custom content that can be included in a future release of all SAS Infrastructure for Risk Management solutions.

• Consulting firms
  Consulting firms develop a custom product on top of SAS Infrastructure for Risk Management solutions.

**Federated Content**

SAS Infrastructure for Risk Management solutions are delivered as *federated content* products. Federated content is computational and reporting logic that is designed, produced, and owned by people outside SAS Research & Development. This might be a SAS department that is not SAS Research & Development, a third-party consulting company, and so on.

For more information about federated content, see Chapter 3, “SAS Infrastructure for Risk Management Federated Content,” on page 9.
Chapter 3
SAS Infrastructure for Risk Management Federated Content

Structure of the SAS Infrastructure for Risk Management Federated Area

Overview

SAS Infrastructure for Risk Management solutions share the same architecture and layout. The differences among the solutions are in the calculation content that is stored in a solution’s federated area. A federated area is a set of folders that has a specified structure and solution-specific calculation content. SAS Infrastructure for Risk Management developers must organize their content in federated areas.

Note: The SAS Infrastructure for Risk Management platform is shipped with a platform-level federated area. The platform federated area contains only those elements that are required to make the platform run when a SAS Infrastructure for Risk Management solution is installed. There is no content in the platform federated area.

CAUTION:

Do not modify the SAS Infrastructure for Risk Management platform federated area.

A federated area can contain the following elements:

- flows – files that describe the job flow
- code – string message data, nodes (including Java nodes), or macros
• input files – SAS data sets, CVS files, Microsoft Excel templates, or XBRL templates
• documentation and tooltips files – information that is presented to the end user through the user interface

Only the flows, nodes, and input files are federated content. Federated content is shared by multiple federated areas. All of the other content is local to a federated area and cannot directly be shared between federated areas. However, SAS Infrastructure for Risk Management must know about the other content areas in order to deliver all functionality.

Note: The distinction between federated and non-federated content is important in order to help you maintain future releases.

The following sections describe the components of a federated area and the content of the directories in the federated area.

Federated Area Directory Location

When you install SAS Infrastructure for Risk Management, you must install the platform federated area during installation. The platform federated area contains the elements that are required for SAS Infrastructure for Risk Management to run.

By default, the platform federated area is created in SAS-configuration-directory/Levn/AppData/SASIRM/. The name of the platform federated area is fa.0.3.3.

The following figure shows the basic structure of the SAS Infrastructure for Risk Management platform federated area folder:

![Federated Area Directory Location](image)

**CAUTION:**

Do not modify the SAS Infrastructure for Risk Management platform federated area.

The following figure shows the basic structure of the federated area directory of a SAS Infrastructure for Risk Management solution (SAS Firmwide Risk for Solvency II):
Note: Federated areas can contain more folders or fewer folders than appear in these examples.

Config Directory

Developers use the files in the config directory to configure the behavior of job flows. The following figure shows the structure of a SAS Infrastructure for Risk Management solution’s federated area config directory:

The config directory contains the following files:

- job_flow_definitions.csv
  A spreadsheet of job flow definitions. The first column is the category in which the job flow definition resides. The second column is the identifier of the job flow definition. The third column indicates whether the job flow can be run as solo, group, or both. The fourth column is a pipe ( | ) delimited list of the configuration sets for which the job flow is visible in the Create Instance window of the user interface.

- libnames.txt
  Maps the static input tables that are used by SAS Infrastructure for Risk Management. This file maps a logical name (LIBNAME) to the directory location of the static input tables.

- macrovarload.txt
Lists SAS data sets that define global macro variables that must be loaded before a node executes.

Note: In order for the macro variables to be available, nodes must include the macro variables data sets as input.

**Job Flow Directory**

The following figure shows the structure of a SAS Infrastructure for Risk Management solution’s federated area jobflow directory:

The jobflow directory contains job flows or subdirectories that contain job flows. Job flows are graphical representations of the enrichment and analytical processing that is performed to complete analyses and to prepare reports. In other words, a job flow is a diagram that describes the sequence of calculation steps that it performs.

Job flows consist of one of the following:

- a sequence of nodes
- a sequence of subflows
- input and output data objects

Job flows are categorized as definitions and instances. A job flow has only one definition, but it can have many instances. One user can have multiple instances of the same job flow. In addition, many users can have multiple instances of the same job flow. An example of two instances of the same job flow is the same calculation that is performed using data from different base dates.

Subdirectories within the jobflow directory are displayed as Categories in the SAS Infrastructure for Risk Management web application user interface. For the preceding jobflow directory, QRT – Assets and Investments, QRT – Balance Sheet and QRT – Group Reporting, and QRT – Intragroup Transactions are displayed as Categories in the user interface.

**Source Directory**

The source directory contains code that delivers SAS Infrastructure for Risk Management functionality.
The following figure shows the structure of a SAS Infrastructure for Risk Management solution’s federated area source directory:

- **doc** (contains the solution-level federated content documentation files)
- **Java**
  - **bin** (binary files — Java code can be delivered as Java files or compiled class files)
  - **lib** (JAR files)
  - **nodes** (Java code that is directly invoked by flows)
- **lua**
  - **luarisk** (Lua risk libraries)
  - **luastl** (Lua collection, utility, and graph libraries)
  - **plugin** (module that encodes and decodes JSON data)
  - **sas** (Lua code for various functions and operations)
- **sas**
  - **nodes** (SAS code that is directly invoked by flows)
  - **smd** (string message data)
  - **ucmacros** (compiled or uncompiled)

*Note:* The umacros folder might contain subfolders.

*Note:* Depending on the SAS Infrastructure for Risk Management solution, additional folders might appear in the sas directory.

---

**SAS Infrastructure for Risk Management Federated Content Development**

**Overview**

Federated content is contained in federated areas. Federated content is the mechanism by which developers add custom content to SAS Infrastructure for Risk Management. The list of all the federated areas defines the federated content.

Only flows, nodes (including Java nodes), and input files are federated in the sense that these resources are shared across federated areas. All other federated area content, including macros, Lua code, and so on, is not shared. These non-shared resources are
accessible only from within the specific federated areas. Nodes that are written in both SAS and Java can be federated.

**Federated Content Processing**

Only flow files, nodes (.sas files), and input data is shared across federated areas in order to compose the federated content. All other content is isolated to its federated area. That is, a node in federated area 1 cannot call a macro in federated area 2. For federated content, SAS Infrastructure for Risk Management searches the federated areas, from highest to lowest precedence (by the federated ID assigned in metadata and in lexical order), until the desired content is found.

**Federated Job Flows**

Flows (.bpmn files) are federated. When searching for a job flow definition, the solution searches from the highest precedence federated area to the lowest precedence federated area. For example, if federated area 2 contains a file named flow1.bpmn and the federated area 1 also contains a file named flow1.bpmn, the file in federated area 2 is used to create any new instance of a flow. After an instance is created, the instance does not change its definition. That is, later adding a flow1.bpmn file to a higher precedence federated area does not affect existing instances of previously created flows using this definition. However, all new instances use the new definition.

**Federated Nodes**

As with job flows, nodes that are identified within a flow are searched for in federated areas from highest to lowest precedence.

*Note:* Nodes with the same name are assumed to be the same content. Therefore, a node named node1.sas accepts the same input tables and produces the same output tables as other nodes with the same name, regardless of their federated location.

As with job flow definition files, changing or adding a new version of a node does not affect existing job flow instances. New executions of an instance use the newest definition of node1.sas.

During execution of a node, the context of that execution environment is isolated to the federated area in which it resides. Any macros or Lua code that are called by the node must exist in the federated area of the node.

Nodes can have some input and output SAS data sets and files that are partitioned. Partitioned nodes enable large amounts of data to be partitioned into smaller units of data and calculated across multiple cores. The node recombines the results of the partitioned data. For detailed information about partitioned nodes, see the documentation included in the generic sample federated area (fa.sample.3.3) that is installed with SAS Infrastructure for Risk Management 3.3. This federated area contains two sample flows that demonstrate the capabilities and functionality of SAS Infrastructure for Risk Management.

**Federated Input Tables**

Input tables are shared across multiple federated areas. All static input tables that are used by SAS Infrastructure for Risk Management nodes must be mapped using the libnames.txt file.

*CAUTION:*
Directly accessing SAS data sets that are not mapped via the libnames.txt file is not permissible. All tasks must define all of their inputs and outputs.

The libnames.txt file is located in the config folder of the federated area. All static input tables reside in the landing_area folder. Mappings are relative to the landing area. The file maps a logical name (libref) to a folder.

Examples:

GLOBAL=%la/base/global

This statement specifies the folder base/global within the federated area under the landing_area directory. The libref GLOBAL should refer to that path.

Nodes can reference tables using one-, two-, or three-level names. Here are examples:

- GLOBAL
- GLOBAL.myglobal
- GLOBAL.myglobal.sas7bdat

Processing of the latter two examples is identical, since the sas7bdat suffix is assumed. One-level names are processed somewhat differently than two- and three-level names.

