



ARIS Risk & Compliance Manager **INSTALLATION**

Version 9.8 - Service Release 7

December 2016

This document applies to ARIS Risk & Compliance Manager Version 9.8 and to all subsequent releases. Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Copyright © 2010 - 2016 Software AG, Darmstadt, Germany and/or Software AG USA Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software AG product names are either trademarks or registered trademarks of Software AG and/or Software AG USA Inc. and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners. Detailed information on trademarks and patents owned by Software AG and/or its subsidiaries is located at <http://softwareag.com/licenses>.

Use of this software is subject to adherence to Software AG's licensing conditions and terms. These terms are part of the product documentation, located at <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to "License Texts, Copyright Notices and Disclaimers of Third Party Products". For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under "License Terms and Conditions for Use of Software AG Products / Copyright and Trademark Notices of Software AG Products". These documents are part of the product documentation, located at <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

Contents

1	Text conventions	1
2	ARIS Risk & Compliance Manager	2
3	Important information for system installation	3
4	ARIS Risk & Compliance Manager installation using an Oracle or Microsoft® SQL Server database	4
4.1	Usage of Oracle or Microsoft® databases	4
4.1.1	Installation of Oracle database schema	4
4.1.2	Installation of Microsoft® SQL Server database schema	5
4.2	Usage of PostgreSQL database	6
4.3	Usage of Apache Derby database	6
5	Installing ARIS Risk & Compliance Manager	7
5.1	Installation of ARIS Risk & Compliance Manager	7
5.1.1	Standalone installation via setup	7
5.1.2	Integration of ARIS Design Server runnable	9
5.1.2.1	Start ACC with the generated.apptypes.cfg	9
5.1.2.2	Preparing and configuring the remote repository	9
5.1.2.3	Configuring ARIS Design Server runnable	10
5.2	Integrate ARIS Risk & Compliance Manager in an existing ARIS installation	11
5.2.1	Remove the components that are no longer needed	12
5.2.2	Prevent components that are no longer required from starting	13
5.3	Configuration parameters	13
5.4	Configuration of the e-mail functionality	15
5.5	Change system e-mail addresses	16
5.6	Migrate from the test installation to a productive system	17
6	Installation of a customer-specific version (Customizing)	19
7	Install a new version of ARIS Risk & Compliance Manager	20
7.1	Data backup	20
7.2	Run the update setup	21
7.3	Data migration	21
7.3.1	Migrate data from ARIS document storage	21
7.3.2	ARIS Risk & Compliance Manager database migration	24
7.4	Import of modeled users into User Management	25
7.4.1	Export modeled users from ARIS Architect	26
7.4.2	Import modeled users into User Management	26
7.4.3	Update users in ARIS Risk & Compliance Manager	27

7.5	Connection to a directory service (LDAP).....	27
7.6	Password encryption in runtime configuration	27
7.7	The configuration of event enabling in ARIS Risk & Compliance Manager	28
8	Installing ARIS Architect components.....	30
9	Preparing the MashZone server for dashboard integration	31
10	Connection to ARIS Publisher.....	32
11	Common errors	34
11.1	Database problems	34
12	System requirements	35
12.1	Oracle system and settings	35
12.2	Microsoft® SQL Server system and settings	37
12.3	Acrobat Reader	37
12.4	Microsoft Office/Excel	37
13	Glossary	38
14	Software AG support	39
15	Disclaimer.....	40
16	Index	i

1 Text conventions

Menu items, file names, etc. are indicated in texts as follows:

- Menu items, keyboard shortcuts, dialogs, file names, entries, etc. are shown in **bold**.
- Content input that you specify is shown in **<bold and within angle brackets>**.
- Single-line example texts are separated at the end of a line by the character ↵, e.g., a long directory path that comprises multiple lines.
- File extracts are shown in the following font:

`This paragraph contains a file extract.`

2 ARIS Risk & Compliance Manager

ARIS Risk & Compliance Manager is a Web application. ARIS Risk & Compliance Manager uses Java Servlets and Java Server Pages (JSP) which, in addition to a Java environment (JDK), require a Web, i.e., Servlet container (Apache Tomcat) as runtime environment. The data is stored in a relational database system and is exchanged with the application via a JDBC interface. You can use ARIS Risk & Compliance Manager with the **Apache Derby** database for testing purposes. You need the **Oracle** database system or **Microsoft® SQL Server** for full productive operation.

If an updated version of this document is available, you will find it here:

<http://aris.softwareag.com/ARISDownloadCenter/ADCDocumentationServer>

(<http://aris.softwareag.com/ARISDownloadCenter/ADCDocumentationServer>)

3 Important information for system installation

If you want to install the system technically and/or functionally without service support from Software AG, you need extensive knowledge about the systems to be installed, the target subject matter, as well as the target systems and their interdependencies. Due to the multitude of platforms and the hardware and software configurations that influence each other, it is only possible to describe specific installations. It is impossible to document all settings and dependencies.

4 ARIS Risk & Compliance Manager installation using an Oracle or Microsoft® SQL Server database

Use the standard database system (PostgreSQL), an Oracle or Microsoft® SQL Server database, for productive operation of ARIS Risk & Compliance Manager. Use of the Derby database is permitted for testing purposes only. Note that a new database should be set up for production purposes. Please do not use test data in your productive system.

REQUIRED COMPONENTS

To operate the application, the following components must be installed:

- ARIS Risk & Compliance Manager (including required applications, such as User Management or ARIS document storage)

If using Oracle or Microsoft® SQL Server as the standard database system:

- Oracle or Microsoft® SQL Server database
- ARIS Risk & Compliance Manager database schema
- Database driver for Oracle or Microsoft® SQL Server

In the following, installation with automatic setup will be described. If you want to use Oracle or Microsoft® SQL Server as a DBMS you need to install the database and database schema first.

4.1 Usage of Oracle or Microsoft® databases

Install the Oracle database with the Oracle installation program or the Microsoft® SQL Server database with the corresponding installation programs. Follow the instructions in the installation program, as well as the documentation provided by the manufacturers. During this step of the procedure, note the SID or the database names of the new database instance and also the account, i.e., the user name and the password of the system user.

4.1.1 Installation of Oracle database schema

The supplied ARIS Risk & Compliance Manager package includes several database scripts that assist you in preparing the database for ARIS Risk & Compliance Manager. To execute them, you need to have an Oracle client installed (sqlplus).

Batch file and available scripts:

- **rebuild.bat**
Main script for starting the installation.
- **rebuild.sql**
To enter data.
- **init_user.sql**
To create the new Oracle user schema for ARIS Risk & Compliance Manager.

Procedure

1. Edit the **rebuild.bat** file and the **rebuild.sql** script.
2. In the **rebuild.bat** file, enter the values for the password and the SID (Page 4) instead of the expressions in angle brackets.
3. There must be a space before **@rebuild.sql: sqlplus system/<password>@<SID>@rebuild.sql**.
4. Insert the SID in the file **rebuild.sql: connect &username/&password@<SID>**.
5. Start the **rebuild.bat** file.
6. Enter the user name and a password. Please note this information because you will need it later in the installation.

The remaining scripts will then be executed in the correct sequence. The database does not contain a database schema with tables yet. These will be automatically created when you start the ARIS Risk & Compliance Manager server for the first time. Observe any error messages while the scripts are running. The **drop user <user name> cascade** command may result in an error message the first time it is executed because the user does not yet exist at this point. When the script is executed again, the user is first deleted and then created again. All other commands must run without errors.

4.1.2 Installation of Microsoft® SQL Server database schema

The supplied ARIS Risk & Compliance Manager package includes several database scripts that assist you in preparing the database for ARIS Risk & Compliance Manager. Run the scripts on the host computer of the SQL server.

- **install.bat**
Main script for initializing an ARIS Risk & Compliance Manager database user and entering the data **database name**, **user name**, and **password**.
- **recreate_database.bat**
Runs the **recreate_database.sql** SQL script.
- **recreate_database.sql**
Generates the database instance for ARIS Risk & Compliance Manager.
- **recreate_dbuser.bat**
Runs the **drop_dbuser.sql** and **create_dbuser.sql** SQL scripts.
- **drop_dbuser.sql**
Deletes the ARIS Risk & Compliance Manager database user.
- **create_dbuser.sql**
The generation of users by ARIS Risk & Compliance Manager and the assignment of privileges.

Warning

If a database with the same name already exists, it will be deleted.

Procedure

7. Edit the file **install.bat**.
8. In the **install.bat** file replace the expression enclosed in angle brackets with the current password **sa** (system user) of the SQL server user.
9. Also replace the path information **<pathinfo>**.
10. Run **install.bat**.
11. Enter a database name, user name, and password. Please note this information because you will need it later in the installation.

The database schema is installed.

4.2 Usage of PostgreSQL database

PostgreSQL database will be installed automatically, if ARIS or ARIS Risk & Compliance Manager is installed via setup.

4.3 Usage of Apache Derby database

Version 9.8.6 of ARIS Risk & Compliance Manager is the last version which supports Apache Derby database. In addition to the standard database system, ARIS Risk & Compliance Manager is supplied with the Apache Derby database. It can be installed during the ARIS Risk & Compliance Manager installation if required. If you run ARIS Risk & Compliance Manager with the Apache Derby database, the term **Demo version** is displayed in ARIS Risk & Compliance Manager user interface. This option is only available if **Demo scenario** has been selected as the installation size. Use of the Derby database is permitted for testing purposes only.

