software AG

ARIS RISK & COMPLIANCE MANAGER
INSTALLATION GUIDE

VERSION 10.0 - SERVICE RELEASE 9

July 2019

Contents

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.`
- Warnings have a colored background:

  Warning

  This paragraph contains a warning.

2   Introduction

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, that is, 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 **PostgreSQL** database for testing purposes or small environments (up to fifty concurrent users). 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).

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 (12.1.0.2.0)

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 * 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

- 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: For details on the supported operating systems, refer to the **ARIS System Requirements** guide.
- Main memory: Minimum 8 GB RAM
- Controller: SAS (RAID0)
- Hard disks: In RAID array (example: RAID0, 2x146 GB (SAS 15000 UPM))

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.
- Browsers: For details refer to the **ARIS System Requirements** guide.

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

The following describes installation with automatic setup. 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, that is, 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_arcm_user.sql**

    If a user specified in **envset.bat** already exists, this user will be deleted and then newly created.

- **envset.bat**

    Batch to enter database data.

If you install ARIS Risk & Compliance Manager in parallel to ARIS Connect or ARIS Design Server, specify a separate application user (name of the database user) for ARIS Risk & Compliance Manager so that the data of ARIS Risk & Compliance Manager and ARIS is stored in separate databases.

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

5.1.2.1 Using Microsoft® SQL Server (mixed mode)

Install the Microsoft® SQL Server. The supplied ARIS Risk & Compliance Manager package includes several database scripts that assist you in preparing the database for ARIS Risk & Compliance Manager. The following files are needed to create a database for MS 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, before you execute the script, delete the database and the login of the database.

Prerequisites

- An operating Microsoft SQL Server database. If you have not yet installed the Microsoft SQL Server, please follow the instructions in the Microsoft installation program, as well as the documentation provided by the manufacturer. The external database management system is not included in this package. If you need help in setting up ARIS using your external database system, please contact Software AG. Please note that this service is not subject to the standard Software AG software maintenance agreement and that these changes can only be performed if you requested and agreed on them.

- You need to know the port number, the database name of the new database instance and also the user name and the password of the application user.

- You have downloaded the latest version of the Microsoft SQL Server JDBC driver, for example, sqljdbc4-4.0.2206.100.jar from the Microsoft Download Center to a directory of your choice.

- SQL scripts and all additional files. All scripts and files are located on the installation medium (Add-ons\DatabaseScripts\ARIS Risk & Compliance Manager\MSSQL) or they can be downloaded from the ARIS Download Center (aris.softwareag.com).

Procedure

1. Adjust the settings used by all configuration scripts.

   Edit the **envset.bat** file to specify the connection data of the Microsoft SQL server instance. It is a good idea to write down the credentials. They must be entered later during the ARIS setup process. To specify the connection data of the Microsoft SQL instance, modify the highlighted parameters:

   ```
   @ECHO OFF
   REM
   REM You may edit this section for customizing purposes.
   REM

   REM If you use named instances then append a "\" and the name of your instance
   SET MSSQL_SAG_MSSQL_SERVER_NAME=localhost

   REM The login name that is used to execute this script
   SET MSSQL_SAG_MSSQL_LOGIN_NAME=localhost\username

   REM name of database that will be created by the script.
   SET MSSQL_SAG_DATABASE_NAME=ARCM10DB

   REM folder in which the database files should be stored.
   SET MSSQL_SAG_FILEGROUP_FILE_DIR=F:\msqldata\ARCM10DB

   REM credentials of the login that is used by the application.
   SET MSSQL_SAG_APP_USER=ARCM10
   SET MSSQL_SAG_APP_PWD=*ARIS!1dm9n#
   ```

2. Execute the **inst.bat** file. This creates the database including the application user. The application user (APP_USER) is the Microsoft SQL user connecting ARIS Risk & Compliance Manager and the Microsoft SQL database. The default user name is **ARCM10**. Note that you may have changed that name in the **envset.bat** earlier. The values must be entered later during the ARIS Server setup process.