The following example assumes that the following three federated areas were previously defined.

com.sas.solutions.risk.irm.fa.0.3.3=/sas-configuration-directory/Levn/AppData/SASIRM/fa.0.3.3
com.sas.solutions.risk.irm.fa.2=/sas-configuration-directory/Levn/AppData/SASIRM/fa2
com.sas.solutions.risk.irm.fa.2.5=/sas-configuration-directory/Levn/AppData/SASIRM/fa2.5

If a one-level name is specified, then SAS Infrastructure for Risk Management searches each libnames.txt file for the mapping in question from highest to lowest precedence. For example, if the table references GLOBAL, then SAS Infrastructure for Risk Management searches the libnames.txt file in federated area 2.5. (Federated area 2.5 has the highest precedence because 2 > 1, and 2.5 > 2.) SAS is looking for a mapping for GLOBAL. If found, that path is added to the concatenated LIBNAME statement that is used to define GLOBAL. This path is the first path in the libref path. If the mapping is not found, the search continues through the federated areas for a libnames.txt file that contains a mapping for GLOBAL. If no mapping is found, the node fails with an error.

Processing two- or three-level names is similar, except that SAS Infrastructure for Risk Management has the information that is required to verify that the actual table exists. As before, SAS Infrastructure for Risk Management searches for a mapping in the libnames.txt file. If the mapping is not found, the search continues to the next federated area (by precedence). However, if a mapping is found, SAS Infrastructure for Risk Management verifies that the file actually exists in the folder that is specified in the mapping. If a mapping is not found, the search continues. Mapping enables content developers to overwrite a single table without having to override all tables using the same mapping (LIBNAME). If the table cannot be located, the node is not created and the SAS Infrastructure for Risk Management New Instance wizard displays an error that the instance cannot be created.

Consider the case of a pair of two-level names, GLOBAL.table1 and GLOBAL.table2, that use the same mapping that is described above. Both tables reside in federated area 1, but only table1 resides in federated area 2. The following LIBNAME statement is generated:
LIBNAME GLOBAL ("/sas-configuration-directory/Levn/AppData/SASIRM/fa2/landing_area/base/global" "/sas-configuration-directory/Levn/AppData/SASIRM/fa1/landing_area/base/global");

As this statement indicates, table1.sas7bdat is found in federated area 2 (sas-configuration-directory/Levn/AppData/SASIRM/fa2/landing_area/base/global), and table2.sas7bdat is found in federated area 1 (sas-configuration-directory/Levn/AppData/SASIRM/fa1/landing_area/base/global).

Note that the search for mappings uses the following case order:

1. as specified in the flow definition (for example, “GloBal”, if so specified in the flow definition)
2. all uppercase (for example, “GLOBAL”)
3. all lowercase (for example, “global”)
4. initial capitalization (for example, “Global”)

It is recommended that you use three-level names in your flow definitions and uppercase mappings in your libnames.txt file.
Chapter 4
What’s New In SAS Infrastructure for Risk Management 3.3

The following features and enhancements are introduced in SAS Infrastructure for Risk Management 3.3:

• Folders that contain subsets of input data can now be versioned by date (8-character string – mmddyyyy) or by date time (14-character string – mmddyyyyhhmmss).

• The name of a SAS Infrastructure for Risk Management solution can now be displayed in the banner of the web application. This is an optional feature that you can configure when installing SAS Infrastructure for Risk Management.

• Nodes can have input and output SAS data sets and files that are partitioned. Partitioned nodes enable large amounts of data to be partitioned into smaller units of data and calculated across multiple cores. The node recombines the results of the partitioned data.

• Users can upload new data without affecting server operations. Via the Live ETL feature, after new data is uploaded, associated job flows are automatically recalculated without affecting server operations.

• Data object pooling streamlines processing for the SAS Infrastructure for Risk Management solutions. If two flows contain the same nodes, the results of the first run are stored and reused when the other node is executed. This feature speeds up calculations because nodes that have not changed are not rerun. Therefore, if a node appears to be running instantly, it might be because the data object pooling feature has detected that the task does not need to rerun.

• SAS Infrastructure for Risk Management 3.3 supports SAS 9.4 Intelligence Platform middle-tier server clustering.

• More granular permission levels can now be configured.

• A generic sample federated area (fa.sample.3.3) is installed with SAS Infrastructure for Risk Management. This federated area contains two sample flows that demonstrate the capabilities and functionality of SAS Infrastructure for Risk Management. For details about the sample flows, see the documentation that included in the generic sample federated area.
Part 2

Deploying SAS Infrastructure for Risk Management

Chapter 5
Performing Pre-installation Tasks ........................................ 21

Chapter 6
Installing SAS Infrastructure for Risk Management ............... 27

Chapter 7
Performing Post-installation Tasks ..................................... 33
Overview of the Pre-installation Tasks

Before you install SAS Infrastructure for Risk Management, complete the pre-installation tasks that are included in the following checklist.

Table 5.1  Pre-installation Checklist

<table>
<thead>
<tr>
<th>Completed?</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verify your system requirements.</td>
</tr>
<tr>
<td></td>
<td>Complete the pre-installation tasks for SAS Intelligence Platform.</td>
</tr>
<tr>
<td></td>
<td>Create the SAS Infrastructure for Risk Management user accounts.</td>
</tr>
<tr>
<td></td>
<td>Create a SAS Software Depot.</td>
</tr>
<tr>
<td></td>
<td>Obtain a Deployment Plan.</td>
</tr>
<tr>
<td></td>
<td>Complete the Pre-installation Checklist That Accompanies Your Deployment Plan</td>
</tr>
<tr>
<td></td>
<td>Set SAS Web Application directory permissions on UNIX.</td>
</tr>
<tr>
<td></td>
<td>Check for Installation Notes.</td>
</tr>
</tbody>
</table>
### Completed? Task

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Obtain a deployment plan.</td>
</tr>
<tr>
<td></td>
<td>Complete the pre-installation checklist that accompanies your deployment plan.</td>
</tr>
<tr>
<td></td>
<td>Check for installation notes.</td>
</tr>
</tbody>
</table>

### Verify Your System Requirements

Ensure that your system meets the minimum system requirements for SAS Infrastructure for Risk Management.


*Note:* Depending on the solution installed with SAS Infrastructure for Risk Management, system requirements might be greater.

### Complete the Pre-installation Tasks for SAS Intelligence Platform

SAS Infrastructure for Risk Management is built on SAS Intelligence Platform.

Before you begin to install SAS Intelligence Platform and your SAS Infrastructure for Risk Management solution, you must complete a set of pre-installation tasks for SAS Intelligence Platform. These tasks include installing various third-party components, confirming your operating system requirements, creating the required user accounts, and obtaining your SAS software.

For more information about third-party components, see the [Third-Party Software Requirements](http://support.sas.com/documentation/prod-p/irm/index.html) website.


The *SAS Intelligence Platform: Installation and Configuration Guide* provides pre-installation tasks and instructions to guide you through a typical installation of SAS Intelligence Platform.
Create the SAS Infrastructure for Risk Management User Accounts

Valid host operating system accounts are required for SAS Infrastructure for Risk Management administrative and product users. You can use existing operating system accounts.

SAS Infrastructure for Risk Management administrative and product users also require access to the workspace server.

If the workspace server is running on the Windows operating system, note that the operating system accounts must also have the following privileges:

- Log on as a batch job
- Create Symbolic Link

These settings are located under Control Panel → Administrative Settings → Local Security Policy → Local Policies → User Rights Assignment.

Users can use internal metadata accounts instead of operating system accounts to access the software. The only account that must exist as an operating system account is the account that is used to launch the SAS Workspace Server (that is, the SAS General Server User).

For more information about setting up external user accounts, see the SAS Intelligence Platform: Installation and Configuration Guide.

Create a SAS Software Depot

A SAS Software Depot is a file system that consists of SAS installation files that represent one or more software orders. The depot contains one or more deployment plans, a SAS installation data file, order data, and product data. The depot also contains the SAS Deployment Wizard executable, which is the tool that you use to install and initially configure SAS Infrastructure for Risk Management.

To download your SAS order and simultaneously create a SAS Software Depot, complete the following steps:

1. Using the SAS Software Depot administrator account (or a user account with depot Read, Write, and Execute privileges), log on to the machine on which you want to create the SAS Software Depot.

2. Locate your original Software Order Email, and click the link that is provided in the Download the SAS Download Manager step in the Your Deployment Instructions section of the email.

3. On the install.depot web page, click the link for the SAS Download Manager that is appropriate for your operating system.

4. When prompted by your browser, select the option that enables you to save the file to disk.

5. Specify the location at which to save the file.

6. When your browser has finished downloading the SAS Download Manager, run it.
7. In the Choose Language window, select the language that you want the SAS Download Manager to use when it displays text and click OK.

8. If you are prompted for proxy information, provide the proxy server settings that are required in order for the SAS Download Manager to access the Internet.

9. On the Order Information page in the SAS Download Manager wizard, enter your order number and the SAS installation key.

10. On the Specify Order Details page, add a description to distinguish this order from other SAS orders.

11. Review the list of SAS products that are included in your order.

12. On the Specify Order Options page, select the **Include complete order contents** option in order to include the entire order in the SAS Software Depot.