From now on PostgreSQL database should be used, which is implemented as standard database since version 9.8.4. Use the standard database system (PostgreSQL), an Oracle or Microsoft® SQL Server database, for productive operation of ARIS Risk & Compliance Manager. Note that a new database should be set up for production purposes. Please do not use test data in your productive system. If you have selected **Large** as the installation size, an Oracle or Microsoft® SQL database should be used.

5 Installing ARIS Risk & Compliance Manager

Since version 9.8.6 ARIS reporting is supported by ARIS Risk & Compliance Manager. Some of the ARIS Risk & Compliance Manager reports are now executed by ARIS Design Server server. The settings like output format and execution context can be changed easily.

To use this feature ARIS Design Server runnable is needed additionally in an ARIS Risk & Compliance Manager installation. As it is not integrated in the setup so far, the runnable must be added manually to the installation.

There are two options to install ARIS Risk & Compliance Manager including usage of ARIS reporting:

- Installation of ARIS Risk & Compliance Manager via setup and add ARIS Design Server runnable (Page 7)
- Integrate ARIS Risk & Compliance Manager runnable in an existing ARIS installation (Page 9) (includes ARIS Design Server runnable in all cases)

5.1 Installation of ARIS Risk & Compliance Manager

5.1.1 Standalone installation via setup

Make sure that the port number is not used by any other software. This is particularly important if you have installed the Oracle server on the same computer. A web server may already be installed at port **80**, which is also the default port for the Apache web server that is also installed as a load balancer. The installation sources are available as a ZIP file via download or on installation media.

These instructions assume a local installation. This means that ARIS Risk & Compliance Manager is installed on the server on which the setup is run. In addition to local installation, you can install ARIS Risk & Compliance Manager via remote installation on another server. To do so, please read chapter **3.4 ARIS remote installations (Windows operating system)** in the **Server Installation and Administration Guide**.

Procedure

1. If you have the installation sources as a ZIP file, first unpack the file for ARIS Risk & Compliance Manager to a new directory. To do so, enter the password for the ZIP file that you have received from Software AG. Ensure that the path data is applied when you unpack the file. In WinZip, for example, this is done by selecting the **Use folder names** option. You can also put the ARIS Risk & Compliance Manager installation media into the CD-ROM drive.
2. Open the **Setup** directory, and run the **setup.exe** file.
3. Click **Next**. The license agreements are displayed.
4. To accept the license agreements, click **Next**. The **Installation scenario** dialog is displayed.
5. Select the installation scenario **Perform installation on this active computer** and click **Next**.
6. Enter the directory in which you want to install ARIS Risk & Compliance Manager and click **Next**.

-
7. To use the suggested path, you do not need to make any changes.
 8. In the next dialog, do not make any changes and click **Next**.
 9. Select an existing license file used automatically by setup. Alternatively, you can do so after installation in User Management.
 10. Click **Next**.
 11. Activate the relevant modeling approach for ARIS Risk & Compliance Manager and click **Next**. You cannot change the modeling approach after installation is complete.
 12. Specify the port number for the connection to the Web application server and click **Next**.
 13. Enter the name of the mail server and the default e-mail address, if this information is already available. If the mail server requests authentication enter an e-mail account and password.
 14. Click **Next**.
 15. If necessary, activate event enabling. Refer to the detailed information (Page 28) for the individual configuration options.
 16. Click **Next**. The **System settings** dialog is displayed.
 17. Select the installation size in order to determine the memory allocated for ARIS Risk & Compliance Manager: **Demo scenario** = 1GB, **Medium** = 4GB, **Large** = 8GB.
 18. Click **Next**. The **Select database system** dialog is displayed.
 19. Select the relevant database. **Standard database system** for a PostgreSQL database and **Derby (for demonstration purposes only)** for an Apache Derby database. For Oracle or Microsoft® SQL Server an appropriate database driver must also be provided, which is to be installed by the setup program. The driver can be downloaded from Oracle/Microsoft.
 20. If you have selected Oracle or Microsoft® SQL, perform the following additional steps.
 - a. Enter the name of the database server.
 - b. Enter the port number of the database server.
 - c. Enter the service name of the database (Page 4) (Oracle SID) or the database name of the database instance (Microsoft® SQL Server).
 - d. Enter the name and password of the database (Page 4) user.
 21. Click **Next**.
 22. Click **Install** to start the installation.

ARIS Risk & Compliance Manager is installed.

You can use the entries **Start ARIS Risk & Compliance Manager** and **Stop ARIS Risk & Compliance Manager** in the installed program group to start and stop the runnables. To open ARIS Risk & Compliance Manager, enter the address **http://<server name>/arcm** in the browser.

5.1.2 Integration of ARIS Design Server runnable

This section requires basic knowledge of how to use ARIS Cloud Controller command line tool (ACC).

Prerequisite

Always run ACC connected to your agent(s), either

- using the command line switches to connect to a single agent (-h, -u, -pwd) in case of a single node installation, or
- using a node file (passed to ACC with a -n switch) or
- by manually issuing **add node** commands for a distributed installation.

Only an ARIS Design Server runnable which has the same version number, service and hotfix level is integratable in an ARIS Risk & Compliance Manager installation.

Warning

When adding the ARIS Design Server runnable to an installation that was installed via setup, you will not be able to update this installation with an update setup, as the setup will recognize that the installation has been tampered with.

5.1.2.1 Start ACC with the generated.apptypes.cfg

Start ARIS Cloud Controller with **generated.apptypes.cfg**.

Procedure

1. Click **Start menu > ARIS > Administration**.
2. Right-click ARIS Cloud Controller.
3. Enter the parameter **-c** in the **Target** box.
4. Enter the path to the **generated.apptypes.cfg**.

Before proceeding with the next steps, restart ARIS Cloud Controller.

Example

```
C:\SoftwareAG\ARIS9.8\server\acc\acc.bat -c  
"C:\SoftwareAG\ARIS9.8\server\generated.apptypes.cfg" -h localhost -u "Clous" -p 9001 -pwd  
"g3h31m"
```

5.1.2.2 Preparing and configuring the remote repository

To install additional runnables into an agent that has not yet installed an instance of this particular type, you need to make the agent use a remote repository that contains the runnable(s) in question.

For manually performed installations, a remote repository might already be available. If so, the following steps might not be necessary.

Normally, a remote repository is a server containing the runnables, but it can be a local directory too, in case there is no server available:

- **File-based repository**

The easiest approach is to copy the content of the folder

<DVD_Root>\Setups\Windows\repo to a physical drive on the machine on which you want to add the HD server, e.g. **c:\arisrepo**. In this example, the URL to your remote repository would be **file://c:/arisrepo**. The next folder in **c:\arisrepo** must be the folder **com**.

- **Server-based remote repository**

For a distributed installation, you might want to use a real remote repository. It can be any HTTP or FTP server that is reachable from the machine on which you want to add the HD server. In that case, copy the content of the folder **<DVD_Root>\Setups\Windows\repo** to your HTTPD or FTP server into a suitable location. Example: You use a HTTP server with URL **http://internal.mycompany.com** and you copy the files into the subfolder **arisrepo** in the document root of that HTTP server. The URL to your ARIS repository would be **http://internal.mycompany.com/arisrepo**.

Now configure the agent to use the remote repository for downloading the runnables by running the command **set remote.repository.url = "<remoteRepositoryURL>"**, in order to replace the **<remoteRepositoryURL>** placeholder with the URL to your ARIS repository.

Using the examples above, the commands would be **set remote.repository.url = "file://c:/arisrepo/"** and **set remote.repository.url = "http://internal.mycompany.com/arisrepo"**.

For installations via setup, the agent always has to use runnables from its local repository. The command to do so is **set local.repository.only=false**. Now the agent will use the remote repository you configured above.

5.1.2.3 Configuring ARIS Design Server runnable

Like most of the runnables, ARIS Design Server runnable can be installed in S, M or L size. The essential difference between the runnable sizes is, the consumed memory size and number of processible requests. We recommend M size, since ARIS Design Server is generating all reports of ARIS Risk & Compliance Manager.

To configure ARIS Design Server runnable in M size, issue the command **configure abs_m abs_m**. To install a runnable with size S or L, replace **abs_m** with **abs_s** or **abs_l**. The logical name (**instance ID**) of the runnable is freely selectable. So **abs** can be replaced with any suitable unique name, i.e. the name must not be used for any other runnable in the same installation.

As soon as the configuration is finished successfully, the bundle can be started like any other runnable using **start abs_m**. Now ARIS Design Server is connected to the infrastructure.

5.2 Integrate ARIS Risk & Compliance Manager in an existing ARIS installation

ARIS Risk & Compliance Manager installation can be integrated in an existing ARIS Design Server or ARIS Connect installation, which is based on the same version number, service and hotfix level.

From Version 9.5 user management is carried out centrally in User Management. Therefore, users are no longer created in ARIS Risk & Compliance Manager. User Management for all ARIS products, which is not to be confused with Administration in ARIS Risk & Compliance Manager, serves to manage users, user groups, function and license privileges, licenses, documents, and configurations. This enables single sign-on for various ARIS products. The following procedure relates to the installation size **Medium (arcm_m/postgres _m)**. Use **arcm_l/postgres _l** for the installation size **Large**.

