



ARIS RISK & COMPLIANCE MANAGER **INSTALLATION GUIDE**

VERSION 10.0 - SERVICE RELEASE 12

April 2020

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 - 2020 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

Contents.....	1
1 Text conventions.....	1
2 Introduction.....	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.....	4
4.3 Acrobat Reader.....	4
4.4 Microsoft Office/Excel.....	4
5 ARIS Risk & Compliance Manager installation using an Oracle or a Microsoft® SQL Server database.....	5
5.1 Installation of an Oracle or a Microsoft® database.....	5
5.1.1 Install an Oracle database schema.....	6
5.1.2 Install a Microsoft® SQL Server database schema (mixed mode/Windows authentication).....	6
5.2 Usage of a PostgreSQL database.....	6
5.3 Manual configuration of the database for ARIS Risk & Compliance Manager.....	7
5.3.1 Add tenant schema of ARIS Risk & Compliance Manager.....	7
5.3.2 Provide and integrate the database driver.....	8
5.3.3 Configure the database connection pool.....	8
6 Installation of ARIS Risk & Compliance Manager.....	9
6.1 Installation with the setup.....	9
6.2 Integrate ARIS Risk & Compliance Manager in an existing ARIS installation.....	11
6.3 Configure parameters.....	12
6.4 Configuration of the e-mail functionality.....	15
6.5 Change e-mail addresses.....	15
6.6 Migrate from the test installation to a productive system.....	16
7 Installation of a customer-specific version (Customizing).....	17
8 Glossary.....	18
9 Legal information.....	19
9.1 Documentation scope.....	19
9.2 Data protection.....	19
9.3 Restrictions.....	20
10 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 as **<bold text in angle brackets>**.
- Example texts that are too long to fit on a single line, such as a long directory path, are wrapped to the next line by using ↵ at the end of the line.
- 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.

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.

4 System requirements

4.1 Oracle system and settings

Follow the instructions provided in the **ARIS Server Installation** and **ARIS System Requirements** guides.

4.2 Microsoft® SQL Server system and settings

Follow the instructions provided in the **ARIS Server Installation** and **ARIS System Requirements** guides.

4.3 Acrobat Reader

The Adobe Reader must be installed on the client side in order to display PDF reports.

4.4 Microsoft Office/Excel

A Microsoft® Excel version 2003 or higher must be installed on the client side 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 Installation 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 Install an Oracle database schema

Follow the instructions provided in the **ARIS Server Installation** guide to prepare the Oracle database. After you set up the database, use the corresponding script again to create the ARIS Risk & Compliance Manager database schema. You can use an individual schema name, but it must be unique to the schema names of other ARIS applications:

```
cip_create_schema_for_tenant.bat <arcm_tenant_schema>
```

Example for schema name ARIS10_ARCM_DEFAULT

```
cip_create_schema_for_tenant.bat ARIS10_ARCM_DEFAULT
```

If you want to restore database backups of previous versions, you also need a migration schema:

```
cip_create_schema_for_tenant.bat <arcm_tenant_schema_migration>
```

Example for schema name ARIS10_ARCM_DEFAULT_MIGRATION

```
cip_create_schema_for_tenant.bat ARIS10_ARCM_DEFAULT_MIGRATION
```

The database schema does not yet contain any table. They 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.

5.1.2 Install a Microsoft® SQL Server database schema (mixed mode/Windows authentication)

Follow the instructions provided in the **ARIS Server Installation** guide to prepare the Microsoft® SQL Server database with mixed mode or Windows authentication. After you set up the database, use the corresponding script again to create the ARIS Risk & Compliance Manager database schema. You can use an individual schema name, but it must be unique to the schema names of other ARIS applications:

```
create_schema_for_tenant.bat <arcm_tenant_schema>
```

Example for schema name ARCM_DEFAULT

```
create_schema_for_tenant.bat ARCM_DEFAULT
```

If you want to restore database backups of previous versions, you also need a migration schema:

```
create_schema_for_tenant.bat <arcm_tenant_schema_migration>
```

Example for schema name ARCM_DEFAULT_MIGRATION

```
create_schema_for_tenant.bat ARCM_DEFAULT_MIGRATION
```

The database schema does not yet contain any table. They 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.