The Microsoft® SQL Server is installed and running. 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.

5.1.2.2 Using Microsoft® SQL Server (Windows authentication)

Install the Microsoft® SQL Server. The supplied ARIS Risk & Compliance Manager package includes several database scripts that assist you in preparing the database for ARIS Risk & Compliance Manager. The following files are needed to create a database for MS 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.

Prerequisites

- An operating Microsoft SQL Server database. If you have not yet installed the Microsoft SQL Server, please follow the instructions in the Microsoft installation program, as well as the documentation provided by the manufacturer. The external database management system is not included in this package. If you need help in setting up ARIS using your external database system, please contact Software AG. Please note that this service is not subject to the standard Software AG software maintenance agreement and that these changes can only be performed if you requested and agreed on them.

- You need to know the port number, the database name of the new database instance and also the user name and the password of the application user.

- You have downloaded the latest version of the Microsoft SQL Server JDBC driver, for example, sqljdbc4-4.0.2206.100.jar from the Microsoft Download Center to a directory of your choice.

- SQL scripts and all additional files. All scripts and files are located on the installation medium (Add-ons\DatabaseScripts\ARIS Risk & Compliance Manager\MSSQL) or they can be downloaded from the ARIS Download Center (aris.softwareag.com).

- You have downloaded the **sqljdbc_auth.dll** file (https://www.microsoft.com).

Procedure

1. Adjust the settings used by all configuration scripts.

   Edit the **envset.bat** file to specify the connection data of the Microsoft SQL server instance. It is a good idea to write down the credentials. They must be entered later during the ARIS setup process. To specify the connection data of the Microsoft SQL instance, modify the highlighted parameters:

```
@ECHO OFF
REM
REM You may edit this section for customizing purposes.
REM

REM If you use named instances then append a "\" and the name of your instance
SET MSSQL_SAG_MSSQL_SERVER_NAME=localhost

REM The login name that is used to execute this script
```

> **Warning**
>
> The login name used to run the script (MSSQL_SAG_MSSQL_LOGIN_NAME) must be different from the Windows user used to run the service (see **create_arcm_user.sql** file; <domainaccount>).

```
SET MSSQL_SAG_MSSQL_LOGIN_NAME=localhost\username

REM name of database that will be created by the script.
SET MSSQL_SAG_DATABASE_NAME=ARCM10DB

REM folder in which the database files should be stored.
SET MSSQL_SAG_FILEGROUP_FILE_DIR=F:\msqldata\ARCM10DB

REM credentials of the login that is used by the application.
SET MSSQL_SAG_APP_USER=ARCM10
SET MSSQL_SAG_APP_PWD=*ARIS!1dm9n#
```

2. Edit the **create_arcm_user.sql** file:

   a. If the login to be used does not exist, change the **CREATE LOGIN** command as follows:

   CREATE LOGIN **[<domain account>]** FROM WINDOWS WITH DEFAULT_DATABASE=[$(database)]

   b. In the **CREATE USER** command for login, replace **$(username)** with the domain account to be used:

   CREATE USER **[$(username)]** FOR LOGIN **[<domain account>]**

   c. If the login to be used already exists, delete the following highlighted section from the file:

   USE [$(database)]

   GO

   CREATE LOGIN $(username) WITH PASSWORD=N'$(password)', DEFAULT_DATABASE=[$(database)]

   GO

   d. In the **CREATE USER** command for login, replace **$(username)** with the domain account to be used:

   CREATE USER **[$(username)]** FOR LOGIN **[<domain account>]** with default schema = **$(username)**

   e. In the **GRANT IMPERSONATE ON USER** command, replace **$(username)** with the domain account to be used:

   GRANT IMPERSONATE ON USER::$(username) TO [<domain account>]

3. Execute the **inst.bat** file. This creates the database including the application user. The application user (APP_USER) is the Microsoft SQL user connecting ARIS Risk & Compliance Manager and the Microsoft SQL database. The default user name is **ARCM10**. Note that you may have changed that name in the **envset.bat** earlier. The values must be entered later during the ARIS Server setup process.