Warning

Do not use setup to install ARIS Risk & Compliance Manager on a server on which an ARIS Design Server or ARIS Connect server is already installed. The ARIS Risk & Compliance Manager installation would overwrite the infrastructure of the existing ARIS installation.

Procedure

1. Install ARIS Design Server via setup on a server. Information on the installation is available in the **ARIS Server Installation and Administration Guide**.
2. Start ARIS Design Server.
3. Install (Page 7) ARIS Risk & Compliance Manager on another server via setup.
4. Start ARIS Cloud Controller for the ARIS Risk & Compliance Manager installation using **Start > ARIS > ARIS Cloud Controller**.
5. Enter the command **reconfigure arcm_m**
zookeeper.connect.string="<ARISDesignServer>:2181" in the console.
6. As the placeholder for **<ARISDesignServer>**, enter the name of the server that you used in step 1 for ARIS Design Server.
7. If you did not change the port keep the default settings.
8. To use the standard database system, enter the command **reconfigure postgres _m**
zookeeper.connect.string="<ARISDesignServer>:2181" in the console.
9. As the placeholder for **<ARISDesignServer>**, enter the name of the server that you used in step 1 for ARIS Design Server.
10. If you did not change the port keep the default settings.
11. Use the **list** command to check whether all components have the status **STOPPED**.
12. Start ARIS Risk & Compliance Manager with the command **start arcm_m**. The suffix **_m** should be adapted according to the installation size (Small, Medium, Large) you have selected for the memory.

ARIS Risk & Compliance Manager is connected to ARIS Design Server and can access both User Management and ARIS document storage.

To open ARIS Risk & Compliance Manager in a browser, enter the server name of **ARIS Design Server** followed by **/arcm**.

As ARIS Risk & Compliance Manager no longer requires the other components on the server, they can either be removed (Page 12) or configured in such a way that they will no longer be started automatically when starting the server.

See also

ARIS Cloud Controller

(http://documentation.softwareag.com/aris/aris95e/ARIS_Server_Installation_and_Administration_Guide.pdf)

5.2.1 Remove the components that are no longer needed

Remove components that are no longer needed.

Warning

The disadvantage of removing the components is that you will not be able to update this installation using a setup. In that case, you would need to update the ARIS Risk & Compliance Manager component manually using an update command.

Procedure

1. Make sure that the ARIS Risk & Compliance Manager component has started. To do this, open ARIS Cloud Controller for the ARIS Risk & Compliance Manager installation using **Start > ARIS > ARIS Cloud Controller**.
2. Use the **list** command to check whether the **arcm_s** component has the status **STARTED** and all others have the status **STOPPED**.
3. Enter the command **deconfigureall** and confirm with **Y**. This command removes all components that have the status **STOPPED**.

The components that are not required have been removed.

5.2.2 Prevent components that are no longer required from starting

Prevent the components that are no longer required from starting.

Procedure

1. Open ARIS Cloud Controller for the ARIS Risk & Compliance Manager installation (**Start > ARIS > ARIS Cloud Controller**).
2. Enter the command **set autostart.mode=autostart.flag**.
3. For the components that are no longer required, set **autostart property** to **false**:
 - e. **set zoo_m property autostart="false"**
 - f. **set postgres_m property autostart="false"**
 - g. **set couchdb_m property autostart="false"**
 - h. **set elastic_m property autostart="false"**
 - i. **set adsadmin_m property autostart="false"**
 - j. **set umcadmin_m property autostart="false"**
 - k. **set loadbalancer_m property autostart="false"**

The components that are no longer required will no longer be started automatically when the server is restarted. However, the command **startall** in ARIS Cloud Controller still starts all components.

5.3 Configuration parameters

Most parameters that can be used to influence the behavior of ARIS Risk & Compliance Manager are provided in the file **<ARIS Risk & Compliance Manager installation directory>\server\bin\work\work_arcm_m\base\webapps\arcm\WEB-INF\runtimeconfig.xml**. They have the following format:

```
<parameterList name="applicationlayer">
  <!--entries per page in a list-->
  <parameter name="application.view.entriesPerPage" value="20"/>
  <!-- edit only in consultation of Software AG -->
  <parameter name="application.batchserver.enable.remoteconnection"
value="false"/>
  <!-- edit only in consultation of Software AG -->
  <parameter name="application.batchserver.resend.trails" value="5"/>
</parameterList>
```

The most important parameters are described in detail below. All parameters not specified are used internally and should not be changed. Preset values are listed in brackets.

APPLICATION.VIEW.ENTRIESPERPAGE

param-value	Description
20	Specifies how many list entries are to be output per page (20 in this example).

SERVERURL

param-value	Description
http://<host>:<port>/<Context>	To ensure that the specified link to the application is correct in the notifications (internal or e-mail), you must adapt this entry to your requirements.

WHISTLEBLOWEMAIL

param-value	Description
adminpleaseChangeEmail_at_your_server	Specifies the e-mail address to which whistle-blow e-mails are sent.

SCHEDULER SETTINGS

In the following, the various scheduler settings are explained. Schedulers run time-controlled jobs. The two most important parameters are only listed once as they are identical for subsequent jobs for this type of configuration:

- generatorJobTestcases
- monitorJobTestcases
- generatorJobRiskAssessment
- monitorJobRiskAssessment
- generatorJobSOPProcess
- monitorJobSOPProcess
- generatorJobSurvey
- monitorJobQuestionnaire
- monitorJobSurvey
- monitorJobIssue
- generatorJobAudit
- monitorJobAudit
- generatorJobPolicy
- monitorJobPolicy
- updaterJobPolicy
- cleaningJob
- jobListCleaningJob

STARTSCHEDULER

Switch for the time control. Test cases are generated and checked using a kind of Cronjob. The Quartz scheduler is used.

param-value	Description
false	Disables time control.
true	Enables time control.

EXECUTIONTIME

Here, you can enter the execution times for the Quartz scheduler (see **Scheduler settings**). They are specified as **Cron Expressions!**. More information on the Quartz scheduler (<http://www.quartz-scheduler.org/documentation/quartz-2.1.x/tutorials/tutorial-lesson-06>) is provided on the Website.

CLIENTEXCLUDINGLIST

Here, you can enter clients that are to be excluded from a job. Separate the clients by comma.

CLIENTINCLUDINGLIST

Here, you can enter clients that are to be included in a job. Separate the clients by comma. All other clients will be ignored by the jobs.

5.4 Configuration of the e-mail functionality

You can configure ARIS Risk & Compliance Manager in such a way that e-mails are sent automatically in certain situations, e.g., to a tester to whom a test case has been assigned. To send e-mails, an external mail server with SMTP support is used, which is normally already set up and available. No SMTP mail server is included with ARIS Risk & Compliance Manager.

Procedure

1. Start ARIS Cloud Controller.
2. To configure the SMTP host parameter, enter **reconfigure arcm_m smtp.host="< IP address or valid DNS name of the outgoing mail server>"**.
3. If SMTP authentication is enabled on the mail server, enter **reconfigure arcm_m smtp.account="<SMTP account user name>"** to configure the **smtp.account** parameter.
4. If SMTP authentication is enabled on the mail server, enter **reconfigure arcm_m smtp.password="<SMTP account password>"** to configure the **smtp.password** parameter.
5. If no valid e-mail address is defined for sending automatic e-mails, enter **reconfigure arcm_m smtp.default.sender.address="<Fallback sender>"** to configure the **default.sender.address** parameter.
6. To apply the changes to the mail configuration, stop the ARIS Risk & Compliance Manager component using **stop arcm_m** and restart it using **start arcm_m**.

The e-mail function is configured.

In ARIS Risk & Compliance Manager, e-mails and internal messages are sent in the language defined for the client if the corresponding object in the message is client-specific. For general messages, such as requesting a new password, the set system language is used.

5.5 Change system e-mail addresses

After installing ARIS Risk & Compliance Manager all e-mail addresses of the predefined users (such as the system user) are set to the invalid e-mail address **adminpleaseChangeEmail_at_your_server**. For productive operation you must replace them with valid addresses as follows.

RUNTIMECONFIG.XML

- **parameter name="WhistleBlowEmail"**
value="adminpleaseChangeEmail@example.com"/>
- **WhistleBlowAnonymousSender (<parameter name="WhistleBlowAnonymousSender"**
value="adminpleaseChangeEmail@example.com"/>
- **<parameter name="default.sender.address"**
value="changeEmail@example.com"/>

In ARIS Risk & Compliance Manager, you must change the e-mail addresses of the following users:

- System administrator (system)
- Internal system (internal system user)
- Job user (jobUser)

5.6 Migrate from the test installation to a productive system

We recommend that you keep the server (Apache TomEE) of the test system and productive system separate. Depending on the load on the production and test system, it may also be necessary to separate the system hardware. Migrating from a test installation to a productive system requires a new installation of ARIS Risk & Compliance Manager on the productive hardware.

It is possible to redirect ARIS Risk & Compliance Manager to the productive database by adjusting the parameters for the database connection. To do this, you must change the database parameters in ARIS Cloud Controller. The following procedure relates to the installation size **Medium (arcm_m)**. Use **arcm_l** for the installation size **Large**.

