



SAS[®] Infrastructure for Risk Management 3.4: Administrator's Guide

The correct bibliographic citation for this manual is as follows: SAS Institute Inc. 2017. *SAS® Infrastructure for Risk Management 3.4: Administrator's Guide*. Cary, NC: SAS Institute Inc.

SAS® Infrastructure for Risk Management 3.4: Administrator's Guide

Copyright © 2017, SAS Institute Inc., Cary, NC, USA

All Rights Reserved. Produced in the United States of America.

For a hard copy book: No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, or otherwise, without the prior written permission of the publisher, SAS Institute Inc.

For a web download or e-book: Your use of this publication shall be governed by the terms established by the vendor at the time you acquire this publication.

The scanning, uploading, and distribution of this book via the Internet or any other means without the permission of the publisher is illegal and punishable by law. Please purchase only authorized electronic editions and do not participate in or encourage electronic piracy of copyrighted materials. Your support of others' rights is appreciated.

U.S. Government License Rights; Restricted Rights: The Software and its documentation is commercial computer software developed at private expense and is provided with RESTRICTED RIGHTS to the United States Government. Use, duplication, or disclosure of the Software by the United States Government is subject to the license terms of this Agreement pursuant to, as applicable, FAR 12.212, DFAR 227.7202-1(a), DFAR 227.7202-3(a), and DFAR 227.7202-4, and, to the extent required under U.S. federal law, the minimum restricted rights as set out in FAR 52.227-19 (DEC 2007). If FAR 52.227-19 is applicable, this provision serves as notice under clause (c) thereof and no other notice is required to be affixed to the Software or documentation. The Government's rights in Software and documentation shall be only those set forth in this Agreement.

SAS Institute Inc., SAS Campus Drive, Cary, NC 27513-2414

March 2024

SAS® and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.

Other brand and product names are trademarks of their respective companies.

3.4-P1:irmag

Contents

PART 1 Introduction to SAS Infrastructure for Risk Management 1

Chapter 1 • Welcome to SAS Infrastructure for Risk Management	3
What Is SAS Infrastructure for Risk Management?	3
Using the SAS Infrastructure for Risk Management: Administrator's Guide	3
What's New in SAS Infrastructure for Risk Management 3.4	4
Chapter 2 • SAS Infrastructure for Risk Management Architecture	5
SAS Infrastructure for Risk Management Architecture	5
SAS Infrastructure for Risk Management Data Flow	7
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	14

PART 2 Deploying SAS Infrastructure for Risk Management 19

Chapter 4 • 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 5 • Installing SAS Infrastructure for Risk Management	27
Overview of the Installation Tasks	27
Review the File System Structure	27
Install SAS Infrastructure for Risk Management	28
Install Federated Content	31
Chapter 6 • Performing Post-installation Tasks	33
Overview of the Post-installation Tasks	33
Use the Instructions.html File	34
Groups, Roles, and Capabilities	34
Configure the Metadata Accounts	35
Apply SAS Security Updates	37
Configure SAS Infrastructure for Risk Management to Use HTTP over an SSL Connection	38
Access the SAS Infrastructure for Risk Management Solution Web Application	38

Access the SAS Infrastructure for Risk Management SAS-based Interface	38
Back Up Content	39

PART 3 Migrating and Upgrading SAS Infrastructure for Risk Management 41

Chapter 7 • Upgrade and Migration Overview	43
About Migrating and Upgrading	43
Releases That Support Migration or Upgrade	43
Chapter 8 • Migrating SAS Infrastructure for Risk Management	45
About the Migration Process	45
Review Additional Documentation	46
Design Your Migration	47
Create a Migration Package in Your Source Environment	47
Migrate SAS Infrastructure for Risk Management	47
Migrate Federated Content	49
Troubleshoot Migration Errors	50
Chapter 9 • Upgrading SAS Infrastructure for Risk Management	53
About the Upgrade Process	53
Perform the Pre-upgrade Tasks	54
Upgrade SAS Infrastructure for Risk Management	54
Troubleshoot Upgrade Errors	55

PART 4 Administering SAS Infrastructure for Risk Management 57

Chapter 10 • Additional Administrative Tasks	59
Configure Middle-Tier Server Clustering On SAS Infrastructure for Risk Management	59
Add a Solution to an Existing Deployment	60
Add Additional Federated Areas	60
Load New Data via Live ETL	62
Enable WebDAV Access to SAS Infrastructure for Risk Management Data	64
View Input and Output Data Sets in SAS Studio	65
Simplify Access to Third-Party Data with Generic Libraries	65
Define a Temporary Data Library for Large Data Sets	67
Back Up and Restore Job Flow Instances	67
Configure the Development Environment	70
Chapter 11 • Troubleshooting	73
Gather Information	73
Enable Detailed Logging	75
Fix Your Web Application Log File Display	76
Log and Configuration File Locations	76

Part 1

Introduction to SAS Infrastructure for Risk Management

<i>Chapter 1</i>	
Welcome to SAS Infrastructure for Risk Management	3
<i>Chapter 2</i>	
SAS Infrastructure for Risk Management Architecture	5
<i>Chapter 3</i>	
SAS Infrastructure for Risk Management Federated Content	9

Chapter 1

Welcome to SAS Infrastructure for Risk Management

What Is SAS Infrastructure for Risk Management?	3
Using the SAS Infrastructure for Risk Management: Administrator's Guide	3
What's New in SAS Infrastructure for Risk Management 3.4	4

What Is SAS Infrastructure for Risk Management?

SAS Infrastructure for Risk Management is a high-performance job execution engine with web-based and SAS-based user interfaces that you can order and deploy with one or more SAS solutions. SAS Infrastructure for Risk Management solutions are delivered as industry-specific content releases that you download after you install SAS Infrastructure for Risk Management. Calculations are performed using job flows.

For development purposes, you can order SAS Infrastructure for Risk Management 3.4 as a stand-alone product that you can use to create custom content using parallel programs called job flows. For information about SAS Infrastructure for Risk Management 3.4 development using the SAS-based interface, see *SAS Infrastructure for Risk Management 3.4: Programmer's Guide*.

The SAS Infrastructure for Risk Management platform is designed to be customizable and flexible. The architecture of SAS Infrastructure for Risk Management provides a simplified way to develop and run the fastest analytics.

Using the SAS Infrastructure for Risk Management: Administrator's Guide

SAS Infrastructure for Risk Management: Administrator's Guide is for administrators who are responsible for installing and configuring content that uses SAS Infrastructure for Risk Management as a platform.

This administrator must perform the following tasks:

- Use SAS Download Manager to download a SAS Software Depot to each machine on which an installation is performed.
- Install and configure the SAS Intelligence Platform and the SAS Infrastructure for Risk Management platform and associated content modules.

- Use 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*.

For information about how to develop parallel programs and federated content for the SAS Infrastructure for Risk Management platform, see *SAS Infrastructure for Risk Management: User's Guide*.

What's New in SAS Infrastructure for Risk Management 3.4

SAS Infrastructure for Risk Management 3.4 provides a higher level of automation and integration than prior releases. SAS Infrastructure for Risk Management 3.4 supports workflows that integrate the SAS MultiVendor Architecture, SAS Viya, third-party data sources, and deep learning.

SAS Infrastructure for Risk Management 3.4 introduces the role of a developer persona and provides SAS Studio support for an integrated development platform for high-performance analytics that leverages the power of parallel computing.

SAS Infrastructure for Risk Management 3.4 introduces the following features and enhancements:

- private custom content development using SAS Studio, which provides the following capabilities:
 - task and job flow development
 - backing up and restoring job flow instances
 - macros that simplify data partitioning
 - data visualization
- the enhanced New Instance window, which provides the following features:
 - uploading input files when creating a job flow instance
 - hierarchical selection of base dates and entities
 - display of the federated area identifier associated with the job flow instance
- ability to edit the name and description of an existing job flow instance
- summary diagram for a job flows
- support for temporary libraries, which reduce disk space footprint
- support for generic library definitions in the libnames.txt file of a federated area, which simplifies access to third-party data
- fixes and performance enhancements