4. After the installation of ARIS Risk & Compliance Manager, open the properties dialog of the Windows service and click the **Log on** tab.

5. Select **This account**.

6. Click **Browse** and specify the name of the domain account to be used.

7. Enter the password and click **OK**.

8. Restart the service.

9. Copy the downloaded **sqljdbc_auth.dll** file (https://www.microsoft.com) to **%windir%\System32**.

10. Click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller** (see **ARIS Cloud Controller (ACC) Command-Line Tool.pdf**). If you have changed the ARIS Agent's default user credentials during this procedure, you are prompted for that password you have chosen.

11. Start the **zookeeper** runnable to modify the database connection string. Enter, for example:

    start zookeeper_m

12. Add the **integratedSecurity=true** parameter to the database service:

    To update an existing service, use the following command to edit the URL, for example:

    update external service <service ID> url="jdbc:sqlserver://<database server>:<database port>;DatabaseName=<database name>;integratedSecurity=true"

    If you register a new service, the **integratedSecurity=true** parameter must also be added to URL, for example:

    register external service db url="jdbc:sqlserver://<database server>:<database port>;DatabaseName=<database name>;integratedSecurity=true" driverClassName="com.microsoft.sqlserver.jdbc.SQLServerDriver" username="<user name>" password="<password>" maxIdle=15 maxActive=300 maxWait=10000 removeAbandoned=false removeAbandonedTimeout=600 logAbandoned=true initialSize=0 testOnBorrow=true validationQuery="select 1" defaultAutoCommit=false rollbackOnReturn=true host=<database server> jmxEnabled=true

13. Click **Start > All Programs > ARIS > Administration > Start ARIS Server**. If you have changed the ARIS Agent's default user credentials during this procedure, you are prompted for that password you have chosen. The start process will take a while.

The Microsoft® SQL Server is installed and running.

5.2 Usage of a PostgreSQL database

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

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

In some cases, it may 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 has been 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 may 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 (**Start > ARIS Cloud Controller**).
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 to assign a service ID to the database, for example, **db-arcm0000000001**.
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, for example, **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 previously started ARIS Risk & Compliance Manager with the standard database (PostgreSQL), 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 the 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 has been 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 may 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 (**Start > ARIS Cloud Controller**).
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, for example, **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, for example, **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 previously started ARIS Risk & Compliance Manager with the standard database (PostgreSQL), 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 the 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 (**Start > ARIS Cloud Controller**).
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]**, for example, **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 dbsp.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 as 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 dbsp.dbmsSystem=postgresql

   Insert the name of the PostgreSQL instance that is to be used for **[instance name]**, for example **postgres_m**.
7. If you previously started ARIS Risk & Compliance Manager with the standard database (PostgreSQL) or another database service, 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**, for example, **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 also installed during the installation of ARIS Risk & Compliance Manager with the 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 with the setup

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 Server 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, activate **I accept the terms of the license agreement**. The **Installation scenario** dialog is displayed.

5. Select the installation scenario **Install ARIS Server on this active computer** and click **Next**.

6. Deselect **ARIS Connect/ARIS Design Server**.

7. Select **ARIS Risk & Compliance Manager** and click **Next**.

8. Enter the directory in which you want to install ARIS Risk & Compliance Manager and click **Next**.

9. To use the suggested path, you do not need to make any changes.

10. If you want to specify an external IP address for incoming requests, enter the computer name or the IP address and click **Next**.

11. Change the agent user's credentials if necessary and click **Next**.

12. Change the HTTP and HTTPS ports if necessary and click **Next**.

13. Select the installation size in order to determine the memory allocated for ARIS Risk & Compliance Manager: **Demo scenario** = 1GB, **Medium** = 4GB, **Large** = 8GB.

14. 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.

15. Click **Next**. The **Select database system** dialog is displayed.

16. 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.

17. 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 7) (Oracle SID) or the database name of the database instance (Microsoft® SQL Server).

    d. Enter the name and password of the database (Page 6) user.

