



ARIS Risk & Compliance Manager

INSTALLATION GUIDE

Version 10.0 - Service Release 2

October 2017

This document applies to ARIS Risk & Compliance Manager Version 10.0 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 - 2017 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 about system installation	3
4	System requirements	4
4.1	Oracle system and settings	4
4.2	Microsoft® SQL Server system and settings	5
4.3	Acrobat Reader	6
4.4	Microsoft Office/Excel	6
5	ARIS Risk & Compliance Manager installation using an Oracle or a Microsoft® SQL Server database	7
5.1	Usage of an Oracle or a Microsoft® database	8
5.1.1	Installation of an Oracle database schema	8
5.1.2	Installation of a Microsoft® SQL Server database schema	9
5.2	Usage of a PostgreSQL database	10
5.3	Manual configuration of the database for ARIS Risk & Compliance Manager	10
5.3.1	Make an Oracle database available to ARIS Risk & Compliance Manager	10
5.3.2	Make a Microsoft® SQL Server database available to ARIS Risk & Compliance Manager	12
5.3.3	Make a PostgreSQL database available to ARIS Risk & Compliance Manager	14
6	Installation of ARIS Risk & Compliance Manager	15
6.1	Standalone installation via setup	15
6.2	Integrate ARIS Risk & Compliance Manager in an existing ARIS installation	17
6.2.1	Remove the components that are no longer needed	19
6.2.2	Prevent components that are no longer required from starting	19
6.3	Configuration parameters	20
6.4	Configuration of the e-mail functionality	23
6.5	Change system e-mail addresses	23
6.6	Migrate from the test installation to a productive system	23
7	Installation of a customer-specific version (Customizing)	24
8	Glossary	25
9	Disclaimer	26
10	Software AG support	27
11	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 about 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. For further information, see the ARIS Risk & Compliance Manager Installation Guide.

4 System requirements

4.1 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 ARIS Risk & Compliance Manager at one time.

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

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. 1600 x 800 pixels is recommended.
- Software: Microsoft® Internet Explorer version 11.0, Mozilla Edge, Mozilla Firefox version 23.x or higher, Google Chrome.

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

4.2 Microsoft® SQL Server system and settings

SYSTEM

- Microsoft® SQL Server 2014
- Microsoft® SQL Server 2016

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))

4.3 Acrobat Reader

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

4.4 Microsoft Office/Excel

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

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

For productive operation of ARIS Risk & Compliance Manager, use the standard database system (PostgreSQL) or an Oracle or Microsoft® SQL Server database. Note that a new database should be set up for productive operation. 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 is described. If you want to use Oracle or Microsoft® SQL Server as a DBMS you must install the database and database schema first.

5.1 Usage of an Oracle or a Microsoft® database

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.

5.1.1 Installation of an 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 must have an Oracle client installed (sqlplus). The following batch file and scripts are available:

- **create_arcm_user.bat**
Main script for starting the installation.
- **create_arcm_user.sql**
To create Oracle users for ARIS Risk & Compliance Manager.
- **drop_armc_user.sql**
If an user specified in **envset.bat** already exists, this user will be deleted and then newly created.
- **envset.bat**
Batch to enter database data.

Procedure

1. Edit the **envset.bat** file.
2. In the **envset.bat** file, enter the values described in the script.
3. Start the **create_arcm_user.bat** file.

The remaining scripts will then be executed in the correct sequence. The database does not contain a database schema with tables yet. These are created automatically 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 can result in an error message the first time it is executed because the user does not yet exist. When the script is executed again, the user is first deleted and then created again. All other commands must run without errors.

5.1.2 Installation of a 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.

- **inst.bat**
Main script for initializing an ARIS Risk & Compliance Manager database and user.
- **create_arcm_user.sql**
Generates the database user for ARIS Risk & Compliance Manager.
- **create_db.sql**
Generates the database instance for ARIS Risk & Compliance Manager.
- **envset.bat**
Batch to enter database data.

Warning

If a database with the same name already exists, the script will fail. Therefore, delete the database and the login of the database, before you execute the script.

Procedure

1. Edit the **envset.bat** file.
2. In the **envset.bat** file, enter the values described in the script.
3. Start the **install.bat** file.

The database does not contain a database schema with tables yet. These are created automatically when you start ARIS Risk & Compliance Manager server for the first time. Observe any error messages while the scripts are running.

5.2 Usage of a PostgreSQL database

If ARIS or ARIS Risk & Compliance Manager is installed via setup, the PostgreSQL database is installed automatically.