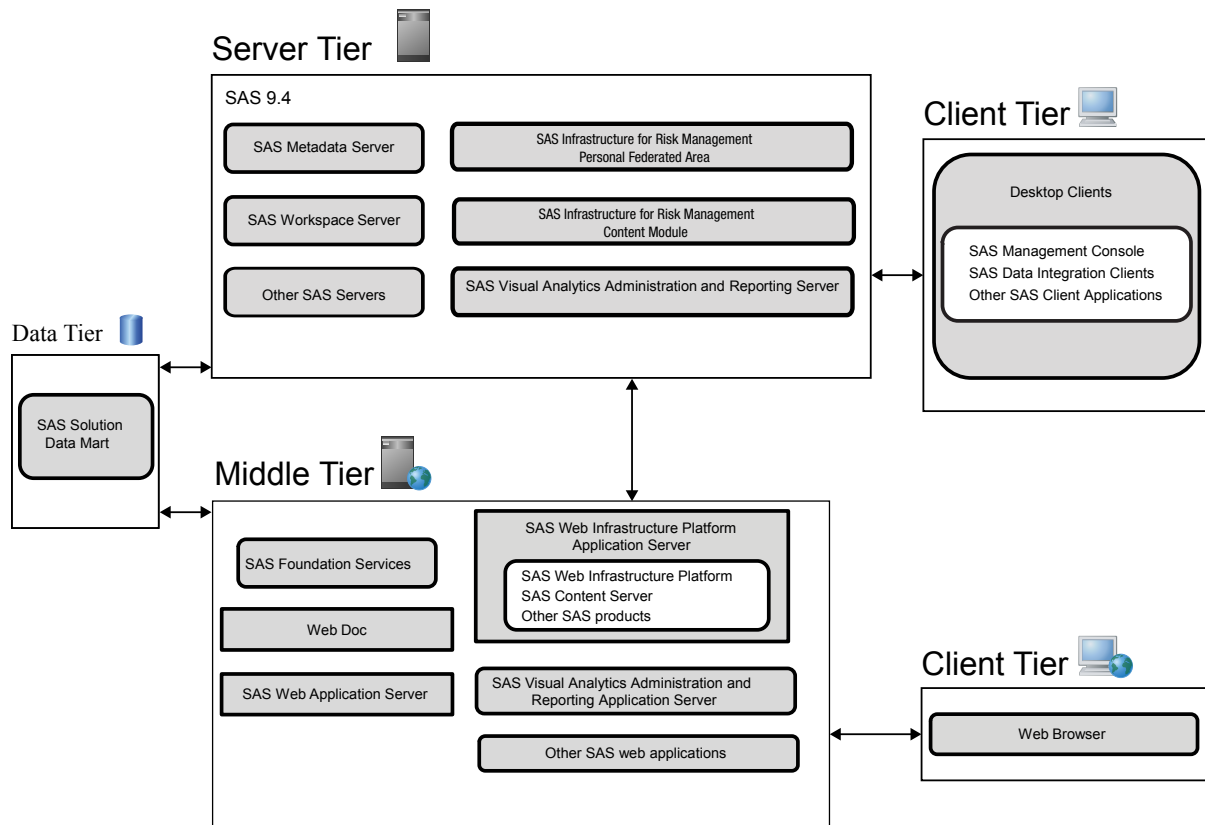
Chapter 2

SAS Infrastructure for Risk Management Architecture

SAS Infrastructure for Risk Management Architecture	5
SAS Infrastructure for Risk Management Data Flow	7
SAS Infrastructure for Risk Management Distributed Development	7
Overview	7
Contributors	8
Federated Content	8

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

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

Middle Tier

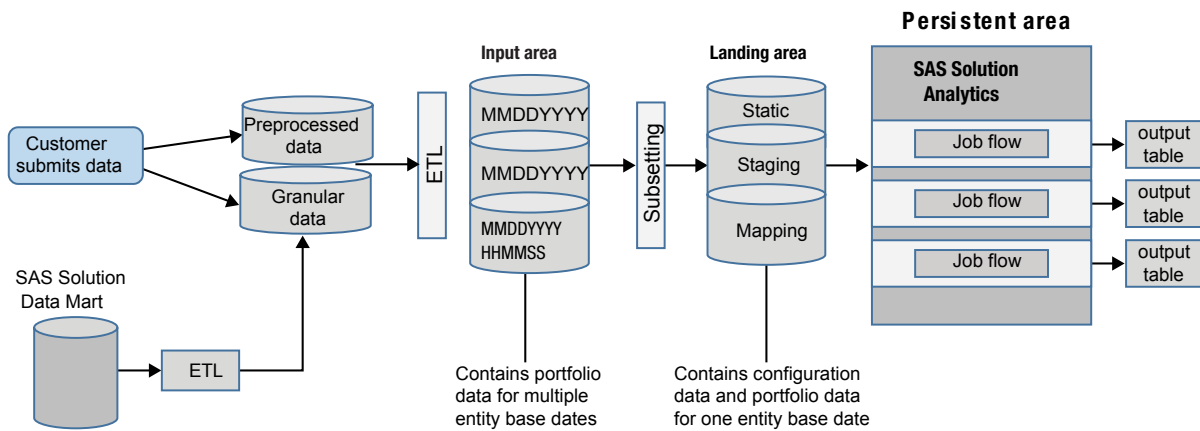
- receives and processes web requests from the client tier and passes these requests to the server tier and the data tier
- contains a web application server in addition to web applications such as the SAS Infrastructure for Risk Management web application

Client Tier

- initiates requests (via desktop client applications or web browsers) to perform the necessary work and to view formatted output
- contains the SAS Infrastructure for Risk Management web application, which is from systems that are part of the client tier, for your access
- contains the GUI, which 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.



Here is the basic data flow process for SAS Infrastructure for Risk Management:

1. Data is supplied to a solution in one of the following ways:
 - The customer submits data directly to the landing area of a federated area.
 - When the system is running, the customer submits data directly to the input 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 of a federated 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 – **mmddyyyy**) or date and time (14-character string – **mmddyyyyhhmmss**).
3. The output of the job flow is placed in the *persistent area*. The persistent area is a Read/Write area for input and output tables (XLSX, XBRL, 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 that runs on the SAS Infrastructure for Risk Management platform.

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, you can break those flows. For example, you might break the flows if you changed the number or nature of the outputs of a subflow. Therefore, coordination of development groups is also necessary to ensure the integrity of the code that is being developed.
- With the exception of loading data, all installed federated areas are read-only.
- The personal federated area can be modified within the parameters described in *SAS Infrastructure for Risk Management 3.4: Programmer's Guide*.
- Once installed, a federated area must never 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*. 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	9
Overview	9
Federated Area Folder	10
Landing_Area Folder	11
Config Folder	12
Job Flow Folder	13
Source Folder	13
SAS Infrastructure for Risk Management Federated Content Development	14
What is Federated Content?	14
Federated Content Processing	14
Federated Job Flows	15
Federated Tasks	15
Federated Input Tables	15
How Federated Input Tables Are Processed	16
The Personal Federated Area	17

Structure of the SAS Infrastructure for Risk Management Federated Area

Overview

The federated content that runs on the SAS Infrastructure for Risk Management platform shares the same architecture and layout. The differences among the content are in the calculation content that is stored in the *federated area* of the federated content.

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 a federated area.

A federated area contains the following elements:

- flows – files that describe the job flow
- code – string message data, tasks (including Java tasks), 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

It is important to understand the distinction between federated and non-federated content in order to maintain future releases or to develop content.

Only the flows, tasks, and input files are *federated content*, which means that this content is shared among multiple federated areas. All 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.

When you install SAS Infrastructure for Risk Management 3.4, the following federated areas are also installed:

- fa.0.3.4 contains only those elements that are required to make the platform run. There is no content in the platform federated area.
- fa.sample.3.4 contains sample content to use for testing the SAS Infrastructure for Risk Management installation and to use as a reference.
- fa.*user_name* is an optional *personal federated area*. The personal federated area is created on demand. In a personal federated area, developers can write content using parallel programs called job flows.

CAUTION:

Do not modify or delete a federated area. Installed federated areas should not be changed. You cannot delete or modify the content of a federated area on disk, and you cannot delete or modify the federated area identifier that is metadata. If you modify or delete a federated area, database corruption and loss of data might occur.

However, here are two exceptions:

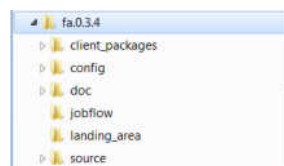
- You can upload data to the input area or the landing area of a federated area other than the platform federated area.
- If you are a content developer, you can modify and delete the content your personal federated area (typically using the scripting client). The system manages the integrity of the job flow instances that reference your personal federated area. However, you cannot delete your personal federated area. For information about developing content using a personal federated area, see *SAS Infrastructure for Risk Management 3.4: Programmer's Guide*.

The following sections describe the elements of a federated area and the content of the folders in a federated area.

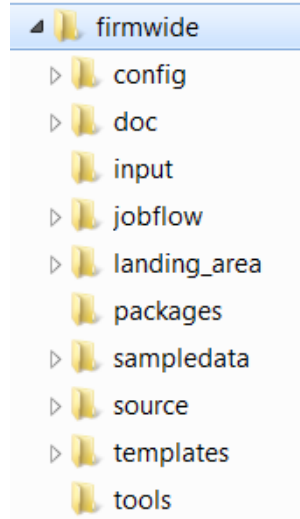
Federated Area Folder

When you install SAS Infrastructure for Risk Management, a platform federated area is created in the *SAS-configuration-directory/Levn/AppData/SASIRM/fa.0.3.4*.

Here is the basic structure of the SAS Infrastructure for Risk Management platform federated area (fa.0.3.4) folder:



Here is the basic structure of a SAS Infrastructure for Risk Management solution (SAS Firmwide Risk for Solvency II) federated area folder:

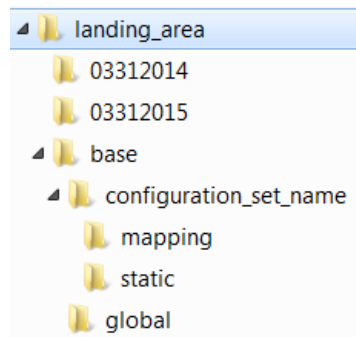


Note: A federated area can contain more folders or fewer folders than appear in these examples. However, a federated area must always contain these subfolders: config, doc, jobflow, landing_area, and source.

Landing_Area Folder

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** folder in a federated area:



The landing area contains the following:

- The base date folders (named **mmddyyyy**) or date time folders (named **mmddyyyyhhmmss**) for which calculations are performed.
These folders contain the data sets that pertain to the specific base date.
- The base folder, which contains configuration sets. Each configuration set contains the following folders:
 - 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 location of these tables is mapped by using the `libnames.txt` file in the config folder.