18. Click **Next**.

19. 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 with the User Management of this server. For detailed information, refer to the User Management online help or the ARIS Installation and Administration Guides.

20. Enter the default **Server task sender address** for ARIS Risk & Compliance Manager that is used as the sender e-mail address for messages triggered by scheduled server tasks.

21. Optionally, enable whistleblower tips to be sent. In this case, you have to specify an e-mail address for the whistleblower tip recipient and the whistleblower tip sender. You can change both addresses later in the system configuration of ARIS Risk & Compliance Manager.

22. Activate **Use TLS/SSL encryption** to prevent password sniffing.

23. 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.

24. 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.

25. 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.

26. If you want to enable customizing for ARIS Risk & Compliance Manager, select **Import now** and specify your customizing file.

27. Activate the relevant modeling approach for ARIS Risk & Compliance Manager and click **Next**. You cannot change the modeling approach after installation is complete.

28. If necessary, activate event enabling. For detailed information on configuring and adapting 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**.

29. 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

Up to ARIS version 10.0.3, you had to install ARIS Connect server and ARIS Risk & Compliance Manager on separate servers. From ARIS version 10.0.4, you can install them on the same server. However, you can still use a separate server for ARIS Risk & Compliance Manager, for example, to improve the performance.

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. ARIS Administration/User Management for all ARIS products, which is not to be confused with the Administration in ARIS Risk & Compliance Manager, serves to manage users, user groups, function and license privileges, licenses, and configurations. This enables single sign-on (page 28) 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 with external services in the ARIS Cloud Controller. Therefore, a new external service is created and used automatically if you install ARIS Risk & Compliance Manager with 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 with the 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 13).
4. Install (Page 18) ARIS Risk & Compliance Manager on another server with the setup.
5. Open ARIS Cloud Controller (ACC) console (**Start > ARIS Cloud Controller**).
6. Enter the command **set 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. Use the **list** command to check whether all components have the status **STOPPED**.

a. If not installed with the 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 ****.

10. 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 22), or deactivated in order to prevent they are 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. Open ARIS Cloud Controller (ACC) console (**Start > 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 Deactivate runnables that are no longer required from starting

Deactivate the components that are no longer required from starting.

Procedure

1. Open ARIS Cloud Controller (ACC) console (**Start > ARIS Cloud Controller**).

2. Deactivate the runnables that are no longer required, set **autostart property** to **false:**

   a. Deactivate **zoo_m**.

   b. Deactivate **postgres_m**.

   c. Deactivate **cloudsearch_m**.

   d. Deactivate **elastic_m**.

   e. Deactivate **umcadmin_m**.

   f. Deactivate **adsadmin_m**.

   g. Deactivate **abs_m**.

   h. Deactivate **loadbalancer**.

The runnables that are no longer required are deactivated, that is, the command **startall** in ARIS Cloud Controller does not start them anymore.

6.3 Configure parameters

If you want to configure ARIS Risk & Compliance Manager, use the parameters in **Administration > General > System management > System 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 with 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, that is, users are logged out automatically.

ARCM.CONFIG.ENTRIESPERPAGE

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

SCHEDULER SETTINGS

You can configure ARIS Risk & Compliance Manager with parameters in **System configuration**. The parameters that are marked as 🔒 **Locked** in the **Editable** column must be edited using ARIS Cloud Controller. Parameters without the lock symbol can be edited.

Procedure

1. Click 🔧 **Administration**. The **General** menu item is displayed initially.
2. Under **System management**, click **System configuration**. The configuration parameters are displayed.
3. To display the scheduled server tasks, filter the system configuration by **Server task schedules**. The search result displays all scheduled server tasks with their current values.
4. Click ✏ **Edit** in the row of the parameter you want to change. The **Specify parameter value** dialog opens.
5. Make the relevant changes, for example, to activate a feature, replace **false** with **true**.
6. Click **OK**.

The changes are immediately applied and stored in the database. Click ↩ **Reset** in the row of the relevant parameter to reset the default value.

