software AG

ARIS Risk & Compliance Manager
ADMINISTRATION GUIDE

Version 10.0 - Service Release 1

July 2017

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.`

2   ARIS Risk & Compliance Manager

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

If an updated version of this document is available, you will find it here: http://aris.softwareag.com/ARISDownloadCenter/ADCDocumentationServer (http://aris.softwareag.com/ARISDownloadCenter/ADCDocumentationServer)

3 Administration

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

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

Examples - Commands for ARIS Cloud Controller

```
reconfigure arcm_m arcm.config.eventProviderActive="true"
reconfigure arcm_m arcm.config.eventProviderUrl="nsp://localhost:9000"
reconfigure arcm_m arcm.config.eventTypeStoreLocation="
C:/SoftwareAG/common/EventTypeStore"
reconfigure arcm_m arcm.config.eventConfigurationLocation="
C:/SoftwareAG/profiles/SPM/configuration"
reconfigure arcm_m
arcm.config.eventSecurityFilePath="C:/SoftwareAG/common/conf/event/routing/event
-routing-security.xml"
```

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, e.g., nsp://localhost:9000.

- **arcm.config.eventTypeStoreLocation**

  Specifies the absolute path to a locally available event type store. If the instance of the Universal Messaging server is located on the same host, the store for this installation can be used. Example: C:\SoftwareAG\common\EventTypeStore

- **arcm.config.eventConfigurationLocation**

  The absolute path to the base directory of a specific event routing configuration is required. If the instance of the Universal Messaging server is located on the same host, the basic configuration for this installation can be used. Example: C:\SoftwareAG\profiles\SPM\configuration

- **arcm.config.eventSecurityFilePath**

  This parameter should contain the absolute path for the security configuration file. If the host is identical, the file for the Universal Messaging server installation can be referenced. Example: C:\SoftwareAG\common\conf\event\routing\event-routing-security.xml

- **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 EVENT TYPES

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

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

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

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

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

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

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

Warning

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

3.2   Import of modeled users into User Management

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

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

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

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

3.2.1   Export modeled users from ARIS Architect

Export the modeled users from ARIS Architect.

Procedure

1. Start **ARIS Architect**.
2. Open the database whose modeled users you want to export for the import into User Management.
3. Right-click the main group.
4. Click **Evaluate > Start report**.
5. Select the **ARIS Risk & Compliance Manager** category.
6. Select the report **ARCM user export for User Management**.
7. Click **Next**.
8. Select the output settings.
9. 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.

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 the Enter key without specifying a password.

The users are imported into User Management.

3.2.3 Synchronize users with User Management

You can synchronize users in ARIS Risk & Compliance Manager with users in User Management to update the data in ARIS Risk & Compliance Manager. Users are managed centrally in User Management for all ARIS products. This is not to be confused with the Administration in ARIS Risk & Compliance Manager. Users are still assigned to user groups in ARIS Risk & Compliance Manager. The user groups in 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**.
2. Under **Functions > Synchronize with User Management**, click **Synchronize**. User data in ARIS Risk & Compliance Manager is replaced by data from User Management. This updates function and license privileges, names, passwords, e-mail addresses, etc., and users are deactivated.

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

3.3 Installing ARIS Architect components

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

3.4 Connection to a directory service (LDAP)

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

3.5 Prepare the MashZone server for dashboard integration

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

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

As a precaution, redirection of content from MashZone to other systems, such as ARIS Risk & Compliance Manager, in MashZone is limited to the **SAMEORIGIN** option by default, i.e., the MashZone server only responds to its own requests. Therefore, the **SAMEORIGIN** restriction must be disabled in the web.xml file. More detailed information about X-Frame options can be found here (https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options).

Procedure

1. Open the web.xml file
   (<MashZoneInstallDir>\MashZoneNG\apache-tomee-jaxrs\webapps\mashzone\WEB-INF\
   web.xml)

2. Add these lines:

```
<init-param>
          <param-name>antiClickJackingEnabled</param-name>
          <param-value>false</param-value>
</init-param>
```

into the following section, so that it looks as follows:

```
<filter>
      <filter-name>HTTP Header Security Filter</filter-name>

<filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-c
lass>
      <init-param>
           <param-name>antiClickJackingEnabled</param-name>
           <param-value>false</param-value>
      </init-param>
              <init-param>
```

```
                        <param-name>antiClickJackingOption</param-name>
                        <param-value>SAMEORIGIN</param-value>
        </init-param>
        <init-param>
                <param-name>hstsEnabled</param-name>
                <param-value>true</param-value>
        </init-param>
        <init-param>
                <param-name>hstsMaxAgeSeconds</param-name>
                <param-value>604800</param-value>
        </init-param>
    </filter>
```

3. Save your changes.

4. Restart the MashZone server.

The MashZone is prepared for the dashboard integration.