STANDARD DATABASE

Procedure

1. Start ARIS Cloud Controller and stop the ARIS Risk & Compliance Manager component with **stop arcm_m**.
2. Use **show instance arcm_m** to display the current and available database parameters.
3. Start the ARIS Risk & Compliance Manager component with **start arcm_m**.
4. If you want to switch to a database system other than the standard database system, enter **reconfigure arcm_m dbms.system="infrastructure"**. The standard database system is activated. ARIS Risk & Compliance Manager obtains the other connection parameters from the ARIS infrastructure.
5. Start the ARIS Risk & Compliance Manager component with **start arcm_m**.

ORACLE

Procedure

1. Start ARIS Cloud Controller and stop the ARIS Risk & Compliance Manager component with **stop arcm_m**.
2. Use **show instance arcm_m** to display the current and available database parameters.
3. To change the database driver parameters, enter **reconfigure arcm_m dbms.driver="oracle.jdbc.driver.OracleDriver"**.
4. To change the database URL, enter **reconfigure arcm_m dbms.url="jdbc:oracle:thin:@<DBserver>:<port>:<SID>"**.
5. To change the database user, enter **reconfigure arcm_m dbms.user="<DB User name>"**.
6. To change the password for the database user, enter **reconfigure arcm_m dbms.-pwd="<DB User password>"**.
7. For licensing reasons, we are unable to supply you with the Oracle JDBC database drivers. Download the appropriate database driver from the Internet and store it on the server on which ARIS Risk & Compliance Manager is installed. Enter **enhance arcm_m with**

commonsClasspath local file <Path>\\<to>\\<driver JAR> in ARIS Cloud Controller to integrate the database driver.

8. Start the ARIS Risk & Compliance Manager component with **start arcm_m**.

MICROSOFT® SQL SERVER

Procedure

1. Start ARIS Cloud Controller and stop the ARIS Risk & Compliance Manager component with **stop arcm_m**.
2. Use **show instance arcm_m** to display the current and available database parameters.
3. To change the database driver parameters, enter **reconfigure arcm_m dbms.driver="com.microsoft.sqlserver.jdbc.SQLServerDriver"**.
4. To change the database URL, enter **reconfigure arcm_m dbms.url="jdbc:sqlserver://[server]:<port>;DatabaseName=[database]"**.
5. To change the database user, enter **reconfigure arcm_m dbms.user="<DB User name>"**.
6. To change the password for the database user, enter **reconfigure arcm_m dbms.-pwd="<DB User password>"**.
7. For licensing reasons, we are unable to supply you with the Microsoft® SQL Server database drivers. Download the appropriate database driver from the Internet and store it on the server on which ARIS Risk & Compliance Manager is installed. Enter **enhance arcm_m with commonsClasspath local file <Path>\\<to>\\<driver JAR>** in ARIS Cloud Controller to integrate the database driver.
8. Start the ARIS Risk & Compliance Manager component with **start arcm_m**.

6 Installation of a customer-specific version (Customizing)

ARIS Risk & Compliance Manager can be extensively customized to fulfill customer requirements. These adjustments are made in XML and Java files and later combined in a ZIP file. This ZIP file must be imported with the ARIS Cloud Controller after installing ARIS Risk & Compliance Manager.

Procedure

1. Install (Page 7) ARIS Risk & Compliance Manager.
2. After the installation, start the ARIS Cloud Controller using **Start > ARIS > Administration**.
3. Stop ARIS Risk & Compliance Manager using **Start > ARIS > Stop ARIS Risk & Compliance Manager**.
4. In the console, enter the command **enhance <ARCM-runnable> with customizing local file "<path to CustomizingZip>"**. The name of the ARIS Risk & Compliance Manager component depends on the type of installation. Possible names for **<ARCM-runnable>** include: **arcm_s**, **arcm_m** or **arcm_l**. Make sure that you always use double quotation marks (""") to indicate the ZIP file path.
5. Start ARIS Risk & Compliance Manager with **Start > ARIS > Start > ARIS Risk & Compliance Manager**

ARIS Risk & Compliance Manager was extended with customer-specific adjustments.

7 Install a new version of ARIS Risk & Compliance Manager

From ARIS Risk & Compliance Manager version 9.5 new versions can be updated via update setup. To update an ARIS Risk & Compliance Manager installation, the following steps must be performed manually. Before running the setup, the ARIS Risk & Compliance Manager and ARIS document storage databases should be backed up.

Warning

The migration cannot be undone.

- Data backup (Page 20)
- Run the update setup (Page 21)
- Data migration (Page 21)
 - Migrate data from ARIS document storage (Page 21)*
 - ARIS Risk & Compliance Manager database migration (Page 24)
- Import modeled users to User Management (Page 25)
- Connect to a directory service (LDAP) (Page 27)*
- Password encryption in the runtime configuration (Page 27)*
- Configuration of event enabling in ARIS Risk & Compliance Manager (Page 28)*

The steps marked with * are optional depending on the previously used version and the range of functions used.

7.1 Data backup

Perform the recommended steps to back up the data. If you are using ARIS document storage for the first time, there is no need to back up the ARIS document storage data.

Procedure

1. Stop the existing installation.
2. Back up the data in your productive database. If you use Oracle, please use **dataPump**.
3. Back up the ARIS document storage CouchDBs.
 - a. To back up the ARIS Risk & Compliance Manager CouchDB, copy the directory **<ARCM 4.x installation directory>\couchdb\var\lib\couchdb** to **<backup directory ARCM 4.x CouchDB>**.
 - b. To back up the Process Governance CouchDB, copy the directory **<APG installation directory>\ads\adsdata\couchdb** to **<backup directory APG CouchDB>**.

The data backup is complete.

7.2 Run the update setup

To install the new version, you no longer have to first uninstall the existing version. All of the settings configured in the setup during the initial installation are automatically transferred. The settings that were changed in the **runtimeconfig.xml** after the installation are not transferred. The download folder containing all the created PDF and Excel reports as well as client and database backups is backed up.

The following parameters can be set in the setup and are automatically transferred during the update setup:

- Modeling approach (risk-based or control-based)
- Mail server configuration (ARIS Risk & Compliance Manager and User Management)
- Event processing (event server, port and EventTypeStore)
- Database configuration

All other subsequent changes that you have made in the **runtimeconfig.xml** (e.g., job settings) must be transferred to the updated **runtimeconfig.xml** again after the update. You should make a note of these settings so that you can configure them again after the update.

7.3 Data migration

You must migrate your existing data in order to use it in a newer version of ARIS Risk & Compliance Manager. This also applies when upgrading within a main release, e.g., from version 9.7 to 9.8.

The data migration consists of two parts:

- Migration of ARIS document storage (only relevant when updating from version 4).
- Migration of the ARIS Risk & Compliance Manager database. Databases from versions older than 3.1 SR4 are no longer supported. If you want to migrate an older version, please contact the Software AG support team (Page 39).

To perform the migration, commands in the Windows prompt (CMD) and commands in ARIS Cloud Controller (ACC) must be run. The running environment (CMD or ACC) appears before the respective command to be run. ARIS Cloud Controller (ACC) is available in the Windows Start menu after the installation (**Start > ARIS > Administration > ARIS Cloud Controller**). The Windows prompt is part of the operating system (**Start > Accessories > Command Prompt**).

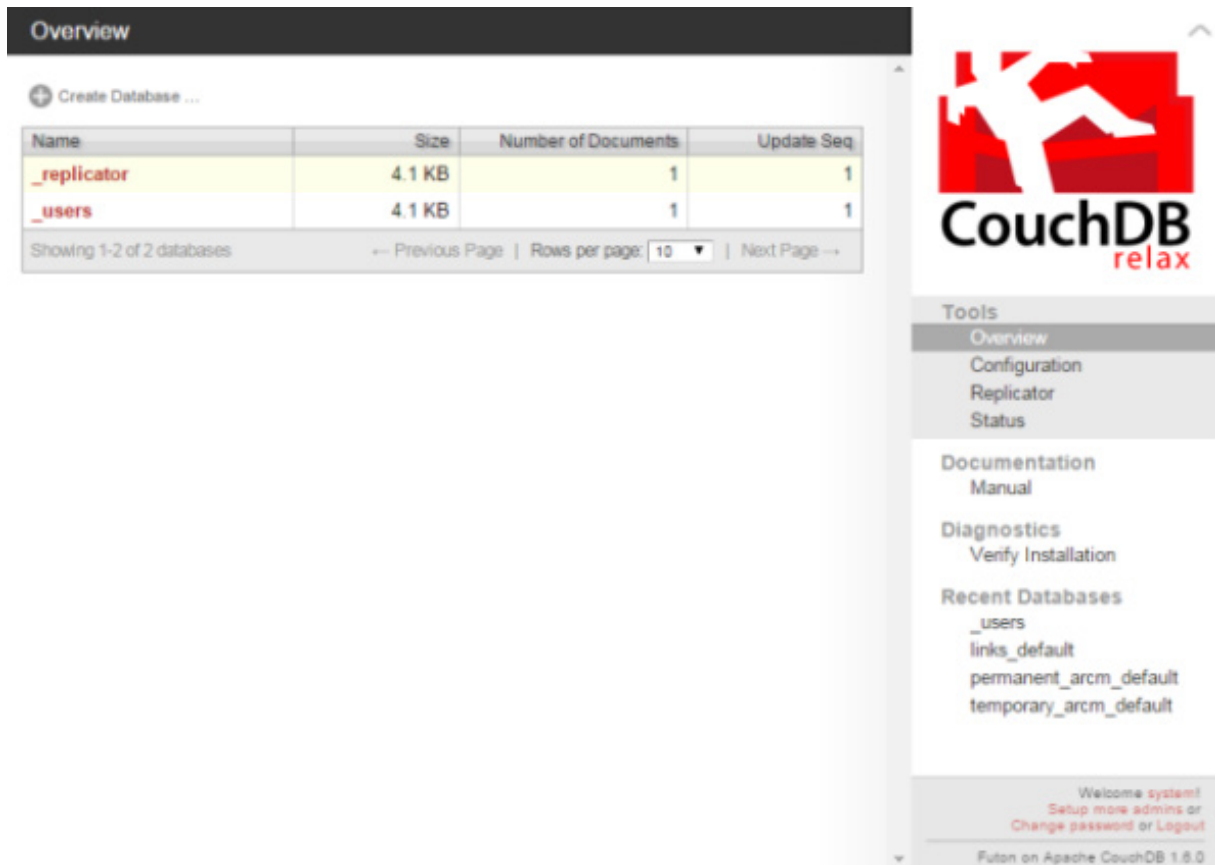
7.3.1 Migrate data from ARIS document storage