Examples

- **Hide empty attributes**

  If this parameter is set to **true**, empty attributes of ARIS Risk & Compliance Manager objects are not displayed when forms, reports, or data in ARIS Connect are opened in read-only mode.

- **Unlock objects locked by other users**

  If this parameter is set to **true**, users can remove the offline processing object lock set by other users, provided all users involved are members of the same offline processing group of the object.

- **Use colors of ARIS Connect**

  If this parameter is set to **false**, the customized colors of the active ARIS Connect configuration set are not used for ARIS Risk & Compliance Manager.

STARTSCHEDULER

Use the **startScheduler** section to activate (**true**) or deactivate (**false**) server tasks.

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

Example

```
[ jobitem | generatorJob ] [ startScheduler | false ] [ executionTime | 0 52 00 ?
* SUN-SAT ] [ excludedEnvironments | ] [ includedEnvironments | ] [ objecttypes |
TESTCASE ]
```

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 is provided on the Quartz home page (http://www.quartz-scheduler.org).

EXCLUDEENVIRONMENTS

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

INCLUDEENVIRONMENTS

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

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, for example, 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 SMPT configuration during the installation with the setup, configure it manually in ARIS Administration/User Management. For more information on customizing 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 e-mail addresses

You can change the e-mail address of the whistleblower tip recipient, whistleblower tip sender, and the server task sender. All other e-mail addresses can only be changed in ARIS Administration/User Management. For detailed information, refer to configure parameters (Page 23).

Procedure

To do so, open the system configuration, filter the list with **E-mail**, and make your changes.

The changes are immediately applied and stored in the database. Click ↰ **Reset** in the row of the relevant parameter to reset the default value.

6.6 Migrate from the test installation to a productive system

You are recommended keeping 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 13). 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. From version 10.0.4 you can also upload customized ZIP files during the setup.

Warning

The existing customizing is deleted during the enhancement of the new customizing.

Procedure

1. Install (Page 18) ARIS Risk & Compliance Manager. Installation is completed.

2. Open ARIS Cloud Controller (ACC) console (**Start > ARIS Cloud Controller**).

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, for example, 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.

SINGLE SIGN-ON (SSO)

With single sign-on (SSO) users authenticate only once with their user name and password to access all services, programs, and computers without logging in again. If services, programs, and computers request a new authentication, the authentication is handled by the underlying SSO mechanism.

9 Legal information

9.1 Documentation scope

The information provided describes the settings and features as they were at the time of publishing. Since documentation and software are subject to different production cycles, the description of settings and features may differ from actual settings and features. Information about discrepancies is provided in the Release Notes that accompany the product. Please read the Release Notes and take the information into account when installing, setting up, and using the product.

If you want to install technical and/or business system functions without Software AG's consulting services, you require extensive knowledge of the system to be installed, its intended purpose, the target systems, and their various dependencies. Due to the number of platforms and interdependent hardware and software configurations, we can only describe specific installations. It is not possible to document all settings and dependencies.

When you combine various technologies, please observe the manufacturers' instructions, particularly announcements concerning releases on their Internet pages. We cannot guarantee proper functioning and installation of approved third-party systems and do not support them. Always follow the instructions provided in the installation manuals of the relevant manufacturers. If you experience difficulties, please contact the relevant manufacturer.

If you need help installing third-party systems, contact your local Software AG sales organization. Please note that this type of manufacturer-specific or customer-specific customization is not covered by the standard Software AG software maintenance agreement and can be performed only on special request and agreement.

If a description refers to a specific ARIS product, the product is named. If this is not the case, names for ARIS products are used as follows:

Name	Includes
ARIS products	Refers to all products to which the license regulations of Software AG standard software apply.
ARIS Clients	Refers to all programs that access shared databases via ARIS Server, such as ARIS Architect or ARIS Designer.
ARIS Download clients	Refers to ARIS clients that can be accessed using a browser.

9.2 Data protection

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR).

Where applicable, appropriate steps are documented in the respective administration documentation.

9.3   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.

10   Index