5.3 Manual configuration of the database for ARIS Risk & Compliance Manager

In some cases, it can be necessary to configure the database connection manually instead of using the setup. This chapter describes the procedure for the different database systems supported by ARIS Risk & Compliance Manager.

5.3.1 Make an Oracle database available to ARIS Risk & Compliance Manager

Once an Oracle database was prepared as described above, some additional steps are required to make it available to ARIS Risk & Compliance Manager. They are usually performed by the setup, but in specific situations it can be necessary to configure the database connection manually.

MAKE ORACLE AVAILABLE AS A SERVICE OF TYPE DB_ARCM

Procedure

1. Open ARIS Cloud Controller (ACC) console.
2. Stop the ARIS Risk & Compliance Manager component with **stop arcm_m** if necessary.
3. Execute the following command:

```
register external service db_arcm dbmsSystem="oracle" url="
jdbc:oracle:thin:@[host]:1521:[sid]"
driverClassName="oracle.jdbc.OracleDriver" username="[user]"
password="[password]" host="[host]" initialSize="10" maxActive="500"
maxIdle="50" minIdle="10" maxWait="30000" removeAbandoned="false"
removeAbandonedTimeout="60" logAbandoned="false"
```

4. Replace the items in the square brackets [...] with the values you used for your Oracle installation. This will assign a service ID, e.g., **db-arcm0000000001**, to the database.
5. You can adapt the values for the connection pool parameters **initialSize**, **minIdle**, **maxActive**, **maxIdle**, **maxWait**, **removeAbandoned**, **logAbandoned**, and **removeAbandonedTimeout** if needed.

Note that the service ID increases each time the command **register external service** is executed.

6. You can check the result by executing the command **show service [service Id]** in ARIS Cloud Controller, e.g., **show service db-arcm0000000001**.

The command **list services** displays an overview of all services.

ASSIGN THE TENANT OF ARIS RISK & COMPLIANCE MANAGER TO THE SERVICE OF TYPE DB_ARCM

Procedure

1. If you started ARIS Risk & Compliance Manager with the standard database (PostgreSQL) before, you must remove this assignment. To do so, execute the command

unassign tenant [ARIS Risk & Compliance Manager tenant name] from service db-arcm0000000000

Example: **unassign tenant default from service db-arcm0000000000**

Use the ARIS Cloud Controller command: **show external service [service name]** to find the relevant service. Use the command **list services** to display a list of all services. The correct service type is **DB_ARCM**.

2. Execute the ARIS Cloud Controller command: **assign tenant [ARCM tenant name] to service [service ID]** to assign the tenant of ARIS Risk & Compliance Manager to the Oracle service.

Example: **assign tenant default to service db-arcm0000000001**

If you want to use a different external service later, you must remove this assignment before registering the new one.

The tenant of ARIS Risk & Compliance Manager is assigned to the service of type DB_ARCM.

PROVIDE AND INTEGRATE THE DATABASE DRIVER

Procedure

1. Download the appropriate database driver from the Internet. (For licensing reasons, database drivers are not supplied.)
2. Store it on the server on which ARIS Risk & Compliance Manager is installed.
3. To integrate the database driver, enter the command **enhance arcm_m with commonsClasspath local file <Path>\\<to>\\<driver JAR>** in ARIS Cloud Controller (ACC).

The Oracle database is now available for ARIS Risk & Compliance Manager.

5.3.2 Make a Microsoft® SQL Server database available to ARIS Risk & Compliance Manager

Once a Microsoft® SQL Server database was prepared as described above, some additional steps are required to make it available to ARIS Risk & Compliance Manager. They are usually performed by the setup, but in specific situations it can be necessary to configure the database connection manually.

MAKE MICROSOFT® SQL SERVER AVAILABLE AS SERVICE OF TYPE DB_ARCM

Procedure

1. Open ARIS Cloud Controller (ACC) console.
2. Stop the ARIS Risk & Compliance Manager component with **stop arcm_m** if necessary.
3. Execute the following command:

```
register external service db_arcm dbmsSystem="mssql" url="
jdbc:sqlserver://[host]:1433;DatabaseName="[database]"
driverClassName="com.microsoft.sqlserver.jdbc.SQLServerDriver"
username="[user]" password="[password]" host="[host]" initialSize="10"
maxActive="500" maxIdle="50" minIdle="10" maxWait="30000"
removeAbandoned="false" removeAbandonedTimeout="60"
logAbandoned="false"
```
4. Replace the items in the square brackets [...] with the values you used for Microsoft® SQL Server installation. This will assign a service ID, e.g., **db-arcm0000000001**, to the database.
5. You can adapt the values for the connection pool parameters **initialSize**, **minIdle**, **maxActive**, **maxIdle**, **maxWait**, **removeAbandoned**, **logAbandoned**, and **removeAbandonedTimeout** if needed.
Note that the service ID increases each time the command **register external service** is executed.
6. You can check the result by executing the command **show service [service Id]** in ARIS Cloud Controller, e.g., **show service db-arcm0000000001**.