Migrate the data from ARIS document storage in order to use it in a newer ARIS Risk & Compliance Manager version. If you are using ARIS document storage for the first time or are updating it based on a 9.x version, you do not need to perform the migration. If you are switching from version 4.x to the latest version, you must migrate the data from ARIS document storage. In the 4.x versions, there were separate installations of ARIS document storage for ARIS Business Server with a connection to Process Governance and ARIS Risk & Compliance Manager. As of version 9, there is only one common ARIS document storage.

The next section describes the steps for merging and migrating the two document repositories.

Procedure

1. Stop the ARIS Risk & Compliance Manager ACC runnable: **stop <arcm-runnable>**. All other runnables must be running.
2. Check the CouchDB content (**http://<your host>:19975/_utils/** - basic authentication, login data of a user who has the **Document administrator** function privilege).
3. The CouchDB content should now appear as follows:



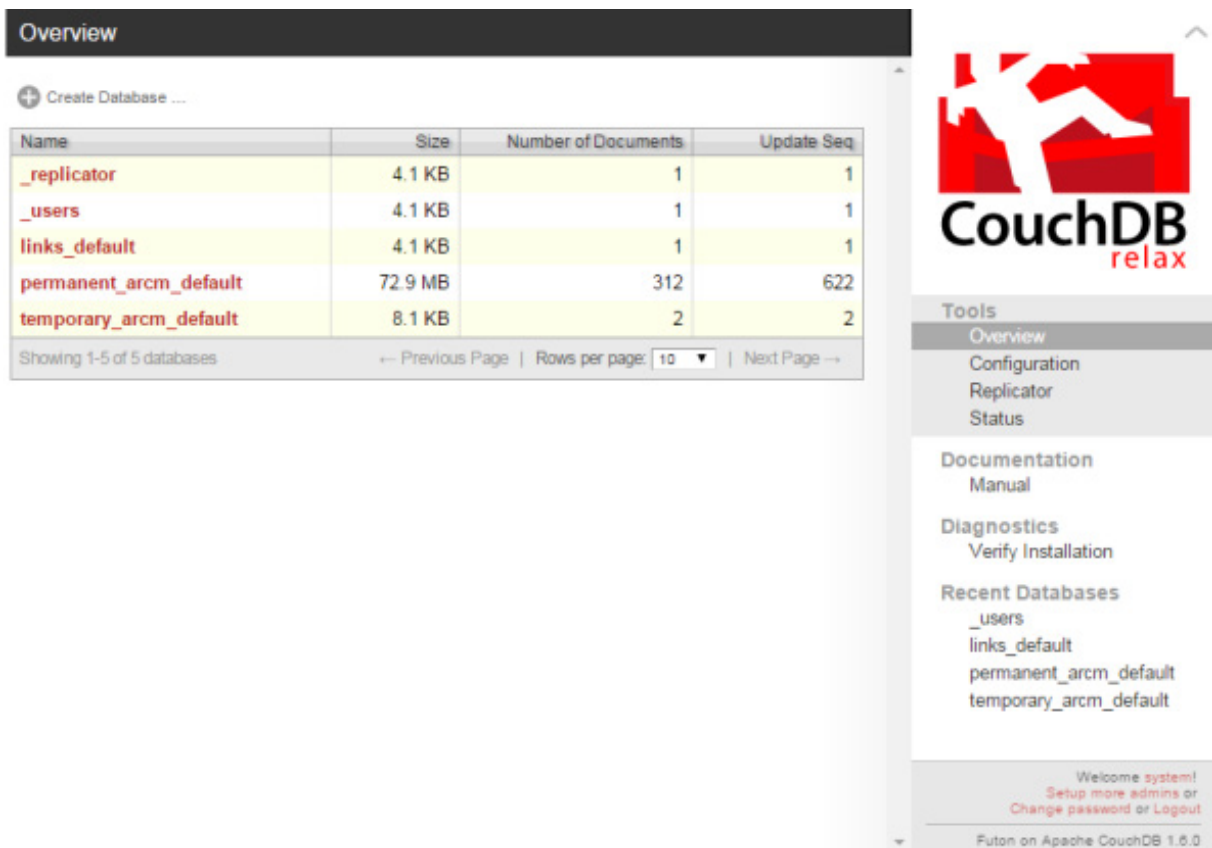
The screenshot shows the CouchDB Overview page. At the top, there is a 'Create Database ...' button. Below it is a table with the following data:

Name	Size	Number of Documents	Update Seq
_replicator	4.1 KB	1	1
_users	4.1 KB	1	1

Below the table, it says 'Showing 1-2 of 2 databases' and 'Rows per page: 10'. To the right of the table is the CouchDB logo with the text 'CouchDB relax'. Below the logo is a 'Tools' menu with options: Overview, Configuration, Replicator, Status. Below that is a 'Documentation' menu with 'Manual'. Below that is a 'Diagnostics' menu with 'Verify Installation'. Below that is a 'Recent Databases' menu with options: _users, links_default, permanent_arcm_default, temporary_arcm_default. At the bottom right, there is a 'Welcome system!' message with links for 'Setup more admins or Change password or Logout' and 'Futon on Apache CouchDB 1.8.0'.

4. Start the Windows prompt (CMD) and switch to the directory **<ARCM installation directory>\server\bin\work\work_adsadmin_m\tools\bin**.
 - a. Start the ARIS Risk & Compliance Manager CouchDB migration:
CMD: **y-admintool.bat migrate -r arcm -s "<backup directory ARCM 4.x CouchDB>" -t "<ARCM installation directory>\server\bin\work\work_couchdb_m\data**
 - b. Start the Process Governance CouchDB migration:
CMD: **y-admintool.bat migrate -s "<backup directory Governance CouchDB>" -t "<ARCM installation directory>\server\bin\work\work_couchdb_m\data"**

In the CouchDB overview, new databases should now be displayed with documents:



The screenshot shows the CouchDB overview page. At the top left, there is a 'Create Database ...' button. Below it is a table with the following data:

Name	Size	Number of Documents	Update Seq
_replicator	4.1 KB	1	1
_users	4.1 KB	1	1
links_default	4.1 KB	1	1
permanent_arcm_default	72.9 MB	312	622
temporary_arcm_default	8.1 KB	2	2

Below the table, it says 'Showing 1-5 of 5 databases' and 'Rows per page: 10'. The sidebar on the right contains the CouchDB logo, a 'Tools' menu with options like Overview, Configuration, Replicator, Status, Documentation, Diagnostics, and Recent Databases. At the bottom of the sidebar, there is a 'Welcome system!' message and the version 'Futon on Apache CouchDB 1.6.0'.

5. Start the CouchDB reindexing process:

CMD: **y-admintool.bat -t default reindex -u <USER> -p <PASSWORD>**

Replace **<USER>** and **<PASSWORD>** with the login data of a user who has the **Document administrator** function privilege.

6. After reindexing, the number of documents has increased:

Name	Size	Number of Documents	Update Seq
_replicator	4.1 KB	1	1
_users	4.1 KB	1	1
links_default	4.1 KB	1	1
permanent_arcm_default	72.9 MB	314	624
temporary_arcm_default	12.1 KB	4	4

Showing 1-5 of 5 databases ← Previous Page | Rows per page: 10 | Next Page →

Tools

- Overview
- Configuration
- Replicator
- Status

Documentation

- Manual

Diagnostics

- Verify Installation

Recent Databases

- [_users](#)
- [links_default](#)
- [permanent_arcm_default](#)
- [temporary_arcm_default](#)

Welcome system!
Setup more admins or
Change password or Logout

Futon on Apache CouchDB 1.6.0

The migration of data from ARIS document storage is complete.

7.3.2 ARIS Risk & Compliance Manager database migration

Migrate your existing database in order to use it in a newer version of ARIS Risk & Compliance Manager.