3.6   Use of SAML2 authentication for dashboard connections

The SAML2 single sign-on authentication is supported by MashZone NextGen Business Analytics since release 9.12. In order to use it for dashboard connections in ARIS Risk & Compliance Manager, additional configurations and settings for the SAML2 support are required in User Management. Detailed information on the configuration of SAM2L is provided in the documentation of User Management.

3.7   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 Risk & Compliance Manager with the export report and imported to ARIS Risk & Compliance Manager. In addition, you can publish the ARIS Architect database with ARIS Publisher. After importing the master data into ARIS Risk & Compliance Manager, the connection to ARIS Publisher can be configured via the 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. User Management for all ARIS products, which is not to be confused with Administration in ARIS Risk & Compliance Manager, serves to manage users, user groups, function and license privileges, licenses, documents, and configurations. This enables single sign-on for various ARIS products.

Procedure

USER MANAGEMENT

1. Open User Management.

2. Create a user group and a user in User Management.

3. Assign the user group to the user.

4. Assign the function privilege **Publisher administrator** to the user group.

ARIS ARCHITECT

1. Start **ARIS Architect**.

2. Click **ARIS > Administration**. **Administration** opens.

3. Log in to the database you want to export.

4. Click **Users** in the navigation. Users and user groups are displayed.

5. Right-click the previously created user group.

6. Click **Properties**.

7. Click **Function privileges**.

8. Enable the check box for the **Database export** privilege. (The product-specific privileges are not centrally assigned in User Management but in the respective ARIS product.)

9. Click **Access privileges**.

10. Assign the user group at least the access privilege **Read** for the main group.

11. Click **Pass on privileges** to apply the privileges to all subgroups.

12. Click **OK**.

13. Publish the relevant database.

14. After the export, change the status to **Activated**.

ARIS PUBLISHER

1. Open ARIS Architect.

2. Log in using the **root** user and the password **root**.

3. Open the **Groups** module. The user group you created is displayed.

4. In the row of the group, click **Assign**. The dialog opens.

5. Assign the group previously created in User Management to ARIS Publisher.

6. Click **Save**.

ACTIVATE ARIS PUBLISHER INTEGRATION IN ARIS RISK & COMPLIANCE MANAGER

Prerequisite

You have the **System administrator** role.

1. Open ARIS Risk & Compliance Manager.

2. Click **Administration**.

3. Under **System management**, click **Environments**.

4. Click the name of the relevant environment.

5. Under **Settings for ARIS Publisher integration** click **Yes**.

6. Enter the ARIS Publisher link in the **Object link** box in the following form:

http://<BusinessPublisherServer>:19990/businesspublisher/link.do?login=<us er

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** box in the following form and replace the **objectguid** parameter with **modelguid**:

   http://<BusinessPublisherServer>:19990/businesspublisher/link.do?login=<us er

   name>&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 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.

3.8 Backup and restore runnable via 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 manual for ARIS Cloud Controller, chapters **Back up a tenant** and **Restore a tenant**.

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, e.g., text, audio, image.

Oracle service ID (SID)

Unique identifier required by Oracle to identify the database instance.

Simple Mail Transfer Protocol (SMTP)

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

5 Software AG support

ON THE WEB

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

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

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

BY PHONE

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

+800 ARISHELP

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

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

6   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.

7   Index

A

ARIS Architect components 7

ARIS Publisher 8

C

Connect directory service 7

E

Event enabling 3

G

Global Unique Identifier (GUID) 12

I

Import of modeled users into User
  Management 5

Introduction 2

J

Java Database Connectivity (JDBC) 12

L

LDAP 7

M

Multi-purpose Internet Mail Extension
  mapping 12

O

Oracle service ID 12

S

Simple Mail Transfer Protocol (SMTP) 12

Support 13

U

Users
    Export modeled users from ARIS Architect
      5
    Import modeled users into User
      Management 6
    Import of modeled users into User
      Management 5
    Update users in ARIS Risk & Compliance
      Manager 6