ARIS RISK & COMPLIANCE MANAGER
ADMINISTRATION GUIDE

VERSION 10.0 - SERVICE RELEASE 10

October 2019

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.

Contents

Contents I

1 Text conventions 1

2 Introduction 2

3 Administration 3

3.1 Configuration of event enabling in ARIS Risk & Compliance Manager 3
3.2 Transfer modeled users 5

3.2.1 Export modeled users 5
3.2.2 Import modeled users into User Management 6
3.2.3 Synchronize users with ARIS Administration/User Management 7

3.3 Connection to a directory service (LDAP) 8
3.4 Connection to ARIS Publisher 8
3.5 Backup and restore runnable using ARIS Cloud Controller 10
3.6 Backup and restore runnable using ARIS Tenant Management 10

4 Glossary 11

5 Legal information 12

5.1 Documentation scope 12
5.2 Data protection 12
5.3 Disclaimer 13

6 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 Administration

3.1 Configuration of event enabling in ARIS Risk & Compliance Manager

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

Examples - Commands for ARIS Cloud Controller

```
reconfigure arcm_m arcm.config.eventProviderActive="true"
reconfigure arcm_m arcm.config.eventProviderUrl="nsp://localhost:9000"
reconfigure arcm_m arcm.config.eventSagInstallationLocation="C:/SoftwareAG"
reconfigure arcm_m
arcm.config.eventRoutingConfigurationLocation="C:/EventsRoutingConfiguration
reconfigure arcm_m arcm.config.eventProviderServiceAlias="UniversalMessaging"
reconfigure arcm_m arcm.config.useDurableEventSubscriptions="true"
```

MEANING OF PARAMETERS

- **arcm.config.eventProviderActive**

  Central specification to activate event enabling. If the value false is specified, the service is not started. If true, the other parameters must contain valid values.

- **arcm.config.eventProviderUrl**

  The parameter must contain the valid URL of a Universal Messaging server instance, for example, nsp://eventserver:9000.

- **arcm.config.eventProviderServiceAlias**

  The identifier of the service or more precisely of the message settings to use. Default is **UniversalMessaging**.

- **arcm.config.eventSagInstallationLocation**

  Specifies the absolute path to the root directory of a local SAG installation or to the root directory of the extracted non-osgi client archive. Example: C:\SoftwareAG

- **arcm.config.eventRoutingConfigurationLocation**

  Specifies the absolute path to an arbitrary directory where the routing configuration is stored. During the first start-up of the application, the **DigitalEventServices** subdirectory is automatically created to save the out-of-the-box configuration. Example: C:\EventsRoutingConfiguration

- **arcm.config.useDurableEventSubscriptions**

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

SUPPORT DIGITAL EVENT TYPES

Predefined digital event types are provided in order to generate defined objects from the events received in ARIS Risk & Compliance Manager. During the first start-up of the application, the specific digital event types, bundled under the **des.aris.arcm** namespace, are automatically created in the **event types** default location of the SAG installation. Example: C:/SoftwareAG/common/DigitalEventServices/TypeRepository/eventtypes/des/aris/arcm

They need to be copied into the TypeRepository of the event-generating system. The sending of events with the digital event types provided in ARIS Risk & Compliance Manager is part of Complex Event Processing. Further information on this can be found in the Complex Event Processing documentation.

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

If ARIS Risk & Compliance Manager and the Universal Messaging server are not located on the same host, the required configurations and resources cannot be directly referenced and used. In this case, the resources can be extracted from SAG installation with the tool **NonOsgiClientArchiveCreator**, provided in the **Add-ons/UniversalMessaging/ARCM** folder of the ARIS Risk & Compliance Manager installation medium. **NonOsgiClientArchiveCreator.zip** must be unpacked to the host system of the SAG installation, then **createClientArchive** (batch script or shell script) can be executed. Both scripts require an existing java runtime installation on the host system. On a Linux system, it can be necessary to change the privileges for the root folder of the unpacked tool, for example, sudo chmod –R 777 ./ . The **creatClientArchive** script prompts the path of the local SAG installation and then extracts all required resources, including the license information, to the archive **./build/UniversalMessagingNonOsgiClient.zip**. Then the **UniversalMessagingNonOsgiClient.zip** archive must be unpacked to the host system of the ARIS Risk & Compliance Manager installation and referenced as already described for configuration parameter **arcm.config.eventSagInstallationLocation**.