13. On the Specify SAS Software Depot Options page, complete the following steps:
   - In the **SAS Software Depot Directory** field, specify the location to which the software is downloaded and the SAS Software Depot is built.
   - (Optional) To enable the SAS Download Manager to evaluate and optimize your depot after downloading your order, select the **Remove duplicate files and save space option**. This optimization is performed on the entire depot after the latest download has been added. Therefore, all software in the depot—not just the software being downloaded—is optimized.
   - If the directory that you specify does not exist, the wizard informs you. If you want the wizard to create the directory for you, click Yes.

14. On the Final Review page, click **Download** to begin downloading, uncompressing, and creating a SAS Software Depot for your SAS order.

15. When the download is complete, click **Finish** to close the SAS Download Manager.

For information about copying a depot or subsetting your order, see “Creating a SAS Software Depot” in *SAS Intelligence Platform: Installation and Configuration Guide* at http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/install94.html.

---

### Obtain a Deployment Plan

A *deployment plan* is a preselection of the software that is installed by the SAS Deployment Wizard. It contains a description of what the plan deploys, identifies the target machines, and lists the software to be installed and configured. It is an XML file and is named `plan.xml`.

SAS Infrastructure for Risk Management solution installation plan files are custom deployment plans that have been created by a SAS Installation Representative specifically for your site. The representative emails the XML file (or a ZIP file containing an XML file) to you.

Before installing, ensure that you copy the plan file to a location from which the SAS Deployment Wizard can obtain it during installation.

Complete the Pre-installation Checklist That Accompanies Your Deployment Plan

Your deployment plan download contains a checklist.pdf file and a checklist.rtf file. Both files contain the same pre-installation checklist, which you must complete before deploying a SAS Infrastructure for Risk Management solution.

The checklist includes tasks that are specific to your deployment. It also includes information about the third-party software, the operating system accounts and groups, and the ports that are required before starting the deployment.

Set SAS Web Application Directory Permissions on UNIX

On UNIX systems, the SAS Web Application Server stores its license files in the /etc/opt/vmware/vfabric folder. Therefore, this folder must be created with Write access for the SAS installer account before beginning your deployment. This change is required on each machine on which the SAS Web Application Server is deployed, regardless of whether you are running VMware.

To create the directory with the appropriate permissions, complete the following steps:

1. Log on as the root user.
2. Create the following directory:
   `/etc/opt/vmware/vfabric`
3. Run the following commands:

   ```bash
   chown -R SAS installer user /etc/opt/vmware/vfabric
   chgrp -R group name of the SAS installer user /etc/opt/vmware/vfabric
   ```

Note: Some sites have security settings that require these changes to be made at the /etc/opt level rather than at the /etc/opt/vmware level. Therefore, access to the root user might be required at installation time to make these changes.

Check for Installation Notes

Chapter 6
Installing SAS Infrastructure for Risk Management

Overview of the Installation Tasks

To install and configure SAS Infrastructure for Risk Management, complete the tasks that are included in the following checklist.

<table>
<thead>
<tr>
<th>Completed?</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Review the structure of the SAS Infrastructure for Risk Management file system.</td>
</tr>
<tr>
<td></td>
<td>Install the hot fixes for SAS Infrastructure for Risk Management 3.3 and for SAS 9.4 M4.</td>
</tr>
<tr>
<td></td>
<td>Install and configure SAS Infrastructure for Risk Management.</td>
</tr>
<tr>
<td></td>
<td>Download and install the SAS Infrastructure for Risk Management solution’s federated content package.</td>
</tr>
</tbody>
</table>

Review the File System Structure

After you install and configure SAS Infrastructure for Risk Management, by default, the following directories exist:
<table>
<thead>
<tr>
<th>Directory</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS-installation-directory</td>
<td>• Linux: /SAS-installation-directory/SASHome/</td>
</tr>
<tr>
<td></td>
<td>• Windows: C:\Program Files\SASHome\</td>
</tr>
<tr>
<td>!SASROOT (SAS Foundation Directory)</td>
<td>• Linux: /SAS-installation-directory/SASHome/9.4/</td>
</tr>
<tr>
<td></td>
<td>• Windows: C:\Program Files\SASHome\SASFoundation\9.4\</td>
</tr>
<tr>
<td>SAS_configuration_directory</td>
<td>• Linux: /SAS-installation-directory/config/Levn/</td>
</tr>
<tr>
<td></td>
<td>• Windows: C:\SAS\Config\Levn/</td>
</tr>
<tr>
<td>SAS Infrastructure for Risk Management data directory (the product's root data directory)</td>
<td>• Linux: /SAS-configuration-directory/Levn/AppData/SASIRM/</td>
</tr>
<tr>
<td></td>
<td>• Windows: \SAS-configuration-directory\Levn\AppData\SASIRM\</td>
</tr>
<tr>
<td>SAS Deployment Wizard Installation Summary</td>
<td>• Linux: /SAS-configuration-directory/Levn/Documents/DeploymentSummary.html</td>
</tr>
<tr>
<td></td>
<td>• Windows: \SAS-configuration-directory/Levn\Documents\DeploymentSummary.html</td>
</tr>
<tr>
<td>SAS Deployment Wizard configuration logs</td>
<td>• Linux: /SAS-configuration-directory/Levn/Logs/Configure</td>
</tr>
<tr>
<td></td>
<td>• Windows: \SAS-configuration-directory/Levn/Logs\Configure</td>
</tr>
<tr>
<td>Web application server logs</td>
<td>• Linux: /SAS-configuration-directory/Levn/Web/Logs</td>
</tr>
<tr>
<td>Note: By default, some logging is enabled. You can configure additional logging in the SAS Management Console.</td>
<td>• Windows: \SAS-configuration-directory/Levn/Web/Logs</td>
</tr>
<tr>
<td>SAS Infrastructure for Risk Management middle-tier staging directory</td>
<td>• Linux: /SAS-configuration-directory/Levn/Web/Staging</td>
</tr>
<tr>
<td></td>
<td>• Windows: \SAS-configuration-directory/Levn/Web\Staging</td>
</tr>
</tbody>
</table>

**Install Hot Fixes**

If hot fixes are available for your product, you must install the hot fix after installation, but before configuration.

To find applicable hot fixes, complete one or more of the following tasks, as appropriate:

• Use the tool at http://ftp.sas.com/techsup/download/hotfix/HF2/SASHFADD.html to create a customized report that lists the hot fixes that are available for the installed SAS products. This tool also generates the scripts that automate the download of the hot fixes.

• Use the SAS Deployment Manager to find and apply the hot fixes.


---

**Install SAS Infrastructure for Risk Management**

You can install SAS Infrastructure for Risk Management on just one machine or on several machines as listed in your customized deployment plan (plan.xml file).

The SAS Deployment Wizard pages that you see during installation depend on the following:

• the prompt level that you choose

• the SAS tier on which you are deploying SAS Infrastructure for Risk Management

• the contents of your custom order

*Note:* Although the SAS Deployment Wizard contains steps for all of the products that are a part of your deployment, this section describes only those steps that pertain to SAS Infrastructure for Risk Management. In addition, this installation example explains how to install on a single machine using the **Typical** prompting level.

To install a SAS Infrastructure for Risk Management solution, complete the following steps:

1. Using the SAS Installer account (or an account that is a member of the Windows Administrators group), log on to the machine on which to install the SAS Infrastructure for Risk Management solution.

2. Navigate to the highest-level directory in your SAS Software Depot.

3. Using the `setup` command appropriate for your operating system, start the SAS Deployment Wizard.

4. On the Select Deployment Type page, select **Perform a Planned Deployment** and ensure that both **Install SAS Software** and **Configure SAS Software** are selected.
5. On the Select Deployment Step and Products to Install page, select **Step 1: Server and Middle Tier** and click **Next**. (In this example, the server tier and the middle tier are installed on the same machine.)

6. On the Select Deployment Task page, select **Install SAS Software** and click **Next**.

7. On the SAS IRM Server Configuration page, enter a password for the SAS Infrastructure for Risk Management super user and click **Next**.

![SAS Deployment Wizard](image)

**Note:** The IRM super user is a built-in internal account that has privilege levels significantly beyond those of most user accounts. A member of the super user accounts can perform system-level administrative tasks. The IRM super user is a member of the predefined **IRM:Access All Entities** role.

8. (Optional) On the SAS IRM Mid-tier Configuration page, enter the name of the SAS Infrastructure for Risk Management solution that you are installing. The name that
you enter is displayed on the banner of the web application. By default, SAS Infrastructure for Risk Management is displayed in the banner.

*Note:* When a web application is at 100% zoom and the screen resolution is 1280 x 1024, a limited number of letters, numbers, and spaces can be seen in the banner. In addition, do not use single or double quotation marks in the solution name.

9. On the SAS IRM Database Configuration page, enter the credentials for accessing the SAS Infrastructure for Risk Management database and click **Next**.

10. When the Deployment Summary page is displayed, review the list of products to be installed and click **Start**.

The SAS Deployment Wizard launches the installation and configuration process and provides an ongoing status update.
11. When the installation and configuration process completes, the Deployment Complete page appears.