- static

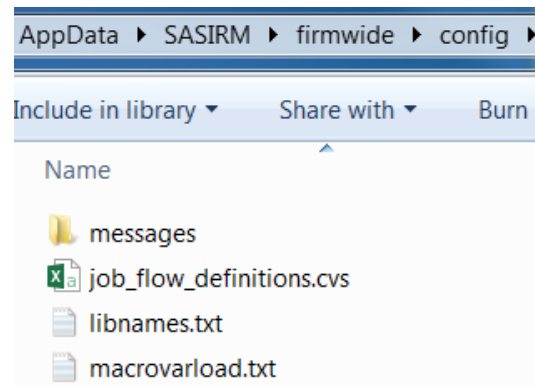
Contains *input tables* that make up the configuration data model. These tables contain a historical repository of risk configurations for SAS Infrastructure for Risk Management. The location of these tables is mapped by using the `libnames.txt` file in the config folder.

Note: The landing area of a federated area might contain additional folders.

Config Folder

Developers use the files in the config folder to configure the behavior of job flows.

Here is the structure of the config folder:



The config folder contains the following files:

- `job_flow_definitions.csv`

Contains 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 (using the `LIBNAME` statement) to the location of the directory that contains the static input tables.

Note: With SAS Infrastructure for Risk Management 3.4, you can also define generic libraries in the `libnames.txt` file that can be used as input data.

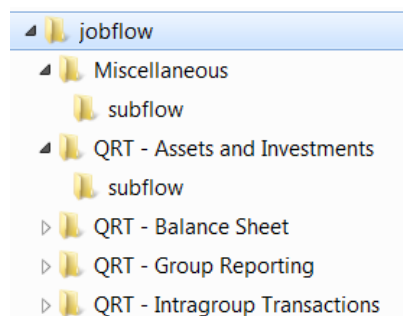
- `macrovarload.txt`

Lists SAS data sets that define global macro variables that must be loaded before a task executes.

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

Job Flow Folder

Here is the structure of the job flow folder:



The job flow folder contains *job flow definitions* or subdirectories that contain job flow definitions. A job flow definition is the program file that connects one or more tasks that need to be executed to complete a job.

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 job flow folder are displayed as **Categories** in the SAS Infrastructure for Risk Management web application user interface. The categories are defined in the `job_flow_definitions.csv` file.

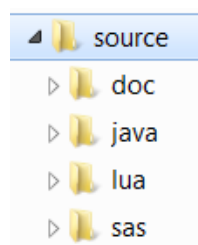
Job flows consist of one of the following elements:

- the tasks that are required to complete a job
- subflows
- input and output data files that are associated with the tasks

Source Folder

The source folder contains code that delivers the content functionality.

Here is the structure of the source folder:



The following folders are included in the source folder:

- `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
 - umacros (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 folder.

SAS Infrastructure for Risk Management Federated Content Development

What is Federated Content?

- *Federated content* is contained in *federated areas*.
- Federated content is the mechanism by which developers add custom content to SAS Infrastructure for Risk Management.
- Only flows, tasks (including Java tasks), and input files are considered to be federated because the content is shared across federated areas. All other content in a federated area (macros, Lua code, and so on) is not shared. This non-shared content is accessible only from within the federated area in which it is located.

Note: Tasks that are written in both SAS and Java can be federated.

Federated Content Processing

- Only job flow files, tasks (.sas files), and input tables are federated content that is shared across multiple federated areas. All other content is specific to the federated area in which it is located and is not shared. For example, a task in federated area 1 cannot call a macro in federated area 2.
- SAS Infrastructure for Risk Management searches for federated content in federated areas from the highest to lowest precedence (by the federated ID assigned in metadata and in alphabetical order), until it finds the content.

Federated Job Flows

- Job flow files are shared across federated areas.
- When searching for a job flow definition, SAS Infrastructure for Risk Management searches the federated areas from the highest to lowest precedence. For example, if federated area 2 contains a file named flow1 and federated area 1 also contains a file named flow1, the file in federated area 2 is used for creating a new instance of a job flow.
- After a new instance is created, the instance does not change the definition. For example, if a flow1 file is added later to a federated area that is at a higher precedence, the existing instances of previously created flows that use this definition are not affected. However, new instances will use the new definition.

Federated Tasks

- Like job flows, tasks that are identified within a flow are searched for in federated areas from the highest to lowest precedence.
- Tasks with the same name are assumed to be the same content. Therefore, a task named task1.sas accepts the same input tables and produces the same output tables as other tasks with the same name, regardless of their federated location.
- Like job flow definition files, changing or adding a new version of a task does not affect existing job flow instances. However, new executions of an instance will use the newest definition of task1.sas.
- During execution of a task, the context of that execution environment is isolated to the federated area in which it resides. Any macro or Lua code that is called by the task must exist in the same federated area of the task.
- Tasks can have input and output files that are partitioned. Partitioned tasks enable large amounts of data to be partitioned into smaller units of data and calculated across multiple cores. The task recombines the results of the partitioned data.

For detailed information about partitioned tasks, see the documentation that is included in the generic sample federated area (fa.sample.3.4). The sample 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 tasks must be mapped in 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 (using the LIBNAME statement) to a folder.

For example, `GLOBAL=%1a/base/global` specifies the folder `base/global` within the federated area in the `landing_area` folder. The libref `GLOBAL` should refer to that path.

- Tasks can reference tables using one-, two-, or three-level names. Here are examples of table names:
 - GLOBAL
 - GLOBAL.myglobal
 - GLOBAL.myglobal.sas7bdat

Note: The latter two examples are processed identically. In the second example, the `sas7bdat` suffix is assumed, by default. One-level names are processed somewhat differently than two- and three-level names.

- SAS Infrastructure for Risk Management 3.4 supports generic library definitions in the `libnames.txt` file of a federated area. Use of generic library definitions simplifies access to third-party data. For information about defining generic libraries, see [“Simplify Access to Third-Party Data with Generic Libraries”](#) on page 65.

How Federated Input Tables Are Processed

This section explains how federated input tables are processed by SAS Infrastructure for Risk Management.

Assume that the following three federated areas exist:

- `com.sas.solutions.risk.irm.fa.0.3.4` — `/sas-configuration-directory/Levn/AppData/SASIRM/fa.0.3.4`
- `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 in the federated area from the 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 2.5 is greater than 2.)

SAS Infrastructure for Risk Management is looking for a mapping for `GLOBAL`. If it finds a mapping, it adds the path to the concatenated `LIBNAME` statement that is used to define `GLOBAL`. This path is the first path in the `LIBNAME` statement. 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 task fails with an error.

Processing two- or three-level names is similar to processing one-level names, 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 it does not find a mapping, it searches the next federated area (by precedence). If SAS Infrastructure for Risk Management finds a mapping, it verifies that the file actually exists in the folder that is specified in the mapping.

Mapping enables content developers to overwrite a single table without having to override all tables using the same mapping (`LIBNAME`).

If SAS Infrastructure for Risk Management cannot locate the table, the task is not created and the SAS Infrastructure for Risk Management New Instance wizard reports 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 was previously described. Both tables reside in federated area 1, but only GLOBAL.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');
```

According to the LIBNAME statement, the tables are located as follows:

- table1.sas7bdat is found in federated area 2 (*sas-configuration-directory/Levn/AppData/SASIRM/fa2/landing_area/base/global*)
- table2.sas7bdat is found in federated area 1 (*sas-configuration-directory/Levn/AppData/SASIRM/fa1/landing_area/base/global*)

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”)

Note: SAS recommends that you use three-level names in your job flow definitions and uppercase mapping in your libnames.txt files.

The Personal Federated Area

SAS Infrastructure for Risk Management 3.4 introduces support for a developer persona. When logging on to SAS Infrastructure for Risk Management for the first time, the developer’s personal federated area is automatically created. A personal federated area is where a developer creates content using parallel programs called job flows.

For information about the SAS Infrastructure for Risk Management personal federated area, see *SAS Infrastructure for Risk Management 3.4: Programmer’s Guide*.

Part 2

Deploying SAS Infrastructure for Risk Management

<i>Chapter 4</i>	
Performing Pre-installation Tasks	21
<i>Chapter 5</i>	
Installing SAS Infrastructure for Risk Management	27
<i>Chapter 6</i>	
Performing Post-installation Tasks	33

Chapter 4

Performing Pre-installation Tasks

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

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 4.1 *Pre-installation Checklist*

Completed?	Task
	Verify your system requirements.
	Complete the pre-installation tasks for SAS Intelligence Platform.
	Create the SAS Infrastructure for Risk Management user accounts.
	Create a SAS Software Depot.
	Download and install the required third-party software.

Completed?	Task
	Set SAS Web Application directory permissions on UNIX. (This task is required only for SAS deployments that predate the SAS 9.4M7 February 2022 release.)
	Obtain a deployment plan.
	Complete the pre-installation checklist that accompanies your deployment plan.
	Check for installation notes.

Verify Your System Requirements

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

For a list of the requirements, see System Requirements – SAS Infrastructure for Risk Management 3.4 at <http://support.sas.com/documentation/prod-p/irm/index.html>.

Note: Depending on the federated content that is installed, the system requirements might differ.

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 SAS Infrastructure for Risk Management, 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](#) website.

The *SAS 9.4 Intelligence Platform: Installation and Configuration Guide* provides pre-installation tasks and instructions to guide you through a typical installation of SAS Intelligence Platform.

Before you install SAS Infrastructure for Risk Management, review the [SAS 9.4 Intelligence Platform: Installation and Configuration Guide](#).

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 a SAS installation data file, order data, and product data.

The depot also contains the SAS Deployment Wizard, which is the tool that you use to install and initially configure SAS 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 and specify the location where to save the file.
5. When your browser has finished downloading the SAS Download Manager, run it.

6. In the Choose Language window, select the language that you want the SAS Download Manager to use when it displays text and click **OK**.
7. 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.
8. On the Order Information page in the SAS Download Manager, enter your order number and the SAS installation key.
9. On the Specify Order Details page, add a description to distinguish this order from other SAS orders.
10. Review the list of SAS products that are included in your order.
11. 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.
12. On the Specify SAS Software Depot Options page, complete the following steps:
 - a. In the **SAS Software Depot Directory** field, specify the location of the directory in which to download the software and build the SAS Software Depot.
 - b. (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.
 - c. 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**.
13. On the Final Review page, click **Download** to begin downloading, uncompressing, and creating a SAS Software Depot for your SAS order.
14. When the download is complete, click **Finish** to close the SAS Download Manager.

For information about copying a depot or subsetting your order, see *SAS 9.4 Intelligence Platform: Installation and Configuration Guide*.

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. The deployment file is an XML file that 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.

For more information about deployment plans, see "[Planning Your Deployment](#)" in *SAS Intelligence Platform: Installation and Configuration Guide*.

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

Note: This task is required only for SAS deployments that predate the SAS 9.4M7 February 2022 release.

On UNIX systems, the SAS Web Application Server stores its license files in the `/etc/opt/vmware/vfabric` folder. Therefore, you must create this folder 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:

```
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

For additional information, check the SAS Installation Notes that are available on the SAS Customer Support website. You can search for SAS Installation Notes for SAS Infrastructure for Risk Management and solutions at <http://support.sas.com/notes/index.html>.

Chapter 5

Installing SAS Infrastructure for Risk Management

Overview of the Installation Tasks	27
Review the File System Structure	27
Install SAS Infrastructure for Risk Management	28
Install Federated Content	31

Overview of the Installation Tasks

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

Completed?	Task
	Review the structure of the SAS Infrastructure for Risk Management file system.
	Install and configure SAS Infrastructure for Risk Management.
	Download and install the SAS Infrastructure for Risk Management solution's federated content package.

Review the File System Structure

After you install and configure SAS Infrastructure for Risk Management, by default, the following directories exist:

Directory	Default Location
<i>SAS-installation-directory</i>	<ul style="list-style-type: none"> Linux: <i>/SAS-installation-directory/SASHome/</i> Windows: <i>C:\Program Files\SASHome\</i>

Directory	Default Location
!SASROOT (SAS Foundation Directory)	<ul style="list-style-type: none"> Linux: <code>/SAS-installation-directory/SASHome/SASFoundation/9.4/</code> Windows: <code>C:\Program Files\SASHome\SASFoundation\9.4\</code>
SAS_configuration_directory	<ul style="list-style-type: none"> Linux: <code>/SAS-installation-directory/config/Levn/</code> Windows: <code>C:\SAS\Config\Levn\</code>
SAS Infrastructure for Risk Management data directory (the product's root data directory)	<ul style="list-style-type: none"> Linux: <code>/SAS-configuration-directory/Levn/AppData/SASIRM/</code> Windows: <code>\SAS-configuration-directory\Levn\AppData\SASIRM\</code>
SAS Deployment Wizard Installation Summary	<ul style="list-style-type: none"> Linux: <code>/SAS-configuration-directory/Levn/Documents/DeploymentSummary.html</code> Windows: <code>\SAS-configuration-directory\Levn\Documents\DeploymentSummary.html</code>
SAS Deployment Wizard configuration logs	<ul style="list-style-type: none"> Linux: <code>/SAS-configuration-directory/Levn/Logs/Configure</code> Windows: <code>\SAS-configuration-directory\Levn\Logs\Configure</code>
Web application server logs <i>Note:</i> By default, some logging is enabled. You can configure additional logging in the SAS Management Console.	<ul style="list-style-type: none"> Linux: <code>/SAS-configuration-directory/Levn/Web/Logs</code> Windows: <code>\SAS-configuration-directory\Levn\Web\Logs</code>
SAS Infrastructure for Risk Management middle-tier staging directory	<ul style="list-style-type: none"> Linux: <code>/SAS-configuration-directory/Levn/Web/Staging</code> Windows: <code>\SAS-configuration-directory\Levn\Web\Staging</code>

Install SAS Infrastructure for Risk Management

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.

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

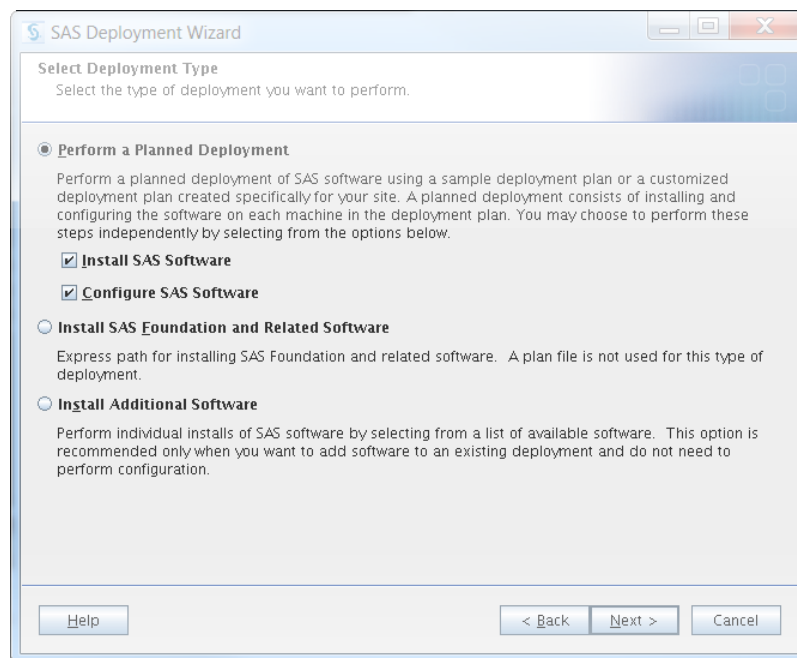
- the contents of your custom order
- the plan.xml file

CAUTION:

Do not add spaces to the installation and configuration paths when installing SAS Infrastructure for Risk Management. If you add a space to the paths, it causes the SAS Infrastructure for Risk Management server to fail. The default paths (C:\SASHome and C:\Config) do not contain spaces.

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 that is 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

SAS IRM Super User Credentials
Enter a password for the SAS IRM internal super user.

Super User ID:
sasirmsu

Password:
[Empty]

Confirm password:
[Empty]

Help < Back Next > Cancel

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.

SAS Deployment Wizard

SAS IRM Mid-tier Configuration
SAS IRM Mid-tier allows the user to customize the name displayed in the web application header and banners. Select a name which will be displayed in the web application title and banners.

SAS IRM Web Application Name:
SAS Infrastructure for Risk Management

Help < Back Next > Cancel

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.

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

The screenshot shows a window titled "SAS Deployment Wizard" with a sub-header "SAS IRM Database Credentials". Below the sub-header is the instruction "Enter a password for accessing the SAS IRM database." There are four input fields: "Database Name:" with the text "irmdb", "User ID:" with the text "irmadmin", "Password:" (empty), and "Confirm password:" (empty). At the bottom of the window are three buttons: "Help", "< Back", and "Next >" (highlighted), and a "Cancel" button.

- 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.

- 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.

If you ordered SAS Infrastructure for Risk Management 3.4 as part of a solution (such as SAS Firmwide for Solvency II), after you install and configure SAS Infrastructure for Risk Management, you must download, unzip, and install the solution's federated content. For information about downloading and installing federated content, see "[Install Federated Content](#)" on page 31.

Install Federated Content

The federated content that runs on SAS Infrastructure for Risk Management shares the same architecture and layout. The difference between the federated content in different federated areas is the calculation content that is delivered in a SAS Infrastructure for Risk Management 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:

- Access the Downloads page at <https://support.sas.com/downloads/>.

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 SAS Infrastructure for Risk Management solution, use the installation instructions that are provided with the package to install and verify the content.

Chapter 6

Performing Post-installation Tasks

Overview of the Post-installation Tasks	33
Use the Instructions.html File	34
Groups, Roles, and Capabilities	34
About Capabilities	34
Predefined Roles and Capabilities for SAS Intelligence Platform	34
Predefined Group and Roles	34
Configure the Metadata Accounts	35
Apply SAS Security Updates	37
Configure SAS Infrastructure for Risk Management to Use HTTP over an SSL Connection	38
Access the SAS Infrastructure for Risk Management Solution Web Application .	38
Access the SAS Infrastructure for Risk Management SAS-based Interface	38
Back Up Content	39

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.

Completed?	Task
	Follow the instructions in the Instructions.html file.
	Create the metadata user accounts and assign the user to groups.
	Apply applicable SAS security updates and manually move updated JAR files to the required location.
	Access the SAS Infrastructure for Risk Management solution user interface through your web browser.

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

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.

Application	Documentation
Metadata Server	<i>SAS Intelligence Platform: System Administration Guide</i>
Desktop Applications	<i>SAS Intelligence Platform: Desktop Application Administration Guide</i>
Web Applications	<i>SAS Intelligence Platform: Web Application Administration Guide</i>

Predefined Group and Roles

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

SAS Infrastructure for Risk Management also has a built-in internal super user (sasirmsu). This user is defined in SAS Management Console with the user ID sasirmsu@saspw). The sasirmsu super user is also a member of IRM:Access All Entities role.

The naming convention of roles is extended to include other actions, in addition to access

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

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

For information about creating roles, see *SAS Management Console: Guide to Users and Permissions* at <http://support.sas.com/documentation/onlinedoc/sasmc/index.html>.