The command **list services** displays an overview of all services.

ASSIGN THE TENANT OF ARIS RISK & COMPLIANCE MANAGER TO THE SERVICE OF TYPE DB_ARCM

Procedure

1. If you started ARIS Risk & Compliance Manager with the standard database (PostgreSQL) before, you must remove this assignment. To do so, execute the command

unassign tenant [ARIS Risk & Compliance Manager tenant name] from service db-arcm0000000000

Example: **unassign tenant default from service db-arcm0000000000**

Use the ARIS Cloud Controller command: **show external service [service name]** to find the relevant service. Use the command **list services** to display a list of all services. The correct service type is **DB_ARCM**.

2. Execute the ARIS Cloud Controller command: **assign tenant [ARCM tenant name] to service [service ID]** to assign the tenant of ARIS Risk & Compliance Manager to the Oracle service.

Example: **assign tenant default to service db-arcm0000000001**

If you want to use a different external service later, you must remove this assignment before registering the new one.

The tenant of ARIS Risk & Compliance Manager is assigned to the service of type DB_ARCM.

PROVIDE AND INTEGRATE THE DATABASE DRIVER

Procedure

1. Download the appropriate database driver from the Internet. (For licensing reasons, database drivers are not supplied.)
2. Store it on the server on which ARIS Risk & Compliance Manager is installed.
3. To integrate the database driver, enter the command **enhance arcm_m with commonsClasspath local file <Path>\\<to>\\<driver JAR>** in ARIS Cloud Controller (ACC).

The Microsoft® SQL Server database is now available for ARIS Risk & Compliance Manager.

5.3.3 Make a PostgreSQL database available to ARIS Risk & Compliance Manager

You can configure a PostgreSQL instance manually to make it available to ARIS Risk & Compliance Manager.

Procedure

1. Open ARIS Cloud Controller (ACC) console.
2. Stop the ARIS Risk & Compliance Manager component with **stop arcm_m** if necessary.
3. Check the settings by executing the command **show instance [instance name]**, e.g., **show instance postgres_m**.
4. Check if the **plugin.apptypes** parameter contains **DB_ARCM**.
Otherwise, configure the instance of the PostgreSQL runnable that is to be used for ARIS Risk & Compliance Manager as follows.
5. Execute the command **reconfigure [instance name] plugin.apptypes=DB_ARCM dbbsp.dbmsSystem=postgresql** to assign the **DB_ARCM** app type and the **PostgreSQL** instance type.
6. If ARIS Risk & Compliance Manager is using the same PostgreSQL instance like ARIS Server, the app type database used by ARIS Server must be preserved. To do so, execute the command:

```
reconfigure [instance name] plugin.apptypes=DB,DB_ARCM  
dbbsp.dbmsSystem=postgresql
```

Insert the name of the PostgreSQL instance that is to be used for **[instance name]**, e.g. **postgres_m**.

7. If you started ARIS Risk & Compliance Manager with the standard database (PostgreSQL) or another database service before, you must remove this assignment. In this case, execute the command:

```
unassign tenant [ARCM tenant name] from service [service ID]
```

Example: **unassign tenant default from service db-arcm0000000000**

Use the ARIS Cloud Controller command: **show instance [instance name] verbose**, e.g., **show instance postgres_m verbose**, to find the relevant PostgreSQL instance. Use the command **list services** to display a list of all services. The correct service type is **DB_ARCM**.

8. Assign the tenant of ARIS Risk & Compliance Manager with the relevant service by executing the ARIS Cloud Controller command:

```
assign tenant default to service [service ID]
```

Example: **assign tenant default to service db-arcm0000000001**

The PostgreSQL database instance is now available for ARIS Risk & Compliance Manager.

6 Installation of ARIS Risk & Compliance Manager

From version 9.8.6, ARIS reports are supported by ARIS Risk & Compliance Manager. Some of the ARIS Risk & Compliance Manager reports are now run by ARIS Server. The settings like output format and execution context can be changed easily.