A status icon is displayed next to each software application. The status icon indicates whether the installation process completed successfully, completed with warnings, or completed with errors for that application.

After you have installed and configured SAS Infrastructure for Risk Management, you must download, unzip, and install the federated content package for your Infrastructure for Risk Management solution. For information about downloading and installing solution-specific federated content, see the next section, “Install Your Solution’s Federated Content”.

---

Install Your Solution’s Federated Content

SAS Infrastructure for Risk Management solutions share the same architecture and layout. The difference between the solutions is the calculation content that is delivered in a SAS Infrastructure for Risk Management solution federated content package.

SAS delivers the federated content for a solution as a downloadable content release that is located on the Downloads support page.

To obtain the content release for your solution, complete the following steps:

2. Locate the content release for your solution. You can search alphabetically, by product category, or by release date.
3. If prompted, enter your SAS Profile logon credentials and click Sign in.
4. To initiate the download, click the ZIP filename of the content release.
5. In the SAS License Validation window, enter your site number for verification and click Submit.
6. In the SAS License Agreement for Download window, click Accept to agree to the license agreement and proceed with the download.
7. After you have downloaded the content release for your Infrastructure for Risk Management solution, use the installation instructions that are provided with the package to install and verify the content.
Chapter 7
Performing Post-installation Tasks

Overview of the Post-installation Tasks
After installing SAS Infrastructure for Risk Management, complete the post-installation tasks in the following checklist before using SAS Infrastructure for Risk Management.

<table>
<thead>
<tr>
<th>Completed?</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Follow the instructions in the Instructions.html file.</td>
</tr>
<tr>
<td></td>
<td>Create the metadata user accounts and assign the user to groups.</td>
</tr>
<tr>
<td></td>
<td>Access the SAS Infrastructure for Risk Management solution user interface through your web browser.</td>
</tr>
</tbody>
</table>
Use the Instructions.html File

At the end of the installation process for SAS Infrastructure for Risk Management, the SAS Deployment Wizard produces a document named Instructions.html.

Note: If the server tier and the middle tier are hosted on separate machines, there is an Instructions.html file for each machine.

The Instructions.html file is located in the `SAS-configuration-directory/Levn/Documents/` directory. Follow the instructions that are provided in the document.

Groups, Roles, and Capabilities in SAS Infrastructure for Risk Management

About Capabilities

Here are the key points about capabilities in SAS Infrastructure for Risk Management:

- Unlike permissions, which affect access to data, content, and metadata, capabilities affect access to features and functionality.
- Administrators assign capabilities to roles. The groups to which a user is assigned define the capabilities of that user.

Predefined Roles and Capabilities for SAS Intelligence Platform

The predefined roles and capabilities for SAS Intelligence Platform are provided in the following documents.

<table>
<thead>
<tr>
<th>Application</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata Server</td>
<td>SAS Intelligence Platform: System Administration Guide</td>
</tr>
<tr>
<td>Desktop Applications</td>
<td>SAS Intelligence Platform: Desktop Application Administration Guide</td>
</tr>
<tr>
<td>Web Applications</td>
<td>SAS Intelligence Platform: Web Application Administration Guide</td>
</tr>
</tbody>
</table>

Predefined Group and Roles for SAS Infrastructure for Risk Management

SAS Infrastructure for Risk Management comes with the predefined role: **IRM:Access All Entities**. This role is configured in the SAS Management Console during installation. This role is assigned the Allow Access to All Entities capability, which is also predefined in SAS Infrastructure for Risk Management.
Users who are members of the IRM: Access All Entities role can perform the following actions:

- create job flow instances that are based on this entity and its children
- modify or delete non-published instances that they own
- share private job flow instances
- view public job flow instances that are based on this entity and its children

Note: By default, the SAS General Servers group, the SAS IRM Super User, and if configured, the SAS Demo User are assigned to this role.

You can use the predefined roles or create roles to meet your business requirements.


---

**Configure the Metadata Accounts for SAS Infrastructure for Risk Management**

All users must have a metadata account on the SAS Metadata Server for the SAS Infrastructure for Risk Management web application. Users are not required to have an operating system account.

For information about importing user accounts from a provider such as LDAP into the SAS metadata, see the “User Import Macros” appendix in SAS Intelligence Platform: Security Administration Guide at http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html.

To configure a SAS Infrastructure for Risk Management metadata user account for a user that has an operating system account, complete the following steps:

1. Start SAS Management Console and connect as a SAS administrator (for example, sasadm@saspw).
2. Right-click the User Manager plug-in and select New ⇒ User. The New User Properties window is displayed.
3. On the General tab, complete the following:
   a. In the Name field, enter a user ID for the user. This ID is used to log on to the application.
      
      **Tip**: Avoid using spaces or special characters in the Name field. Not all components support spaces and special characters.
   
   b. In the Display Name field, enter the name that you want to associate with the user ID.
4. On the Accounts tab, complete the following:
   a. Click New to create a new SAS Metadata account for the user. The New Login Properties window is displayed.
   
   b. In the User ID field, enter the user ID. It corresponds to the user ID that is used to log on to the SAS Infrastructure for Risk Management solution. Do not enter a password.
   c. Select an Authentication Domain (for example, DefaultAuth), and click OK.
5. On the Group and Roles tab, complete the following:
a. In the **Available Groups and Roles** section, select the group to which you want the user to belong. For example, select **IRM: Access All Entities** to permit the user access to all entities. Move the group to the **Member of** section.

b. To create a custom role for granting access to selected entities and capabilities, select **New Role** from the **User Manager** plug-in. In the **Name** field, enter **IRM: Action Entity Entity_Role Entity_Name** as the name for the role, where:
   - **Action** — Valid values are **Access** (create, view, and modify job flow instances of a specified entity), **Publish** (publish job flow instances of a specified entity), or **Delete** (delete job flow instances of a specified entity).
   - **Entity-Role** — (Optional) Valid values are **Solo** or **Group** permissions. The default is **Group**.
   - **Entity-Name** — A valid value matches the name of the entity exactly.

c. Continue to add users to groups, as necessary.

6. Click **OK** to create the new user. The new user appears in the **User Manager** list.

To configure a SAS Infrastructure for Risk Management metadata user account for a user that does not have an operating system, complete the following steps:

1. Start SAS Management Console and connect as a SAS administrator (for example, sasadm@saspw).

2. Right-click the **User Manager** plug-in and select **New User**. The New User Properties window is displayed.

3. On the **General** tab, complete the following:
   - a. In the **Name** field, enter a user ID for the user. It is the user ID that is used to log on to the application.
   
   **Tip** Avoid using spaces or special characters in the **Name** field. Not all components support spaces and special characters.
   
   b. In the **Display Name** field, enter the name that you want to associate with the user ID.

4. On the **Accounts** tab, complete the following:
   - a. Click **Create Internal Account**. The New Internal Account for New User window is displayed.
   
   b. Enter a password for the new user and click **OK**.

5. On the **Group and Roles** tab, complete the following:
   - a. In the **Available Groups and Roles** section, select the group to which the user belongs. For example, select **IRM: Access All Entities** to permit the user to access all entities. Move the group to the **Member of** section.
   
   b. To create a custom role for granting access to selected entities and capabilities, select **New Role** on the **User Manager** plug-in. In the **Name** field, enter **IRM: Action Entity Entity_Role Entity_Name** as the name for the role, where:
      - **Action** Valid values are **Access** (create, view, and modify job flow instances of a specified entity), **Publish** ( publish job flow instances of a specified entity), or **Delete** (delete job flow instances of a specified entity).
      - **Entity-Role** (Optional) Valid values are **Solo** or **Group** permissions. The default is **Group**.
Configure SAS Infrastructure for Risk Management to Use HTTP over an SSL Connection

To configure SAS Infrastructure for Risk Management to use HTTP over SSL, complete the following steps:

2. In the subdirectories, locate the following two SAS/SECURE JAR files: sastpj.rutil.jar and sas.rutil.jar.
3. Copy the files to the Java file folder for the platform federated area / sas_config_directory/Lev/n/AppData/SASIRM/fa.0.3.3/source/ java/lib.
4. Restart the SAS Infrastructure for Risk Management web application server.

Access the SAS Infrastructure for Risk Management Solution Web Application

You can access the SAS Infrastructure for Risk Management user interface through your web browser at http://Your_Middle_Tier_Host:port/SASIRM.

For more information about this URL and the port number, see the Instructions.html file that is generated for SAS Infrastructure for Risk Management.

By default, SAS Infrastructure for Risk Management is configured to run on port 7980 on Linux systems. However, verify the port number by checking the Instructions.html file.