Configure the Metadata Accounts

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 9.4 Intelligence Platform: Security Administration Guide*.

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_ID
```

 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_ID** — 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_ID** as the name for the role, where:

- **action** — Valid values are **Access** (create, view, and modify job flow instances for 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_ID** — A valid value matches the name of the entity exactly.

Here is an example of a custom role that enables a user to publish instances for an entity named ENTITY_BE:

```
IRM: Publish Entity ENTITY_BE
```

Here is an example of a customer role that enables a user to create, view and modify job flow instances for the same entity (ENTITY_BE):

```
IRM: Access Entity ENTITY_BE
```

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

Apply SAS Security Updates

As a part of the hot-fix process, SAS delivers security fixes.

After you apply a security fix to an existing SAS Infrastructure for Risk Management deployment, any updated JAR files in that security fix that also exist in the SAS Infrastructure for Risk Management platform federated area (fa.0.3.4) must be manually copied from where the files are installed to where they are located in the SAS Infrastructure for Risk Management platform federated area.

Here is a table that lists the JAR file or files by SAS security update that you have to manually copy to the SAS Infrastructure for Risk Management platform federated area after applying the security update to an existing deployment.

Table 6.1 SAS Security Updates and Updated JAR Files

SAS Security Update	Updated JAR Files
SAS Security Update 2018-09	<code>commons_io_2.6.0.0_SAS_20180621100654/commons-io.jar</code>

To obtain SAS Security Updates and to access detailed information about how to apply security updates to your SAS Infrastructure for Risk Management installation, see [SAS Security Updates and Hot Fixes](#).

After you apply the security update, complete the following steps:

1. Back up the SAS Infrastructure for Risk Management platform federated area.
2. Stop the SAS Infrastructure for Risk Management web application server.
3. Copy the updated JAR file or files from the SAS Versioned JAR Repository location:

```
/SASHome/SASVersionedJarRepository/eclipse/plugins/
```

to the SAS Infrastructure for Risk Management platform federated area location:

```
/SAS-configuration-directory/LevN/AppData/SASIRM/fa.0.3.4/  
source/java/lib/
```

Note: Ensure that you overwrite the existing JAR file or files in the SAS Infrastructure for Risk Management platform federated area.

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

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:

1. Navigate to `/SASHome/SASVersionedJarRepository/eclipse/plugins/`.
2. In the subdirectories, locate the following two SAS/SECURE JAR files: `sastpj.rutil_version-number.jar` and `sas.rutil_version-number.jar` where *version-number* is a variable that indicates the release of the file.
3. Copy the files to the Java file folder for the platform federated area `/sas_config_directory/Levn/AppData/SASIRM/fa.0.3.4/source/java/lib`.
4. Restart the SAS Infrastructure for Risk Management web application server.

For information, see [SAS 9.4 Intelligence Platform: Security Administration Guide](#).

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.

Access the SAS Infrastructure for Risk Management SAS-based Interface

SAS Infrastructure for Risk Management 3.4 provides a SAS-based programming interface using SAS Studio. This interface provides the following capabilities:

- task and job flow development
- backing up and restoring job flow instances
- macros that simplify data partitioning
- data visualization

For information about configuring and using the programming interface, see *SAS Infrastructure for Risk Management 3.4: Programmer's Guide*.

Back Up 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

<i>Chapter 7</i>	
Upgrade and Migration Overview	43
<i>Chapter 8</i>	
Migrating SAS Infrastructure for Risk Management	45
<i>Chapter 9</i>	
Upgrading SAS Infrastructure for Risk Management	53

Chapter 7

Upgrade and Migration Overview

About Migrating and Upgrading	43
Releases That Support Migration or Upgrade	43

About Migrating and Upgrading

You can move software from a previous release to the current release of SAS Infrastructure for Risk Management using either of the following methods:

- 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 8, “Migrating SAS Infrastructure for Risk Management,”](#) on page 45.

- 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 9, “Upgrading SAS Infrastructure for Risk Management,”](#) on page 53.

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.

Migration from the Specified Release	Migration to SAS Infrastructure for Risk Management 3.4
3.1	No
3.2	Yes
3.3	Yes
3.4	Yes

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.

Upgrade from the Specified Release	Upgrade to SAS Infrastructure for Risk Management 3.4
3.1	No
3.2	Yes
3.3	Yes

Chapter 8

Migrating SAS Infrastructure for Risk Management

About the Migration Process	45
Review Additional Documentation	46
Design Your Migration	47
Create a Migration Package in Your Source Environment	47
Migrate SAS Infrastructure for Risk Management	47
Migrate Federated Content	49
Troubleshoot Migration Errors	50

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).

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

Completed?	Task
	Review additional documentation.
	Design your migration.
	Create a migration package in your source environment.
	Back up your source system.
	Migrate SAS Infrastructure for Risk Management.
	Migrate the solution's federated content.

CAUTION:

Ensure that you follow the steps included in this chapter when migrating a system. Performing any step that is not documented could result in an installation that SAS Infrastructure for Risk Management does not support. For questions about whether SAS Infrastructure for Risk Management supports a configuration step that is not clearly documented, 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 3.4

<http://support.sas.com/documentation/prod-p/irm/index.html>

- SAS Notes

SAS Notes provides late-breaking installation information. You can search for SAS Notes for SAS Infrastructure for Risk Management and SAS Infrastructure for Risk Management solutions at <http://support.sas.com/notes/index.html>.

- *SAS 9.4 Intelligence Platform 9.4: Migration Guide*

Design Your Migration

To design your migration, complete the following tasks:

- Review “High-Level SAS Migration Requirements” in *SAS 9.4 Intelligence Platform: Migration Guide*

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 3.4 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.

For information about how to use the SAS Migration Utility, see *SAS 9.4 Intelligence Platform: Migration Guide*.

Migrate SAS Infrastructure for Risk Management

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

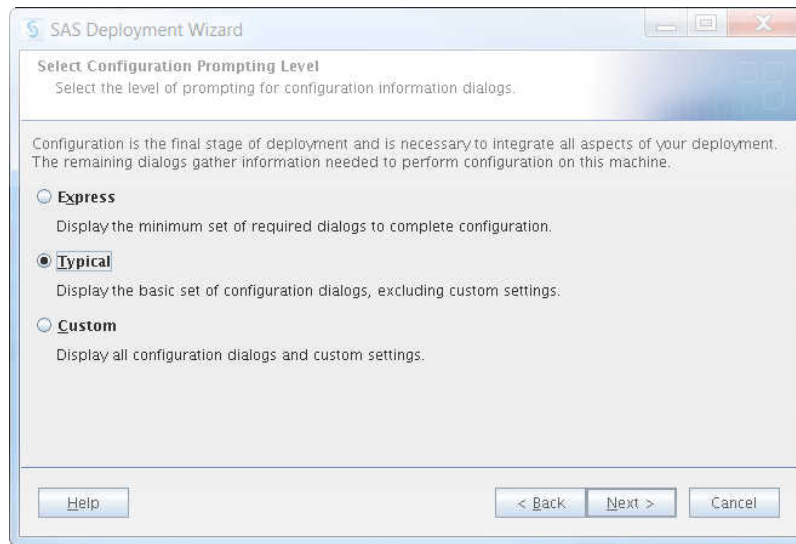
When you perform a migration for SAS Infrastructure for Risk Management, the process is similar to a typical out-of-the-box deployment. The primary difference between the two methods is that during the SAS Deployment Wizard session, you select the **Perform Migration** option on the Migration Information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

CAUTION:

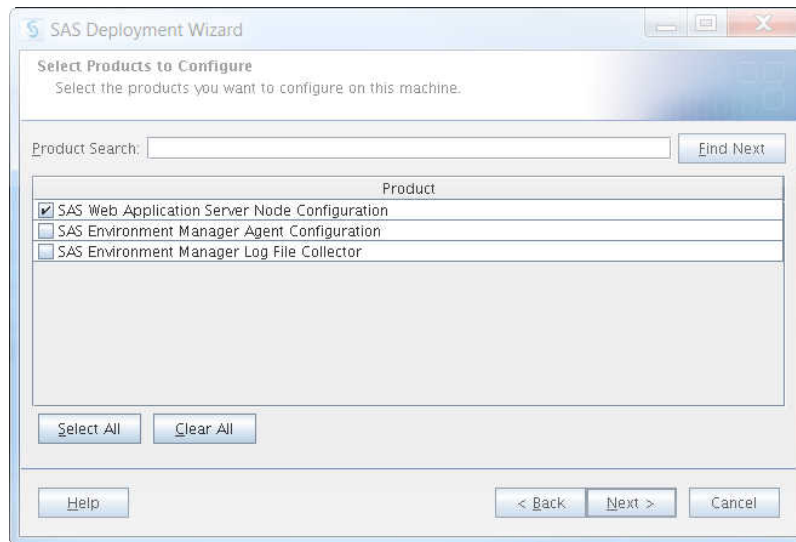
Before beginning the migration process, ensure that you back up your installation.

When migrating, note the following differences between a migration and a typical out-of-the-box deployment:

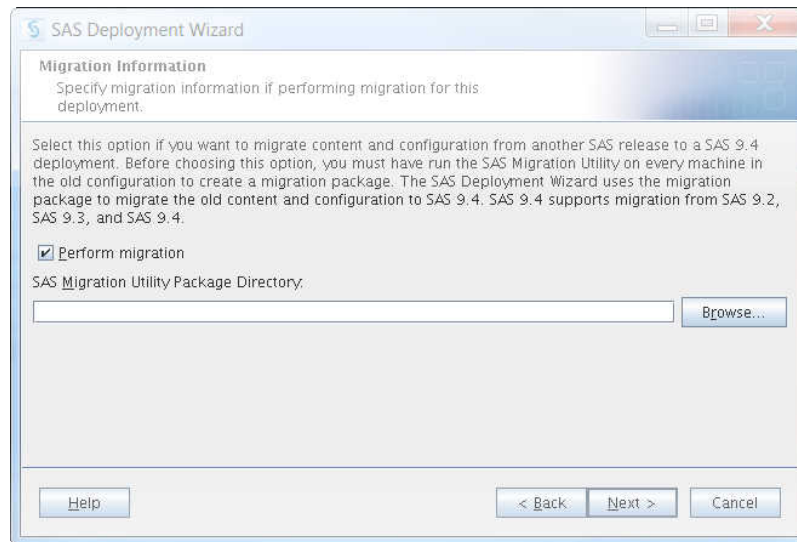
1. To configure all products in one execution of the SAS Deployment Wizard, click **Typical** on the Configuring Prompting Level page.



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**.

For detailed information about each page of the SAS Deployment Wizard, see *SAS 9.4 Intelligence Platform: Migration Guide, Second Edition*.

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:

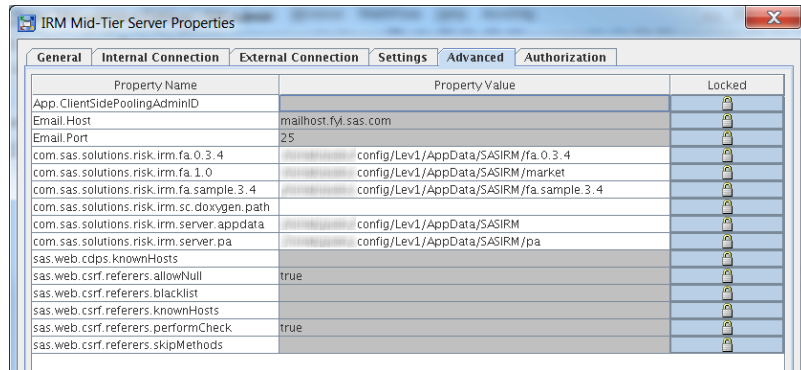
1. Copy all federated areas from the source location to the exact same location on the target system.

This includes the following:

- all of the platform federated areas from earlier releases (for example, com.sas.solutions.risk.irm.fa.0.3.1, com.sas.solutions.risk.irm.fa.0.3.2, and com.sas.solutions.risk.irm.fa.0.3.3)
 - where applicable, earlier versions of QRT federated area
 - earlier versions of the current federated areas
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.



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.
5. To complete the migration, 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 or instances generated the error or errors. The SASIRMServer log is located 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 previous installation.
4. Restore the source system database backup.
5. Restore the source system persistent area backup.

6. Using your notes from Step 2, review each instance that did not successfully migrate, and address the issue or issues 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 9

Upgrading SAS Infrastructure for Risk Management

About the Upgrade Process	53
Perform the Pre-upgrade Tasks	54
Upgrade SAS Infrastructure for Risk Management	54
Troubleshoot Upgrade Errors	55

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*.

The steps to perform an upgrade are similar to those required for a migration. However, the federated areas 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. This includes the following:

- all of the platform federated areas from earlier releases (for example, com.sas.solutions.risk.irm.fa.0.3.1, com.sas.solutions.risk.irm.fa.0.3.2, and com.sas.solutions.risk.irm.fa.0.3.3)
- where applicable, earlier versions of 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.

Completed?	Task
	Perform the pre-upgrade tasks.
	Upgrade SAS Infrastructure for Risk Management.

CAUTION:

Ensure that you follow the steps included in this chapter when upgrading a system. Performing any step that is not documented could result in an installation that SAS Infrastructure for Risk Management does not support. For questions about

whether SAS Infrastructure for Risk Management supports a configuration step that is not clearly documented, contact SAS Technical Support (at <http://support.sas.com/techsup> before you proceed.

Perform the Pre-upgrade Tasks

Before upgrading, ensure that you complete the following tasks:

1. Review *SAS 9.4 Guide to Software Updates*.
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 9.4 Intelligence Platform: System Administration Guide*.

3. Understand how the SAS Deployment Wizard upgrades SAS software. For more information, see “Adding, Updating, and Upgrading SAS Software” in *SAS 9.4 Intelligence Platform: Installation and Configuration Guide*.
4. Locate and familiarize yourself with your SAS software order. For more information, see “Reviewing Your Software Order,” in *SAS 9.4 Guide to Software Updates*.
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 using the SAS Deployment Wizard.

When running the SAS Deployment Wizard from your SAS Infrastructure for Risk Management 3.4 depot, point to 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*.

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 or instances generated the error or errors. The SASIRMServer log is located 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 previous 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 or issues 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.

Part 4

Administering SAS Infrastructure for Risk Management

<i>Chapter 10</i>	
Additional Administrative Tasks	59
<i>Chapter 11</i>	
Troubleshooting	73

Chapter 10

Additional Administrative Tasks

Configure Middle-Tier Server Clustering On SAS Infrastructure for Risk Management	59
Add a Solution to an Existing Deployment	60
Add Additional Federated Areas	60
Load New Data via Live ETL	62
Overview	62
Setting Permissions	63
Creating an Input Area	63
Invoking Live ETL	63
Enable WebDAV Access to SAS Infrastructure for Risk Management Data	64
View Input and Output Data Sets in SAS Studio	65
Simplify Access to Third-Party Data with Generic Libraries	65
About Using Generic Libraries	65
Standard Library Definition	66
Generic Library Definition	66
Define a Temporary Data Library for Large Data Sets	67
Back Up and Restore Job Flow Instances	67
Backing Up Job Flow Instances	68
Restoring Job Flow Instances	69
Configure the Development Environment	70

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

SAS Infrastructure for Risk Management 3.4 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).

For information about middle-tier server clustering, see *SAS 9.4 Intelligence Platform Middle-Tier Administration Guide* at <http://support.sas.com/documentation/cdl/en/bimtag/68217/HTML/default/viewer.htm#titlepage.htm>.

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 Federated Content](#)” on page 31.
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 “[Add Additional Federated Areas](#)” on page 60.

Add Additional Federated Areas

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

Adding 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`.

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