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

Warning

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

3.2 Transfer modeled users

3.2.1 Export modeled users

Synchronizing ARIS Risk & Compliance Manager with data from ARIS does not transfer the modeled users from ARIS Architect to ARIS Administration/User Management. Instead, you can export the modeled users from ARIS Architect with the report **ARCM user export for User Management** and import the users with the file **create_user.bat** into ARIS Administration/User Management. Then, synchronize (Page 7) the users in ARIS Risk & Compliance Manager with users in ARIS Administration/User Management to transfer the user accounts to ARIS Risk & Compliance Manager. For detailed information on managing users in ARIS Administration/User Management, refer to the ARIS Administration/User Management help. For detailed information on backup, restore, and synchronization of users, refer to the **ARIS Risk & Compliance Manager Administration Guide** (**Administration > Transfer modeled users**).

Note that users who are modeled in ARIS Architect only are not automatically available in ARIS Risk & Compliance Manager.

This procedure is only relevant for product trainings and showcases. In productive systems users are managed centrally in ARIS Administration/User Management (ARIS Connect) for all ARIS products.

The following attributes of a user are exported: login, first name, last name, and e-mail address. The report also identifies the license privileges a user needs. The following rules apply:

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

Prerequisites

- You need the **Read** access privilege for the groups in which the database items are saved.
- The items were saved.
- You have access to this script. Access to scripts can be restricted to certain user groups.

Procedure

1. Start ARIS Architect.
2. Click **ARIS >** **Explorer**. The **Explorer** tab opens.
3. Click **Navigation** in the bar panel if the **Navigation** bar is not activated yet.
4. Open the database whose modeled users you want to export.
5. Right-click the main group.
6. Click **Evaluate > Start report**.

7. Select the **ARIS Risk & Compliance Manager** category.
8. Select the report **ARCM user export for User Management**.
9. Click **Next**.
10. Select the output settings.
11. Click **Finish**.

A text file with the login, first name, last name, and e-mail address attributes is exported. Users excluded from the export due to missing attributes are displayed. You can use this information to specify the required attributes and export all users by restarting the report.

Now import (Page 6) the users with the file **create_user.bat** into ARIS Administration/User Management.

3.2.2 Import modeled users into User Management

Import the modeled users into User Management.

Procedure

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

The users are imported into User Management.

Now synchronize (Page 7) the users in ARIS Risk & Compliance Manager with users in ARIS Administration/User Management.

3.2.3 Synchronize users with ARIS Administration/User Management

You can synchronize users in ARIS Risk & Compliance Manager with users in ARIS Administration/User Management to update the data in ARIS Risk & Compliance Manager. Users are managed centrally in ARIS Administration/User Management (ARIS Connect) for all ARIS products. This is not to be confused with **Administration** in ARIS Risk & Compliance Manager. Users are still assigned to user groups in ARIS Risk & Compliance Manager. The user groups in ARIS Administration/User Management do not match those in ARIS Risk & Compliance Manager.

Prerequisite

You have the **User manager**, **User group manager**, **System administrator**, or **Environment administrator** role.

Procedure

1. Click **Administration > Users**.
2. Under **Users management > Synchronize with User Management**, click **Synchronize**. User data in ARIS Risk & Compliance Manager is replaced by data from ARIS Administration/User Management. This updates function and license privileges, names, passwords, e-mail addresses, etc., and users are activated.

The dialog closes. **Administration > Monitoring > Server tasks** is displayed. The server task is output under **Server tasks in progress**. When complete, the server task is listed under **Completed server tasks (last 10)**.

3.3 Connection to a directory service (LDAP)

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

3.4 Connection to ARIS Publisher

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

Prerequisite

ARIS Risk & Compliance Manager and ARIS Publisher use the same User Management to manage users. 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 11) for various ARIS products.

Procedure

USER MANAGEMENT

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

ARIS ARCHITECT

1. Start ARIS Architect.
2. Click **ARIS >**  **Administration**. The **Administration** tab opens.
3. Log in to the database you want to export.
4. Click **Users** in the navigation. Users and user groups are displayed.
5. Right-click the previously created user group.
6. Click **Properties**.
7. Click **Function privileges**.