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. Follow the instructions provided in the **ARIS Server Installation** guide, chapter **Database connection**. The following steps are independent of the database system in use.

5.3.1 Add tenant schema of ARIS Risk & Compliance Manager

After you installed the database connection according to the instructions in the previous chapters, you can add the tenant schema of ARIS Risk & Compliance Manager.

Procedure

1. Start ARIS Cloud Controller (ACC).

To start ACC under a Windows operating system, click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller**. If you have changed agent user credentials, you must enter the user name and/or the password.

To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead.

2. Enhance the existing assignment of the tenant to the external service of type **DB** with the corresponding ARCM schema configuration.

The parameter **com.aris.arcm.db.schema.migration** is only required if you want to restore database backups of previous versions and the migration schema is already created.

3. Enter:

```
set tenant <tenant name> data for service DB
```

```
com.aris.arcm.db.schema=<arcm_tenant_schema>
```

```
com.aris.arcm.db.schema.migration=<arcm_tenant_migration_schema> Example for default tenant:
```

```
set tenant default data for service DB
```

```
com.aris.arcm.db.schema=ARIS10_ARCM_DEFAULT
```

```
com.aris.arcm.db.schema.migration=ARIS10_ARCM_DEFAULT_MIGRATION
```

The tenant schema of ARIS Risk & Compliance Manager is available.

5.3.2 Provide and integrate the database driver

Provide and integrate the database driver for ARIS Risk & Compliance Manager.

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_<s, m, or l> with commonsClasspath local file <Path>\\<to>\\<driver JAR>** in ARIS Cloud Controller (ACC).

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

Example for Oracle

Assumed that the driver jar file is located under **C:/driver**, the command is:

```
enhance arcm_m with commonsClasspath local file  
"C:/driver/ojdbc<version_number>.jar"
```

5.3.3 Configure the database connection pool

The default connection pool configuration of ARIS Risk & Compliance Manager can be modified for all database systems by adding specific parameters to the external service registration of **DB** type. To avoid conflicts with pool parameters of other ARIS products, the prefix **com.aris.arcm.dbcp.*** is used. Supported parameters are:

- **com.aris.arcm.dbcp.initialSize**,
- **com.aris.arcm.dbcp.maxActive**, **com.aris.arcm.dbcp.maxWait**
- **com.aris.arcm.dbcp.maxIdle**, **com.aris.arcm.dbcp.minIdle**
- **com.aris.arcm.dbcp.removeAbandoned**
- **com.aris.arcm.dbcp.removeAbandonedTimeout**,
com.aris.arcm.dbcp.logAbandoned

Procedure

1. Start ARIS Cloud Controller (ACC).
2. Enter:

```
update external service <dbserviceID> com.aris.arcm.dbcp.initialSize=<size>  
com.aris.arcm.dbcp.maxActive=<size>
```

Example:

```
update external service db0000000001 com.aris.arcm.dbcp.initialSize=15  
com.aris.arcm.dbcp.maxActive=100
```

The default connection pool configuration 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 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. For detailed information, refer to the **ARIS Server Installation Guide - Windows** chapter **ARIS remote installations**.

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 (Page 6), 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 (Oracle SID) or the database name of the database instance (Microsoft® SQL Server).
 - d. Enter the name and password of the database 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 ARIS Administration online help.
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 must 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. If necessary, activate event enabling. For detailed information on configuring and adapting event enabling, refer to the **ARCM - Administration Guide** chapter **Configuration of event enabling in ARIS Risk & Compliance Manager** and to the **ARCM - Customizing Guide** chapter **Adapt and extend event enabling**.

28. 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

From ARIS version 10.0.12, you can install ARIS Risk & Compliance Manager with the ARIS Server setup you used to install ARIS Connect Server.