The ARIS Server runnable is as well installed during the installation of ARIS Risk & Compliance Manager via setup. If you use a dedicated ARIS Server, you can integrate the ARIS Risk & Compliance Manager runnable into an existing ARIS installation.

6.1 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**. This 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 the 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, read chapter **ARIS remote installations** in the **ARIS Server Installation Guide - Windows**.

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 **Install ARIS Server 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. Select **ARIS Risk & Compliance Manager** and click **Next**.
8. To use the suggested path, you do not need to make any changes.
9. In the next dialog, do not make any changes and click **Next**.
10. Change the agent user's credentials if necessary and click **Next**.
11. Change the HTTP and HTTPS ports if necessary and click **Next**.
12. Select the installation size in order to determine the memory allocated for ARIS Risk & Compliance Manager: **Demo scenario** = 1GB, **Medium** = 4GB, **Large** = 8GB.

13. Select a license file automatically used by the setup. Alternatively, you can select a license file in User Management after the installation procedure is complete.
14. Click **Next**. The **Select database system** dialog is displayed.
15. Select the relevant database: **Standard database system** for a PostgreSQL database. For Oracle or Microsoft® SQL Server, an appropriate database driver that is installed during setup must also be provided. The driver can be downloaded from Oracle/Microsoft.
16. 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 8) (Oracle SID) or the database name of the database instance (Microsoft® SQL Server).
 - d. Enter the name and password of the database (Page 8) user.
17. Click **Next**.
18. Enter the SMTP mail processing parameters of an existing account to enable ARIS Risk & Compliance Manager to send notifications, or configure SMTP e-mail processing later.
Some parameters can also be managed via User Management of this server. For detailed information, refer to the User Management online help or the ARIS Installation and Administration Guides.
19. Activate **Use TLS/SSL encryption** to prevent password sniffing.
20. Only if your mail server requires SMTP authentication, select the option **SMTP authentication** and enter the user's credentials.
If you enter these parameters but your mail server does not require SMTP authentication, the connection will be rejected.
21. If you want to use a proxy server, enter all proxy processing parameters. You can also enter them later, using User Management of this server. See the online help of User Management.
22. Configure the start option: Select **Start automatically** if you want to have the server started up with every restart of your operating system.
Select **Start manually** if you want to start/stop the server on the active computer manually.
23. Activate the relevant modeling approach for ARIS Risk & Compliance Manager and click **Next**. You cannot change the modeling approach after installation is complete.
24. If necessary, activate event enabling. For detailed information on how to configure and adapt event enabling, refer to **ARIS Risk & Compliance Manager Administration Guide > The configuration of event enabling in ARIS Risk & Compliance Manager** and **ARIS Risk & Compliance Manager Customizing Guide > Adapt and extend event enabling**.
25. 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.

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

An ARIS Risk & Compliance Manager installation can be integrated into an existing ARIS Server installation that is based on the same version number, service level, 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**.

From version 10.0 of ARIS Risk & Compliance Manager, the database setting is configured via external services in the ARIS Cloud Controller. Therefore, a new external service is created and used automatically if you install ARIS Risk & Compliance Manager via the setup. But if you integrate ARIS Risk & Compliance Manager with an existing ARIS installation, you must create this external service manually in the ARIS installation environment (zookeeper of the ARIS installation).

Warning

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

Procedure

1. Install ARIS Server via setup on a server. For detailed information, see **ARIS Server Installation - Windows** (Installation > Initial installation > Server).
2. Start ARIS Server.
3. Create an external service for ARIS Risk & Compliance Manager on the ARIS Server to specify the database connection. For details, see Manual configuration of the database for ARIS Risk & Compliance Manager (Page 10).
4. Install (Page 15) ARIS Risk & Compliance Manager on another server via setup.
5. Start ARIS Cloud Controller for the ARIS Risk & Compliance Manager installation using **Start > ARIS > ARIS Cloud Controller**.
6. Enter the command **reconfigure arcm_m zookeeper.connect.string="<ARISServer>:14281"** in the console.
7. As a placeholder for **<ARISServer>**, enter the name of the server that you used in step 1 for ARIS Server.
8. If you did not change the port keep the default settings.
9. To use the standard database system, enter the command **reconfigure postgres _m zookeeper.connect.string="<ARISServer>:14281"** in the console.
10. As a placeholder for **<ARISServer>**, enter the name of the server that you used in step 1 for ARIS Server.