8. Enable the check box for the **Database export** privilege. (The product-specific privileges are not centrally assigned in User Management but in the respective ARIS product.)
9. Click **Access privileges**.
10. Assign the user group at least the access privilege **Read** for the main group.
11. Click **Pass on privileges** to apply the privileges to all subgroups.
12. Click **OK**.
13. Publish the relevant database.
14. After the export, change the status to **Activated**.

ARIS PUBLISHER

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

ACTIVATE ARIS PUBLISHER INTEGRATION IN ARIS RISK & COMPLIANCE MANAGER

Prerequisite

You have the **System administrator** role.

1. Start ARIS Risk & Compliance Manager.
2. Click  **Administration**. The **General** menu item is displayed initially.
3. Under **System management**, click **Environments**.
4. Click the name of the relevant environment. The form is displayed.
5. Under **ARIS Publisher integration settings > ARIS Publisher integration**, click **Yes**.
6. Enter the ARIS Publisher link in the **Object link** field in the following form:

   http://<BusinessPublisherServer>:19990/businesspublisher/link.do?login=<user name>&password=<password>&localeid=1033&ph=<exportID>&objectguid={GUID}
7. Replace the placeholders in the following manner:
   a. **<BusinessPublisherServer>** = Name or IP address of the ARIS Publisher Server.
   b. **<User name>** = Name of the user that was previously created.
   c. **<Password>** = Password of the user that was previously created.
   d. **<exportID>**
      1. Open a model in ARIS Publisher.
      2. Right-click an object.

3. Click **Copy link**.
4. Copy the parameter **ph** with its value in the link displayed and replace **<exportID>** with it.

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

8. Enter the link you created previously in the **Model link** field in the following form and replace the **objectguid** parameter with **modelguid**:

   http://<BusinessPublisherServer>:19990/businesspublisher/link.do?login=<username>&password=<password>&localeid=1033&ph=<exportID>&modelguid={GUID}

9. Replace the placeholders.
10. Click **Save**.

The ARIS Publisher integration is activated.

PERFORM A TEST

1. Log into ARIS Risk & Compliance Manager with the **Test manager** role.
2. Open a risk that was generated by the master data file import.
3. Click **Object link** and **Model link** in the **Function** row.

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

3.5 Backup and restore runnable using ARIS Cloud Controller

ARIS Risk & Compliance Manager allows generating and restoring database snapshots from within the web application. Additionally, the tenant backup and restore functionality of ARIS Cloud Controller (ACC) can be used to generate runnable backup files that include a database snapshot and all deployed customizations. For details, see the **ARIS Cloud Controller (ACC) Command-Line Tool** manual, chapters **Back up a tenant** and **Restore a tenant**.

3.6 Backup and restore runnable using ARIS Tenant Management

ARIS Tenant Management allows backing up and restoring tenant-specific data of ARIS Risk & Compliance Manager. The generated runnable backup files include a database snapshot and all deployed customizations. For detailed information, refer to **ARIS Tenant Management Guide**.

Note: Restoring tenant-specific data using ARIS Tenant Management requires that the backup files contain the same customization as the deployed instances of ARIS Risk & Compliance Manager. If this is not the case, manually deploy the customization on the relevant instances.

4 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.

5 Legal information

5.1 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.

5.2 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.

5.3 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.

6 Index

A

ARIS Publisher • 8

B

Backup and restore
- Via ARIS Cloud Controller • 10
- Via ARIS Tenant Management • 10

C

Connect directory service • 8

E

Event enabling • 3

G

GLOBAL UNIQUE IDENTIFIER (GUID) • 11

I

Introduction • 2

J

JAVA DATABASE CONNECTIVITY (JDBC) • 11

L

LDAP • 8

M

MULTI-PURPOSE INTERNET MAIL EXTENSION MAPPING • 11

O

ORACLE SERVICE ID • 11

S

SIMPLE MAIL TRANSFER PROTOCOL (SMTP) • 11

U

Users
- Export from ARIS Architect • 5
- Import into User Management • 6
- Update in ARIS Risk & Compliance Manager • 7