Back Up SAS Content

It is recommended that you implement a system to back up and restore metadata, databases, and disk drive content that is generated by SAS Infrastructure for Risk Management. For more information about how to back up SAS content, see “Best Practices for Backing Up and Restoring Your SAS Content” on SAS Intelligence Platform documentation website.
Part 3

Migrating and Upgrading SAS Infrastructure for Risk Management

Chapter 8
Upgrade and Migration Overview ........................................ 41

Chapter 9
Migrating SAS Infrastructure for Risk Management ............... 43

Chapter 10
Upgrading SAS Infrastructure for Risk Management .............. 51
Chapter 8
Upgrade and Migration
Overview

About Migrating and Upgrading

The following two options are available for moving software from a previous release to the current release of SAS Infrastructure for Risk Management:

• migration

The process of moving SAS metadata and other data and files from one instance of SAS Infrastructure for Risk Management to another instance of SAS, as part of an installation on a new machine.

Migration typically involves new hardware. For example, you might migrate your machine from a development system to a production system, or you might migrate hardware from an older server to a newer server. Migration attempts to preserve as much of your current content and configuration as possible.

For more information see, see Chapter 9, “Migrating SAS Infrastructure for Risk Management,” on page 43.

• upgrade

Involves updating SAS Infrastructure for Risk Management from a previous version to a new version on the same supporting platform.

This option does not require new hardware and can be performed on the same operating system.

For more information, see Chapter 10, “Upgrading SAS Infrastructure for Risk Management,” on page 51.

Releases That Support Migration or Upgrade

The following table lists the releases of SAS Infrastructure for Risk Management that can be migrated to the current release of SAS Infrastructure for Risk Management.
The following table lists the releases of SAS Infrastructure for Risk Management that can be upgraded to the current release of SAS Infrastructure for Risk Management.

<table>
<thead>
<tr>
<th>Upgrade from the Specified Release</th>
<th>Upgrade to SAS Infrastructure for Risk Management 3.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Yes</td>
</tr>
<tr>
<td>3.2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Migration from the Specified Release</th>
<th>Migration to SAS Infrastructure for Risk Management 3.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Yes</td>
</tr>
<tr>
<td>3.2</td>
<td>Yes</td>
</tr>
<tr>
<td>3.3</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Chapter 9
Migrating SAS Infrastructure for Risk Management

About the Migration Process

The operating system to which you are migrating (target) must have the same number of machines on the same operating systems as the system from which you are migrating (source). Also, the target system must have a database from the same vendor as the database on the source system.

To migrate SAS Infrastructure for Risk Management, complete the tasks that are included in the following checklist.

<table>
<thead>
<tr>
<th>Completed?</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Review additional documentation.</td>
</tr>
<tr>
<td></td>
<td>Design your migration.</td>
</tr>
<tr>
<td></td>
<td>Create a migration package in your source environment.</td>
</tr>
<tr>
<td></td>
<td>Back up your source system.</td>
</tr>
<tr>
<td></td>
<td>Migrate SAS Infrastructure for Risk Management.</td>
</tr>
<tr>
<td></td>
<td>Migrate the solution’s federated content.</td>
</tr>
</tbody>
</table>

CAUTION:
Ensure that you follow the steps in this chapter when migrating a system. Performing a step that is not documented could result in an installation that SAS Infrastructure for Risk Management does not support. If you have questions about a step, contact SAS Technical Support at http://support.sas.com/techsup before you proceed.

Review Additional Documentation

Before you start your migration, review the following documents:

- **Quick Start Guide**
  
  This document is shipped with your SAS software and is also available online:

  - Windows:  
    http://support.sas.com/documentation/installcenter/94/win/index.html
  - Linux:  
    http://support.sas.com/documentation/installcenter/94/unx/index.html

- **Software Order Email (SOE)**
  
  This email is sent to your site to provide information about your order.

- **SAS order information (SOI)**

  The SOI file indicates when the order was placed and provides a list of the products that are in your order. The SOI is in your SAS Software Depot at /install_doc/order-number/soi.html.

- **SAS software summary**

  The summary provides information about the products that are in your order and specifies the software that supports your order. The SAS software summary is in your SAS Software Depot at install_doc/order-number/ordersummary.html.

  *Note:* The SAS Deployment Wizard installs only what is listed in the deployment plan. The SAS software summary might list more products than are included in the deployment plan.

- **SAS 9.4 system requirements**

  http://support.sas.com/resources/sysreq/index.html

- **System Requirements – SAS Infrastructure for Risk Management 3.3**


- **SAS Notes**


- **SAS Intelligence Platform 9.4: Migration Guide**

  http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/install94.html
Design Your Migration

To design your migration, complete the following tasks:

- Review “High-Level SAS Migration Requirements” in *SAS Intelligence Platform: Migration Guide* at http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/install94.html. Compare these requirements to your current deployment and develop a plan for moving your SAS content (data and configuration) to a SAS Infrastructure for Risk Management 3.3 system.

- Run the SAS Migration Utility that is provided in your SAS Software Depot. The utility creates a migration analysis report that enables you to answer the following questions:
  - Which SAS products currently reside on each machine?
  - Which SAS products require maintenance before you can migrate them?
  - Contact your SAS Installation Representative to obtain a valid SAS 9.4 deployment plan for your current SAS deployment.
  - Schedule time for your migration so that users are aware of when the system is unavailable.

Create a Migration Package in Your Source Environment

Use the SAS Migration Utility to create a migration package that contains your current SAS data and configuration information from the source system. You use this migration package as input to the SAS Deployment Wizard when you migrate to the target system.


Migrate SAS Infrastructure for Risk Management

*Note:* The following migration process explains how to migrate a single machine installation.

When you perform a migration for SAS Infrastructure for Risk Management, the process is similar to a typical out-of-the-box deployment. The primary difference between the two methods is that during the SAS Deployment Wizard session, you select the Perform Migration option on the Migration Information page. The following points identify the differences between a typical out-of-the-box deployment and a migration.

*CAUTION:*

Before beginning the migration process, ensure that you back up your installation.
When migrating, note the following differences between a migration and a typical out-of-the-box deployment:

1. To configure all products in one execution of the SAS Deployment Wizard, click Typical on the Configuring Prompting Level page.

2. During a migration, SAS Deployment Wizard makes one configuration pass for the SAS Application tier. Therefore, you must select all products for configuration in a migration scenario.

3. To migrate SAS Infrastructure for Risk Management, select Step 1: Server and Middle Tier on the Select Deployment Step and Products to Install page.

4. On the Migration Information page, select Perform migration and click Browse to navigate to the migration package that was generated by the SAS Migration Utility.
5. Click Next.

6. When complete, in the target environment, stop the SAS Infrastructure for Risk Management web application server.

7. Complete the migration by manually copying the federated areas and persistent area from the source system to the target system. For information about copying the federated content, see the next section, “Migrate Federated Content”.

## Migrate Federated Content

After migrating SAS Infrastructure for Risk Management, you must migrate the content in the federated areas and the persistent area from the source system to the target system.

*Note:* Before completing the steps in this section, ensure that the SAS Infrastructure for Risk Management web application server is stopped.

To migrate federated content, complete the following steps:

1. Copy all federated areas from the source location to the exact same location on the target system. The federated areas include the following:
   - all the platform federated areas from earlier releases (for example, `com.sas.solutions.risk.irm.fa.0.3.1` and `com.sas.solutions.risk.irm.fa.0.3.2`)
   - where applicable, earlier versions of the QRT federated area
   - earlier versions of the current federated areas

   *Note:* SAS Infrastructure for Risk Management 3.1 supports only one federated area.

2. Copy the persistent area folder from the source location to the exact same location on the target system. Ensure that the ownership and permissions of the files and folders in the persistent area are retained during the copy.

3. In SAS Management Console on the target system, change the persistent area path to point to the newly copied persistent area by completing the following steps:
a. From the **Plug-ins** tab, select **Application Management ➔ Configuration Manager ➔ SAS Application Infrastructure**.

b. Right-click **IRM Mid-Tier Server** and select **Properties**.

c. On the IRM Mid-Tier Server Properties window, select the **Advanced** tab.

d. Ensure that the **Property Value** of the **com.sas.solutions.risk.irm.server.pa** points to the location of the persistent area folder.

**Note**: The location of the persistent area must be exactly the same on the target system as it was on the source system.

![IRM Mid-Tier Server Properties Window](image)

4. Ensure that the contents of the persistent area are owned by the installer and that the SAS General Server user account owns data and messages.

If migrating from SAS Infrastructure for Risk Management 3.2 to SAS Infrastructure for Risk Management 3.3, you have completed the process for migrating federated content and can restart the SAS Infrastructure for Risk Management web application server.

**Note**: The following steps apply only to a SAS Infrastructure for Risk Management 3.1 to SAS Infrastructure for Risk Management 3.3 migration. The solution in this example is SAS Firmwide for Solvency II.

To complete the migration of SAS Infrastructure for Risk Management 3.1 federated content to SAS Infrastructure for Risk Management 3.3 federated content, complete these additional steps:

1. In the installation directory (`SAS-installation-directory/SASFoundation/9.4/misc/rmifirmmva/install`), complete the following tasks:

   a. Edit the `irmmigrate.properties` file to include the path to the original federated area and to the new federated area.