11. If you did not change the port keep the default settings.
12. Use the **list** command to check whether all components have the status **STOPPED**.
 - a. If not installed via ARIS Risk & Compliance Manager setup, provide an appropriate database driver for Oracle or Microsoft® SQL Server. To do so, enhance arcm_m with the commonsClasspath local file: **<ojdbc.jar-file.jar>**.
 - b. Replace **<ojdbc.jar-file.jar>** by a real file name and its path using the character **** or **/** for ****.
13. 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 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 Server followed by **/arcm**. As ARIS Risk & Compliance Manager no longer requires the other components on the server, they can be either removed (Page 19), or configured in such a way that they will no longer be started automatically when the server is started.

6.2.1 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.

6.2.2 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**:
 - a. **set zoo_m property autostart="false"**
 - b. **set postgres_m property autostart="false"**
 - c. **set couchdb_m property autostart="false"**
 - d. **set elastic_m property autostart="false"**
 - e. **set adsadmin_m property autostart="false"**
 - f. **set umcadmin_m property autostart="false"**
 - g. **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.


6.3 Configuration parameters

If you want to configure ARIS Risk & Compliance Manager, use the parameters in **Administration > Configuration > Show configuration**. There are two groups of parameters:

- **Parameters which can be changed while the application is running**

Click  **Edit** to change the values of these parameters. Changes are applied immediately and stored in the database. Click  **Reset** to return to default value.

- **Parameters which require a re-start of the system after they are changed**

The parameters that cannot be edited here are marked as  **Locked** in the **Editable** column. Configure them via ARIS Cloud Controller by executing reconfigure commands. The affected server instances are restarted afterwards. If the installation contains several instances of ARIS Risk & Compliance Manager server, all of them must be configured identically to ensure consistent behavior.

Example: **reconfigure arcm_m arcm.config.dbCaseSensitive=false**

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.

ARCM.CONFIG.KEEPALIVETIME

param-value	Description
60	Specifies the timeout of the automatic logout in seconds. After this time period, inactive user sessions are terminated, i.e., users are logged out automatically.

ARCM.CONFIG.ENTRIESPERPAGE

param-value	Description
20	Specifies the number of entries per page for object lists.

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
- generatorJobSOProcess
- monitorJobSOProcess
- 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.

EXCLUDEENVIRONMENTS

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

INCLUDEENVIRONMENTS

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

6.4 Configuration of the e-mail functionality

You can configure ARIS Risk & Compliance Manager in such a way that e-mails are sent automatically in specific situations, e.g., to a tester to whom a test case was 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. If you did not specify the SMTP configuration during the installation via setup, configure it manually in User Management. For more information on how to customize the SMTP settings, refer to the ARIS Connect Administrator User Manual.

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

6.5 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. Replace them with valid addresses (**Administration > Users > <user_xy>**). The e-mail addresses of the following users must be replaced:

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

6.6 Migrate from the test installation to a productive system

It is recommended that you keep the server of the test system and productive system separate. Depending on the load on the production and test system, it can 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 (Page 10). To do this, you must change the database parameters in ARIS Cloud Controller.

7 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 15) 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.

8 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.

9 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.

6 Software AG support

ON THE WEB

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

Click <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

11 Index

C

- Change system e-mail addresses • 23
- Configuration parameters • 20
- Customizing • 24

E

- E-mail functionality • 23

G

- Global Unique Identifier (GUID) • 25

I

- Installation and configuration
 - Important information • 3
 - Installation of ARIS Risk & Compliance Manager • 15
 - Integrate in ARIS • 17
 - Microsoft® SQL Server database schema installation • 9
 - Migrate from the test installation to a productive system • 23
 - Oracle database schema • 8
 - Oracle or Microsoft® SQL Server database • 7
 - Prevent components that are no longer required from starting • 19
 - Remove components that are no longer required • 19
 - Standalone installation via setup • 15
- Introduction • 2

J

- Java Database Connectivity (JDBC) • 25

M

- Manual configuration of the database for
 - ARIS Risk & Compliance Manager • 10
 - Microsoft® SQL Server database • 12
 - Oracle database • 10
 - PostgreSQL database • 14
- Multi-purpose Internet Mail Extension mapping • 25

O

- Oracle service ID • 25

S

- Simple Mail Transfer Protocol (SMTP) • 25
- Support • 27
- System requirements
 - Acrobat Reader • 6

- Microsoft® Office/Excel • 6
- Microsoft® SQL Server • 5
- Oracle system • 4

U

- Usage of a PostgreSQL database • 10
- Usage of an Oracle or a Microsoft® databases • 8