```
com.sas.solutions.risk.irm.fa.1.0.3=/sas-configuration-
directory/Levn/AppData/SASIRM/fa1
```

This statement defines a federated root of `/sas-configuration-directory/Levn/AppData/SASIRM/fa1`.

- The ID for a federated area can contain numeric characters, alphabetic characters, and periods only.

Note: Identifiers that start with the number zero (0) are reserved for functionality content that is delivered by the SAS Infrastructure for Risk Management platform federated area. Do not use these identifiers when adding an additional federated area.

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

```
com.sas.solutions.risk.irm.fa.0.3.4=/config/Lev1/AppData/fa.0.3.4
com.sas.solutions.risk.irm.fa.2=/config/Lev1/AppData/fa_life
com.sas.solutions.risk.irm.fa.c=/config/Lev1/AppData/fa_cpmm
com.sas.solutions.risk.irm.fa.sample.3.4=/config/Lev1/AppData/fa.sample.3.4
```

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.

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

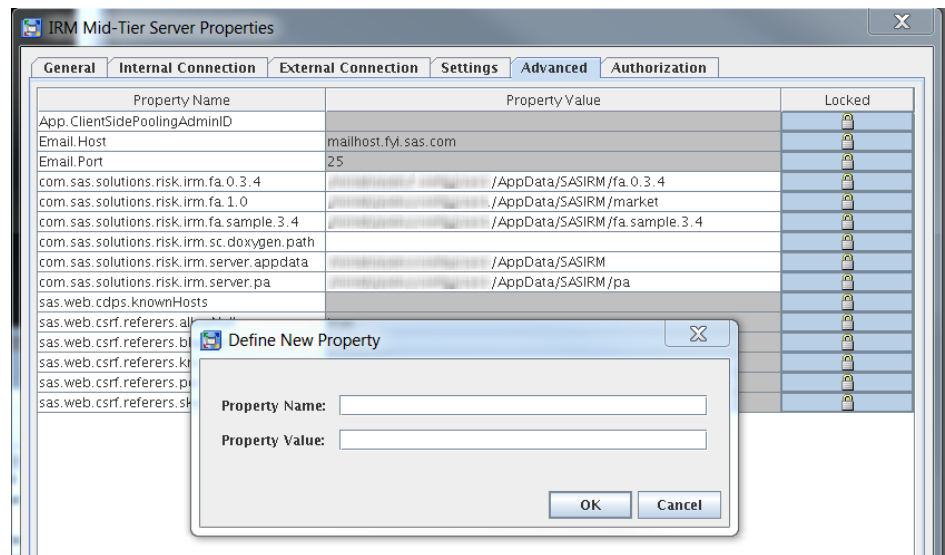
1. Stop the SAS Infrastructure for Risk Management web application server by running the following command in the appropriate directory.

```
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.

For more information about stopping SAS Web Application Servers, see *SAS 9.4 Intelligence Platform: Middle-Tier Administration Guide*.

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 **Advanced** 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 the number zero (0).
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.
For more information about starting SAS Web Application Servers, see *SAS 9.4 Intelligence Platform: Middle-Tier Administration Guide*.

Load New Data via Live ETL

Overview

In SAS Infrastructure for Risk Management 3.4, 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.