   In addition, enter the path to the new base date directories. If more than one base date was defined in the federated area on the source system, enter an additional base date directory. If there was only one base date defined in the federated area on the source system, comment out the second base date in the `irmmigrate.properties` file on the target system.

   b. Edit the `irmmigrate.sql` file by replacing

   `@New_FA_ID@`
with the identifier of the existing federated area. However, do not use a zero (0) or the letter “z” as the first character. For example, when migrating the federated area with id=0.3.1, replace

@New_FA_ID@

with 3.1.

2. Run the following commands:
   a. To set the required variables, run:
      On Windows:
      \SAS-configuration-directory\Lev\level_env.bat
      On Linux:
      /SAS-configuration-directory/Lev/level_env.sh
      Note: This command must be run before running launchant.sh.
   b. To start the SAS Infrastructure for Risk Management migration file, run the following command:
      On Windows:
      \SAS-configuration-directory\Utilities\launchant.bat -file
      \SAS-installation-directory\SASHome\SASFoundation\9.4\misc\rmifirmmva\install\irmmigrate.xml
      On Linux:
      /SAS-configuration-directory/Utilities/launchant.sh -file
      /SAS-installation-directory/SASHome/SASFoundation/9.4/misc/rmifirmmva/install/irmmigrate.xml

3. Download the QRT federated area included in the SAS Firmwide for Solvency II federated content package. For information about downloading federated content packages for SAS Infrastructure for Risk Management solutions, see “Install Your Solution’s Federated Content” on page 32.

4. Connect to the SAS Infrastructure for Risk Management database that was automatically configured by SAS Deployment Wizard during installation in the \WebInfrastructurePlatformDataServer.


5. Run the irmmigrate.sql script located in the \SAS-installation-directory\SASHome\SASFoundation\9.4\misc\rmifirmmva\install\directory.

6. In the target environment, restart the SAS Infrastructure for Risk Management web application server.
Troubleshoot Migration Errors

If you receive any errors during migration, complete the following tasks on the target system:

1. Examine the SASIRMServer log to determine which instance generated the error. The SASIRMServer log is in one of the following locations:
   - Linux: `SAS-configuration-directory/Levn/Web/Logs/SASServer8_1/`
   - Windows: `SAS-configuration-directory\Levn\Web\Logs\SASServer8_1\`

2. For each instance that did not successfully migrate, note the instance key, the instance name, and the error reason.

3. Uninstall the newer SAS Infrastructure for Risk Management installation and re-install the prior installation.

4. Restore the system database backup.

5. Restore the persistent area backup.

6. Using your notes from Step 2, review each instance that did not successfully migrate, and address the issue that caused the error. If necessary, re-create the instance.

7. Re-install the new version of SAS Infrastructure for Risk Management and migrate the federated content.

8. If necessary, repeat the steps 1 through 7 until all instances migrate successfully.
Chapter 10

Upgrading SAS Infrastructure for Risk Management

About the Upgrade Process

When upgrading, ensure that you follow the instructions in the SAS Intelligence Platform documentation. For more information, see SAS 9.4 Guide to Software Updates at http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/install94.html.

The steps to perform an upgrade are similar to those required for a migration. However, the federated area and the persistent area do not need to be copied, since they are already located in the required location.

However, when performing an upgrade, ensure that you do not remove any federated areas. The federated areas include the following:

- all the platform federated areas from earlier releases (for example, com.sas.solutions.risk.irm.fa.0.3.1 and com.sas.solutions.risk.irm.fa.0.3.2)
- where applicable, earlier versions of the QRT federated area
- earlier versions of the current federated areas

To upgrade SAS Infrastructure for Risk Management, complete the tasks that are included in the following checklist.

<table>
<thead>
<tr>
<th>Completed?</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Perform the pre-upgrade tasks.</td>
</tr>
<tr>
<td></td>
<td>Upgrade SAS Infrastructure for Risk Management.</td>
</tr>
<tr>
<td></td>
<td>Migrate the solution’s federated content. This step applies to only SAS Infrastructure for Risk Management 3.1 upgrades.</td>
</tr>
</tbody>
</table>
Perform the Pre-upgrade Tasks

Before upgrading, ensure that you complete the following tasks:


2. Back up your existing system.

   **CAUTION:**
   
   The upgrade writes over the existing system. If any problems are encountered, it might be necessary to recover the existing system from backup. Keep in mind that your existing system can be corrupted to the point of being unusable and unrecoverable.

   **Note:** When you back up your system, ensure that you also back up the SAS Metadata Server. For more information, see “Backing Up and Recovering the SAS Metadata Server” in *SAS Intelligence Platform: System Administration Guide* at [http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html](http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html).


5. Download your order and create a SAS Software Depot. For instructions about how to download and create a SAS Software Depot, see “Create a SAS Software Depot” on page 23.

6. Stop all SAS services that are running in your environment.

Upgrade SAS Infrastructure for Risk Management

You upgrade SAS Infrastructure for Risk Management with the SAS Deployment Wizard.

When running the SAS Deployment Wizard, point to the downloaded depot and the location of your existing *SAS-installation-directory*. The SAS Deployment Wizard upgrades your installation to the new version.

For complete instructions about upgrading SAS Infrastructure for Risk Management from one version to another version on the same machine, see *SAS 9.4 Guide to Software Updates* at [http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/install94.html](http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/install94.html).
Migrate Federated Content

Note: This section applies only to a SAS Infrastructure for Risk Management 3.1 to a SAS Infrastructure for Risk Management 3.3 upgrade. The solution used in this section is SAS Firmwide for Solvency II.

If you are upgrading from SAS Infrastructure for Risk Management 3.1 to SAS Infrastructure for Risk Management 3.3, you must complete the steps in this section.

After completing the steps in this section, you will have a SAS Infrastructure for Risk Management 3.3 installation with your existing 3.1 federated content preserved as 3.3 content. The upgrade does not require the calculations to be rerun because the results from the source system are preserved on the target system.

To migrate federated content, complete the following steps:

1. In the target environment, stop the SAS Infrastructure for Risk Management web application server.

2. In the installation directory (/SAS-installation-directory/SASFoundation/9.4/misc/rmifirmmva/install), complete the following tasks:
   a. Edit the irmmigrate.properties file to include the path to the original federated area and to the new federated area.
      In addition, enter the path to the new base date directories. If more than one base date was defined in the federated area on the source system, enter an additional base date directory. If there was only one base date defined in the federated area on the source system, comment out the second base date in the irmmigrate.properties file on the target system.
   b. Edit the irmmigrate.sql file by replacing @New_FA_ID@ with the identifier of the existing federated area. However, you cannot use a zero (0) or the letter “z” as the first character. For example, if you are migrating the federated area with id=0.3.1, replace @New_FA_ID@ with 3.1.

3. Run the following commands:
   a. To set the required variables, run:
      On Windows:
      \SAS-configuration-directory\Lev\level_env.bat
      On Linux:
      /SAS-configuration-directory/Lev/level_env.sh
      Note: This command must be run before running launchant.sh.
   b. To start the SAS Infrastructure for Risk Management migration file, run the following command:
On Windows:
\SAS-configuration-directory\Utilities\launchant.bat -file
\SAS-installation-directory\SASHome\SASFoundation\9.4\misc\rmifirmmva\install\irmmigrate.xml

On Linux:
/SAS-configuration-directory/Utilities/launchant.sh -file
/SAS-installation-directory/SASHome/SASFoundation/9.4/misc/irmfmmva/install/irmmigrate.xml

4. Download the QRT federated area included in the SAS Firmwide for Solvency II federated content package. For information about downloading federated content packages for SAS Infrastructure for Risk Management solutions, see “Install Your Solution’s Federated Content” on page 32.

5. Connect to the SAS Infrastructure for Risk Management database that was automatically configured by SAS Deployment Wizard during installation in the /SAS-configuration-directory\Lev\WebInfrastructure\PlatformDataServer.


6. Run the irmmigrate.sql script located in the /SAS-installation-directory\SASHome\SASFoundation\9.4\misc\rmifirmmva\install\ directory.

7. In the target environment, restart the SAS Infrastructure for Risk Management web application server.

---

**Troubleshoot Upgrade Errors**

If you receive any errors when migrating federated content after upgrading your SAS Infrastructure for Risk Management, complete the following tasks:

1. Examine the SASIRMServer log to determine which instance generated the error. The SASIRMServer log is in one of the following locations:
   - Linux: SAS-configuration-directory\Lev\Web\Logs\SASServer8_1/
   - Windows: SAS-configuration-directory\Lev\Web\Logs\SASServer8_1/

2. For each instance that did not successfully migrate, note the instance key, the instance name, and the error reason.

3. Uninstall the newer SAS Infrastructure for Risk Management installation and re-install the prior installation.

4. Restore the system database backup.

5. Restore the persistent area backup.
6. Using your notes from Step 2, review each instance that did not successfully migrate, and address the issue that caused the error. If necessary, re-create the instance.

7. Re-install the new version of SAS and migrate the federated content.

8. If necessary, repeat the steps 1 through 7 until all instances migrate successfully.
Part 4

Administering SAS Infrastructure for Risk Management

Chapter 11
Managing Federated Areas ........................................ 59

Chapter 12
Additional Administrative Tasks .................................. 63

Chapter 13
Troubleshooting ......................................................... 67
Each federated area has its own landing area. The landing area is the Read-only data mart of a SAS Infrastructure for Risk Management solution. It contains the data objects (for example, SAS data sets) that are required for the flows that are defined in that federated area.