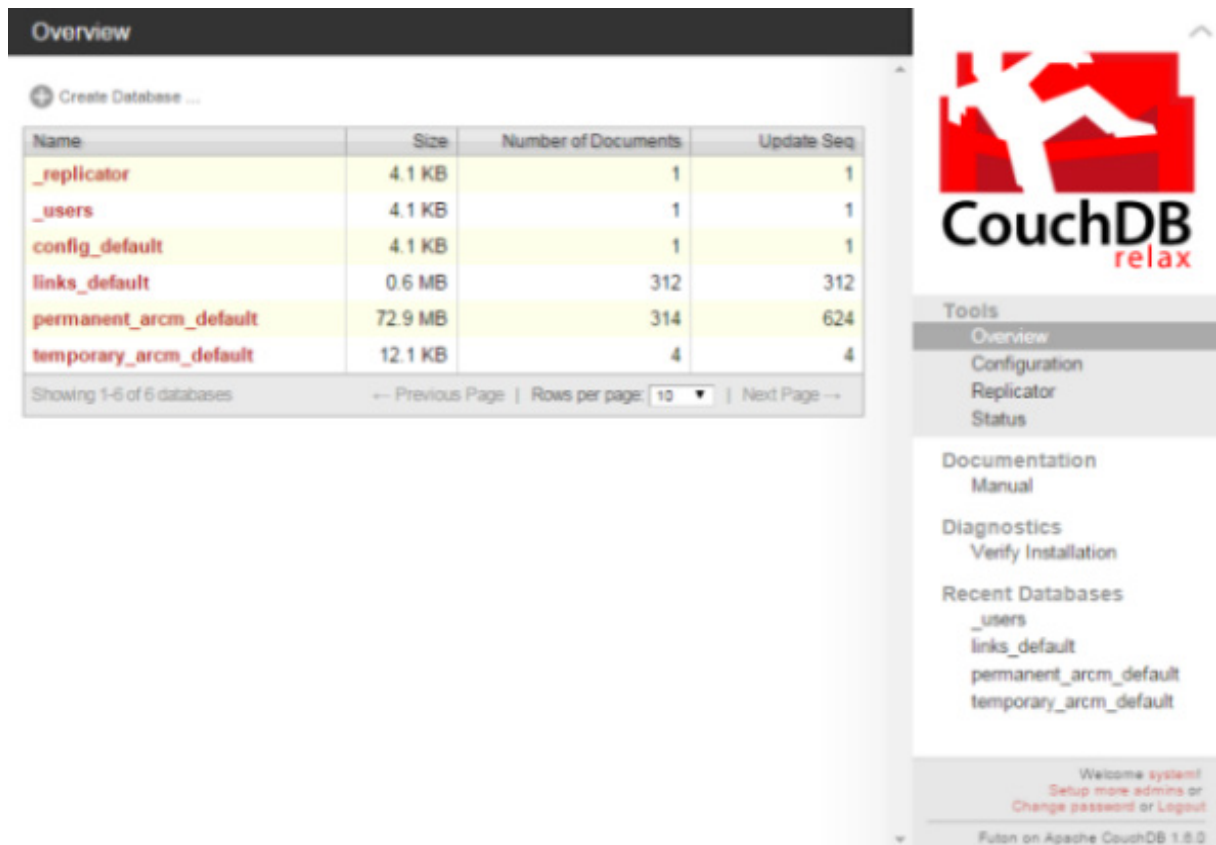
Requirement

The **system** user has the **Document administrator** function privilege. The migration of the document link cannot be performed without this function privilege. If required, assign this function privilege before carrying out the migration and remove it again later.

Procedure

1. Stop the ARIS Risk & Compliance Manager runnable
ACC: **stop <arcm-runnable>**. All other runnables must be running.
2. Activate the data migration using the ARCM runnable via ARIS Cloud Controller (ACC):
ACC: **reconfigure <arcm-runnable> dbms.autoStartMigration=true**
3. Start the data migration by starting the ARIS Risk & Compliance Manager runnable:

ACC: **start <arcm-runnable>**. Depending on the volume of data, it may take some time to start. The CouchDB content should now appear as follows:



The screenshot shows the CouchDB Relax interface. The main area displays an 'Overview' page with a table of databases. The table has four columns: Name, Size, Number of Documents, and Update Seq. The databases listed are: _replicator (4.1 KB, 1 document, update seq 1), _users (4.1 KB, 1 document, update seq 1), config_default (4.1 KB, 1 document, update seq 1), links_default (0.6 MB, 312 documents, update seq 312), permanent_arcm_default (72.9 MB, 314 documents, update seq 624), and temporary_arcm_default (12.1 KB, 4 documents, update seq 4). Below the table, it says 'Showing 1-6 of 6 databases' and 'Rows per page: 10'. The sidebar on the right contains a 'Tools' menu with options: Overview, Configuration, Replicator, Status, Documentation Manual, Diagnostics Verify Installation, and Recent Databases (listing _users, links_default, permanent_arcm_default, and temporary_arcm_default). At the bottom of the sidebar, there is a 'Welcome system!' message and 'Futon on Apache CouchDB 1.8.0'.

Name	Size	Number of Documents	Update Seq
_replicator	4.1 KB	1	1
_users	4.1 KB	1	1
config_default	4.1 KB	1	1
links_default	0.6 MB	312	312
permanent_arcm_default	72.9 MB	314	624
temporary_arcm_default	12.1 KB	4	4

4. Deactivate the automatic migration via ARIS Cloud Controller (ACC):

ACC: **stop <arcm-runnable>**.

ACC: **reconfigure <arcm-runnable> dbms.autoStartMigration=false**

5. Start ARIS Risk & Compliance Manager for productive operation.

ACC: **start <arcm-runnable>**.

This completes the data migration.

7.4 Import of modeled users into User Management

After the import of a database export from ARIS Architect and subsequent import into ARIS Risk & Compliance Manager, all imported users are deactivated. They can be activated by creating them manually in User Management and then synchronizing with ARIS Risk & Compliance Manager (**Administration > Synchronize with User Management**). The report **ARCM user export for User Management** does this automatically by exporting all modeled users of a database (**Person** object type). The following attributes of a user are exported:

- Login
- First name
- Last name
- E-mail address

The report also identifies the license privileges a user needs. The following rules apply:

- If a user is not assigned to any user group, the user is assigned the **Contribute** license privilege. Users without group assignment are authorized to perform tasks in issue management.
- If a user is assigned to a user group with the Incident owner or Policy addressee role, this user is assigned the **Contribute** license privilege.
- For all other role assignments, the user is assigned the **Operate** license privilege.

7.4.1 Export modeled users from ARIS Architect

Export the modeled users from ARIS Architect.

Procedure

1. Open ARIS Architect.
2. Open the database whose modeled users you want to export for the import into User Management.
3. Right-click the main group.
4. Click **Evaluate > Start report**.
5. Select the ARIS Risk & Compliance Manager category.
6. Select the report **ARCM user export for User Management**.
7. Select the output settings.
8. Click **Finish**.

A text file with the attributes Login, First and Last name, and E-mail address is exported.

7.4.2 Import modeled users into User Management

Import the modeled users into User Management.


Procedure

1. Put the ARIS Risk & Compliance Manager installation media into the CD-ROM drive.
2. Copy the file **create_user.bat** from the **Content** folder to the folder **<ARCM installation folder>\server\bin\work\work_umcadmin_s\tools\bin**.
3. Copy the text file you created using the **ARCM user export for User Management** report into the same folder.
4. In the file **create_user.bat**, replace the entry **set INPUTFILE** with the name of the export file.
5. Save the change.
6. Run the file **create_user.bat**. You can assign a password for all imported users. If you do not want to assign a password, press the Enter key without specifying a password.

The users are imported into User Management.

7.4.3 Update users in ARIS Risk & Compliance Manager

Update the users in ARIS Risk & Compliance Manager with the data from User Management.

1. Log in to ARIS Risk & Compliance Manager as system administrator.
2. Click  **Administration**.
3. Under **Actions**, click **Synchronize with User Management**. User data in ARIS Risk & Compliance Manager is replaced by data from User Management. This updates function and license privileges, names, passwords, e-mail addresses, etc., and users are deactivated.

The dialog closes. **Monitoring > Jobs and imports/exports** is displayed. The job is output under **Waiting jobs and imports/exports**. When complete, the job is listed under **Completed jobs and imports/exports**. The imported users are activated in ARIS Risk & Compliance Manager.

7.5 Connection to a directory service (LDAP)

In contrast to previous versions, LDAP is no longer directly connected with ARIS Risk & Compliance Manager. The LDAP connection must be configured in User Management instead. Information on this is available in the **ARIS Server Installation and Administration Guide**, chapter **Set up ARIS for LDAP server operation**.

7.6 Password encryption in runtime configuration

User IDs, passwords, or other security-sensitive information always used to be plain text in the runtime configuration of ARIS Risk & Compliance Manager (**runtimeconfig.xml**). Now a new option is available that allows this information to be encrypted during server startup. For this, the **encrypted="false"** XML attribute must be inserted into the required parameter line. As a consequence, the contents of the **value** attribute is encrypted during server startup and the **encrypted** flag is set to **true**. For this to work, the XML attributes **encrypted** and **value** must be written in the same line.

Example

Before: `<parameter name="dbms.pwd" encrypted="false" value="sox"/>`

After: `<parameter name="dbms.pwd" encrypted="true" value="72a5e995b3996dc0ca5882bf42dafd1e"/>`

To increase data safety it is recommended that you mark the configuration file as read-only after encryption.