Here is an example of the input area in the federated area:

```

/federated_area
...
/landing_area
/input_area
    /03312017
        entity.sas7bdat
        ...
    /03312016
        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.

Enable WebDAV Access to SAS Infrastructure for Risk Management Data

SAS Infrastructure for Risk Management uses WebDAV to provide users an easy way to access to the following types of SAS Infrastructure for Risk Management information:

- job flow definition files
- input and output SAS data sets and their corresponding Microsoft Excel files
- task log files
- the execution status of job flow instances and sub-flow instances
- the execution of status of tasks
- the navigation hierarchy of the data

Before using WebDAV to access SAS Infrastructure for Risk Management data, note the following restrictions:

- The scope of data that a user can access is controlled by permissions that are associated with the user's log on credentials.
- The content of a flow instance is accessible only to the owner of the flow. If the instance is shared, the content is accessible to users that have access to the business entities of the flow instance.
- The contents of the SAS Infrastructure for Risk Management WebDAV servlet are Read-Only and cannot be deleted.

SAS Infrastructure for Risk Management users can access the data store in a centralized location on a remote server using WebDAV by using either of the following methods:

- Access the data from a WebDAV drive that is mapped to your computer:
 1. Map the SAS Infrastructure for Risk Management WebDAV servlet drive to your computer. For information about mapping the WebDAV servlet drive to your computer, refer to the documentation for your operating system.
 2. Access the drive on your local system and click your user ID to navigate to the data that you want to access.
- Use the LIBNAME statement to directly map a libref to a WebDAV URL.

Associate a libref with a SAS library to enable access to WebDAV. The following example associates the libref that is named davdata with the WebDAV directory / **users/mydir/datadir** on the WebDAV server www.websserver.com:

```
libname davdata v9 "https://www.websserver.com/users/mydir/datadir"
webdav user="mydir" pw="12345";
```

For detailed information about using the LIBNAME statement for WebDAV server access, see *SAS 9.4 Statements: Reference, Fifth Edition*.

View Input and Output Data Sets in SAS Studio

You can view SAS Infrastructure for Risk Management solution data set input and output, SAS data sets, and files in SAS Studio.

To view SAS Infrastructure for Risk Management input and output files in SAS Studio, complete the following steps:

1. In the SAS Infrastructure for Risk Management web application, open the job flow instance for which you want to view the input and output files for a task.
2. Right-click the input or output files for a task and select **Open in SAS Studio** from the pop-up menu. The file is displayed in SAS Studio.

When using this feature, note the following limitations:

- To download and view 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 is sent the SASIRMServer.log that indicates that the resource cannot be locked.

Simplify Access to Third-Party Data with Generic Libraries

About Using Generic Libraries

Each federated area contains a libnames.txt file in which you allocate various libraries. SAS Infrastructure for Risk Management 3.4 supports the generic library statements in the libnames.txt file. This feature simplifies access to third-party data that is located outside of a federated area. For example, this data could be located in a relational database management system, Hadoop, CAS, and so on. This data can also be used as input or output data for a federated area.

In prior releases, SAS Infrastructure for Risk Management only supported the definition of SAS libraries located within a federated area in the libnames.txt file of that federated area.

Here is an example of the libnames.txt file for a federated area in which no generic libraries have been allocated:

```
# Input Libnames definition
# All Keys should be upper case
# Parameters:
#   - %la -> Resolves to the Landing Area of the Federated Content
#   - %bd -> Resolves to the Base Date (ddmmyyyy)
#   - %cs -> Resolves to the Configuration Set
```

```

#
#Allocation of Global lib
GLOBAL=%la/base/global

#Allocation of Landing Area libs
LA_STGMK=%la/%bd
RP_INPUT=%la/report_input

LA_STTMK=%la/base/%cs/static
LA_MAPMK=%la/base/%cs/mapping

#Allocation of Persistent Area common libs
RPTMRT = /opt/sas/reportmart

```

Standard Library Definition

Here is the syntax that you use to define a standard SAS Infrastructure for Risk Management library entry in the libnames.txt file:

```
GLOBAL=%la/base/global
```

where:

- GLOBAL is the name of the library.
- %la resolves to the landing area of the federated area.
- /base/global is the path to the library in the federated area that is allocated in the libnames.txt file.

Generic Library Definition

Before you define a generic library, note the following:

- You can define a generic library only as an input library.
- In the libnames.txt file, you must start the statement for the generic library with the keyword LIBREF.
- The exact syntax for the LIBREF statement follows the equal sign (=) in the libnames.txt file. Depending on the type of library that you are defining, engine information, database, and schema might also be required.
- A generic library definition that contains %pa is ignored and flagged as an error.
- If a generic library is used by multiple federated areas, you must define that generic library in the exact same way in the libnames.txt file of each federated area.
- Generic libraries are supported for SAS tasks.
- Generic libraries with user credentials must be owned by SAS General Servers.
- You must specify the authentication domain of the generic library.

Here is a syntax that you use to define a generic library entry in the libnames.txt file:

```
LIBREF <LIB_NAME>=<engine_verbatim>; IRMAUTHDOMAIN=<Domain>,<user>
```

where:

- LIBREF is the keyword to begin the definition.
- LIB_NAME is the name of the generic library.

- `engine_verbatim` is the engine and location to use to access the files in the library.
- (Optional) `IRMAUTHDOMAIN` is the keyword to specify the authentication domain and user.

Here are some additional examples of generic libraries defined in the `libnames.txt` file:

```
# Input Libnames definition

#Allocation of Generic Libraries
LIBREF PGLIB=POSTGRES SERVER="localhost" DATABASE="mydb" PORT=9432;IRMAUTHDOMAIN=MyAuthDomain
LIBREF NODMNWIN=BASE "C:/";IRMAUTHDOMAIN=none
LIBREF NODMNLAX=BASE "/tmp";IRMAUTHDOMAIN=none
LIBREF ELIB= POSTGRES SERVER="localhost" DATABASE="mydb" PORT=9432
```

Define a Temporary Data Library for Large Data Sets

A *temporary library* is a data library that is promptly and automatically deleted as soon as is no longer needed during the execution of a job flow. Using temporary libraries minimizes the disk space footprint of large data sets.

Before you define a temporary library, note the following restrictions:

- Since temporary data is nonpersistent data, it does not participate in the data object pooling process. Therefore, during the execution of a job flow, tasks with any temporary data as its input or output is always executed.
- You can define a temporary library only for libraries that are generated as outputs from SAS tasks.
- A `NodeData` object must provide a method (for example, `Boolean isNonPersistentData()`), which returns the value, `True`, if the data is in a temporary data library.

To define a temporary library, enter the following statement in the `libnames.txt` file of the federated area in which you want to create the temporary library:

```
MK_CONF=%TMPLIB
```

Back Up and Restore Job Flow Instances

SAS Infrastructure for Risk Management 3.4 provides two scripts that a user can use to back up all information specific to job flow instances in a Microsoft Excel file. After backing up a user's instances, the file is used to restore the instances on a different machine or a different version of SAS Infrastructure for Risk Management. These scripts are executed in SAS Studio (connected to a SAS Infrastructure for Risk Management server). The information in this section assumes that users have logged on to SAS Infrastructure for Risk Management and created job flow instances.

Backing Up Job Flow Instances

Before you back up job flow instances, ensure that all users who created the existing job flow instances that you are backing up have passwords that have been configured for their user accounts.

To verify that SAS Infrastructure for Risk Management users have passwords that have been configured for their accounts, complete the following steps:

1. Log on to SAS Management Console and select **User Manager** from the **Plug-ins** tab.
2. Right-click the user name and select **Properties** ⇒ **Accounts**.
3. In the logins defined for the user list, select the user row and click **Edit**. The Edit Login Properties dialog box is displayed.
4. If necessary, enter a password in the **Password** field and the same password in the **Confirm Password** field, and click **OK**.
5. Exit SAS Management Console.

To back up instances created by a specific user, complete the following steps:

1. Log on to SAS Studio as the user who created or modified the job flow instances that you are backing up.
2. Press **F4** to open a new SAS program in the work area.
3. In the work area, click the **Code** tab, enter the following:

```
%irm_bkup_instances(debug={TRUE | FALSE}, logOptions= ,
bkup_file_path=path-to-where-to-create-the-backup-file
```

where:

- debug — Enables or disables debug logging. The default is False.
- logOptions — Specifies standard SAS logging options such as mprint, mlogic, symbolgen, and so on. The default is blank.
- bkup_file_path — Specifies the path to a writable location where the backup file will be created.

4. Click .

After executing the script, the following should occur:

- A tabular display of instances created by or shared with the logged in user should appear in the **Results** tab
- A ZIP file named bkup_inst_YYYYMMDD_HH-MI-SS.zip is located in the Navigation pane under **Files (Home)**. To view the contents of the file, double-click the name of the file. Inside the ZIP file is an .xlsx file named existing_instances_username.xlsx, where *username* is the name of the user whose job flow instances you backed up. This file contains the tabular listings that are displayed under the **Results** tab.

Note: The ZIP file is saved at the location that you specified for the bkup_file_path parameter. You will use this ZIP file to restore the job flow instances.

- If a job flow instance had uploaded input data, the uploaded data sets are located in instance-specific folders. The name of the folder is the instance key. The name of the

folder that contains the data sets corresponds to the libref of the data sets in the job flow instance.

Note: To view any errors or warnings that occurred during the execution of the backup script, click the **Log** tab.


Restoring Job Flow Instances

After you have backed up job flow instances, you can restore the instances on a different machine or different version of SAS Infrastructure for Risk Management.

1. Copy the ZIP file of the backed up instances to the target machine.
2. If desired, you can unzip the file and edit the existing_instances_username.xlsx file. You can change the names of instances or delete the row of an instance if you do not want to re-created it on the target machine. If you make edits, ensure that you save the file. It is not necessary to re zip the file after making edits.
3. Log on to the SAS Infrastructure for Risk Management web application as the same user that executed the backup instances process.
4. Ensure the following:
 - That there are no instances with the same name as an instance in the .xlsx file of backed up instances.
 - That the user on the target machine has the same roles (such as access entities, publishing entities, and so on) as they had on the source machine.
 - That the user has Write permissions to where the ZIP file or unzipped directory is copied over.
5. Log on to SAS Studio as the same user who executed the backup instances process.
6. Press **F4** to open a new SAS program in the work area.
7. In the work area, click the **Code** tab, enter the following:

```
%irm_restore_instances(bkup_dir=absolute-path, debug={TRUE | FALSE},
logOptions= , pollInterval=number-of-seconds, maxWait=max-seconds
```

where:

- backup_dir — Specifies the absolute path to the backed up instances, including the ZIP file or directory name if the file is unzipped.
 - debug — (Optional) Enables or disables debug logging. The default is FALSE.
 - logOptions — (Optional) Specifies standard SAS logging options such as mprint, mlogic, symbolgen, and so on. The default is blank.
 - pollInterval — (Optional) Number of seconds between checks of instance creation. The default is 10.
 - maxWait — (Optional) Maximum number of seconds to wait for an instance creation to complete. The default is 3600.
8. Click .

After executing the script, the following should occur:

- A tabular display of instances created in the restore session should be displayed in the **Results** tab

- A ZIP file named `restore_inst_YYYYMMDD_HH_MI_SS` is located in the Navigation pane under **Files (Home)**. You can view the contents of this file in SAS Studio or by navigating to the physical location of the file on the target machine. Inside the ZIP file should be an `.xlsx` file named `latest_instances_username.xlsx`, where `username` is the name of the user whose job flow instances you restored. This file contains the tabular listings that are displayed under the **Results** tab.

Note: The ZIP file is saved at the location that you specified for the `bkup_file_path` parameter. You will use this ZIP file to restore the job flow instances.

- Instances with status of 4 (success) or of 6 (published) are created. Other instances, if any, in the `existing_instances_username.xlsx` are ignored.
- Instances with the same name that exist on the target machine are not created again. If the debug parameter in macro invocation is set to `TRUE`, a list of these duplicated instances is printed to the log. To view this list, click the **Log** tab. To enable the restore instances procedure to create duplicate instances, you must delete the instances on the target machine or edit the names of the instances in the source `.xlsx` file.

Configure the Development Environment

To configure the development environment, complete the following tasks on the SAS Infrastructure for Risk Management mid-tier server:

1. Enable development mode.
 - a. In SAS Management Console, select **Plug-ins** ⇒ **Application Management** ⇒ **Configuration Manager** ⇒ **SAS Application Infrastructure**.
 - b. Right-click **IRM Mid-Tier Server** and select **Properties**.
 - c. In the IRM Mid-Tier Server Properties window, select the **Advanced** tab and add the property and value:

Property Name	Property Value
<code>com.sas.solutions.risk.irm.server.devmode</code>	<code>true</code>

- d. Click **OK**.
2. Verify that Doxygen is installed and configured on the SAS Infrastructure for Risk Management server.

For information about installing Doxygen on your system, refer to the Doxygen documentation:

<https://www.doxygen.nl/index.html>

3. Set the value for the Doxygen property in SAS Management Console.
 - a. Select **Plug-ins** ⇒ **Application Management** ⇒ **Configuration Manager** ⇒ **SAS Application Infrastructure**.
 - b. Right-click **IRM Mid-Tier Server** and select **Properties**.
 - c. In the IRM Mid-Tier Server Properties window, select the **Advanced** tab and add the following property and value:

Property Name	Property Value
com.sas.solutions.risk.irm.sc.doxygen.path	<i>path-to-the-Doxygen-binary-file</i>

The value for the property varies depending on where Doxygen is installed. Here are two examples:

- Windows:
`C:\Program Files\doxygen\bin\doxygen.exe`
- UNIX:
`/usr/bin/doxygen`

d. Click **OK**.

4. Create a programmer's account for each programmer who will be using the SAS Infrastructure for Risk Management scripting client to create parallel programs. This is the account that a programmer will use to log on to the SAS Infrastructure for Risk Management web application to automatically create their personal federated area.

The programmer's account must have the same primary operating system group of the user account under which stored process servers and SAS workspace servers run.

Here is an example:

```
sudo useradd -g primary-OS-group user-ID
```

where:

- *primary-OS-group* is the primary operating system group of the user account under which stored process servers and SAS workspace servers run.
- *user-ID* is the user ID of the programmer's account.

The configuration of the programmer's account enables files and folders that are created to be discovered by stored process servers and SAS workspace servers.

Note: A programmer's account can be a local account. However, it must be able to authenticate on the SAS metadata server and launch processes on the workspace server.

5. In SAS Management Console, configure the SAS Infrastructure for Risk Management metadata user account for each programmer account in the **DefaultAuth** authentication domain and as a member of **IRM: Access All Entities**.
6. Restart the SAS Infrastructure for Risk Management web application server.

For more information about starting SAS Web Application Servers, see *SAS 9.4 Intelligence Platform: Middle-Tier Administration Guide*.

Chapter 11

Troubleshooting

Gather Information	73
Overview	73
Information about Your Environment and Configuration	74
Problem Description	74
Sample Test Data	75
Enable Detailed Logging	75
Fix Your Web Application Log File Display	76
Log and Configuration File Locations	76

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/Levn/Web/Common/LogConfig/*
- Windows: *SAS-configuration-directory\Levn\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/Levn/Web/Logs/SASServer8_1/* by default:

- *SASIRM.log* — contains messages from the SAS Infrastructure for Risk Management client.
- *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 9.4 Intelligence Platform: Middle-Tier Administration Guide*.

For information about the log4j configuration file, see <http://logging.apache.org/log4j/index.html> and <http://logging.apache.org/log4j/1.2/manual.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:

```
<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.

```
<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\Levn\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/Levn/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.

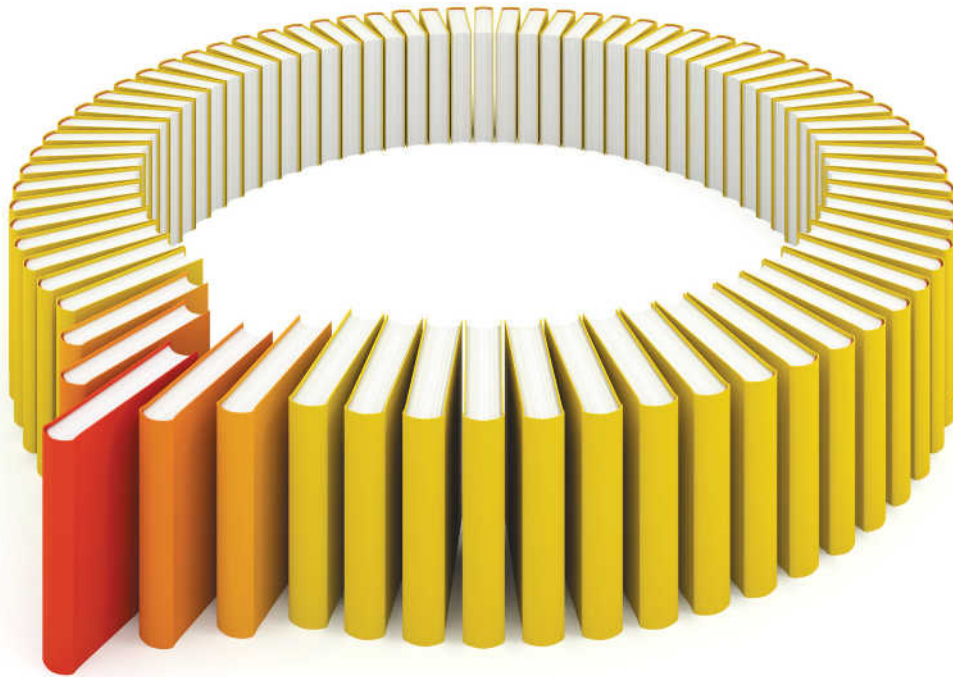
Log and Configuration File Locations

The following table lists the log files that might contain relevant logging information.

Table 11.1 Log Files

File	Default Location
SAS Deployment Wizard Summary	<i>/SAS-configuration-directory/Documents/DeploymentSummary.html</i>
Configuration logs	<i>/SAS-configuration-directory/Logs/Configure</i>
SAS Infrastructure for Risk Management web application logs	<i>/SAS-configuration-directory/Web/Logs</i> <i>Note:</i> 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.
SAS Infrastructure for Risk Management Log4J application log	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 <i>/SAS-configuration-directory/Web/Common/LogConfig/</i>) 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: <ul style="list-style-type: none"> • the location of the log file • file storage properties • use of rolling logs • the number of log files • the maximum size of log files
Object spawner log	<i>/SAS-configuration-directory/ObjectSpawner/Logs</i>
SAS Workspace Server logs	<i>/SAS-configuration-directory/SASApp/WorkspaceServer/Logs</i>
SAS Metadata Server log	<i>/SAS-configuration-directory/SASMeta/MetadataServer/Logs</i>

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.


THE POWER TO KNOW.

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. © 2013 SAS Institute Inc. All rights reserved. S107969US.0613