Here is the structure of the landing_area directory for a SAS Infrastructure for Risk Management federated area:

The landing area contains the following:

- The base date directories (named mmdyyyy) or date time directories (named mmdyyyyyhmms) for which calculations are performed. These directories contain the SAS data sets pertaining to the specific base date.

- The base directory, which contains configuration sets. Each configuration set contains the following directories:
  - mapping
    Contains mapping tables that are designed as stand-alone tables. They are not joined to other tables. Mapping tables map one or more variables to each other.
The mappings are used for transforming some raw data into the forms that are expected by the application. This transformation is part of the data enrichment process. The directory location of these tables is mapped by using the libnames.txt file in the config directory.

- **static**
  
  Contains input tables that make up the configuration data model. These tables contain a historical repository of risk configurations for SAS Infrastructure for Risk Management. The directory location of these tables is mapped by using the libnames.txt file in the config directory.

*Note:* The landing area of a SAS Infrastructure for Risk Management might contain additional folders.

---

**Add Additional Federated Areas**

**Overview**

You can add any number of federated areas to your SAS Infrastructure for Risk Management solution.

Creating a new federated area requires an understanding of how multiple federated areas relate to each other.

**CAUTION:**

Adding a federated area is the only operation that you can perform on a federated area.

When working with federated areas, note that the following operations are not supported and could result in system and data corruption:

- removing an installed federated area
- modifying the content of an installed federated area, with the exception of loading data
- modifying the federated area ID of an installed federated area
- modifying the path of an installed federated area
- adding the same federated area twice using different federated area IDs

Before adding a federated area, note the following:

- SAS Infrastructure for Risk Management defines the property `com.sas.solutions.risk.irm.fa`. This property is followed by a period-separated suffix that is the identifier for the federated area. For example, `com.sas.solutions.risk.irm.fa.1.0.3` defines a federated area with ID `1.0.3`.

*Note:* Identifiers that start with 0 or the letter z are reserved for content that is delivered by SAS. These identifiers should not be used when adding additional federated areas.

Here is a full example of federated content that is supplied for a SAS Infrastructure for Risk Management solution:

`com.sas.solutions.risk.irm.fa.1.0.3=/sas-configuration-directory/Levn/AppData/SASIRM/fal`
This statement defines a federated root of `/sas-configuration-directory/Lev1/AppData/SASIRM/fa1`.

- The ID for a federated area can contain numeric characters, alphabetic characters, and periods only. Identifiers that start with 0 or the letter z are reserved for content that is supplied by SAS. Do not use these identifiers when adding additional federated areas.

- The lexical ordering of identifiers determines the precedence of federated areas, as shown in the following example:

```plaintext
com.sas.solutions.risk.irm.fa.0.3.3=/config/Lev1/AppData/fa.0.3.3
com.sas.solutions.risk.irm.fa.2=/config/Lev1/AppData/fa_life
com.sas.solutions.risk.irm.fa.c=/config/Lev1/AppData/fa_cpmn
com.sas.solutions.risk.irm.fa.sample.3.3=/config/Lev1/AppData/fa.sample.3.3
```

In this example, 2.5 has precedence over 2, and 2 is higher than 1, and so on.

- When adding a federated area, you must define the property `com.sas.solutions.risk.irm.fa` and point to a location that is accessible to the workspace server.

### Adding a Federated Area

To add an additional federated area, complete the following steps:

1. Stop the SAS Infrastructure for Risk Management Web Application Server by running the following command in the appropriate directory.

   ```bash
tcruntime-ctl.sh stop
   ```

   For a non-clustered environment, the web application server is SASServer8_1. For a clustered environment, the web application servers can include SASServer8_2, SASServer_3, and so on, and can be on the same machine or on different machines within the cluster.


2. Create and populate the new federated area directory. Grant Read and Write permissions to the primary SAS group of the spawned server user.

3. In SAS Management Console, add the new federated area property by completing the following steps:

   a. Start SAS Management Console and connect to the appropriate metadata server as a SAS administrator (for example, sasadm@saspw).

   b. On the **Plug-ins** tab, verify that the repository is selected in the **Repository** field. The default repository is **Foundation**.

   c. Select **Application Management ⇧ Configuration Manager ⇧ SAS Application Infrastructure**.

   d. In the main pane, right-click **SAS IRM Mid-Tier Server** and select **Properties**. The IRM Mid-Tier Server Properties window is displayed.

   e. Click the **Advance** tab and then click **Add**. The Define New Property dialog box is displayed.
• In the **Property Name** field, enter `com.sas.solutions.risk.irm.fa.n`, where `n` is an ID that does not start with 0 or z.

  **Note:** Typically, you want the new property to have precedence. Therefore, the ID of the new federated area should be lexicographically greater than the ID of previous federated version IDs.

• In the **Property Value** field, enter the federated area directory path. Click **OK**.

  f. Grant Read permissions to the spawned server on the federated area directory.

  g. Restart the SAS Infrastructure for Risk Management web application server.

Chapter 12
Additional Administrative Tasks

Configure Middle-Tier Server Clustering on SAS Infrastructure for Risk Management

SAS Infrastructure for Risk Management 3.3 supports the SAS 9.4 Intelligence Platform middle-tier server clustering feature.

Horizontal clustering is the practice of deploying SAS Web Application Server instances on multiple machines. This configuration can help improve performance (load balancing) and provide greater availability to guard against hardware failure. If one machine or web application server instance crashes (or an application on one server instance stops), the applications remain available on the other machines (failover).


Add a Solution to an Existing Deployment

If you license more than one SAS Infrastructure for Risk Management product, you can install the second product by completing the following tasks:

1. Download the federated content package for the additional solution. For more information, see “Install Your Solution’s Federated Content” on page 32.
2. After you download the federated content for the additional solution, unzip the content package and use the installation instructions that are provided with the package to install the content.

3. Add the new content as a federated area to SAS Infrastructure for Risk Management. For information about how to add a federated area, see Chapter 11, “Managing Federated Areas,” on page 59.

Load New Data via Live ETL

Overview

In SAS Infrastructure for Risk Management 3.3, you can use the Live ETL feature to upload new data sets without affecting server operations. In other words, Live ETL enables new data sets to be uploaded and associated job flows to be automatically recalculated while all server operations are available. These server operations include (but are not limited to) the following:

- logging in and logging out
- creating job flow instances
- deleting job flow instances
- modifying job flow instances
- executing job flow instances

Live ETL supports the creation of new input data. However, it does not support deleting input data.

Setting Permissions

Ensure that the following permissions are set up for the user-delivered federated areas:

- The landing areas and the contents under it have Write permission to the SAS General Server user.
- The input areas directories have Write permission to the SAS General Server user.

Creating an Input Area

Because data sets in the landing area cannot be modified while job flow instances are running, you must create an input area into which you upload the new data. When creating the input area, note the following:

- The input area is located under the root of the federated area.
- There is one input area per federated area.
- To ensure compatibility with existing deployments, the path of the input area is %FA/input_area, where %FA is the path to the federated area.
The following diagram shows an example of the input area in the federated area:

```
/federated_area
/landing_area
/input_area
  /03312015/
    entity.sas7bdat
    ...
  /03312014/
    entity.sas7bdat
    ...
    funds.sas7bdat
    ...
    last_update.txt
    last_live_etl.success.txt
    ...
```

**Invoking Live ETL**

After you have uploaded the new data sets into the input area, invoke Live ETL by modifying the marker file named last_update.txt to update the file’s timestamp. The file is located in the input area. After the data has been uploaded to the input area and you update the marker file, Live ETL automatically performs the following tasks:

1. Stops the execution of all job flow instances that depend on the data that was uploaded.
2. Stops all new job flow execution requests that use the uploaded data.
3. Copies the content from the input area to the landing area.
4. Reloads the base dates and the configuration sets.
5. Updates the last_live.etl file to indicate whether the process completed successfully or with errors.

After the Live ETL process has been completed, all job flow instances that were affected by the upload have an OUT_OF_DATE status. If an affected instance is running, it is stopped and then marked OUT_OF_DATE. If a new instance is run during the Live ETL process, and is impacted by the Live ETL process, it is not executed and its status is set to OUT_OF_DATE.

---

**View the Input and Output Data Sets in SAS Studio**

At an experimental level, you can view SAS Infrastructure for Risk Management solution data set input and output SAS data sets and files in SAS Studio.

To enable SAS Infrastructure for Risk Management integration, add the `?show-studio=true` parameter at the end of the SAS Infrastructure for Risk Management solution web application URL as follows:

```
http://Your_Middle_Tier_Host:port/SASIRM/?show-studio=true
```
When integration with SAS Studio is enabled, you can right-click the input or output tables for a node and select **Open in SAS Studio** to view the file in SAS Studio.