7.7 The configuration of event enabling in ARIS Risk & Compliance Manager

ARIS Risk & Compliance Manager enables you to subscribe to events from a messaging provider (Universal-Messaging is the default) and use them as a basis for generating defined objects in ARIS Risk & Compliance Manager, e.g. test cases. Control using events is configured during the setup or subsequently using ARIS Cloud Controller.

Examples - Commands for ARIS Cloud Controller

```
reconfigure arcm_m eventenabling.active="true"
reconfigure arcm_m eventenabling.providerUrl="nsp://localhost:9000"
reconfigure arcm_m eventenabling.eventTypeStoreLocation="
C:/SoftwareAG/common/EventTypeStore"
reconfigure arcm_m eventenabling.configurationLocation="
C:/SoftwareAG/profiles/SPM/configuration"
reconfigure arcm_m
eventenabling.securityFilePath="C:/SoftwareAG/common/conf/event/routing/event-ro
uting-security.xml"
reconfigure arcm_m
eventenabling.classpathJarPath="C:/SoftwareAG/common/lib/event-routing-classpath
.jar"
```

MEANING OF PARAMETERS

- **eventenabling.active**
Central specification to activate event enabling. If the value false is specified, the service is not started. If true, the other parameters must contain valid values.
- **eventenabling.providerUrl**
The parameter should contain the valid URL of a Universal Messaging server instance, e.g. nsp://localhost:9000.
- **eventenabling.eventTypeStoreLocation**
Specifies the absolute path to a locally available event type store. If the instance of the Universal Messaging server is located on the same host, the store for this installation can be used. Example: C:\SoftwareAG\common\EventTypeStore
- **eventenabling.configurationLocation**
The absolute path to the base directory of a specific event routing configuration is required. If the instance of the Universal Messaging server is located on the same host, the basic configuration for this installation can be used. Example:
C:\SoftwareAG\profiles\SPM\configuration
- **eventenabling.securityFilePath**
This parameter should contain the absolute path for the security configuration file. If the host is identical, the file for the Universal Messaging server installation can be referenced. Example: C:\SoftwareAG\common\conf\event\routing\event-routing-security.xml
- **eventenabling.classpathJarPath**
This parameter must contain the absolute path to the Java class path archive for the required event routing framework libraries. If the host is identical, the Universal Messaging server

installation can be referenced. Example:

C:\SoftwareAG\common\lib\event-routing-classpath.jar

- **eventenabling.useDurableSubscriptions**

By default, event enabling is based on permanent message subscriptions. This functionality can be disabled by setting the value of this optional parameter to false.

SUPPORT EVENT TYPES

Specific predefined event types are provided in order to generate defined objects from the events in ARIS Risk & Compliance Manager. They need to be copied into the local Event Type Store and the Event Type Store of the event-generating system. The associated files for the Event Type Store are located in the main directory of the ARIS Risk & Compliance Manager installation media in the Event Type Store folder. The content of this folder is then copied into the main directory of the respective Event Type Store.

The sending of events with the event types provided in ARIS Risk & Compliance Manager is part of Complex Event Processing. Further information on this can be found in the Complex Event Processing documentation.

OPERATION OF A SELF-CONTAINED INSTALLATION OF ARIS RISK & COMPLIANCE MANAGER

If ARIS Risk & Compliance Manager and the Universal Messaging server are not located on the same host, the required configurations and resources cannot be directly referenced and used. In this case, the following resources have to be copied from the Universal Messaging server installation to the host system for the ARIS Risk & Compliance Manager installation. Directory structures to be copied (minimum bundle*):

1. <SAG install directory>\common\conf\event\...
2. <SAG install directory>\common\EventTypeStore\...
3. <SAG install directory>\common\lib\...
4. <SAG install directory>\common\runtime\bundles\...
5. <SAG install directory>\profiles\SPM\configuration\event\routing\...

The copied resources can then be used in the event enabling configuration for ARIS Risk & Compliance Manager as previously described.

* For further information about operation of Universal Messaging, particularly configuration using Software AG Platform Manager, refer to the product-specific documentation.

Warning

To guarantee fault-free operation and compatibility, make sure that the version of the copied resources for the ARIS Risk & Compliance Manager installation is always synchronized with the version of the Universal Messaging server used.

8 Installing ARIS Architect components

The macros and reports for ARIS Risk & Compliance Manager are part of the ARIS Design Server/ARIS Connect installation. The installation of other components is therefore not required.

9 Preparing the MashZone server for dashboard integration

You can enable the use of MashZone/MashZone NextGen Business Analytics in ARIS Risk & Compliance Manager to merge, combine, and clearly visualize data in dashboards. This requires changes to the MashZone server settings. For MashZone NextGen Business Analytics these changes are not necessary.

Two different instances of User Management cannot be running parallel on the same computer. Therefore, MashZone and ARIS Risk & Compliance Manager each require a separate instance. The MashZone dashboards are therefore provided by a different server than the ARIS Risk & Compliance Manager interface in which they are embedded.

As a precaution, redirection of content from MashZone to other systems, such as ARIS Risk & Compliance Manager, in MashZone is limited to the **SAMEORIGIN** option by default, i.e., the MashZone server only responds to its own requests. Therefore, the **SAMEORIGIN** restriction in the file **mashzone.properties** has to be replaced with the **ALLOW FROM <URI>** option. Not all browsers support the **ALLOW FROM <URI>** option. More detailed information about X-Frame options can be found here

<https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options>.

Procedure

1. Open the file **mashzone.properties**
(<MashZoneInstallDir>\ppmmashzone\server\bin\work\work_mashzone_m\base\webapps\
\mashzone\WEB-INF\)

2. Add the following lines:

```
mashzone.httpheader.xframe.options.enabled=true  
mashzone.httpheader.xframe.options=ALLOW FROM <Host name of ARIS Risk &  
Compliance Manager>
```

The host name of ARIS Risk & Compliance Manager must be the name of the computer on which ARIS Risk & Compliance Manager is installed, and on which the load balancer for the ARIS Risk & Compliance Manager server is running, for example

arcmserver.subdomain.domain.

3. Save your changes.
4. Restart the MashZone server.

The MashZone is prepared for the dashboard integration.

10 Connection to ARIS Publisher

The master data (users, risks, controls, etc.) should be modeled in ARIS Architect according to the recommended procedure. After modeling, this data can be exported from ARIS Risk & Compliance Manager with the export report and imported to ARIS Risk & Compliance Manager. In addition, you can publish the ARIS Architect database with ARIS Publisher. After importing the master data into ARIS Risk & Compliance Manager, the connection to ARIS Publisher can be configured via the clients. This way, you can, for example, create a link from a risk form in ARIS Risk & Compliance Manager to an object in the published model in order to display the process in ARIS Publisher.

Requirement

ARIS Risk & Compliance Manager and ARIS Publisher use the same User Management to manage users. User Management for all ARIS products, which is not to be confused with Administration in ARIS Risk & Compliance Manager, serves to manage users, user groups, function and license privileges, licenses, documents, and configurations. This enables single sign-on for various ARIS products.

Procedure

USER MANAGEMENT

1. Open User Management.
2. Create a user group and a user in User Management.
3. Assign the user group to the user.
4. Assign the function privilege **Publisher administrator** to the user group.

ARIS ARCHITECT

1. Start **ARIS Architect**.
2. Click **ARIS > Administration**. **Administration** opens.
3. Log in to the database you want to export.
4. Click **Users** in the navigation. Users and user groups are displayed.
5. Right-click the previously created user group.
6. Click **Properties**.
7. Click **Function privileges**.
8. Enable the check box for the **Database export** privilege. (The product-specific privileges are not centrally assigned in User Management but in the respective ARIS product.)
9. Click **Access privileges**.
10. Assign the user group at least the access privilege **Read** for the main group.
11. Click **Pass on privileges** to apply the privileges to all subgroups.
12. Click **OK**.
13. Publish the relevant database.
14. After the export, change the status to **Activated**.


ARIS PUBLISHER

1. Open ARIS Architect.
2. Log in using the **root** user and the password **root**.
3. Open the **Groups** module. The user group you created is displayed.
4. In the row of the group, click **Assign**. The dialog opens.
5. Assign the group previously created in User Management to ARIS Publisher.
6. Click **Save**.

ARIS RISK & COMPLIANCE MANAGER

1. Open ARIS Risk & Compliance Manager.
2. Open the client you imported the master data into.
3. Enter the ARIS Publisher link in the **Object link** row in the following form:
4. `http://<BusinessPublisherServer>:19990/businesspublisher/link.do?login=<user name>&password=<password>&localeid=1033&ph=<exportID>&objectguid={GUID}`
5. Replace the placeholders in the following manner:
 - a. **<BusinessPublisherServer>** = Name or IP address of the ARIS Publisher server.
 - b. **<User name>** = Name of the user that was previously created.
 - c. **<Password>** = Password of the user that was previously created.
 - d. **<exportID>**
 1. Open a model in ARIS Publisher.
 2. Right-click an object.
 3. Click **Copy link**.
 4. Copy the parameter **ph** with its value in the link displayed and replace **<exportID>** with it.

The **{GUID}** placeholder must not be replaced. It is replaced dynamically by ARIS Risk & Compliance Manager.