Procedure



1. Start the ARIS Server setup that was used to install ARIS Connect Server. For detailed information, refer to the **ARIS Server Installation Guide**.
2. Enable **I accept the conditions of this license agreement** if you have read and accepted the license agreements.
3. If ARIS Connect Server is installed on the same server where the setup was started, enable **Install ARIS Server on this active computer**, then click **Next**.
4. Select **ARIS Risk & Compliance Manager** and click **Next**.
5. If you want to enable customizing for ARIS Risk & Compliance Manager, select **Import now** and specify your customizing file. If no customizing is required, click **Next**.
6. 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.
7. Optionally, enable whistleblower tips to be sent. In this case, you must 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.
8. If necessary, activate event enabling. For detailed information on configuring and adapting event enabling, refer to the **ARCM - Administration Guide** chapter **Configuration of event enabling in ARIS Risk & Compliance Manager** and to the **ARCM - Customizing Guide** chapter **Adapt and extend event enabling**.
9. 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.


6.3 Configure parameters

You can configure ARIS Risk & Compliance Manager with parameters in **System configuration**. If you want to configure ARIS Risk & Compliance Manager, use the parameters in **Administration > General > System management > System configuration**. Position the mouse pointer over a property name to display an explanation. 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

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. ARIS reports are not affected by this parameter.

- **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 SMTP 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. You can also specify a **General sender alias for notifications**. For detailed information, refer to configure parameters (Page 12).

Procedure

1. Click  **Administration**. The **General** menu item is displayed initially.
2. Under **System management**, click **System configuration**. The configuration parameters are displayed.
3. Filter the list with **E-mail**. The e-mail configuration parameters are displayed.
4. Position the mouse pointer over a property name to display an explanation.
5. Click  **Edit** in the row of the parameter you want to change. The **Specify parameter value** dialog opens.
6. Make the relevant changes, for example, to activate a feature, replace **false** with **true**.
7. 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.

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 7). 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 installation of a new customer-specific version.

Procedure

1. Install (Page 9) 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.

Example: Assumed that the installation type is **Medium** and the **customizing.zip** file is located under **C:\customizing\customizing.zip**, the command is:

Enhance arcm_m with customizing local file "c:/customizing/customizing.zip"

5. Start ARIS Risk & Compliance Manager with **Start > ARIS > Start > ARIS Risk & Compliance Manager**.

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

If you have previously used ARIS Risk & Compliance Manager without customizing, it is necessary to re-create the database schema, depending on the type of customizing, since the customizing does not automatically enhance the standard database schema.

8 Glossary

In the glossary you will find explanations of basic technical terms.

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 using the consulting services provided by Software AG, 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 describe only 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 Restrictions

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

C

- Change e-mail addresses • 15
- Configure parameters • 12
- Customizing • 17

E

- E-mail functionality • 15

G

- GLOBAL UNIQUE IDENTIFIER (GUID) • 18

I

- Installation and configuration
 - Important information • 3
 - Installation of ARIS Risk & Compliance Manager • 9
 - Installation with the setup • 9
 - Integrate in ARIS • 11
 - Microsoft® SQL Server database schema (mixed mode/Windows authentication) • 6
 - Migrate from the test installation to a productive system • 16
 - Oracle database schema • 6
 - Oracle or Microsoft® SQL Server database • 5
- Introduction • 2

J

- JAVA DATABASE CONNECTIVITY (JDBC) • 18

M

- Manual configuration of the database for ARIS Risk & Compliance Manager • 7
 - Add tenant schema of ARIS Risk & Compliance Manager • 7
 - Microsoft® SQL Server database schema installation (Windows authentication) • 8
 - Provide and integrate the database driver • 8

- MULTI-PURPOSE INTERNET MAIL EXTENSION MAPPING • 18

O

- ORACLE SERVICE ID • 18

S

- SIMPLE MAIL TRANSFER PROTOCOL (SMTP) • 18
- System requirements
 - Acrobat Reader • 4
 - Microsoft® Office/Excel • 4
 - Microsoft® SQL Server • 4
 - Oracle system • 4

U

- Usage of a PostgreSQL database • 6
- Usage of an Oracle or a Microsoft® database • 5