When using this experimental feature, note the following limitations:

- To download and view SAS Infrastructure for Risk Management data sets in SAS Studio, ensure that your user password is saved in your account in metadata.

- SAS Infrastructure for Risk Management does not support Read-only locks on resources. Therefore, when opening a SAS Infrastructure for Risk Management table in SAS Studio, SAS Infrastructure for Risk Management responds to the SAS Studio request to lock a Read-only resource. When this occurs, a warning message in the SASIRMServer.log that indicates that the resource cannot be locked.
Chapter 13
Troubleshooting

Gather Information

Overview

When troubleshooting, try to isolate and describe the problem and the context in which it occurs.

TIP Specific error messages and warnings from SAS logs can help resolve a problem. Start at the top of SAS logs and search for the first error message. An initial error can cause many subsequent errors. Resolving the first error might eliminate subsequent errors.

Awareness of the following general classes of information can help expedite troubleshooting:

- operating system and configuration information
- a detailed description of the problem that includes the error messages and the action that was performed when the problem was encountered
- log files
- other files or screen shots
- sample test data

Before contacting SAS Technical Support, it is recommended that you review the SAS Knowledge Base for installation, problem, and usage notes. For more information, see the support website at http://support.sas.com/resources.
Also, it is recommended that you check for any hot fixes that might be available. For a list of hot fixes, see the SAS Hot Fix Downloads website.

You can use the SAS Hot Fix Analysis, Download and Deployment Tool (available from http://ftp.sas.com/techsup/download/hotfix/HF2/SASHFADD.html) to help automate deployment of hot fixes. This tool analyzes the SAS deployment registry and creates a customized report that lists hot fixes available for the installed SAS products. In addition, it generates scripts that automate the deployment of the hot fixes.

You can contact SAS Technical Support at http://support.sas.com/techsup.

Information about Your Environment and Configuration

If you request help from SAS Technical Support, be prepared with the following information:

• The site number for your organization.
• The name of your company.
• The SAS Infrastructure for Risk Management release number.
• The SAS release number (including the maintenance level or the patch level number).
• The list of installed SAS software releases and the hot fixes that are based on your SAS Deployment Registry. For information about how to obtain this list, see http://support.sas.com/kb/35/968.html.
• The number of tiers that are used in your SAS installation and the version of the operating system that is used for each tier.
• The hardware platform, the operating environment, the amount of physical memory, and the number of processors.
• The server language and the locale.
• A list of any nonstandard customizations that you have incorporated in the installation.
• The version of the SAS Infrastructure for Risk Management solution’s content. For information about where to find the content version number, see the content help.

Problem Description

Provide a complete description of the problem. Include a description of the general task being performed, your role and permissions, and what occurred during the SAS session. Provide details such as the following:

• Are you working with new data or updating existing data?
• How is the problem reproduced?
• What browser and release are you using?
• Is the problem locale-specific? If so, which locales are having problems?
• When did the problem first occur?
• Were any changes made that might have caused the problem? In particular, were any permissions changed on directories? Such changes can have unforeseen consequences.
**Sample Test Data**

If possible, capture the information entered that caused the problem. In certain situations, SAS Technical Support might request your data load files so that they can replicate your operating environment.

---

**Enable Detailed Logging**

SAS Infrastructure for Risk Management uses log4j to perform logging. When SAS Infrastructure for Risk Management begins running, the log4j configuration files for SAS Infrastructure for Risk Management are read from one of the following locations:

- **Linux:** \`SAS-configuration-directory/Web/Common/LogConfig/\`
- **Windows:** \`SAS-configuration-directory\Web\Common\LogConfig\`

The configuration filenames are **SASIRM.log4j.xml** and **SASIRMServer.log4j.xml**.

SAS Infrastructure for Risk Management writes information to the following log files, which are located in \`SAS-configuration-directory\Lev\nWeb/Logs/SASServer8_1/\` by default:

- **SASIRM.log** — contains messages from the SAS Infrastructure for Risk Management.
- **SASIRMServer.log** — contains messages from the SAS Infrastructure for Risk Management server.

To debug a problem, you can change the log level to DEBUG.

SAS Infrastructure for Risk Management should run under this logging level only for capturing additional log information. Do not use this logging level for daily operations of SAS Infrastructure for Risk Management.

**CAUTION:**

Excessive logging can degrade performance. Therefore, use the DEBUG level only when directed by SAS Technical Support.

For detailed information about logging, see *SAS Intelligence Platform: Middle-Tier Administration Guide* at [http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html](http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html).


To enable DEBUG logging for SAS Infrastructure for Risk Management, complete the following steps:

1. Navigate to the **SASIRMServer-log4j.xml** configuration file that is located in one of the following directories:
   - **Linux:** \`SAS-configuration-directory/Web/Common/LogConfig/\`
   - **Windows:** \`SAS-configuration-directory\Web\Common\LogConfig\`

   **Note:** For most troubleshooting purposes, enable DEBUG logging in the **SASIRMServer-log4j.xml** configuration file.
2. Locate the following code:

```xml
<logger name="com.sas.solutions.risk.irm" additivity="false">
  <level value="INFO"/>
  <appender-ref ref="SAS_FILE"/>
  <appender-ref ref="SAS_CONSOLE"/>
</logger>
```

3. Replace “INFO” with “DEBUG” and save the file.

```xml
<logger name="com.sas.solutions.risk.irm" additivity="false">
  <level value="DEBUG"/> 
  <appender-ref ref="SAS_FILE"/> 
  <appender-ref ref="SAS_CONSOLE"/> 
</logger>
```

4. Restart the SAS Infrastructure for Risk Management web application server.

---

**Fix Your Web Application Log File Display**

In some environments (for example, Simplified Chinese), SAS Infrastructure for Risk Management web application log files that are viewed in a web browser contain unreadable content. Log files are unreadable because SAS Infrastructure for Risk Management web application log files are not created with UTF-8 character encoding, but they are displayed on the web browser in UTF-8 character encoding.

To fix the display of an unreadable log file in a Windows environment, complete the following steps:

1. Stop the SAS Infrastructure for Risk Management web application server.
2. Navigate to the `\SAS-configuration-directory\config\Lev\Web\WebAppServer\SASServer8_1\conf` directory.
3. In the `wrapper.conf` file, add the following statement:

   ```
   wrapper.java.additional.n=-Dfile.encoding=UTF-8 
   ```

   where `n` is the next available digit in the series of additional Java parameters.
4. Restart the SAS Infrastructure for Risk Management web application server.

To fix an unreadable log file display in a Linux environment, complete the following steps:

1. Stop the SAS Infrastructure for Risk Management web application server.
2. Navigate to the `/SAS-configuration-directory/config/Lev/Web/WebAppServer\SASServer8_1/bin` directory.
3. Use the `setenv.sh` to set the Java environment to the UTF-8 encoding as follows:

   ```
   JVM_OPTS="Dfile.encoding=UTF-8"
   ```
4. Restart the SAS Infrastructure for Risk Management web application server.

---

**Log and Configuration File Locations**

The following table lists the log files that might contain relevant logging information.
<table>
<thead>
<tr>
<th>File</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration logs</td>
<td>/SAS-configuration-directory/Logs/Configure</td>
</tr>
<tr>
<td>SAS Infrastructure for Risk Management web application logs</td>
<td>/SAS-configuration-directory/Web/Logs</td>
</tr>
<tr>
<td>Note: By default, the log files for the SAS Infrastructure for Risk Management application do not appear at this location unless they are configured in SAS Management Console.</td>
<td></td>
</tr>
<tr>
<td>SAS Infrastructure for Risk Management Log4J application log</td>
<td>SAS Infrastructure for Risk Management uses the open-source Java library Log4j for application logging. The logging behavior is configured in the SASIRM-log4j.xml file and in the SASIRMServer-log4j.xml file (located in /SAS-configuration-directory/Web/Common/LogConfig/) for the SAS Infrastructure for Risk Management middle tier. Most of the details in these files, especially the various logging levels, should not be modified. However, you can customize some information by modifying these files. Here are examples of information that you can modify:</td>
</tr>
<tr>
<td>• the location of the log file</td>
<td></td>
</tr>
<tr>
<td>• file storage properties</td>
<td></td>
</tr>
<tr>
<td>• use of rolling logs</td>
<td></td>
</tr>
<tr>
<td>• the number of log files</td>
<td></td>
</tr>
<tr>
<td>• the maximum size of log files</td>
<td></td>
</tr>
<tr>
<td>Object spawner log</td>
<td>/SAS-configuration-directory/ObjectSpawner/Logs</td>
</tr>
<tr>
<td>SAS Workspace Server logs</td>
<td>/SAS-configuration-directory/SASApp/WorkspaceServer/Logs</td>
</tr>
<tr>
<td>SAS Metadata Server log</td>
<td>/SAS-configuration-directory/SASMeta/MetadataServer/Logs</td>
</tr>
</tbody>
</table>

Note: Note that the paths in the preceding table are different if you choose to set up common directories.
Gain Greater Insight into Your SAS® Software with SAS Books.

Discover all that you need on your journey to knowledge and empowerment.

support.sas.com/bookstore for additional books and resources.