6. Enter the link you created previously in the **Model link** box.
7. Replace the **objectguid** parameter with **modelguid**:
`http://<BusinessPublisherServer>:19990/businesspublisher/link.do?login=<user name>&password=<password>&localeid=1033&ph=<exportID>&modelguid={GUID}`
8. Click  **Save**.
9. Perform a test.
10. Log into ARIS Risk & Compliance Manager with the **Test manager** role.
11. Open a risk that was generated by the master data import.
12. Click in the **Function** box on **Object link** and **Model link**.

ARIS Publisher opens in a new window. The corresponding object or model opens if the connection was configured correctly.

11 Common errors

Many problems can only be identified and eliminated by analyzing the corresponding error messages. To do so, use the log files located in the directory **<ARIS Risk & Compliance Manager installation folder>\server\bin\work\work_arc_m\base\logs**.

11.1 Database problems

SYMPTOM 1

When starting Tomcat, the error message **java.lang.ClassNotFoundException: oracle.jdbc.driver.OracleDriver** is displayed in the DOS box.

CAUSE

No JDBC driver is available.

WORKAROUND

Copy the JDBC driver to the directory **%CATALINA_HOME%\webapps\arc_m\WEB-INF\lib**.

SYMPTOM 2

When starting Tomcat, the error message **java.sql.SQLException: I/O Exception: The Network Adapter could not establish the connection** is displayed in the DOS box.

CAUSE

The database was not started or the Address, Port and/or SID connection parameters are not set correctly.

WORKAROUND

Start the database or correct the connection parameters.

SYMPTOM 3

When starting Tomcat, the error message **java.sql.SQLException: ORA-01017: invalid username/password; logon denied** is displayed in the DOS box.

CAUSE

The user account for the database connection has not been configured correctly.

WORKAROUND

Correct the user data.

12 System requirements

12.1 Oracle system and settings

The following configuration is a minimal configuration. It should be adjusted to the requirements of your ARIS Risk & Compliance Manager system. The configuration of the Oracle system depends on the number of users logged into ARCM at one time.

When installing the ARCM server, the configuration of the Oracle system and that of the ARIS Risk & Compliance Manager connection pool must match. In addition, a firewall may not be installed between the ARCM server and the Oracle DBMS. If this is unavoidable, enable the **dead connection detecten** of the Oracle DBMS system.

SYSTEM

- Oracle 12c Enterprise Edition (12.1.0.1.0)

GENERAL

- Create the ARCM instance as a shared server instance
- `shared_servers` = Processes/10 (minimum 20)
- `open_cursors`: 500
- `session_cached_cursors`: 100
- `sessions`: $(1.1 * \text{Processes}) + 5$
- `processes`: number of users logged in at once (minimum 1000)
- `checkpoint_interval`: 40000
- `checkpoint_timeout`: 0

SGA

- `SGA_MAX_SIZE`: Generally 2/3 of the physical memory available

TABLESPACE SETTINGS

- `SYSTEM`: 500 MB (autoextend on)
- `TEMP`: 300 MB (autoextend on)
- `USERS`: 3 GB (autoextend on)
- `ARCMDATA`: 3 GB (autoextend on)
- `ARCMINDEX`: 8 GB (autoextend on)
- Next-extent: 100 MB

REDO LOG FILES

At least 20 MB for each Redo log file. A Redo log file should be able to contain change data collected during half an hour.

JDBC DRIVER

A JDBC-internal cursor cache can be enabled in the configuration file **runtimeconfig.xml** of ARIS Risk & Compliance Manager. The parameter for this is **dbms.statement.cache.size**. We recommend you set this parameter to 0 and disable this cache. Instead use the **session_cached_cursors** database system setting of the Oracle instance.

APPLICATION SERVER (RECOMMENDED CONFIGURATION)

- Processor: CPU with 8 cores
- Server:
 - Microsoft® Windows Server 2008 R2 Enterprise
 - Microsoft® Windows 2012
 - Red Hat Linux ES 6.4 (64 bit)
- Main memory: Minimum 8 GB RAM
- Controller: SAS (RAID0)
- Hard disks: In RAID array (example: RAID0, 2x146 GB (SAS 15000 UPM))
- Software:
 - JDK 1.7.0 (64-bit)

DATABASE SERVER

- Processor: Intel Xeon X56xx, 2.4 GHz
- Main memory: Minimum 24 GB RAM
- Controller: Dual Channel Ultra320 SCSI (RAID5)
- Hard disks: In RAID array (example: RAID5, 4x146 GB (SAS 15000 UPM))

CLIENT COMPUTER

- Screen resolution: Minimum 1024 x 768 pixels. 1600x800 pixel is recommended.
- Software: Microsoft® Internet Explorer versions 9.0, 10.0, and 11.0, Mozilla Firefox version 23.x or higher, Google Chrome.

Although newer versions have not been approved by Software AG, they can probably be used.

12.2 Microsoft® SQL Server system and settings

SYSTEM

- Microsoft® SQL Server 2012
- Microsoft® SQL Server 2014

DATABASE SERVER

- Processor: Intel Xeon X56xx, 2.4 GHz
- Main memory: Minimum 24 GB RAM
- Controller: Dual Channel Ultra320 SCSI (RAID5)
- Hard disks: In RAID array (example: RAID5, 4x146 GB (SAS 15000 UPM))

12.3 Acrobat Reader

The Adobe Reader must be installed in order to display PDF reports.

12.4 Microsoft Office/Excel

A Microsoft® Excel version 2003 or higher must be installed for displaying Excel reports.

13 Glossary

Global Unique Identifier (GUID)

Unique, cross-database identifier for ARIS elements.

Java Database Connectivity (JDBC)

Interface facilitating communication between a Java application and a database.

Multi-purpose Internet Mail Extension mapping (MIME mapping)

Links a file name extension with the data file type, e.g. text, audio, image.

Oracle service ID (SID)

Unique identifier required by Oracle to identify the database instance.

Simple Mail Transfer Protocol (SMTP)

Transfer protocol specifically designed for exchanging mails. It specifies, for example, how two mail systems interact and what control messages are used for this purpose.

14 Software AG support

ON THE WEB

With a valid support contract you can access the solution database.

Click **<https://empower.softwareag.com/>** (**<https://empower.softwareag.com/>**).

For questions about special installations that you cannot carry out yourself, please contact your local Software AG sales organization.

BY PHONE

With a valid support contract you can reach Global Support ARIS at:

+800 ARISHELP

The "+" stands for the respective prefix for making an international connection in this land.

An example of the number to be dialed within Germany using a land line: 00 800 2747 4357

15 Disclaimer

ARIS products are intended and developed for use by people. Automatic processes such as generation of content and import of objects/artefacts using interfaces can lead to a huge data volume, processing of which may exceed the available processing capacity and physical limits. Physical limits can be exceeded if the available memory is not sufficient for execution of the operations or storage of the data.

Effective operation of ARIS Risk & Compliance Manager requires a reliable and fast network connection. A network with an insufficient response time reduces system performance and can lead to timeouts.

If ARIS products are used in a virtual environment, sufficient resources must be available to avoid the risk of overbooking.

The system has been tested in the **Internal control system** scenario with 400 users logged in simultaneously. It contains 2,000,000 objects. To guarantee adequate performance, we recommend operating with not more than 500 users logged in simultaneously. Customer-specific adaptations, particularly in lists and filters, have a negative impact on performance.

16 Index

A

- ARIS document storage • 21
- ARIS Publisher • 32

C

- Customizing • 19

D

- Database migration • 24
- Database problems • 34

E

- Introduction • 3
- Event enabling • 27

G

- Global Unique Identifier (GUID) • 38

H

- Common errors • 34
 - Database problems • 34

I

- Install the new version • 20
 - Back up data • 20
 - Connect directory service • 27
 - Event enabling • 27
 - Import of modeled users into User Management • 25
 - Migrate ARIS Risk & Compliance Manager database • 24
 - Migrate data • 21
 - Migrate data from ARIS document storage • 21
 - Password encryption • 27
 - Run update setup • 20

Installation and configuration

- Change system e-mail addresses • 16
- ARIS Architect components • 30
- Connect directory service • 27
- E-mail functionality • 16
- Important information • 4
- Integrate in ARIS • 12
- Integration of ARIS Design Server runnable • 10
- Configuration parameters • 14
- Microsoft® SQL Server database schema installation • 6
- Oracle database schema • 5
- Oracle or Microsoft® SQL Server database • 5

- Preparing and configuring the remote repository • 10
- Remove components that are no longer required • 13
- Standalone installation via setup • 8
- Start ACC with the generated.apptypes.cfg • 10
- Prevent components that are no longer required from starting • 13
- Test • 8
- Migrate from the test installation to a productive system • 17

J

- Java Database Connectivity (JDBC) • 38

L

- LDAP • 27

M

- Migration • 24
- Multi-purpose Internet Mail Extension mapping • 38

O

- Oracle
 - Oracle service ID • 38

P

- Password encryption • 27

S

- Simple Mail Transfer Protocol (SMTP) • 38
- Support • 39
- System requirements
 - Acrobat Reader • 37
 - Microsoft® Office/Excel • 37
 - Microsoft® SQL Server • 36
 - Oracle system • 35

U

- Usage of Oracle or Microsoft® databases • 5
 - Usage of Apache Derby database • 7
 - Usage of PostgreSQL database • 7
- Users
 - Export modeled users from ARIS Architect • 26
 - Import modeled users into User Management • 26
 - Import of modeled users into User Management • 25
 - Update users in ARIS Risk & Compliance Manager • 27